SiteMinder Installation Guide

Version 4.1

www.netegrity.com

Netegrity SiteMinder 4.1

Netegrity Inc.
245 Winter St.
Waltham, MA 02451-8799
Phone: (781) 890-1700
Fax: (781) 487-7791
http://www.netegrity.com

This product contains encryption technology. Exporting these encryption algorithms to certain countries may be prohibited or restricted by the laws of the United States.

Some portions of the code are licensed from RSA Data Security, Inc.

NETEGRITY INC. SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE PERFORMANCE OR USE OF THIS MATERIAL.

Contents

Preface 9

About SiteMinder Documentation 9

Print Documentation 9

Online Documentation 10

About this Book 10

Conventions 11

How this Book is Organized 11

Technical Support 13

Chapter 1. Installing the Policy Server on NT 15

Overview 15

System Requirements 15

Before You Begin 16

Installing the Policy Server 16

Reinstalling the Policy Server 19

Accessing the Policy Server User Interface 20

Accessing the Policy Server User Interface Locally 21

Accessing the Policy Server User Interface from Internet Explorer 5.0 22

Uninstalling the Policy Server 24

Chapter 2: Installing the Policy Server on Solaris 29

Overview 29

System Requirements 29

Before you Begin 30

Creating a New Solaris Account 30

About the Solaris System Parameters 30

About the Localization Requirement 31

Running the Policy Server Setup 32

Choosing a LDAP Policy Store 34

Choosing an Oracle Policy Store 36

Storing Audit Logs in an Oracle Database 37

Configuring the Netscape Web Server 38

Accessing the SiteMinder Policy Server User Interface 39

Accessing the Policy Server User Interface Locally 39

Configuring Auto Startup 40

Uninstalling the Policy Server on Solaris 41

Removing the SiteMinder Policy Server 43

Removing SiteMinder References in the obj.conf File 44

Configuring ODBC Data Sources 44

Adding Oracle ODBC Data Sources 45

Chapter 3. Setting up the Policy Store on NT 47

Overview 47

Configuring an NT Policy Server 47

Storing SiteMinder Data in an LDAP Directory 48

Creating an LDAP Policy Store or Key Store 49

Migrating and Moving Policy Store Data 51

Configuring Policy Servers to Use an LDAP Policy Store or Key Store 53

Storing SiteMinder Data in an ODBC Database 57

Before You Begin 58

Exporting the Policy Store Data From the Existing Database 58

Creating the Oracle or SQL Server Database Using the SiteMinder Schema 60

Configuring SiteMinder to Use an Oracle or SQL Database 61

Configuring an ODBC Database as a Policy Store 67

Configuring an ODBC Database to Store Keys, Audit Logs or Token Data 70

Importing the Policy Store Data into the Database 72

Replicating Policy Stores and Configuring Failover 73

Chapter 4. Setting up the Policy Store on Solaris 75

Overview 75

Storing SiteMinder Data in an Oracle Database 75

Before You Begin 76

Storing SiteMinder Data in an LDAP directory 80

Creating an LDAP Policy Store or Key Store 80

Migrating and Moving Policy Store Data 83

Configuring Policy Servers to Use an LDAP Policy Store or Key Store 85

Replicating Policy Stores and Configuring Failover 88

Chapter 5. Setting up a Policy Store on Novell Netware 91

Overview 91

Configuring NDS as a Policy Store 91

Migrating Existing Policy Store Data to NDS 96

Removing Policy Store Data 98

Chapter 6. Installing the Reports Server 101

Overview 101

Installing the Reports Server on NT 102

Changing the Location of the Report Redirect URL 103

Reinstalling the Reports Server 104

Uninstalling the Reports Server 105

Chapter 7. Installing Support for Registration Services 109

Overview 109

Setting up Support for Registration Services 110

Installing a Servlet Engine 110

Installing ServletExec on NT/Netscape 111

Installing ServletExec on NT/IIS 115

Installing ServletExec on Solaris/Netscape 118

Installing ServletExec on Solaris/Apache 124

Testing ServletExec 133

Using JRun for Registration Services 133

Configuring JRun for Solaris/Apache 133

Chapter 8. Installing Web Agents 135

Overview 135

Installing the Web Agent on NT 136

Before You Begin 136

Configuring the Web Agent for IIS 138

Configuring the Web Agent for Netscape 142

Reinstalling a Web Agent on NT 146

Uninstalling a Web Agent from NT 147

Installing a Web Agent on UNIX 148

Before You Begin 148

Configuring Web Agents on Netscape 151

Reconfiguring Web Agents on Netscape 154

Configuring Web Agents for Apache 155

Reconfiguring Web Agents on Apache 161

Optimizing an Environment for Apache 163

Tuning Solaris for the Apache Web Agent 163

Modifying the Apache httpd.conf file 164

Reinstalling a Web Agent on UNIX 165

Uninstalling a Web Agent from UNIX 166

Chapter 9. Installing Affiliate Agents 167

Overview 167

Installing an Affiliate Agent on NT 167

Before you Begin 167

Configuring an Affiliate Agent on NT 169

Reinstalling an Affiliate Agent on NT 173

Uninstalling an Affiliate Agent from NT 174

Installing an Affiliate Agent on UNIX 175

Before you Begin 175

Configuring the Affiliate Agent for UNIX 177

Configuring the Apache httpd.conf File for Apache Servers 181

Reinstalling an Affiliate Agent on UNIX 182

Uninstalling an Affiliate Agent from UNIX 183

Chapter 10.
Upgrading to SiteMinder 4.1 185

Overview 185

Upgrading SiteMinder in a Multiple Policy Server Environment 186

Maintaining Single Sign-on Between 3.6x and 4.1 Web Agents 191

Upgrading SiteMinder in a Single Policy Server Environment 192

Removing a Policy Server From the SiteMinder Environment 195

Configuring a Netscape or Apache Web Agent 196

Configuring an IIS Web Agent 197

Exporting SiteMinder 3.6 Policy Store Data 198

Upgrading the Policy Server to SiteMinder 4.1 199

Upgrading the Policy Server on NT 199

Upgrading the Policy Server on Solaris 201

Importing Policy Store Data 204

Upgrading an ODBC User Directory Schema 205

Upgrading Certificate Mapping 208

Upgrading Web Agents, Cookie Providers and Advanced Authentication Schemes 218

Upgrading Cookie Providers and Advanced Authentication Schemes 218

Upgrading Web Agents, Cookie Providers, and Credential Collectors on UNIX . . . 224

Upgrading the Reports Server 228

Removing the SiteMinder 3.6 Policy Store 230

Removing the 3.6 Policy Store From an LDAP Directory 230

Removing 3.6 Policy Stores, Logs, and Token Data from an ODBC Database 233

Chapter 11. Policy Server Tools 235

Overview 235

Exporting Policy Data Using Smobjexport 235

Importing Policy Data Using Smobjimport 238
Managing an LDAP Policy Store using Smldapsetup 240
Modes 241
Arguments 243
Removing the SiteMinder Policy Store using Smldapsetup .245
Deleting SiteMinder Data in ODBC Databases 246
Checking Solaris Patches With Smpatchcheck 248
Reading RADIUS Log Files With Smreadclog 249
The SiteMinder Test Tool 250
About the SiteMinder Test Tool Interface 251
Testing a Policy 260
Performing Functionality Tests 263
Performing Regression Tests 266
Performing Stress Tests 267
Importing Tokens Using the SiteMinder Token Tool 271

Preface

About SiteMinder Documentation

SiteMinder documentation is provided in two forms: print and online.

Print Documentation

SiteMinder Release Notes

Provides information about new features and known issues in this release.

SiteMinder Installation Guide

Refer to *About this Book* on page 10.

SiteMinder Concepts Guide

Explains SiteMinder solutions for e-business issues as well as basic and advanced SiteMinder components.

SiteMinder Deployment Guide

Provides practical information and guidelines about issues that should be considered before deploying SiteMinder and procedural information about setting up a Web site or portal.

SiteMinder Policy Server Operations Guide

Reference guide for all SiteMinder Policy Server related information.

SiteMinder Agent Operations Guide

Provides conceptual information and procedures for configuring IIS, Netscape, and Apache Web Agents and SiteMinder Affiliate Agents.

SiteMinder Developer’s API Guide

Describes and provides examples for the set of Application Program Interfaces (APIs).

Online Documentation

There are two types of online documentation available for SiteMinder: online help (HTML) and online books (PDF).

Online Help

The following online help systems are available:

- SiteMinder Policy Server User Interface—invoke the HTML-based online help system by selecting **SiteMinder Help** from the **Help** menu or clicking the **Help** button in any of the dialog boxes. This help system provides policy management and configuration management information.
- SiteMinder Policy Server Management Console—invoke the help file by clicking the **Help** button.
- SiteMinder Web Agent IIS Management Console—invoke the help file by clicking the **Help** button.

Online Books

Online versions of the printed documentation are provided in PDF format. The documentation is installed in the doc subdirectory of the SiteMinder installation directory. You can access PDF documentation from the SiteMinder Administration User Interface by selecting **Online Manuals** from the Help menu.

About this Book

The *SiteMinder Installation Guide* describes how to install all of the components that comprise SiteMinder: the Policy Server, the Web Agents, the Affiliate Agents, the Reports Server, authentication schemes, and support for single sign-on environments. This book also provides information about configuring policy stores and installing support for Registration Services.

This book is written with an assumption that the reader is familiar with basic SiteMinder concepts, which are described in the *SiteMinder Concepts Guide*.

Conventions

The following conventions are used in the SiteMinder documentation.

This convention...	Is represented by...	Example
Text that you enter	**`bold courier`**	Enter **YES** or **NO**.
Text that the system displays	`courier`	The system displays the following message: `Process Complete`
Button, menus, menu items	**bold sans serif**	Click **OK** to continue.
Field names	**bold sans serif**	Select the **Enable Web Agent** option.
File names	`sans serif`	Open the `WebAgent.Conf` file.
Path names and file locations	`sans serif`	Navigate to `c:\SiteMinder\Bin`.
Keys	uppercase	Press ENTER.

How this Book is Organized

Chapter 1. Installing the Policy Server on NT

Provides the Policy Server system requirements for Windows NT, and describes how to install, re-install, upgrade, and uninstall the Policy Server on Windows NT.

Chapter 2. Installing the Policy Server on Solaris

Provides the Policy Server system requirements for Solaris, describes how to install the Policy Server and select the policy store, describes how to upgrade the Policy Server and uninstall the Policy Server on Solaris, and provides information about configuring ODBC data sources.

Chapter 3. Setting up the Policy Store on NT

Describes how to configure an NT Policy Server, how to index an LDAP Directory, and how to migrate policy store data.

Chapter 4. Setting up the Policy Store on Solaris

Describes how to store policies in an Oracle database, how to store policies in an LDAP directory, and how to migrate policy store data.

Chapter 5. Setting up the Policy Store on Novell Netware

Describes how to store policies in an NDS directory and how to migrate policy store data.

Chapter 6. Installing the Reports Server

Describes how to install, configure, re-install, and upgrade the Reports server.

Chapter 7. Installing Support for Registration Services

Describes how to install a servlet engine and configure Web Agents to support Registration Services.

Chapter 8. Installing Web Agents

Describes how to install, upgrade, and uninstall Web Agents on IIS, Netscape, and Apache Web servers.

Chapter 9. Installing Affiliate Agents

Describes how to install and configure an Affiliate Agent on NT and Solaris systems.

Chapter 10. Upgrading to SiteMinder 4.1

Describes how to upgrade from previous versions of SiteMinder to SiteMinder 4.1.

Chapter 11. Policy Server Tools

Describes SiteMinder utilities that help administrators manage SiteMinder.

Technical Support

Before contacting Customer Support, please make sure you have the following information:

- The type of computer you are using.
- The operating system version number.
- The product name and version number.
- The license number for your software.
- Type of network devices attached to your computer.
- A description of your problem.

Notify Netegrity Customer Support using any of the following options:

- **E-mail:** support@netegrity.com
- **Toll-free Phone Number:** 1- 877-748-3646 (877-SITEMINDER)
- **Fax:** (781) 672-5850

Chapter 1. Installing the Policy Server on NT

Overview

This chapter describes how to install the SiteMinder Policy Server on a Windows NT system.

System Requirements

The SiteMinder Policy Server requires an Intel Pentium II or better. Ensure that you have the following components installed on your computer:

- **Memory:** 64 MB system RAM (minimum). If you installing a Netscape LDAP Directory Server on the same machine, the minimum system RAM is 128MB.
- **Hard disk space:** 100 MB free disk space for new installation. This system requirement is based on a medium size policy database (about 1,000 policies).
- **Screen resolution:** 800 x 600 or higher to properly view the Policy Server User Interface.
- **Operating System:** Microsoft Windows NT 4.0 Server or Workstation with Service Pack 3, 4, or 5.
- **Web Server:** Microsoft Internet Information Server (IIS) 3.x or later, iPlanet Web Server Enterprise Edition 4.0 or later, or Netscape Enterprise Web Server 3.5.1 or later.
- **Browser:** Netscape Communicator 4.06, 4.5, 4.6 or later, or Microsoft Internet Explorer 4.0, 4.01, or 5.0 (with Java Virtual Machine 4.79.0.2424 or newer). If you use an older 4.x version of Netscape, you must get the Java 1.1 Patch from *http://developer.netscape.com*. You can upgrade your Java Virtual Machine for Internet Explorer from *http://www.microsoft.com/java*.

Before You Begin

To install the SiteMinder Policy Server, you must log into a Windows NT 4.0 account with local administrator privileges.

Installing the Policy Server

The Setup application extracts the SiteMinder Policy Server files and installs them on your computer. The Policy Server is installed, by default, in the `C:\Program Files\Netegrity\SiteMinder` directory.

To install the Policy Server:

1. Exit all applications that are running.
2. Insert the SiteMinder 4.1 CD-ROM into the drive.
3. Run the SiteMinder Policy Server setup program:
    a. Navigate to the `nt` folder on the SiteMinder CD-ROM.

    b. Double-click `Policy-Server-4.1-NT.exe`.

    Setup verifies the following prerequisites:

    - You are logged into an account with local administrator privileges.
    - NT 4.0 with Service Pack 3, 4, or 5 is installed.
    - IIS 3.x or later, iPlanet Web Server Enterprise Edition 4.0 or later, or Netscape Enterprise Web Server 3.5.1 or later is installed.
    - The computer has necessary free disk space.

    If any of the prerequisites are not met, the installation stops, the following message is displayed, and the prerequisites that were not met are identified in the log file referenced in the message:

    ```
    "View the PS-4.1-Install.log file in the
    \Temp\SiteMinder folder for more details. Ensure
    that all prerequisites are met and restart the
    SiteMinder Policy Server 4.1 Setup."
    ```
4. In the **SiteMinder Policy Server - Welcome** dialog box, click **Continue**.

    SiteMinder prepares the Setup Wizard, which will guide you through installing the Policy Server. This step may take a few moments.

5. Read the Welcome message and click **Next**.
6. Read the Software License Agreement and click **Yes** if you accept the agreement.
7. Read the Release Notes, then click **Next**.
8. In the **User Information** dialog box, enter your name and company name and click **Next**.
9. In the **System Reboot Message** dialog box, select the **Continue with Install** option and click **Next**.
10. In the **Configure Web Server** dialog box, select the Web server(s) to configure for the Policy Server.

    The size of the Web servers is listed as 0K because you are only selecting the Web servers—you are not installing any files.

11. In the **Choose Destination Location** dialog box, accept the default installation location or select a different location and click **Next**.
12. In the **Encryption Key** dialog box, complete the following:
    a. In the **Encryption Key** field, enter a case-sensitive, alphanumeric key. The encryption key is a key that secures data sent between the Policy Server and the policy store. The key can be from 6 to 24 characters in length. All policy servers that share a SiteMinder policy store (a database containing policy information) must be configured using the same encryption key. For stronger protection, define a long Encryption Key.

    b. Re-enter the key in the **Confirm Encryption** field.

    c. Take note of this key for future reference.

    d. Click **Next**.
13. In the **Super User Password** dialog box, complete the following:
    a. In the **Password** field, enter a case-sensitive password for the SiteMinder Super User account. The pre-defined SiteMinder Super User account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

    b. Re-enter the password in the **Confirm Password** field.

c. Take note of this password. You will need to enter the SiteMinder user name and the password when you first log into the SiteMinder Policy Server User Interface. You can change the password using the SiteMinder Policy Server Management Console.

Refer to the *SiteMinder Policy Server Operations Guide* for more information about the Policy Server Management Console.

d. After you enter the password, click **Next**.

Note: We recommend that this account not be used in day-to-day operations. Instead, only use this account to access the Policy Server User Interface for the first time and for creating an administrator with system configuration privileges.

14. Review the settings in the **Start Copying Files** dialog box, then click **Next** to continue.

    SiteMinder begins copying files to your system. This part of the installation may take a few moments.

15. Click **Finish** to complete the installation and reboot your system.

    You can now access the Policy Server, as described in *Accessing the Policy Server User Interface* on page 20.

What’s the next step?

Now that you have installed the Policy Server on NT, complete the following:

1. Set up a policy store to store your policy related information, as described in one of the following chapters:

   - *Chapter 3, Setting up the Policy Store on NT* on page 47
   - *Chapter 4, Setting up the Policy Store on Solaris* on page 75
   - *Chapter 5, Setting up a Policy Store on Novell Netware* on page 91

   All Policy Servers in a SiteMinder installation must share the same policy store.

2. Optionally, install the Report Server, as described in *Chapter 6, Installing the Reports Server* on page 101. You only need to install the Report Server if you want the Reports Server to support an Oracle or SQL Server database.
3. Optionally, install support for Registration Services as described in *Chapter 7, Installing Support for Registration Services* on page 109. You only need to install support for Registration Services if you intend to install a Web Agent that provides Registration Services.
4. Install a Web Agent, as described in *Chapter 8, Installing Web Agents* on page 135.

Reinstalling the Policy Server

Install the SiteMinder Policy Server over an existing Policy Server of the same version to restore lost application files or to restore the Policy Server's default installation settings.

To reinstall the Policy Server:

1. Close the SiteMinder Policy Server Management Console if it is running.
2. Complete the first 10 steps of *Installing the Policy Server* on page 16.
3. In the **Policy Server Settings Options** dialog box, select one of the following:

   - **Preserve existing settings**—Retains Policy Server settings that were set using the SiteMinder Policy Server Management Console.

     To complete the reinstallation:

     a. In the Start Copying Files dialog box, click **Next**. SiteMinder begins copying the files.

     b. Click **Finish** to complete the reinstallation.

- **Install default settings**—Replaces your existing SiteMinder Policy Server settings. The existing SiteMinder policy store, Encryption Key, and Super User Account Password are preserved.

  To complete the reinstallation:

  a. In the **Select Program Folder** dialog box, select the program folder and click **Next**.

  b. In the **Start Copying File**s dialog box, click **Next**. SiteMinder begins copying the files.

  c. Click **Finish** to complete the reinstallation.

Accessing the Policy Server User Interface

Once you have installed the Policy Server, access it through a browser. Verify that the browser supports SiteMinder by entering the following URL: `http://www.netegrity.com/UItest`

Note: The URL for the browser test is case-sensitive.

To reduce the time it takes to load the Policy Server User Interface, you can access it locally from your machine. Refer to *Accessing the Policy Server User Interface Locally* on page 21.

To access the SiteMinder Policy Server User Interface using Internet Explorer 5.0, refer to *Accessing the Policy Server User Interface from Internet Explorer 5.0* on page 22 *before* completing the procedure below.

To access the Policy Server User Interface:

1. Complete one of the following:

   - Start your browser and enter the following URL:

     http://*hostname*/siteminder

     where *hostname* is the name of the machine on which the Policy Server is installed.

     For example,

     `http://www.myorg.org/siteminder`

   - From the Start menu, select **Programs | SiteMinder | SiteMinder Policy Server User Interface**.

The system displays your browser with the Administrator login page.

2. Click **Administer SiteMinder**.

   Once the Administration applet has downloaded, the SiteMinder Administration window appears.

3. In the **User Name** field, enter **`SiteMinder`**.

   This user name is the default Super User for which you entered a password during the installation.

4. In the **Password** field, enter the password you defined in step 13 of *Installing the Policy Server* on page 16.

   To change the password, modify the Super User account using the SiteMinder Policy Server Management Console.

   Refer to the *SiteMinder Policy Server Operations Guide* for more information about the Policy Server Management Console.

Accessing the Policy Server User Interface Locally

Accessing the Policy Server User Interface locally from your Web browser reduces the time it takes to load the Policy Server User Interface.

If you access the Policy Server User Interface from Internet Explorer, the Policy Server User Interface files (stored in `sm_admin.cab`) are automatically stored in Internet Explorer’s cache.

If you access the Policy Server User Interface from Netscape Communicator, you can copy the Policy Server User Interface files (stored in `sm_admin.jar`) to the directory where Netscape’s Java classes are located to increase performance.

To access the Policy Server User Interface on a local machine using a Netscape browser:

1. Navigate to the SiteMinder `Admin` directory:

   <*siteminder_installation*>`\Admin`

   where <*siteminder_installation*> is the installed location of SiteMinder.

   For example,

   ```
   C:\Program Files\Netegrity\SiteMinder\Admin
   ```

2. Copy `sm_admin.jar` to the following location:

   <*netscape_communicator_installation*>`\Program\java\classes`

   where <*netscape_communicator_installation*> is the installed location of Netscape Communicator.

   For example,

   ```
   C:\Program Files\Netscape\Communicator
   \Program\java\classes
   ```

3. Restart the Netscape Web browser.
4. If you are prompted to grant additional privileges to Netegrity when you access the Policy Server User Interface, click **Grant**.

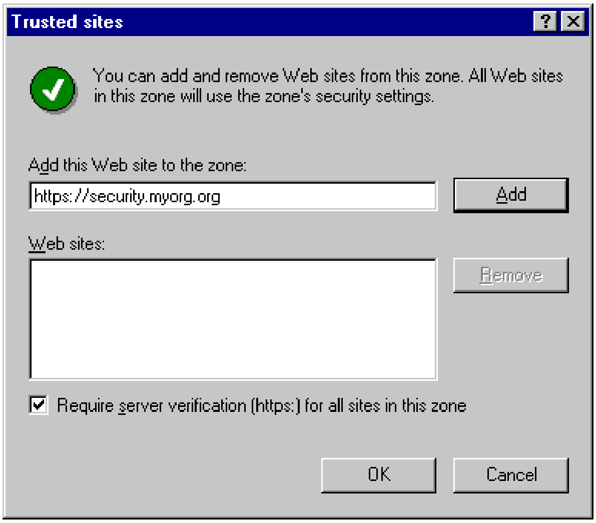
☞ **Note:** If you install a new version of the Policy Server, you must copy the new `sm_admin.jar` file to the Netscape Java classes directory.

Accessing the Policy Server User Interface from Internet Explorer 5.0

If you are using Internet Explorer 5.0, you must add your domain as a trusted site before accessing the Policy Server User Interface.

1. Open Internet Explorer 5.0 and select **Internet Options** from the Tools menu.
2. Select the **Security** tab to bring it to the front.
3. Click the **Trusted Sites** icon to select it, then click the **Sites** button.

The **Trusted sites** dialog box is displayed. The **Require server verification (https) for all sites in this zone** is enabled by default.



You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone: https://security.myorg.org

Web sites:

☑ Require server verification (https:) for all sites in this zone

4. If you are not accessing the Policy Server using a secured connection (https), deselect the **Require server verification (https) for all sites in this zone** check box.

5. In the **Add this Web site to the zone** field, enter the full name of your server including the domain, then click **Add**:

   `http://<`*`servername`*`>.<`*`domain-name`*`>`

   For example,

   `https://security.myorg.org`

☞ **Note:** If you are connecting to the Policy Server User Interface using a secured connection (https), you must include https when specifying the domain. For example, **`https://security.myorg.org`**

6. Click **OK** to save the changes and return to the **Internet Options** dialog box.

7. Click **OK** to exit the **Internet Options** dialog box.
8. Exit Internet Explorer, then restart the browser for the settings to take effect.

Uninstalling the Policy Server

To uninstall the Policy Server, you must log into the account from which the Policy Server was installed originally.

☞ **Note:** Running the uninstallation deletes all Policy Server files and removes all Policy Server settings. If you are using the default local policy store (`smpolicy.mdb`), the policy store is also deleted. To save the policy store for future use, make a copy of the `smpolicy.mdb` file and move it out of the SiteMinder installation location.

To uninstall the Policy Server:

1. Verify that no Web Agents are configured to use the Policy Server you are uninstalling:
   - For IIS Web Agents, make sure the Policy Server you are removing is not listed in the IIS Web Agent Management Console under the **Settings** tab.
   - For Netscape and Apache Web Agents, make sure the Policy Server you are removing is not listed in the `WebAgent.Conf` file. By default, the `WebAgent.conf` file is located in one of the following locations:
     - For Netscape: <*Netscape_installation*>`\https-`*hostname*`\config`

       where <*Netscape_installation*> is the installed location of Netscape servers and <*hostname*> is the name of the Web server on which the Policy Server is installed.

       For example,

       `C:\Program Files\Netscape\server4\https-myserver\config`

- For Apache: /<*apache_installation*>/`conf`

  where <*apache_installation*> is the installed location of the Apache server.

  For example,

  `usr/apache/conf`

To remove the Policy Server from the `WebAgent.conf` file, delete the entire line that begins “`policyserver=`” and contains the IP Address and port numbers for the Policy Server you are uninstalling. Then save `WebAgent.conf`.

📖 Refer to the *SiteMinder Agent Guide* for information on modifying the `WebAgent.conf` file.

☞ **Note:** If the Web Agent is only connected to the Policy Server you are removing, the Web Agent will stop working when you delete the Policy Server from `WebAgent.conf`. To continue using the Web Agent, configure a different Policy Server for the Web Agent to communicate with in `WebAgent.conf`.

2. From the Control Panel, double-click **Add/Remove Programs**.
3. Select SiteMinder Policy Server and click **Add/Remove**.
4. Complete the uninstall by following the instructions on the screen.

☞ **Note:** If the system displays a “Remove Shared File?” message, click **Yes to All**.

5. When the uninstall is finished, exit the **Add/Remove Programs** and Control Panel dialogs.
6. If the system has an iPlanet Web Server Enterprise Edition 4.0 or later, or Netscape Enterprise Web Server 3.5*x* or later, see the section *Uninstalling for Netscape Web Servers* on page 26.
7. Reboot the system.

The Policy Server uninstallation is complete.

Uninstalling for Netscape Web Servers

If you are using an iPlanet Web Server Enterprise Edition 4.0 or later, or Netscape Enterprise Web Server 3.5*x* or later, you must edit the `obj.conf` and `mime.types` files before completing the uninstall process. Start with the `obj.conf` file.

1. Open the `obj.conf` file:

   <*netscape_installation*>/<*server_location*>/https-<*myserver*>\config

   where <*netscape_installation*> is the installed location of Netscape, **<*server_location*>** is the installed location of the Netscape Web servers, and **<*myserver*>** is the name of the Web server on which the Policy Server is installed.

   For example,

   C:\Netscape\Server4\https-machinename\config

2. Remove the following lines:

```
Init fn=”load-modules” funcs=”send_crystal_image”
shlib=C:/WINNT/crystal/crimage.dll”

Init fn=”load-modules” funcs=”CrystalReportServer”
shlib=C:/WINNT/crystal/crweb.dll”

NameTrans fn=pfx2dir from=/smreportsviewer dir=”C:/
WINNT/crystal”

NameTrans fn=pfx2dir from=/SMReportsCgi dir=”C:/
WINNT/Program Files/Netegrity/SiteMinder/
Reports”name=”cgi”

NameTrans fn=pfx2dir from=/SMReports dir=”C:/WINNT/
Program Files/Netegrity/SiteMinder/Reports”

”NameTrans fn=pfx2dir from=/sitemindercgi dir=”C:/
WINNT/Program Files/Netegrity/SiteMinder/Admin”
name=”cgi”

”NameTrans fn=pfx2dir from=/siteminder dir=”C:/WINNT/
Program Files/Netegrity/SiteMinder/Admin”

Service fn=”send_crystal_image” method=” (GET|POST):
type=”magnus-internal/cri”

Service fn=”CrystalReportServer” method=” (GET|POST):
type=”magnus-internal/rpt”
```

3. Open the `mime.types` file under the `..\Netscape\Server4\https-machinename\config` folder and remove the following lines.

   ```
   type=magnus-internal/cri exts=cri
   ```

   ```
   type=magnus-internal/rpt exts=rpt
   ```

4. Reboot the system.

   The Policy Server uninstallation is complete.

Chapter 2: Installing the Policy Server on Solaris

Overview

This chapter describes how to install the SiteMinder Policy Server on a Solaris system, which includes running a setup program and configuring the Web server. When you install the Policy Server on Solaris, you can choose to install the SiteMinder Policy Store (a repository of policy information) in an LDAP directory server or in an Oracle database. Audit logs, for both LDAP and Oracle, can be stored in either Oracle 7, Oracle 8, or a text file.

System Requirements

The SiteMinder Policy Server requires Solaris 2.5.1 or later. The following patches are required and recommended for the following versions of Solaris.

Version	Required Patches	Recommended Patches
Solaris 2.5.1	kernel update and libthread = 103640-31 C++ shared library = 106529-05	None

Solaris 2.6	kernel update = 105181-17
	C++ shared library = 105591-07
	libc = 105210-25
	libthread = 105568-14
		patchadd = 106125-08

Solaris 2.7	kernel update = 106541-08 C++ shared library = 106327-06 libthread = 106980-07	patchadd = 107171-04

Ensure that you have the following components installed on your machine:

- **Memory:** 128 MB RAM
- **Free disk space:** 100 MB free disk space
- **Web Server:** iPlanet Web Server Enterprise Edition 4.0 (or later), or Netscape Enterprise Server version 3.5.1 or later
- **Browser:** Netscape Navigator version 4.07, 4.5, 4.6 or later
- **LDAP Server or Oracle Server:** Netscape iPlanet Directory Server 4.1 (or later) or Netscape Directory Server 3.12 (or later), an Oracle 7.x server, or an Oracle 8.x server, or Novell NDS 8.x must be accessible from the Solaris system on which you are installing the Policy Server

Before you Begin

Before you install the Policy Server, complete the following procedures, if applicable:

- Create a new Solaris account.
- Modify the Solaris system parameters, if necessary.
- Unset the localization variables, if necessary.

Creating a New Solaris Account

Create a new Solaris account with the user name `smuser`. The default shell should be a `ksh`. You may also need to modify the profile for the `smuser` account as indicated later in this chapter.

About the Solaris System Parameters

When the Policy Server is placed under load, it opens a large number of sockets and files. This can become a problem if the default limit parameters are not appropriate for the load.

To view the default limit parameters, type **ulimit -a**. The system displays a message similar to the following:

```
$ ulimit -a
  time(seconds)         unlimited
  file(blocks)          unlimited
  data(kbytes)          2097148
  stack(kbytes)         8192
  coredump(blocks)      unlimited
nofiles(descriptors)    64
vmemory(kbytes)         unlimited
```

The `nofiles` parameter is set to `64` in this example. This is the total number of files (sockets + files descriptors) that this shell and its descendants have been allocated. If this parameter is not set high enough, the Policy Server returns numerous socket errors. The most common socket error is `10024`, or `too many open files`. You must increase this parameter value for proper Policy Server operation under load. You can change this value by running the `ulimit -n` command. For example, to set `nofiles` to `1024`, place the `ulimit -n 1024` command in the `.profile` or `smprofile.ksh` of the `smuser` account.

About the Localization Requirement

Use of the `LC_*` environment variables for localization is not permitted.

If the `L_C*` variables are set by default, they must be `unset` in the `.profile` or `smprofile.ksh` files of the `smuser` account. To identify the available values for the `LANG` environment variable, use the `locale “-a”` command.

Running the Policy Server Setup

1. Log in as `smuser`.
2. Copy `smps-4.1-so.tar` to `smuser`.
3. Untar the `smps-4.1-so.tar` file.
4. Change to the `smps-install` directory.
5. Run the `./smps-install` shell script.

   The installation script checks to see if the required/recommended patches are installed and prepares the Release Notes.

6. Press ENTER to read the Release Notes for important information about installing SiteMinder 4.1.
7. Enter **`y`** to confirm that you want to continue with the installation.

   The installation script displays the prerequisites for installing SiteMinder Policy Server 4.1.

8. Specify a directory path under which the SiteMinder installation directory will be created or press ENTER to use your current location.

   The installation script creates a `siteminder` directory in the specified location. For example, if you specify `/opt`, then this product will be installed in `/opt/siteminder`. If the `siteminder` installation directory already exists make sure that the `smuser` account has proper file permissions to create a subdirectory. If available disk space is found, the installation extracts the files to the chosen directory. This may take a few moments.

   The installation script checks for available space, then installs the SiteMinder Policy Server.

9. To view the License Agreement, press ENTER when prompted.

   The installation script displays the License Agreement.

10. If you have read the License Agreement and agree with the terms, enter **`y`** to continue the installation.

11. Enter and confirm the Encryption Key:

    - If you are installing the first Policy Server in a multiple Policy Server deployment, specify a random, case-sensitive string between 6 and 24 characters long.

    - If you have already installed a Policy Server and this Policy Server will be a part of the same site, enter the Encryption Key you specified during that installation.

    The encryption key is a key that secures data sent between the Policy Server and the policy store. All policy servers that share a SiteMinder policy store must be configured using the same encryption key. For stronger protection, define a long encryption key. For security purposes, the value you enter is not echoed in the terminal window.

12. Select the policy store location.

    - Press ENTER to select an LDAP server and complete the setup described in *Choosing a LDAP Policy Store* on page 34.

      For more information about storing policies in a Netscape LDAP directory, refer to *Storing SiteMinder Data in an LDAP directory* on page 80.

      For more information about storing policies in a Novell LDAP directory, refer to *Chapter 5, Setting up a Policy Store on Novell Netware* on page 91.

    - Enter **B** and press ENTER to select an Oracle server and complete the setup described in *Choosing an Oracle Policy Store* on page 36.

      For more information about storing policies in an Oracle database, refer to *Storing SiteMinder Data in an Oracle Database* on page 75.

Choosing a LDAP Policy Store

The following instructions assume you have completed steps 1-12 of the Policy Server setup procedure in the previous section, and selected the LDAP option in step 12.

The following LDAP directories are supported:

- iPlanet Directory Server 4.1 or later
- Netscape Directory Server 3.12 or later
- Novell NDS 8.0 - 8.3

To configure the LDAP server, you will need to supply the IP address and port of the LDAP server, the root DN under which the SiteMinder schema is placed, and the administrator information for the LDAP directory.

☞ **Note:** This installation cannot be completed using an SSL connection.

To continue the Policy Server installation using an LDAP directory:

1. At the prompt to continue the installation, press ENTER.
2. At the prompt to initialize the LDAP server with the SiteMinder schema, press ENTER.
3. Enter the IP address of the LDAP directory and press ENTER.
4. Enter the port number of the LDAP directory and press ENTER or press ENTER to accept the default number (389).
5. Enter the username (Bind DN) for the LDAP administrator account and press ENTER:
   - For Netscape LDAP, specify the CN of the administrator as follows:

     cn=<*Directory Manager>*, where <*Directory Manager>* is the Bind DN.

   - For NDS, specify the CN of the administrator followed by the root DN as follows:

     cn=<*Directory Manager>*, **o=***<test>,* where <*Directory Manager>* is the Bind DN and *<test>* is the root DN.

   SiteMinder will bind to the LDAP server using this DN.

6. Enter the password for the administrator account and press ENTER.
7. Confirm the password and press ENTER.
8. Enter the root DN as follows, and press ENTER:
   - For Netscape LDAP, specify the root DN as follows:

     o=<*test.com***>**

     where <*test.com*> is the root DN.
   - For NDS, specify the root DN as follows:

     o=<*test*>

     where <*test*> is the root DN.

   The values you have entered are listed in the terminal window.
9. To accept the values, press ENTER.

   The installation script tests the connection with the LDAP server and then prompts you to select your logging preference (text file or Oracle database). To use an Oracle database, you must have an Oracle 7 or Oracle 8 database accessible to the installation.
10. Select your audit logging preference:
    - Press ENTER to use a text file. The location and name of the log file appears in the terminal window.
    - Enter **Y** and press ENTER to use an Oracle database. For more information, refer to *Storing Audit Logs in an Oracle Database* on page 37.
11. Enter and confirm the Super User password.
12. If you want to start the Policy Server, press ENTER.
13. Enter **Y** if you want the **smprofile.ksh** added to the **.profile** file.
14. Configure the Web server as described in *Configuring the Netscape Web Server* on page 38.
15. Optionally, access the SiteMinder Policy Server User Interface as described in *Accessing the SiteMinder Policy Server User Interface* on page 39.

Choosing an Oracle Policy Store

The following instructions assume you have completed steps 1-12 when you ran the Policy Server setup, as described in *Running the Policy Server Setup* on page 32.

To use an Oracle server, you must have one of the following Oracle client configurations installed on the same machine as the SiteMinder Policy Server:

- For Oracle 7, you need sql*net and the appropriate protocol adapter for your network.
- For Oracle 8, you need net8 and the appropriate protocol adapter for your network.
- For Oracle 7 and 8, you need sqlplus.

To continue the Policy Server installation using an Oracle database:

1. After completing steps 1-12 of *Running the Policy Server Setup* on page 32, selecting Oracle as the Policy Store, and reading the Oracle requirements, press ENTER to continue the installation using Oracle.
2. Specify the Oracle client version number:
   - Press ENTER to use Oracle 7, which is the default choice.
   - Enter **`8`** and press ENTER to use Oracle 8.
   - A message appears notifying you that you must copy the **`smprofile.ksh`** to your **`.profile`** file.
3. To copy the **`smprofile.ksh`** to the **`.profile`** file now, press ENTER.
4. Configure the Web server as described in *Configuring the Netscape Web Server* on page 38.
5. Configure the SiteMinder schema, as described in *Storing SiteMinder Data in an Oracle Database* on page 75.
6. Optionally, configure the Policy Server to use an Oracle database for logging audit information, as described in *Storing Audit Logs in an Oracle Database* on page 37.
7. Optionally, access the SiteMinder Policy Server User Interface as described in *Accessing the SiteMinder Policy Server User Interface* on page 39.

Storing Audit Logs in an Oracle Database

SiteMinder allows you to write information about authentication, authorization, and administration events to an audit log. Audit logs can be stored in an Oracle database or a text file.

If you chose an Oracle database for the policy store and you want to use an Oracle database to store the audit information, complete the following procedure.

☞ **Note:** If you chose an LDAP directory for the policy store and you want to use an Oracle database to store event information, you do not need to complete the following procedure. Instead, specify that you want to use an Oracle database for the audit logs when you choose the LDAP policy store, as described in *Choosing a LDAP Policy Store* on page 34.

To store audit logs in an Oracle database:

1. Configure the SiteMinder schema for Oracle as specified in the previous section.
2. Run **`smconsole`** to start the SiteMinder Policy Server Management Console.
3. Click the **Settings** tab to move it to the front.
4. In the **Audit Logging** group, select the **SQL/ODBC Database** option.
5. Click the **ODBC** tab to move it to the front.
6. In the **Select a Database** drop-down menu, select **Audit Logs**.
7. Enter the data source information for the audit log database by completing the following fields:
   - **Data Source Name**—Name of the data source created to store the audit logs.
   - **User Name**—If required, user name of the database account. This user name must have full rights to access the database.

- **Password/Confirm Password**—If required, password of the database account above.
- **Maximum Connections**—The number of ODBC connections per database that SiteMinder can have open.

8. Click **Apply** to save the audit logs database selection or **OK** to save the settings and exit the SiteMinder Policy Server Management Console.

Configuring the Netscape Web Server

1. Change the directory to `$SM_HOME/siteminder`.
2. Log in as the user with permissions to the Netscape Web server directory and run `./smnssetup`**.**

   The system states that the `smnssetup` script will modify the `obj.conf` file. To run SiteMinder, you must update this file.
3. Press ENTER.
4. Enter the Netscape Server Administrator directory:

   /<netscape_installation>/<location>/

   where **<***netscape_installation***>** is the installed location of Netscape and **<***location***>** is the installed location of the Netscape Web servers.

   For example,

   ```
   /usr/netscape/server4
   ```
5. If you have multiple Web servers, select the `https-`<*hostname*> server you want to configure with the Policy Server and press ENTER to continue.

   This completes the necessary modification of the `obj.conf` file.
6. Restart the Netscape `https-`<*hostname*> server.

   The installation is complete. You can now access the SiteMinder Policy Server User Interface, as described in the next section.

Accessing the SiteMinder Policy Server User Interface

Once you have installed the Policy Server, access it through a browser. Verify that the browser supports SiteMinder by entering the following URL: `http://www.netegrity.com/UItest`

Note: The URL for the browser test is case-sensitive.

To reduce the time it takes to load the Policy Server User Interface, you can access it locally from your machine. Refer to *Accessing the Policy Server User Interface Locally* on page 39.

To access the Policy Server User Interface:

1. Start your browser and enter `http://`*<hostname>*`.`*<domain>* `/siteminder` in the URL field.

   The <*hostname*> is the name of the machine on which the Policy Server is installed, such as `mymachine`, and <*domain*> is the cookie domain of the host machine, such as `.myorg.org`. For example:

   ```
   http://mymachine.myorg.org/siteminder
   ```

   The system displays your browser with the administrator login page.

2. Click **Administer SiteMinder**.

3. Enter **`SiteMinder`** as the user name and enter the password you entered during the installation.

   The SiteMinder Policy Server User Interface opens.

Accessing the Policy Server User Interface Locally

Accessing the Policy Server User Interface locally from your Web browser reduces the time it takes to load the Policy Server User Interface.

If you access the Policy Server User Interface from Netscape Communicator, you can copy the Policy Server User Interface files (stored in `sm_admin.jar`) to the directory where Netscape's Java classes are located to increase performance.

To access the Policy Server User Interface on a local machine using a Netscape browser:

1. Navigate to the SiteMinder `Admin` directory:

   <*siteminder_installation*>`/Admin`

   where <*siteminder_installation*> is the installed location of SiteMinder.

   For example,

   ```
   smuser/netegrity/siteminder/admin
   ```

2. Copy `sm_admin.jar` to the following location:

   <*netscape_communicator_installation*>`/program/java/classes`

   where <*netscape_communicator_installation*> is the installed location of Netscape Communicator.

   For example,

   ```
   $HOME/netscape/communicator/Program/java/classes
   ```

3. Restart the Netscape Web browser.
4. If you are prompted to grant additional privileges to Netegrity when you access the Policy Server User Interface, click **Grant**.

☞ **Note:** If you install a new version of the Policy Server, you must copy the new `sm_admin.jar` file to the Netscape Java classes directory.

Configuring Auto Startup

The following steps ensure that the Policy Server services restart automatically when the Solaris system is re-booted.

1. Change the directory to `$SM_HOME/siteminder`.
2. Enter **`su`** and press ENTER**.**

   You are prompted for a password.

3. Enter the root password and press ENTER.

4. Enter **`cp S98sm /etc/rc2.d`** and press ENTER.

   `s98sm` automatically calls the `stop-all` and `start-all` executables, which stop and start the SiteMinder Authentication, Authorization, Accounting and Administration services when the Solaris system is rebooted.

☞ **Note:** If you are using a local LDAP directory server as a policy store, you must configure the LDAP directory to start automatically before starting the Policy Server services automatically.

Uninstalling the Policy Server on Solaris

1. Ensure that no Web Agents are configured to use the Policy Server you are uninstalling:

   - For IIS Web Agents, complete the following:

     a. Access the Web Agent IIS Management Console from the Start menu by selecting **Programs** | **SiteMinder** | **SiteMinder Web Agent NT IIS Management Console**.

     b. In the Console, select the **Servers** tab to move it to the front.

     c. In the Policy Server list, select the Policy Server entry you want to remove and click **Remove**.

     d. SiteMinder removes the Policy Server from the list.

     e. Click **OK** to save your changes and exit the Console.

     f. From the Services control panel, stop and restart the Web server.

   - For Netscape and Apache Web Agents, complete the following:

     a. Open the `WebAgent.conf` file:

        - For NT, the default location is <*netscape_installation*>\ <*serverlocation*>`\https-`<*hostname*>`\config`

          where <*netscape_installation*> is the installed location of Netscape, <*serverlocation*> is the installed location of the Netscape Web servers and <*hostname*> is the name of the server.

For example,

`C:\Netscape\Server4\https-myserver\config`

- For UNIX, the default location is */<server>/<confdirectory>*

  where <*server*> is the installed location of Netscape or Apache Web server on which the Web Agent is installed, and <*confdirectory*> is the name of the directory where that Web server's configuration files are stored.

  For example:

  Apache: `/usr/apache/conf`

  Netscape: `/usr/netscape/server4/https-myserver/config`

b. Remove the IP address and port numbers that correspond to the Policy Server that you are uninstalling from the line that starts with `“policyserver=”`.

   If only one Policy Server is listed, specify the IP address and port numbers of a different Policy Server to continue using the Web Agent to protect your resources.

c. Save `WebAgent.conf`.

d. Stop and start the Web Server to apply the changes.

2. Use the `smuser` account to log into the Solaris environment, and run **`stop-all,`** located in the `/siteminder` directory, to stop the SiteMinder processes.
3. Optionally, save the policy store data to a text file using the `smobjexport` tool, as described in *Chapter 11, Policy Server Tools* on page 235.
4. Optionally, remove the policy store using one of the following tools:
   - To remove a policy store stored in an LDAP directory, use `smldapsetup`.
   - To remove a policy store stored in an Oracle database, use `sm_oracle_ps_delete.ps`.

Refer to *Chapter 11, Policy Server Tools* on page 235 for detailed information on removing the policy store.

5. Remove the SiteMinder Policy Server, as described in the next section.
6. Remove SiteMinder references from the `obj.conf` file, as described in *Removing SiteMinder References in the obj.conf File* on page 44.

Removing the SiteMinder Policy Server

Removing the SiteMinder Policy Server involves deleting the `windu` files and directory, and removing `smprofile.ksh` from `.profile`.

To remove the windu files and directory:

1. Change the directory to `$SM_HOME/siteminder/windu/bin`.
2. Stop the configuration store daemon, by entering: **`./windu_registry stop`**
3. Change the directory to `$SM_HOME`.
4. Enter **`rm -rf siteminder`**, then press ENTER.
5. Enter **`rm -rf $HOME/.windu.*`**, then press ENTER.
6. Enter **`rm $HOME/.windu`**

To remove smprofile.ksh:

1. From your `HOME` directory, open `.profile`.
2. Locate and delete the line in `.profile` that contains `smprofile.ksh`.

   For example,

   ```
   /space/smuser/siteminder/smprofile.ksh
   ```
3. Save `.profile`.

Removing SiteMinder References in the obj.conf File

After removing the SiteMinder files, remove references to SiteMinder from the `obj.conf` file.

To remove SiteMinder references from obj.conf:

1. At the Solaris command line, go to the *<path to netscape root>*`/https-<hostname>/config` folder and remove the following line from the `obj.conf` file (must be root):

   ```
   Init fn="init-cgi" SM_ADM_UDP_PORT="4444"
   SM_ADM_TCP_PORT="4444"

   NameTrans fn="pfx2dir
   from="sitemindercgi"dir="..."name=cgi

   NameTrans fn="pfx2dir
   from="siteminderreportscgi"dir="..."name=cgi

   NameTrans fn="pfx2dir from="siteminder"dir="..."
   ```

2. Save and close the `obj.conf` file.
3. Restart the Web Server.

   The uninstallation is complete.

Configuring ODBC Data Sources

The SiteMinder ODBC data sources are configured using the `system_odbc.ini` file located in `$SM_HOME/siteminder/db`. This file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. The file is initially configured with default settings for each of the standard SiteMinder ODBC data sources. This file must be customized to work for each site. In addition, there may be reasons to add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, `[ODBC Data Sources]`, contains a list of all of the currently available data sources. The name before the “=” refers to a subsequent section of the file describing each individual data source. After the “=” is a comment field.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding Oracle ODBC Data Sources

Adding an Oracle Data source involves adding a new data source name in the `[ODBC Data Sources]` section of the `system_odbc.ini` file and adding a section that describes the data source using the same name as the data source.

The required parameters for adding an Oracle data source are:

- **Driver**—choose between the Oracle7 driver in **`$SM_HOME/siteminder/odbc/lib/NSor713.so`** and the Oracle8 driver in **`$SM_HOME/siteminder/odbc/lib/NSor813.so`**.
- **Description**—descriptive comment.
- **ServerName**—name of the Oracle instance to which you want to connect.
- **AllowUpdateAndDelete=1**—set to **1** to enable read and write access.
- **ApplicationUsingThreads=1**—set to **1** to indicate that the driver will be accessed by a multi-threaded application.
- **EnableScrollableCursors=1**—set to **1** to enable scrollable cursors.
- **CallOpinit** —when using the ORACLE client prior to version 7.3.4.0.1 (SQL*Net 2.3.3), the `CallOpinit` parameter in **`/db/odbc.ini`** must be changed to *1*. By default it is *0*. This switch is required for certain versions of Oracle7 in order to prevent application anomalies.

Additionally, the environment `ORACLE_HOME` variable must point to the directory where Oracle is installed on your system.

Chapter 3. Setting up the Policy Store on NT

Overview

The SiteMinder policy store is the repository for all policy related information. All Policy Servers in a SiteMinder installation must share the same policy store data, either directly or via replication. SiteMinder is installed with tools that allow administrators to move policy store data from one storage facility to another.

Policy Servers installed on NT support the following directories and databases for storing policy store data:

- Microsoft Access (default)
- LDAP— iPlanet Directory Server 4.x, Netscape Directory Server 3.12, Novell NDS 8.0 - 8.3
- Oracle (7.x and 8.x)
- Microsoft SQL Server (6.5 and 7.0)

Configuring an NT Policy Server

When you install the Policy Server on an NT machine, the default policy data store is a Microsoft Access database. You can configure the Policy Server to use an LDAP directory, a SQL Server database, or an Oracle database for the policy store after you have completed the Policy Server installation.

☞ **Note:** The Access database is provided for demonstration purposes only. Generally, this sample database is not used in production sites due to the limitations of Access.

Storing SiteMinder Data in an LDAP Directory

The LDAP directory server can be the same directory server SiteMinder uses for user authentication and authorization, which simplifies the task of administering SiteMinder.

The table below lists the specific items that will be required in the process of creating an LDAP policy store or moving an existing policy store from a non-LDAP database or an LDAP directory to an LDAP directory:

Value	**Description**
Secured Sockets Layer (SSL) Certificate Database	If the targeted LDAP directory service communicates with a Policy Server over SSL, the Netscape database where Certificates are located.
LDAP Server IP Address	The targeted LDAP server IP address.
LDAP Port Number	The port number the targeted LDAP service is listening on.
Distinguished Name (DN)	The DN of an LDAP user with sufficient privileges, i.e. the ability to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object (for example, **`cn=Directory Manager`**).
DN’s Password	The password of the Administrator DN.
policy store Root DN	The DN under which the policy store objects are defined. For example, **`o=test.com.`**

If you are creating a new policy store or key store, refer to *Creating an LDAP Policy Store or Key Store* in the next section.

If you are moving an existing policy store from a non-LDAP database or are migrating an LDAP directory to another LDAP directory, refer to *Migrating and Moving Policy Store Data* on page 51.

Creating an LDAP Policy Store or Key Store

You can use an LDAP directory to store SiteMinder policy store data. SiteMinder keys can be stored in the policy store or in a separate location of the LDAP directory.

Note: Storing keys in a separate directory may be required to implement single sign-on functionality. Refer to the *SiteMinder Policy Server Operations Guide* for detailed infomation on key mangement.

To store policies and\or keys in an LDAP directory:

1. Create an LDAP Directory Server instance.
2. Navigate to <*siteminder_installation*>`\Bin`

   where <*siteminder_installation*> is the installed location of SiteMinder, such as:

   ```
   C:\Program Files\Netegrity\SiteMinder\
   ```

3. Set up the LDAP directory by entering the following command to configure the policy store:

   ```
   smldapsetup reg -h<host> -p<port> -d<userdn>
   -w<userpw> -r<root> -ssl<1/0> -c<cert>
   ```

   where **<***host***>** is the name of the LDAP server; **<***port***>** is the port; **<***userdn***>** is the name of an LDAP user with privileges to create a new LDAP schema**;** **<***userpw***>** is the password for the LDAP user specified by -d; and **<***root***>** is the DN location of the SiteMinder data in the LDAP directory.

   Note: If you are connecting to the LDAP directory over SSL, additionally specify **`-ssl1`** and **`-c<`***cert***`>,`** where **<***cert***>** is the absolute path to SSL client certificate database.

   For example,

   ```
   smldapsetup reg -hldapserver.mycompany.com “-dLDAP
   User” -wMyPassword123 -ro=security.com
   ```

4. Switch the policy store to LDAP by entering the following command:

   ```
   smldapsetup switch
   ```

5. Create the schema by completing one of the following:

   - To set up the new policy store:

     ```
     smldapsetup ldgen -f<filename>
     ```

     ```
     smldapsetup ldmod -f<filename>
     ```

     where <*filename*> is the name of the LDIF file you are creating. For example:

     ```
     smldapsetup ldmod -fpstore.txt
     ```

   - To set up the new key store:

     ```
     smldapsetup ldgen -k -f<filename>
     ```

     ```
     smldapsetup ldmod -k -f<filename>
     ```

     where <*filename*> is the name of the LDIF file you are creating. For example:

     ```
     smldapsetup ldmod -k -fkstore.txt
     ```

Note: For detailed instructions on using `smldapsetup`, refer to *Chapter 11, Policy Server Tools* on page 235.

6. If the key store is being stored in a different LDAP directory than the policy store, enter the following commands:

   a. `smldapsetup reg -k -h<host> -p<port> -d<userdn> -w<userpw> -r<root> -ssl<1/0> -c<cert>`

   b. `smldapsetup ldgen -k -f<filename>`

   c. `smldapsetup ldmod -k -f<filename>`

   Note: These commands are identical to the commands used in steps 3 and 5, with the exception of the **`-k`** switch. The **`-k`** switch indicates that the LDAP directory will be used as a key store.

7. Import the basic SiteMinder objects required to set up a policy store or key store by entering the following command:

   ```
   smobjimport -i<siteminder_installation>\db\smdif
   \smpolicy.smdif -v
   ```

where <*siteminder_installation*> is the installed location of SiteMinder. For example,

```
smobjimport “-iC:\Program Files\Netegrity\SiteMinder
\db\smdif\smpolicy.smdif” -v
```

Migrating and Moving Policy Store Data

Using the `smobjexport` and `smobjimport` tools, you can migrate policy store data from other types of databases into LDAP policy stores or move policy stores in one LDAP directory to another LDAP directory. For more information about these tools, refer to the *Chapter 11, Policy Server Tools* on page 235.

The table below identifies the supported migrations and moves:

From	To
Oracle/SQL Server/Access	LDAP
LDAP	LDAP
LDAP	Oracle/SQL Server/Access

The following procedure applies to the Netscape LDAP directory.

To migrate policy store data to a different LDAP directory:

1. Create an LDAP directory server instance.
2. Export your existing data:
   - To export policy store data, complete the following:
     a. Open a Command Prompt window.
     b. Navigate to <*siteminder_installation*>`\Bin`

        where <*siteminder_installation*> is the installed location of SiteMinder, such as:

        ```
        C:\Program Files\Netegrity\SiteMinder\
        ```

     c. Run the export utility to extract your existing data and specify an output text file to temporarily store the data:

        `smobjexport -o`<*filename*>

where <*filename*> is the name of the output file to which you are exporting the data. This filename should be different than the name you used when creating the policy store (refer to *Creating an LDAP Policy Store or Key Store* on page 49).

For example,

```
smobjexport -opstore.txt
```

Note: For a complete listing of the `smobjexport` parameters, enter **`smobjexport -help`**. Refer to *Chapter 11, Policy Server Tools* on page 235 for information about using `smobjexport`.

3. Configure the Policy Server to use the LDAP directory, as described in *Configuring Policy Servers to Use an LDAP Policy Store or Key Store* on page 53.
4. Restart the LDAP directory server.
5. From the SiteMinder `Bin` directory, enter the following commands to set up the new policy store:

   ```
   smldapsetup ldgen -f<filename>
   ```

   ```
   smldapsetup ldmod -f<filename>
   ```

   where <*filename*> is the name of the LDIF file you are creating. For example:

   ```
   smldapsetup ldmod -fpstore.txt
   ```

   Note: For detailed instructions on using `smldapsetup`, refer to *Chapter 11, Policy Server Tools* on page 235.

6. Import the basic SiteMinder objects required to set up a policy store by entering the following command:

   ```
   smobjimport -i<siteminder_installation>\db\smdif
   \smpolicy.smdif -v
   ```

   where <*siteminder_installation*> is the installed location of SiteMinder. For example,

```
smobjimport “-iC:\Program Files\Netegrity\SiteMinder
\db\smdif\smpolicy.smdif -v
```

7. Change the SiteMinder Super User password by completing the following steps:

   a. Copy `smreg.exe` from the `\nt\tools` directory on the SiteMinder 4.1 CD-ROM to **<*siteminder_installation*>**`\Bin`

   b. Execute the following command:

      ```
      smreg -su <superuserpassword>
      ```

      where **<*superuserpassword*>** is the password for the SiteMinder Super User account.

   c. Delete `smreg.exe`.

      Deleting `smreg.exe` prevents anyone from changing the Super User password.

8. Run the import utility to import your policy store data from the temporary file:

   ```
   smobjimport -i<filename>
   ```

   For example,

   ```
   smobjimport -ipstore.txt
   ```

9. Configure the Policy Server to use the LDAP directory, as described in the next section.

Configuring Policy Servers to Use an LDAP Policy Store or Key Store

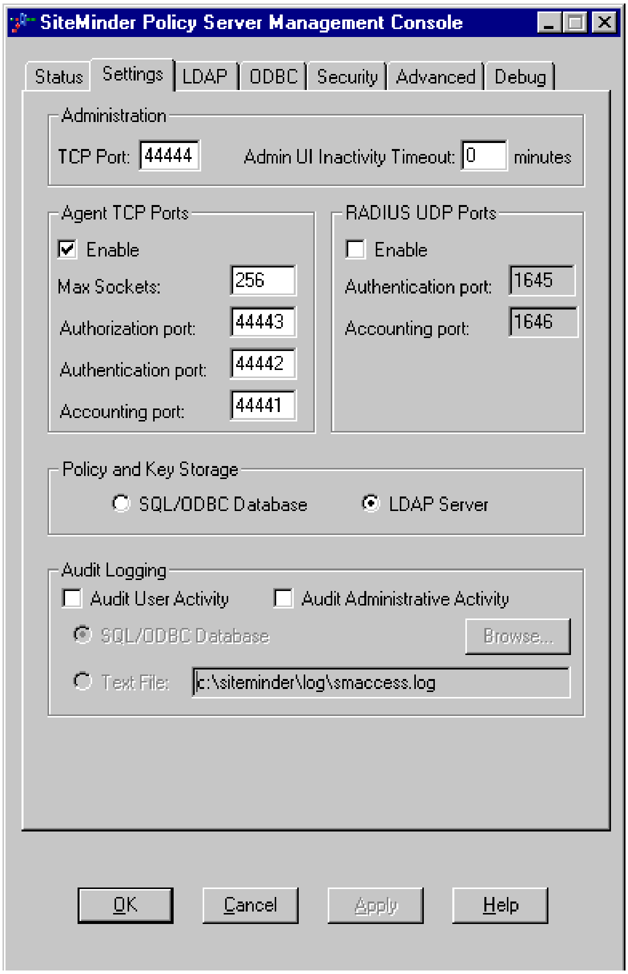
Once you have created a new policy store or key store, or migrated or moved an LDAP policy store, you must configure the Policy Server to use the LDAP directory. You can also use the Policy Server Management Console to configure additional Policy Servers to leverage an existing policy store in an LDAP directory.

Refer to the *SiteMinder Policy Server Operations Guide* for detailed information about using the Policy Server Management Console.

To configure a Policy Server to use a policy store or key store in an LDAP directory:

1. From the Start menu, select **Programs | SiteMinder | SiteMinder Policy Server Management Console**.

   The Console opens as shown in the following graphic.



Administration

TCP Port: 44444 Admin UI Inactivity Timeout: 0 minutes

Agent TCP Ports

☑ Enable

Max Sockets: 256

Authorization port: 44443

Authentication port: 44442

Accounting port: 44441

RADIUS UDP Ports

□ Enable

Authentication port: 1645

Accounting port: 1646

Policy and Key Storage

○ SQL/ODBC Database ● LDAP Server

Audit Logging

□ Audit User Activity □ Audit Administrative Activity

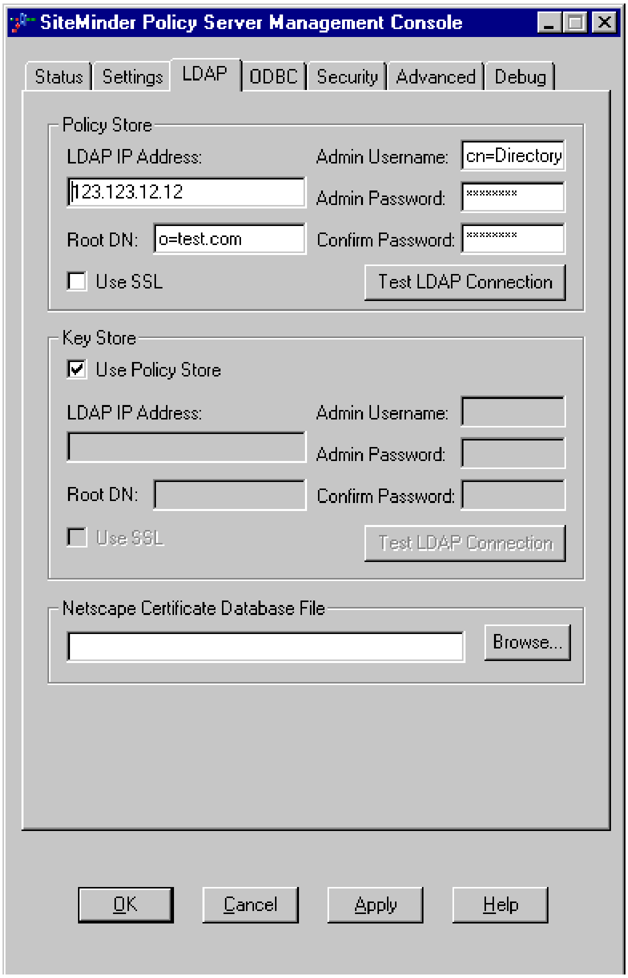
● SQL/ODBC Database Browse...

○ Text File: c:\siteminder\log\smaccess.log

2. Select the **Settings** tab to move it to the front.

3. In the **Policy and Key Storage** group box, select **LDAP Server** and click **Apply**.

4. Select the **LDAP** tab to move it to the front, as shown next.



Policy Store

LDAP IP Address: 123.123.12.12

Admin Username: cn=Directory

Admin Password: *********

Root DN: o=test.com

Confirm Password: *********

☐ Use SSL

Key Store

☑ Use Policy Store

LDAP IP Address:

Admin Username:

Admin Password:

Root DN:

Confirm Password:

☐ Use SSL

Netscape Certificate Database File

5. If you are configuring a policy store, in the **Policy Store** group box, do the following:

   a. In the **LDAP Server** field, enter the IP address and port number of the LDAP directory, separated by a colon (:). For example, enter **`123.123.12.12:321.`** If the port number is not specified, SiteMinder uses port 389 by default.

   b. In the **Root DN** field, enter the LDAP branch under which the SiteMinder schema is located (for example, **`o=test.com`**).

c. In the **Admin Username** field, enter the DN of the LDAP directory administrator for the Policy Server being configured (for example, `cn=Directory Manager`).

d. In the **Admin Password** field, enter the LDAP directory administrator password.

e. In the **Confirm Password** field, re-enter the LDAP directory administrator password.

f. If your system is communicating with the LDAP directory over SSL, select the **Use SSL check box**.

g. If you are using SSL, enter the name of the certificate database in the **Netscape Certificate Database File** field.

   You can specify other types of certificates in this field. The certificate does not need to be Netscape.

h. Click **Apply** to save the settings.

6. If you are configuring a separate key store, in the **Key Store** group box, do the following:

   a. Deselect the **Use Policy Store** check box.

   b. In the **LDAP Server** field, enter the IP address and port number of the LDAP directory, separated by a colon (:). For example, enter **`123.123.12.12:321.`** If the port number is not specified, SiteMinder uses port 389 by default.

   c. In the **Root DN** field, enter the LDAP branch under which the SiteMinder schema is located (for example, `o=test.com`).

   d. In the **Admin Username** field, enter the DN of the LDAP directory administrator for the Policy Server being configured (for example, `cn=Directory Manager`).

   e. In the **Admin Password** field, enter the LDAP directory administrator password.

   f. In the **Confirm Password** field, re-enter the LDAP directory administrator password.

   g. If your system is communicating with the LDAP directory over SSL, select the **Use SSL check box**.

h. If you are using SSL, enter the name of the certificate database in the **Netscape Certificate Database File** field.

   You can specify other types of certificates in this field. The certificate does not need to be Netscape.

i. Click **Apply** to save the settings.

7. Click the **Settings** tab and verify that the **LDAP Server** option is selected in the **Policy and Key Storage** group box.
8. Click **Apply**.
9. Click **Test LDAP Connection** to verify connectivity to the LDAP directory server.
10. Click **OK** to save the settings and close the Console.

Storing SiteMinder Data in an ODBC Database

You can use an SQL or Oracle database to store SiteMinder policy store data. SiteMinder keys, audit logs, and token data can be stored in the policy store or in a separate database.

Note: Storing keys in a separate database may be required to implement single sign-on functionality. Refer to the *SiteMinder Policy Server Operations Guide* for detailed infomation on key mangement.

To set up a SiteMinder Windows NT installation to use a SQL Server or Oracle database for storage of policy information, keys, audit logs, or token data, complete the following tasks:

1. If you are creating a database for policy storage, export the policy store data from the existing policy store, if one exists, as described in *Exporting the Policy Store Data From the Existing Database* on page 58.
2. Configure the SQL Server or Oracle database using the SiteMinder schema, as described in *Creating the Oracle or SQL Server Database Using the SiteMinder Schema* on page 60.

3. Configure SiteMinder to use a SQL Server or Oracle database:

   - To use the database as the policy store, refer to *Configuring SiteMinder to Use an Oracle or SQL Database* on page 61.

   - To use the database to store keys, audit logs, or token data, refer to *Configuring an ODBC Database to Store Keys, Audit Logs or Token Data* on page 70.

4. Import the basic SiteMinder objects contained in `smpolicy.smdif` and the exported policy store data into the SQL Server or Oracle database (if applicable), as described in *Importing the Policy Store Data into the Database* on page 72.

Before You Begin

Make sure one of the following clients and the appropriate drivers are installed on your system:

- Oracle 7 or Oracle 8; or

- SQL Server 6.5 or SQL Server 7.0

Exporting the Policy Store Data From the Existing Database

Export policy store data using the `smobjexport` SiteMinder Policy Server tool. For more information about this utility, refer to the *Chapter 11, Policy Server Tools* on page 235.

Export policy store data for the following reasons:

- You are currently storing your policy store data in an MS Access database, and you want to store it in SQL Server or Oracle.

- You are currently storing your policy store data in a SQL or Oracle database, and you want to store it in another SQL or Oracle database.

☞ **Note:** If there is no existing SiteMinder database, exporting the policy store is unnecessary.

To export policy store data:

1. Open a Command Prompt window and navigate to the *<siteminder_installation>*`\bin` directory, where *<siteminder_installation>* is the installed location of SiteMinder, such as:

   ```
   c:\Program Files\Netegrity\SiteMinder\
   ```

2. Do one of the following:

   - If the policy store data you are exporting uses the same encryption key as the target Policy Server, enter the following and press ENTER:

     ```
     smobjexport -o<filename>
     ```

     where **<***filename***>** is the name of the output file that will contain the exported policy store data.

     For example,

     ```
     smobjexport -opstore.txt
     ```

   - If the policy store data you are exporting does not use the same encryption key as the target Policy Server, export the data in clear text by entering the following on one line:

     ```
     smobjexport -o<filename> -c -d<admin-name> -w<admin-pw>
     ```

     where **<***filename***>** is the name of the output file that will contain the exported policy store data, <*admin-name*> is the name of a SiteMinder administrator that can manage all SiteMinder objects, and <*admin-pw*> is the password for the specified SiteMinder administrator.

     For example,

     ```
     smobjexport -opstore.txt -c-dAdmin -wpassword
     ```

☞ **Note:** If you exported data in clear text, you must specify **`-c`** when you import the data, too.

The data is exported from the current Policy Server database to the ASCII file named `pstore.txt`.

☞ **Note:** For a complete listing of the `smobjexport` parameters, enter **`smobjexport -help`**. Refer to *Chapter 11, Policy Server Tools* on page 235 for information about using `smobjexport`.

Creating the Oracle or SQL Server Database Using the SiteMinder Schema

SiteMinder provides schema files to create schemas for storing policies, keys, logs and token data, such as Encotone TeleID data. The following schema files are provided in the `\SiteMinder\Db\Sql` directory:

Schema File	Description
sm_oracle_ps.sql	Creates the SiteMinder policy store or key store (if you are storing keys in a different database) in an Oracle database.
sm_oracle_logs.sql	Creates the schema for SiteMinder audit logs in an Oracle database.
sm_oracle_token.sql	Creates the schema for storing token data, such as Encotone TeleID data, in an Oracle database.
sm_mssql_ps.sql	Creates the SiteMinder policy store or key store (if you are storing keys in a different database) in an SQL database.
sm_mssql_logs.sql	Creates the schema for SiteMinder audit logs in an SQL database.
sm_mssql_token.sql	Creates the schema for storing token data, such as Encotone TeleID data, in an SQL database.

Create the schemas by importing the appropriate file(s). You can import only the schema files for the schemas you want to use. For example, if you are not supporting token authentication, you do not have to import a token schema.

For information about importing schema files, refer to your database documentation.

Configuring SiteMinder to Use an Oracle or SQL Database

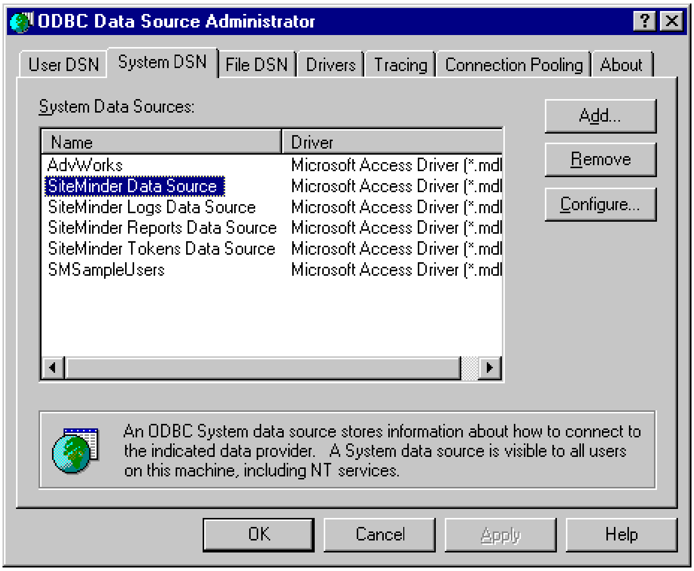
The following steps are involved in configuring the Policy Server to use an Oracle or SQL database to store policies, keys, logs, and token data.

1. Create and configure an Oracle data source or a SQL Server data source using the ODBC Data Source Administrator.
2. Point SiteMinder to use the data source you have created as a policy store. Optionally, point SiteMinder to use the policy store to store keys, audit logs, and token data; or point to a separate database for key, audit log, and\or token data storage.

   Refer to *Configuring an ODBC Database to Store Keys, Audit Logs or Token Data* on page 70 for information on configuring a separate database for key, audit log, and\or token data storage.

To create and configure an Oracle data source:

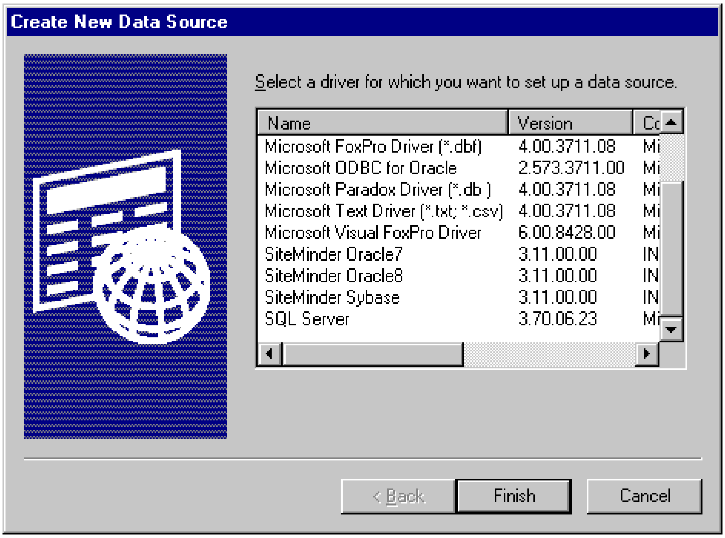
1. From the Control Panel, double-click on ODBC to access the ODBC Data Source Administrator.
2. Click the **System DSN** tab to move it to the front, as shown below.



Name	Driver
AdvWorks	Microsoft Access Driver (*.mdl
SiteMinder Data Source	Microsoft Access Driver (*.mdl
SiteMinder Logs Data Source	Microsoft Access Driver (*.mdl
SiteMinder Reports Data Source	Microsoft Access Driver (*.mdl
SiteMinder Tokens Data Source	Microsoft Access Driver (*.mdl
SMSampleUsers	Microsoft Access Driver (*.mdl

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

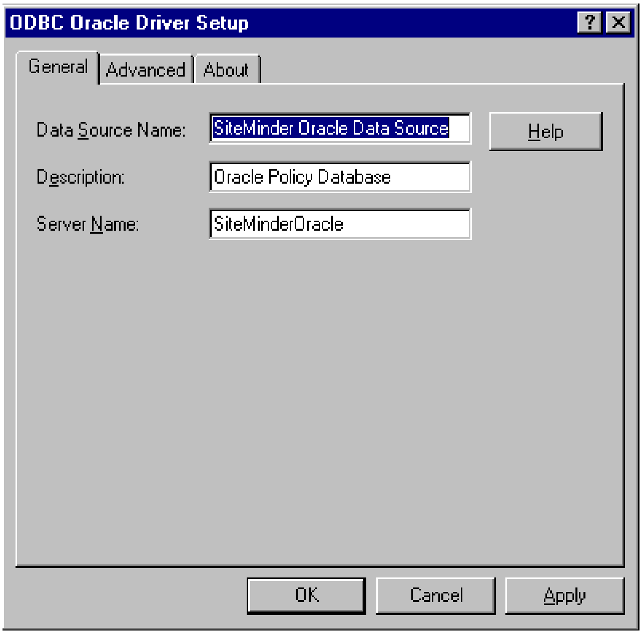
3. Select **SiteMinder Data Source** and click **Add**. The **Create New Data Source** dialog box appears, as shown below.



Select a driver for which you want to set up a data source.

Name	Version	Cc
Microsoft FoxPro Driver (*.dbf)	4.00.3711.08	Mi
Microsoft ODBC for Oracle	2.573.3711.00	Mi
Microsoft Paradox Driver (*.db)	4.00.3711.08	Mi
Microsoft Text Driver (*.txt; *.csv)	4.00.3711.08	Mi
Microsoft Visual FoxPro Driver	6.00.8428.00	Mi
SiteMinder Oracle7	3.11.00.00	IN
SiteMinder Oracle8	3.11.00.00	IN
SiteMinder Sybase	3.11.00.00	IN
SQL Server	3.70.06.23	Mi

4. Select **SiteMinder Oracle7** or **SiteMinder Oracle8** and click **Finish**. The ODBC Driver Setup dialog appears, as shown next.



Data Source Name: SiteMinder Oracle Data Source

Description: Oracle Policy Database

Server Name: SiteMinderOracle

5. Under the **General** tab, do the following:

   a. In the **Data Source Name** field, enter the data source name.

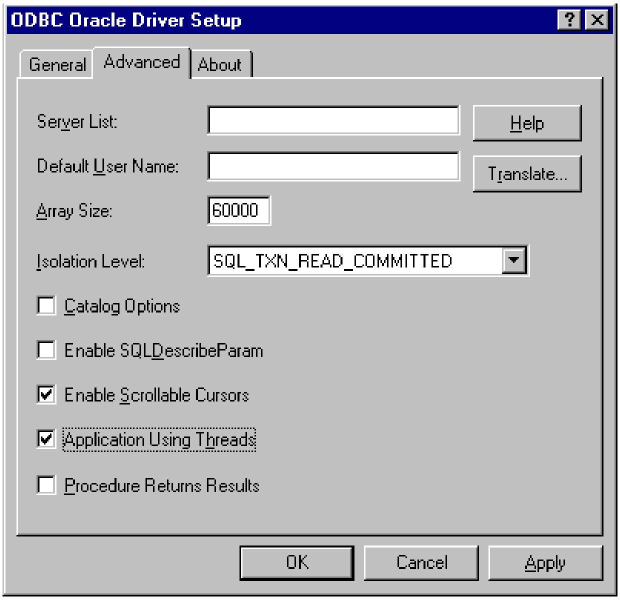
      This name must correspond to the one you will enter in the SiteMinder Policy Server Management Console, as described in *Configuring an ODBC Database as a Policy Store* on page 67.

   b. Optionally, in the **Description** field, enter a description of the data source.

   c. In the **Server Name** field, enter the server name. Do not use blanks in the name.

      This is the Oracle client connection string (TSN name) referenced in the **Oracle Easy Configuration** dialog box.

6. Click the **Advanced** tab to move it to the front, as shown next.



ODBC Oracle Driver Setup

Server List:

Default User Name:

Array Size: 60000

Isolation Level: SQL_TXN_READ_COMMITTED

□ Catalog Options

□ Enable SQLDescribeParam

☑ Enable Scrollable Cursors

☑ Application Using Threads

□ Procedure Returns Results

7. Under the **Advanced** tab, do the following:

   a. Select the **Enable Scrollable Cursors** option.

   b. Select the **Application Using Threads** option.

8. Click **OK** to save the selections and exit the **ODBC Oracle Driver Setup**.

   The configuration is complete. Now you must configure SiteMinder to use the data source you just created.

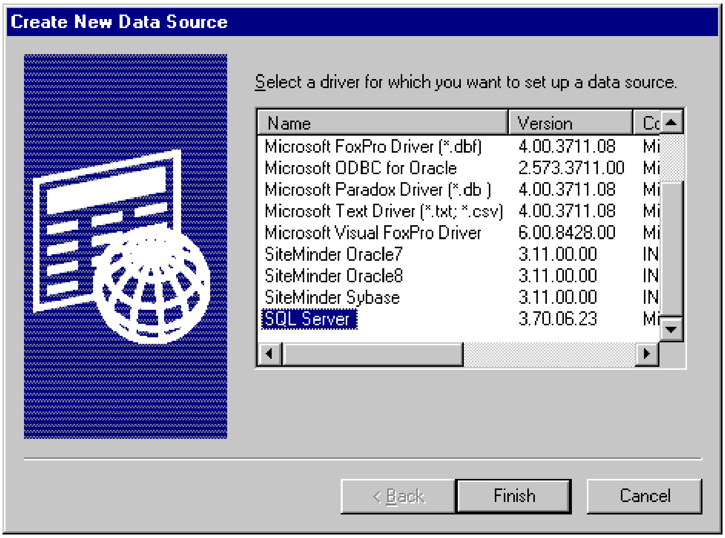
To create and configure a SQL Server data source:

1. From the Control Panel, double-click on **ODBC Data Sources** to access the **ODBC Data Source Administrator.**

2. Click the **System DSN** tab to move it to the front.

3. Select **SiteMinder Data Source** and click **Add**.

The **Create New Data Source** dialog box appears, as shown next.



Select a driver for which you want to set up a data source.

Name	Version	Cc
Microsoft FoxPro Driver (*.dbf)	4.00.3711.08	Mi
Microsoft ODBC for Oracle	2.573.3711.00	Mi
Microsoft Paradox Driver (*.db)	4.00.3711.08	Mi
Microsoft Text Driver (*.txt; *.csv)	4.00.3711.08	Mi
Microsoft Visual FoxPro Driver	6.00.8428.00	Mi
SiteMinder Oracle7	3.11.00.00	IN
SiteMinder Oracle8	3.11.00.00	IN
SiteMinder Sybase	3.11.00.00	IN
SQL Server	3.70.06.23	Mi

4. Select **SQL Server** and click **Finish**.

   The second **Create New Data Source** dialog box appears.

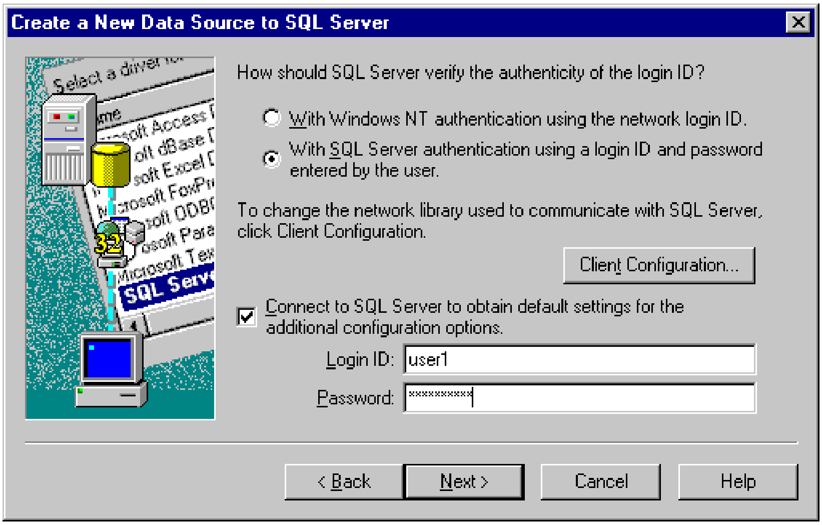
5. Do the following:

   a. In the **Name** field, enter the Data Source name. This name must correspond to the one you will enter in the SiteMinder Policy Server Management Console, as described in the following procedure to configure SiteMinder to use the data source.

   b. (Optional) In the **Description** field, enter a description of the data source.

c. In the **Server** drop-down list, enter the name of an existing SQL server.

d. Click **Next**. The second **Create New Data Source** dialog box appears, as shown below.



Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

○ With Windows NT authentication using the network login ID.

● With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

☑ Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID: user1

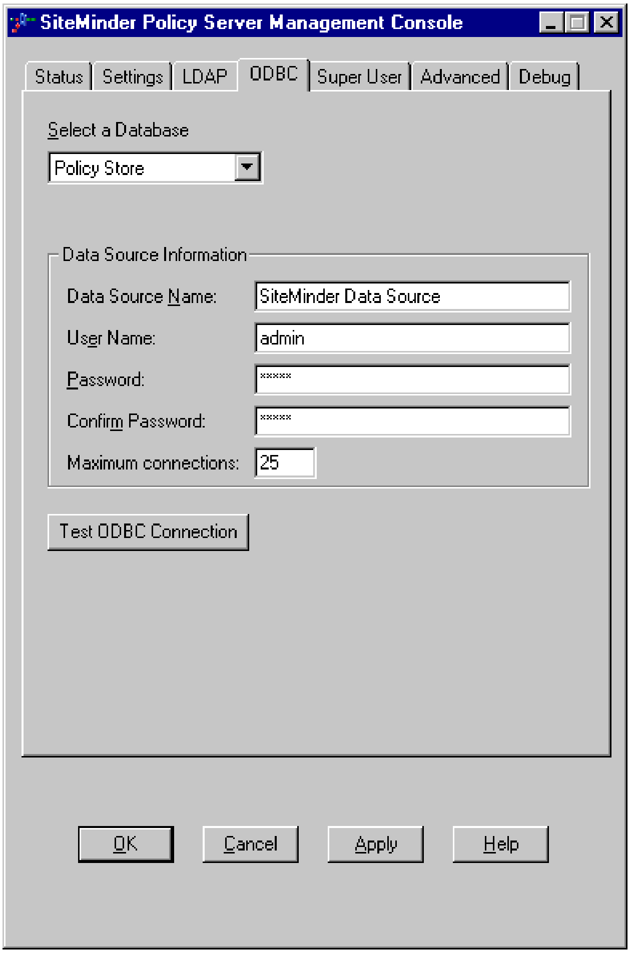
Password: **********

6. Select the **With SQL Server authentication using a login ID and password entered by the user** radio button, then click **Next**.

The configuration is complete. Now you must point SiteMinder to use the data source you just created.

Configuring an ODBC Database as a Policy Store

1. From the Start menu, select **Programs** | **SiteMinder** | **SiteMinder Policy Server Management Console**.
2. Select the **ODBC** tab to move it to the front, as shown next.



Select a Database: Policy Store

Data Source Name: SiteMinder Data Source

User Name: admin

Password: *****

Confirm Password: *****

Maximum connections: 25

3. In the **Select a Database** drop-down list, select **Policy Store**.
4. In the **Data Source Name** field, enter the name of the data source.

   This name must correspond to the name you entered in the **Data Source** field of the **ODBC Driver Setup** dialog box.

5. In the **User Name** and **Password** fields, enter the username and password of the database account that has full access rights to the database.
6. In the **Confirm Password** field, re-enter the password.
7. Specify the maximum number of database connections allocated to SiteMinder. For best performance, retain the default of 25 connections.
8. Click **Apply** to save the settings.

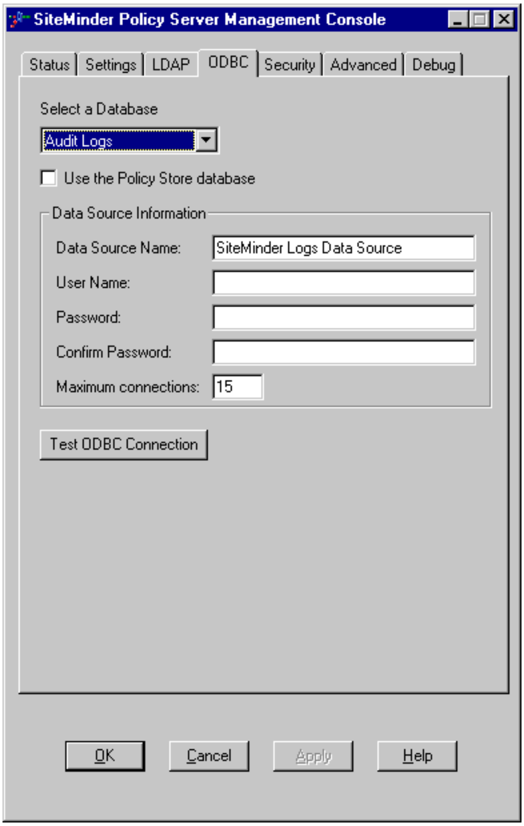
Storing Keys, Audit Logs and Token Data in the Policy Store

You can store keys, logging, and token information in the policy store to simplify administration tasks.

To point SiteMinder to store keys, audit logs and token data in the same database:

1. In the SiteMinder Policy Server Management Console, click the **ODBC** tab to move it to the front.

The following tab is displayed:



Select a Database: Audit Logs

□ Use the Policy Store database

Data Source Information

Data Source Name: SiteMinder Logs Data Source

User Name:

Password:

Confirm Password:

Maximum connections: 15

2. In the **Select a Database** drop-down list, select **Key Store**.
3. Select the **Use the policy store database** check box and click **Apply**.
4. In the **Select a Database** drop-down list, select **Audit Logs**.
5. Select the **Use the policy store database** check box and click **Apply**.
6. In the **Select a Database** drop-down list, select **Token Data**.
7. Select the **Use the policy store database** check box and click **Apply**.
8. Click **Test ODBC Connection** to verify connectivity to the database server.
9. Click **OK** to save the settings and exit the Console.

Configuring an ODBC Database to Store Keys, Audit Logs or Token Data

SiteMinder keys, audit logs, and token information can all be stored in separate databases.

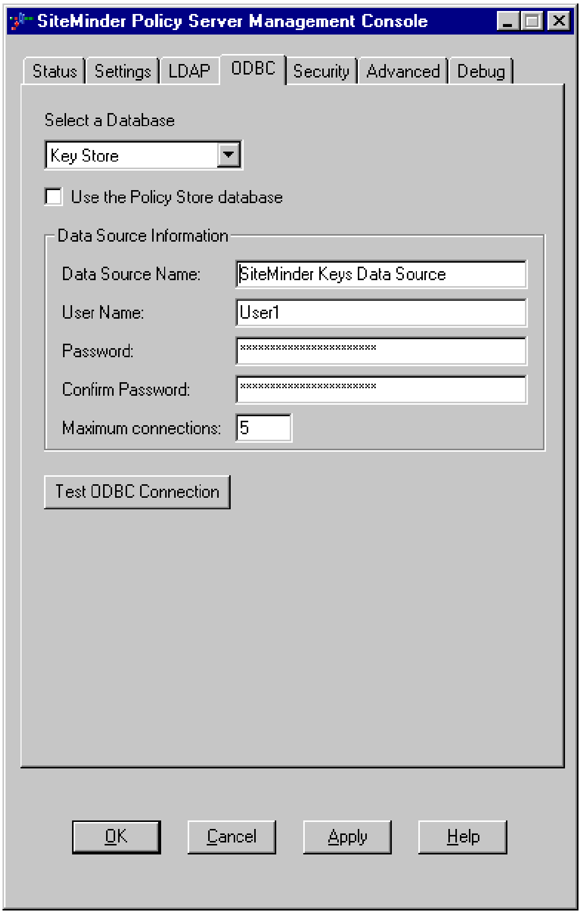
Before configuring an ODBC database to store keys, audit logs or token data, make sure you have created and configured a separate database, as described in *Creating the Oracle or SQL Server Database Using the SiteMinder Schema* on page 60, and *Configuring SiteMinder to Use an Oracle or SQL Database* on page 61.

☞ **Note:** Storing keys in a separate database may be required to implement single sign-on functionality. Refer to the *SiteMinder Policy Server Operations Guide* for detailed infomation on key mangement.

To point SiteMinder to store keys, audit logs and token data in different databases:

1. In the SiteMinder Policy Server Management Console, click the **ODBC** tab to move it to the front.

The following tab is displayed:



SiteMinder Policy Server Management Console

Select a Database: Key Store

□ Use the Policy Store database

Data Source Information

Data Source Name: SiteMinder Keys Data Source

User Name: User1

Password: ************************

Confirm Password: ************************

Maximum connections: 5

2. In the **Select a Database** drop-down list, select **Key Store**.
3. Deselect the **Use the policy store database** check box and click **Apply**.

   The fields in the **Data Source Information** group box become active.
4. In the **Data Source Name** field, enter the name of the data source.

   This name must correspond to the name you entered in the **Data Source** field of the **ODBC Driver Setup** dialog box.

5. In the **User Name** and **Password** fields, enter the username and password of the database account that has full access rights to the database.
6. In the **Confirm Password** field, re-enter the password.
7. Specify the maximum number of database connections allocated to SiteMinder. For best performance, retain the default of 5 connections.
8. Click **Apply** to save the settings.

Importing the Policy Store Data into the Database

Import data for the following reasons:

- To import required SiteMinder objects stored in `smpolicy.smdif`, as described in the next section.
- To import the data you exported into the `pstore.txt` file, as described on page 59.

To import the required policy store objects:

1. Open a command prompt window and navigate to <*siteminder_installation*>`\Bin`, where <*siteminder_installation*> is the installed location of SiteMinder.
2. Import data from the `smpolicy.smdif` file into the policy store by executing the following command:

```
smobjimport -i<siteminder_installation>\Db
\SMdif\smpolicy.smdif
```

For example,

```
smobjimport -iC:\Program Files\Netegrity\SiteMinder
\Db\SMdif\smpolicy.smdif
```

☞ **Note:** Oracle only: If error messages appear during the import, ensure that **Enable Scrollable Cursor** is set in the driver configuration.

3. If you need to create or change the password, copy `smreg.exe` from the Tools folder on the SiteMinder CD-ROM to *<siteminder_installation>*`\Bin` directory on the Policy Server machine and then execute the following command:

   `smreg -su` ***<superuserpassword>***

   The administrator password that you supply here becomes the password for the SiteMinder Super User account.

4. Delete the `smreg.exe` executable.

   Deleting `smreg.exe` prevents anyone from changing the Super User password.

5. Restart the SiteMinder Policy Server for the configuration changes to take effect.

Note: Oracle only: Once the Oracle policy store is setup, administrator user names for the SiteMinder Policy Server User Interface become case sensitive.

To import exported data:

1. Open a Command Prompt window and navigate to the *<siteminder_installation>*`\bin` directory, where *<siteminder_installation>* is the SiteMinder installed location.

2. Enter **`smobjimport -ipstore.txt -v`**.

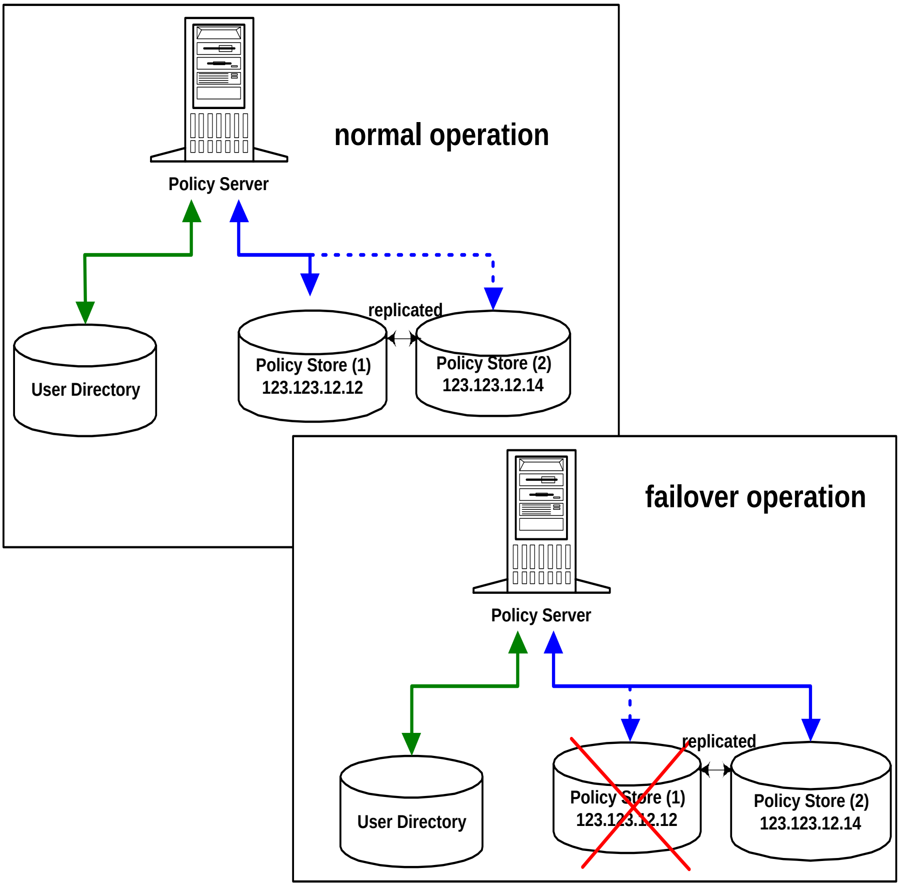
   The contents of the ASCII file named `pstore.txt` are imported into the Oracle or SQL policy store.

Note: For more information about `smobjimport`, refer to *Chapter 11, Policy Server Tools* on page 235.

Replicating Policy Stores and Configuring Failover

To provide consistent and continuous access to the policy store, replicate the policy store on a secondary server and enable failover using the SiteMinder Policy Server Management Console. If failover is enabled and the primary policy store is not available, all policy store operations are automatically redirected to the secondary policy store. The user directory and the policy store can be located in the same LDAP directory.

For example, in the graphic below, policy store 1 is the primary policy store. When this policy store is unavailable, the Policy Server redirects the requests to policy store 2, which is located at a different IP address.



Note: Refer to the *SiteMinder Policy Server Operations Guide* for information on configuring failover.

Chapter 4. Setting up the Policy Store on Solaris

Overview

The SiteMinder policy store is the repository for all policy related information. All Policy Servers in a SiteMinder installation must share the same policy store data, either directly or via replication. Policy Servers installed on Solaris support the following directories and databases for storing policy store data:

- Netscape LDAP directory (default)
- Oracle 7.x and 8.x

When you install the Policy Server on a Solaris system, the default policy store is an LDAP server. To store policy data in an Oracle database, specify the Oracle database when you install the Policy Server.

Storing SiteMinder Data in an Oracle Database

You can use an Oracle database to store SiteMinder policy store data. SiteMinder keys, audit logs, and token data can be stored in the policy store or in a separate database.

☞ **Note:** Storing keys in a separate database may be required to implement single sign-on functionality. Refer to the *SiteMinder Policy Server Operations Guide* for detailed information on key management.

When you store SiteMinder data in an Oracle database, you must configure the policy store or key store from the SiteMinder Policy Server Management Console.

Before You Begin

Before configuring an Oracle database to store SiteMinder data, verify that the following prerequisites have been met:

- The Oracle database that will store the data is installed and running.
- Oracle 7 or Oracle 8 Client software must be accessible from the smuser account. For Oracle 7, you need `sql*net` and the appropriate protocol adapter for your network. For Oracle 8, you need `net8` and the appropriate protocol adapter for your network.
- You can access `sqlplus` from the `smuser` account.
- The `$ORACLE_HOME` variable must exist for `smuser` and must point to a properly installed Oracle product directory.
- An alias must be defined in the `tnsnames.ora` of the client software that points to the appropriate Oracle database.

To store data in an Oracle database:

1. Ensure that the Oracle database instance that will contain the SiteMinder policy data is accessible from the SiteMinder Policy Server machine. Test the communication using `tnsping` or `sqlplus`.
2. Create the SiteMinder schema in the Oracle database:
    a. Log in to Oracle with `sqlplus` (or some other Oracle utility) as the user who administers the SiteMinder Policy Server database information.

    b. Import the scripts for the schemas you want to create:

    $SM_HOME/siteminder/db/<*schema*>

    where <*schema*> is one of the following scripts:

    - **sm_oracle_ps.sql**—Creates the SiteMinder policy store or key store schema (if you are storing keys in a separate database).
    - **sm_oracle_logs.sql**—Creates the schema for storing audit logs.
    - **sm_oracle_token.sql**—Creates the schema for storing token data, such as Encotone TeleID data.

For example,

$SM_HOME/siteminder/db/sm_oracle_ps.sql

Tip: If you are using `sqlplus`, run the schema using an @ sign. For example,

@$SM_HOME/siteminder/db/sm_oracle_ps.sql

Import only the schema files for the schemas that you want to create. For example, if you do not want to support token authentication do not create the schema for token data.

3. Edit the **`$SM_HOME/siteminder/db/system_odbc.ini`** file by replacing the **`stmd`** value for ServerName with the value that is appropriate for your Oracle instance.

   For example,

   `ServerName=`**`MyServer`**

   The modified text should appear as follows:

   ```
   [SiteMinder Data Source]
   Driver=/$SM_HOME/smps-install/siteminder/odbc/lib/NSor713.so
   Description=Oracle7
   ServerName=MyServer
   CallOpinit=0
   AllowUpdateAndDelete=1
   EnableScrollableCursors=1
   ApplicationUsingThreads=1
   ```

4. Configure the SiteMinder Policy Server Console settings:

   a. Run **`smconsole`** to start the SiteMinder Policy Server Management Console.

   b. Under the **Settings** tab, select the **SQL/ODBC Database** option in the **Policy and Key Storage** group box.

   c. Under the **ODBC** tab, select one of the following from the **Select a database** drop-down list:

      - **Policy Store**
      - **Key Store**
      - **Audit Logs**
      - **Token Data**

d. If you selected **Key Store**, **Audit Logs**, or **Token Data**, complete one of the following:

- To store keys, audit logs, or token data in the policy store, ensure the **Use the Policy Store database** check box is selected, then proceed to step i.
- To store keys, audit logs, or token data in a separate database, deselect the **Use the Policy Store database** check box, then proceed to step e.

e. In the **Data Source Name** field, enter the name of the Oracle data source.

f. In the **User Name** and **Password** fields, enter the user name and password for the Oracle instance.

g. In the **Confirm Password** field, re-enter the password.

h. In the **Maximum connections** field, specify the maximum number of database connections allocated to SiteMinder.

i. Optionally, test the connection by clicking **Test ODBC Connection**.

- If it returns a success message, quit the **`smconsole`** and run **`smobjimport -i$SM_HOME/siteminder/bin/smpolicy.smdif -v`**. This adds initial policy data to the schema you created earlier.
- If it returns a failure message, go to `$SM_HOME/db` directory and modify the **`system_odbc.ini`** file based on your requirements.

j. If the settings are correct, click **Apply** to save the settings.

5. Add the Oracle libraries to the `.profile` file of smuser:

a. Open the `.profile` file.

b. Prior to the line that runs the `smprofile.ksh` script, add the Oracle libraries (`$ORACLE_HOME/lib`) to the `LD_LIBRARY_PATH`.

c. Save and exit the file.

d. Run **`smprofile.ksh`** for the new settings to take effect.

e. Ensure that the user profile is correct by logging out and then logging back in.

6. Set the administrator password for the SiteMinder Super User account:

   a. Copy **`smreg`** from the `/solaris/tools` directory of the SiteMinder CD to:

      `$SM_HOME/siteminder/bin`

   b. Run **`smreg -su <`***`administrativepassword`***`>`**

      The administrator password that you supply here becomes the password for the SiteMinder Super User account. The password is case sensitive.

   c. Delete the **`smreg`** executable.

      Deleting **`smreg`** prevents anyone from changing the Super User password.

      The configuration is complete. If you are replicating the Oracle database, refer to *Replicating Policy Stores and Configuring Failover* on page 88.

Storing SiteMinder Data in an LDAP directory

The LDAP directory server can be the same directory server that SiteMinder uses for user authentication and authorization, which simplifies the task of administering SiteMinder.

By default, the policy store is stored in an LDAP directory on Solaris. The table that follows lists the specific items that are required when you install a Policy Server on Solaris and choose to use an LDAP directory:

Value	Description
Secured Sockets Layer (SSL) Certificate Database	If the targeted LDAP directory service communicates with a Policy Server over SSL, the database where Certificates are located.
LDAP Server IP Address	The targeted LDAP server IP address.
LDAP Port Number	The port number the targeted LDAP service is listening on.
Distinguished Name (DN)	The DN of an LDAP user with sufficient privileges, i.e. the ability to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object (for example, `cn=Directory Manager`).
DN's Password	The password of the Administrator DN.
Policy Store Root DN	The DN under which the policy store objects are defined. For example, `o=test.com`

If you are creating a new policy store or key store, refer to *Creating an LDAP Policy Store or Key Store* in the next section.

If you are moving an existing policy store from a non-LDAP database or an migrating an LDAP directory to another LDAP directory, refer to *Migrating and Moving Policy Store Data* on page 83.

Creating an LDAP Policy Store or Key Store

You can use an LDAP directory to store SiteMinder policy store data. SiteMinder keys can be stored in the policy store or in a separate location of the LDAP directory.

☞ **Note:** Storing keys in a separate directory may be required to implement single sign-on functionality. Refer to the *SiteMinder Policy Server Operations Guide* for detailed infomation on key mangement.

To store policies and\or keys in an LDAP directory:

1. Create an LDAP directory server instance.
2. Navigate to `$SM_HOME/bin`.
3. Set up the LDAP directory by entering the following command to configure the policy store:

   smldapsetup reg -h<*host*> -p<*port*> -d<*userdn*> -w<*userpw*> -r<*root*> -ssl<*1/0*> -c<*cert*>

   where **<*host*>** is the name of the LDAP server; **<*port*>** is the port; **<*userdn*>** is the name of an LDAP user with privileges to create a new LDAP schema; **<*userpw*>** is the password for the LDAP user specified by -d; and **<*root*>** is the DN location of the SiteMinder data in the LDAP directory.

   ☞ **Note:** If you are connecting to the LDAP directory over SSL, additionally specify **-ssl1** and **-c<*cert*>,** where **<*cert*>** is the absolute path to SSL client certificate database.

   For example,

   ```
   smldapsetup reg -hldapserver.mycompany.com “-dLDAP
   User” -wMyPassword123 -ro=security.com
   ```
4. Create the schema by completing one of the following:
   - To set up the new policy store:

     smldapsetup ldgen -f<*filename*>

     smldapsetup ldmod -f<*filename*>

     where <*filename*> is the name of the LDIF file you are creating. For example:

     ```
     smldapsetup ldgen -fpstore.txt
     ```

     ```
     smldapsetup ldmod -fpstore.txt
     ```

- To set up the new key store:

  smldapsetup ldgen -k -f<*filename*>

  smldapsetup ldmod -k -f<*filename*>

  where <*filename*> is the name of the LDIF file you are creating. For example:

  smldapsetup ldgen -k -fkstore.txt

  smldapsetup ldmod -k -fkstore.txt

Note: For detailed instructions on using `smldapsetup`, refer to *Chapter 11, Policy Server Tools* on page 235.

5. Import the basic SiteMinder objects required to set up a policy store or key store by entering one of the following commands:

   - If you are importing data to a policy store:

     smobjimport -i<*siteminder_installation*>/db/smdif /smpolicy.smdif -v

     where <*siteminder_installation*> is the installed location of SiteMinder. For example,

     ```
     smobjimport -ismuser/siteminder
     /db/smdif/smpolicy.smdif" -v
     ```

   - If you are importing data to a key store:

     smobjimport -k -i<*siteminder_installation*>/db/smdif /smpolicy.smdif -v

     where <*siteminder_installation*> is the installed location of SiteMinder. For example,

     ```
     smobjimport -k -ismuser/siteminder
     /db/smdif/smpolicy.smdif" -v
     ```

6. Change the SiteMinder Super User password by completing the following steps:

   a. Copy `smreg.exe` from the `/solaris/tools` directory on the SiteMinder 4.1 CD-ROM to <*siteminder_installation*>`/bin`

   b. Execute the following command:

      `smreg -su` <*superuserpassword*>

      where <*superuserpassword*> is the password for the SiteMinder Super User account.

   c. Delete `smreg.exe`.

      Deleting `smreg.exe` prevents anyone from changing the SuperUser password.

Migrating and Moving Policy Store Data

Using the **`smobjexport`** and **`smobjimport`** tools, you can migrate policy store data from other types of databases into LDAP policy stores or move policy stores in one LDAP directory to another LDAP directory. For more information about these tools, refer to the *Chapter 11, Policy Server Tools* on page 235.

The table below identifies the supported LDAP migrations:

From	To
Oracle	LDAP
LDAP	LDAP
LDAP	Oracle

The following procedure applies to the Netscape LDAP directory.

To migrate policy server data to a different LDAP directory:

1. Create an LDAP directory server instance.
2. Export your existing policy store data:

   a. Open a Command Prompt window.

   b. Navigate to `$SM_HOME/bin`.

c. Run the export utility to extract your existing data and specify an output text file to temporarily store the data. For example:

`smobjexport -opstore.smdif -v`

☞ **Note:** For a complete listing of the `smobjexport` parameters, enter **`smobjexport -h`**. For detailed information on using smobjexport, refer to *Chapter 11, Policy Server Tools* on page 235.

3. Configure the Policy Server to use the LDAP Directory as described in *Configuring Policy Servers to Use an LDAP Policy Store or Key Store* on page 85.

4. Restart the LDAP directory server.

5. From the SiteMinder `bin` directory, enter:

   `smldapsetup ldgen -f<`*filename*`>`

   `smldapsetup ldmod -f<`*filename*`>`

   where <*filename*> is the name of the SMDIF file you are generating.

☞ **Note:** SiteMinder Data Interchange Format (SMDIF) is a format that standardizes SiteMinder data so it can be migrated to a different type of policy store.

For example,

```
smldapsetup ldgen -fpstore.smdif
smldapsetup ldmod -fpstore.smdif
```

6. Import the basic SiteMinder objects required to set up a policy store by entering the following command:

   `smobjimport -i<`*siteminder_installation*`>/db/smdif /smpolicy.smdif -v`

   where <*siteminder_installation*> is the installed location of SiteMinder. For example,

```
/smuser/siteminder/db/smdif/smpolicy.smdif
```

7. Change the SiteMinder Super User password by completing the following steps:

   a. Copy `smreg.exe` from the `/solaris/tools` directory on the SiteMinder 4.1 CD-ROM to <*siteminder_installation*>`/bin`

   b. Execute the following command:

      `smreg -su` <*superuserpassword*>

      where <*superuserpassword*> is the password for the SiteMinder Super User account.

   c. Delete `smreg.exe`.

      Deleting `smreg.exe` prevents anyone from changing the SuperUser password.

8. Run the import utility to import your policy store data from the temporary file:

   `smobjimport -i`<*filename*>

   For example,

   `smobjimport -ipstore.smdif`

9. Configure the Policy Server to use the LDAP directory, as described in the next section.

Configuring Policy Servers to Use an LDAP Policy Store or Key Store

Configure a Policy Server to specify a new location of the LDAP server when migrating a policy store in Oracle to a policy store in LDAP. Additionally, you can configure a Policy Server to store SiteMinder keys in the policy store, or specify a new location of the LDAP server for key storage.

To configure a Policy Server to use a policy store or key store in an LDAP directory:

1. Start the Policy Server Management Console by running **`smconsole`**.

☞ **Note:** The policy store settings you specify in the Console must match the settings on the Policy Server from which the LDAP directory was originally configured.

2. Select the **Settings** tab to move it to the front.
3. In the **Policy and Key Storage** group box, select **LDAP Server** and click **Apply**.
4. Select the **LDAP** tab to move it to the front.
5. If you are configuring a policy store, complete the following in the **Policy Store** group box:

    a. In the **LDAP Server** field, enter the IP address and port number of the LDAP directory, separated by a colon (:). For example, enter **`123.123.12.12:321`**. If the port is not specified, SiteMinder uses port 389 as the default.

    b. In the **Root DN** field, enter the LDAP branch under which the SiteMinder policy store is located (for example, **`o=airius.com`**).

    c. In the **Admin Username** field, enter the DN of the LDAP directory administrator for the Policy Server being configured (for example, **`cn=Directory Manager`**).

    d. In the **Admin Password** field, enter the LDAP directory administrator password.

    e. In the **Confirm Password** field, re-enter the LDAP directory administrator password.

    f. If your system is communicating with the LDAP directory over SSL, select the **Use SSL check box.**

    g. If you are using SSL, enter the name of the certificate database in the **Netscape Certificate Database File** field.

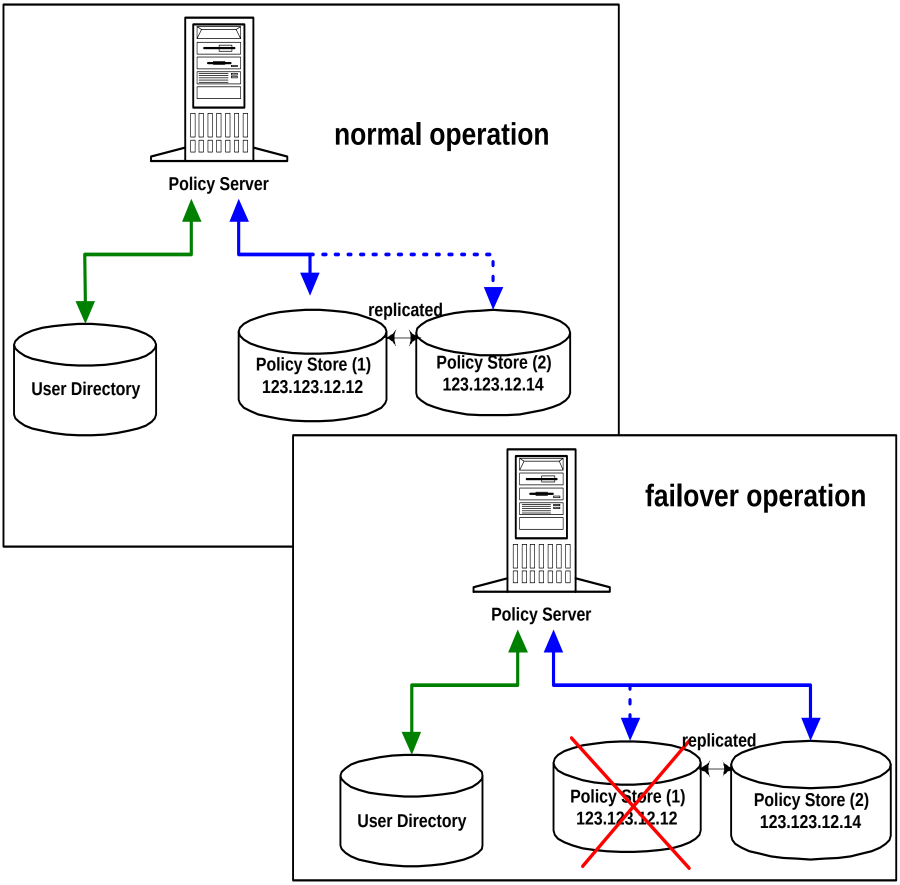
☞ **Note:** You can specify other types of certificates in this field. The certificate does not need to be Netscape.

6. If you are configuring a key store, complete one of the following in the **Key Store** group box:
   - If you want to store keys in the policy store, ensure that the **Use Policy Store** check box is selected, then proceed to step 7.
   - If you want to store keys in a separate location on the LDAP server, complete the following:
     a. In the **LDAP Server** field, enter the IP address and port number of the LDAP directory, separated by a colon (:). For example, enter **`123.123.12.12:321`**. If the port is not specified, SiteMinder uses port 389 as the default.
     b. In the **Root DN** field, enter the LDAP branch under which the SiteMinder policy store is located (for example, **`o=airius.com`**).
     c. In the **Admin Username** field, enter the DN of the LDAP directory administrator for the Policy Server being configured (for example, **`cn=Directory Manager`**).
     d. In the **Admin Password** field, enter the LDAP directory administrator password.
     e. In the **Confirm Password** field, re-enter the LDAP directory administrator password.
     f. If your system is communicating with the LDAP directory over SSL, select the **Use SSL** check box.
     g. If you are using SSL, enter the name of the certificate database in the **Netscape Certificate Database File** field.
7. Click **Apply** to save the settings.
8. Click the **Settings** tab and verify that the **LDAP Server** option is selected in the **Policy and Key Storage** group box.
9. Click **OK** to save the settings and close the Console.
10. Click **Test LDAP Connection** to verify connectivity to the LDAP directory server.

Replicating Policy Stores and Configuring Failover

To provide consistent and continuous access to the policy store, replicate the policy store on a secondary server and enable failover using the SiteMinder Policy Server Management Console. If failover is enabled and the primary policy store is not available, all policy store operations are automatically redirected to the secondary policy store. To simplify administration tasks, the user directory, policy store and key store can be located in the same LDAP directory.

For example, in the graphic below, policy store 1 is the primary policy store. When this policy store is unavailable, the Policy Server redirects the requests to policy store 2, which is located at a different IP address.



Note: Refer to the *SiteMinder Policy Server Operations Guide* for information on configuring failover.

Chapter 5. Setting up a Policy Store on Novell Netware

Overview

In SiteMinder 4.1, you can configure the Policy Server to use an LDAP Novell Directory Server (NDS) directory residing on a NetWare machine as a policy store and user directory.

To use NDS as a policy store or user directory, the NDS schema must be extended to include SiteMinder 4.1 objects. Novell provides a tool, called **`schmap.exe`**, that creates classes, attributes, and the LDAP to NDS mappings from an LDIF file. Once the NDS directory has been prepared, you must import basic policy store objects, stored in `smpolicy.smdif`, before using NDS as the policy store.

Configuring NDS as a Policy Store

Before you begin, ensure you have the following installed:

- NDS Version 8.0 - 8.3
- Novell Client for Windows NT Version 4.7

To configure NDS as a policy store:

1. From the Novell Client, navigate to the `Novell` directory in the directory in which SiteMinder is installed:

   <*siteminder_installation*>`\Novell`

   where <*siteminder_installation*> is the installed location of SiteMinder.

   For example,

   ```
   C:\Program Files\Netegrity\SiteMinder\Novell
   ```

The Novell directory contains the following files:

- `stuffkey.nlm`
- `dsixedit.nlm`
- `schmap.exe`
- `smindex.ncf`
- `smnovell40.ldif`
- `40-index.txt`

2. Copy `schmap.exe` and `smnovell40.ldif` to a temporary location on the NDS server.

   For example,

   ```
   \system\temp
   ```

3. Run `schmap.exe` on the `smnovell40.ldif` file to create SiteMinder attributes:

   ```
   schmap “smnovell40.ldif” “LDAP Group - <group.rootDN>”
   ```

   where **<*group.rootDN*>** is the location in NDS in which the SiteMinder policy store data will reside.

   For example, enter:

   ```
   C:\TEMP\v8>schmap "smnovell40.ldif"
   "LDAP Group - SMLABV8.ou=people.o=test"
   ```

   Note: To modify the NDS Schema you must have rights to the root of your NDS tree. This requires that you log in to NDS as an administrator.

   The **schmap** utility then prompts you to enter your user name and password, for example:

   ```
   Enter User Name: cn=admin.ou=people.o=netegrity
   Enter User Password: ********
   ```

   The utility then displays the following information:

   ```
   Adding Schema Extensions And LDAP To NDS Mappings

   Parsing the schema file...
   Adding schema extensions and mappings...

   SCHMAP End
   ```

4. Refresh the LDAP server to update NDS by completing the following:

   a. From the Novell Client, open the **NetWare Administrator**, then select **Tools | NDS Browser**.

   b. Double click **LDAP server** from the directory tree.

   c. Click the **Refresh NLDAP Server Now** button.

   d. Click the **Catalog Schedule** button.

      The NetWare Administrator displays the **Catalog Schedule** dialog box.

   e. Select **Update Now**.

5. On the server where the SiteMinder Policy Server is installed, open the **Policy Server Management Console** and select the **LDAP** tab to bring it to the front.

6. In the **LDAP** tab, configure the fields for the LDAP policy store.

   The following lists sample values for the fields:

   LDAP IP Address: `123.123.12.12`

   Root DN: `o=test`

   Admin Username: `cn=admin,ou=people,o=test`

   Admin Password: `<masked password>`

   Refer to the *Policy Server Operations Guide* for a complete description of the settings in the **LDAP** tab.

7. Click **Apply** after you have modified the LDAP fields.

8. Click the **Test LDAP Connection** button to test the connection.

   If the connection is successful, SiteMinder returns a confirmation. If it is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered on this tab are correct.

☞ **Note:** Once you have a successful connection, you can modify the NDS policy store from the machine on which the Policy Server is installed.

9. Import `smpolicy.smdif` by completing the following steps:

   a. From the command prompt on the machine the Policy Server is installed, navigate to one of the following locations:

      - On NT, <*siteminder_installation*>`\Bin`

        where <*siteminder_installation*> is the installed location of SiteMinder.

        For example,

        ```
        C:\Program Files\Netegrity\SiteMinder\Bin
        ```

      - On Solaris: <*siteminder_installation*>`/bin`

        where <*siteminder_installation*> is the installed location of SiteMinder.

        For example,

        ```
        $SM_HOME/siteminder/bin
        ```

   b. Execute the following command:

      smobjimport -i<*siteminder_installation*>\db\smdif \smpolicy.smdif

      `Smpolicy.smdif` contains the basic SiteMinder objects required to use NDS as a policy store.

10. Copy the `smreg` executable from the `Tools` directory in the `NT` or `Solaris` directory on the SiteMinder CD-ROM to the SiteMinder `Bin` directory:

    - On NT, **<*siteminder_installation*>\Bin**

      where <*siteminder_installation*> is the installed location of SiteMinder.

      For example,

      ```
      C:\Program Files\Netegrity\SiteMinder\Bin
      ```

- On Solaris, **/<*siteminder_installation*>/bin**

  where <*siteminder_installation*> is the installed location of SiteMinder.

  For example,

  `$SM_HOME/siteminder/bin`

  `Smreg` allows you to create a Super User, called SiteMinder, and specify a corresponding password. The Super User account has the maximum SiteMinder privileges.

11. Go to the SiteMinder `bin` directory where you copied `smreg.exe` and execute the following command:

    smreg -su <*superuser_password*>

    where **<*superuser_password*>** is the password you specify for the SiteMinder Super User account.

    For example:

    ```
    smreg -su password
    ```

    Delete `smreg.exe` when you have finished this step. Deleting `smreg` ensures that non-authorized users cannot change the password. However, if you need to modify the password in the future, you can copy `smreg.exe` from the SiteMinder CD.

12. Refresh the LDAP server as described in step 4 of this procedure.

13. Stop and start all four SiteMinder services:

    - For NT, complete the following:

      a. Start the **SiteMinder Policy Server Management Console**.

      b. Under the **Status** tab, stop each of the services by clicking the **Stop** button in the **Authentication**, **Authorization**, **Accounting**, and **Administration** group boxes.

         The stoplight icon changes from green to red.

c. Click the **Start** button in the **Authentication**, **Authorization**, **Accounting**, and **Administration** group boxes to restart the services.

d. Click **OK** to exit the **SiteMinder Policy Server Management Console**.

- For Solaris, as `smuser`, enter the commands **`stop-all`** followed by **`start -all`**.

Note: You must index the NDS directory immediately after importing `smpolicy.smdif`, executing `smreg,` and restarting the SiteMinder services.

14. Index the NDS policy store using the following procedure:

    a. On the NetWare server, copy the `stuffkey.nlm`, `dsixedit.nlm`, and `smindex.ncf` files from one of the following locations on the SiteMinder CD-ROM to the `\sys\system` directory:

    - For NT, `nt\tools`
    - For Solaris, `solaris/tools`

    b. At the NetWare server console prompt, enter the following command to create the NDS index:

    ```
    smindex.ncf
    ```

    Note: During processing, `smindex.ncf` unloads `NLDAP.nlm` and `DS.nlm` automatically. If a client is connected to NLDAP, `smindex.ncf` cannot unload `NLDAP.nlm` or `DS.nlm`. To unload them manually, enter **`unload NLDAP,`** then **`unload DS`** from the Netware box.

After the index operation is complete, the server reboots.

Migrating Existing Policy Store Data to NDS

You can migrate policy store data from another supported database or directory to NDS. Migrating policy store data allows you to use a different policy store without losing any data.

To migrate data to an NDS policy store:

1. From the command prompt on the machine on which the Policy Server is installed, export your current policy store data by completing the following steps:

   a. From the command line, navigate to the directory in which `smobjexport` is located.

   - For NT, `smobjexport` is located in <*siteminder_installation*>`\Bin.`
   - For UNIX, `smobjexport` is located in <*siteminder_installation*>`/bin.`

   b. Execute `smobjexport`:

   `smobjexport -o`<*filename*>

   where <*filename*> is the name of the output file to which you are exporting data.

   For example,

   ```
   smobjexport -opstore.txt
   ```

2. If you have not already done so, complete all of the steps described in *Configuring NDS as a Policy Store* on page 91.

3. Run the `smobjimport` utility to import the policy store data you exported by entering:

   `smobjimport -i`<*filename*>

   For example,

   ```
   smobjimport -ipstore.txt
   ```

   where <*filename*> is the name of the file to which you exported the policy store data.

☞ **Note:** Refer to *Policy Server Tools* on page 235 for instructions on how to use `smobjexport` and `smobjimport`.

Removing Policy Store Data

Once you have exported your policy store data, you can remove all of the data from the policy store using a SiteMinder utility called `smldapsetup`. Once the data is removed, you can delete the old schema with `schmap.exe.` `Schmap` is a Novell utility that can be used to remove all SiteMinder classes and attributes from NDS.

To remove policy store data from the SiteMinder schema:

1. From the command line, access the directory in which **`smldapsetup`** is located.
   - For NT, **`smldapsetup`** is located in <*installdir*>`\SiteMinder\Bin`.
   - For UNIX, **`smldapsetup`** is located in <*installdir*>`/siteminder/bin`.
2. Execute the following command:

   ```
   smldapsetup remove -a<adminname> -b<adminpw>
   ```

   where <*adminname*> is the name of a SiteMinder administrator with privileges to modify the policy store and <*adminpw*> is the corresponding password.

   Refer to *Chapter 11, Policy Server Tools* on page 235 for instructions on how to use `smldapsetup`.
3. Navigate to the Novell directory under the SiteMinder root.

   For example, <*siteminder_installation*>`\Novell`
4. Copy `schmap.exe` to a temporary location on the NDS server.

   For example,

   ```
   /system/temp/
   ```

5. Execute the following command to remove the SiteMinder attributes from NDS:

   schmap “smnovell40.ldif” “LDAP Group- <*group.rootDN*>” /R

   where **<*group.rootDN*>** is the location in NDS in which the SiteMinder policy store data will reside.

   For example, enter:

   ```
   C:\TEMP\v8>schmap "smnovell40.ldif" "LDAP Group -
   SMLABV8.ou=people.o=test"
   ```

6. Refresh the LDAP server by completing the following:

   a. From the Novell Client, open the **Netware Administrator**, then select **Tools | NDS Browser**.

   b. Double click **LDAP server** from the directory tree.

   c. Click the **Refresh NLDAP Server Now** button.

   d. Click the **Catalog Schedule** button.

      The Netware Administrator displays the **Catalog Schedule** dialog box.

   e. Select **Update Now**.

The SiteMinder schema is removed from NDS.

Chapter 6. Installing the Reports Server

Overview

This chapter describes the steps to install the SiteMinder Reports Server. The SiteMinder Reports Server enables you to connect to a dedicated server running Windows NT that uses an Oracle or SQL Server database for reporting.

When you install the SiteMinder Policy Server on Solaris, no default reporting features are available. You must configure the Policy Server running on Solaris to use the SiteMinder Reports Server on NT to use reporting. The configuration information is defined when you install the Reports Server and when you change the location of the Reports Server.

When you install SiteMinder Policy Server under Windows NT, the installation process creates a default reports server with an ODBC data source pointing to a local Microsoft Access database. If you install the SiteMinder Reports Server, it handles reports in place of the default reports server.

The SiteMinder Reports Server must be installed on a machine running Windows NT 4.0. To use SiteMinder reporting features provided by the Reports Server, you must configure the Policy Server to look to the SiteMinder Reports Server when a user requests a report.

Before You Begin

Verify that the following requirements are met:

- Microsoft Windows NT 4.0 Server or Workstation is installed with Service Pack 3, 4, or 5, and you are logged into an account with local administrator privileges.
- Microsoft IIS 3.x or later, or Netscape Enterprise Server 3.51 or later is installed on your computer.
- If the SiteMinder audit logs are stored using Oracle, an Oracle client is installed.
- If the SiteMinder audit logs are stored using SQL Server, a SQL client is installed.

Installing the Reports Server on NT

1. From the SiteMinder Policy Server CD-ROM, run **`ReportsServer-4.1-NT.exe`** located in the `nt` folder.
2. In the **SiteMinder Reports Server - Welcome** dialog box, click **Continue**.
3. Read the Welcome message and click **Next**.
4. Read the Software License Agreement and click **Yes** if you accept the agreement.
5. In the **Choose Destination Location** dialog box, accept the default location or enter a different location and click **Next**.
6. In the **SiteMinder Policy Server Information** dialog box, complete the following:
    a. Enter the name of the system that the Policy Server was installed on, such as **`mymachine1`**.
    b. Enter the IP address of the Policy Server, such as **`123.123.12.12`**.
    c. Enter the SiteMinder Administration Server port number, such as **`44444`**.
    d. Click **Next**.
7. Select the type of database that contains the logging information from which the reports will be generated.

8. If you selected an Oracle Database, complete the fields in the **Oracle Database Information** dialog box:

   a. Enter the database service name in the **Service** field.

   b. Click **Next** to continue the installation.

8. If you selected SQL Server database, enter the name of the SQL Server that hosts the database and click **Next**.

9. In the **Setup Complete** dialog box, select whether or not to reboot your system now and click **Finish**.

☞ **Note:** You must reboot the machine after you install the Reports Server.

Changing the Location of the Report Redirect URL

To use your dedicated Reports Server from your Solaris or NT Policy Server, you must modify the Report Redirect URL to point to the machine on which the Reports Server is installed. The file to modify is named `smRedirect.txt` and is located in the `...\SiteMinder\reports` folder on the Policy Server machine. The Policy Server you use must be the one that you configured during the Reports Server installation.

To change the location of the report redirect URL:

1. Using a text editor, open the `smRedirect.txt` file.

2. Replace the `<machine name>` string with either the IP address or the machine name of the Reports Server machine.

   For example change:

   `http://<`*machine name*`>/SmReportsCgi/SmReportsCgi.exe` to

   `http://123.12.12.12/SmReportsCgi/SmReportsCgi.exe`

3. Save and exit the `smRedirect.txt` file.

Now you can view SiteMinder reports. To do this, log into the Policy Server User Interface and from the **Tools** menu, select **Reports**.

Reinstalling the Reports Server

Install the SiteMinder Reports Server over an existing Reports Server of the same version to restore lost application files. Reinstalling allows you to retain the database settings defined for the existing Reports Server.

To reinstall the Reports Server:

1. From the SiteMinder Policy Server CD-ROM, run **`ReportsServer-4.1-NT.exe`** located in the `nt` folder.
2. In the **SiteMinder Reports Server NT** dialog box, click **Continue**.
3. Read the Welcome message and click **Next**.
4. Read the Software License Agreement and click **Yes** to accept the agreement.
5. In the **Reports Server Database Settings Options** dialog box, select one of the following:
   - **Preserve existing database settings**—Retains existing Reports Server database settings. The setup reinstalls the new functionality.

     In the **SiteMinder Policy Server Information** dialog box, complete the following to preserve the existing database settings:

     a. Enter the name of the system that the Policy Server was installed on, such as **`mymachine1`**.

     b. Enter the IP address of the Policy Server, such as **`123.123.12.12`**.

     c. Enter the SiteMinder Administration Server port number, such as **`44444`**.

     d. In the **Setup Complete** dialog box, select whether or not to reboot your system now and click **Finish**.

☞ **Note:** You must reboot the system before you use the Reports Server.

- **Install new database settings**—Allows you to enter new Reports Server database settings. The setup will proceed with a reinstall of the new functionality. Complete the following:

  a. In the **SiteMinder Policy Server Information** dialog box, complete the following:

     1. Enter the name of the system that the Policy Server was installed on, such as **`mymachine1`**.
     2. Enter the IP address of the Policy Server, such as **`123.123.12.12`**.
     3. Enter the SiteMinder Administration Server port number, such as **44444**.

  b. Select the type of database that contains the logging information.

  c. If you selected Oracle database, complete the fields in the **Oracle Database Information** dialog box:

     1. Enter the database service name in the **Service** field.
     2. Click **Next** to continue the installation.

  d. If you selected SQL Server database, enter the name of the SQL Server that hosts the database and click **Next**.

  e. In the Setup Complete dialog box, select whether or not to reboot your system now and click **Finish**.

☞ **Note:** You must reboot the system after you install the Reports Server.

Uninstalling the Reports Server

Before you uninstall the Reports Server, stop the Crystal Web Page Server and the Netscape or IIS Web server.

To uninstall the Reports Server:

1. Double-click **Add/Remove Programs** from the Control Panel.
2. Select SiteMinder Reports Server as the program for uninstallation and click **Add/Remove**.
3. Follow the instructions on the screen.

4. Click **OK** to return to the Control Panel.
5. Exit the Control Panel.
6. Reboot the system. The SiteMinder Reports Server is uninstalled.

Uninstalling for IIS 4.0 Environments

If you are using IIS 4.0, open the Microsoft Management Console and do the following:

1. Open the system computer name in the Internet Information Server.
2. Double click Default Web Site and delete the following SiteMinder virtual directories:
   - `SMReports`
   - `SMReportsCGI`
   - `smreportsviewer`
3. Exit the Microsoft Management Console.
4. Reboot the system. The Reports Server uninstallation is complete.

Uninstalling for Netscape Enterprise 3.x Web Servers

If you are using a Netscape Enterprise Web server, you must edit the `obj.conf` and `mime.types` files before completing the uninstall process. Start with the `obj.conf` file.

1. Open the `obj.conf` file from \<*netscape_installation*>\<*server_location*>**`\https-`**<*myserver*>**`\config`**

   where <*netscape_installation*> is the installed location of Netscape, <*server_location*> is the installed location of the Netscape Web servers, and <*myserver*> is the name of the server on which the Reports Server is installed.

   For example,

   ```
   \Netscape\Suitespot\https-myorg\config
   ```

2. Remove the following lines.

   ```
   Init fn=”load-modules” funcs=”send_crystal_image” shlib=C:/
   WINNT/crystal/crimage.dll”
   ```

   ```
   Init fn=”load-modules” funcs=”CrystalReportServer” shlib=C:/
   WINNT/crystal/crweb.dll”
   ```

   ```
   NameTrans fn=pfx2dir from=/smreportsviewer dir=”C:/WINNT/
   crystal”
   ```

   ```
   NameTrans fn=pfx2dir from=/SMReports dir=”C:/WINNT/Program
   Files/Netegrity/SiteMinder/Reports Server ”
   ```

   ```
   NameTrans fn=pfx2dir from=/SMReportsCGI dir=”C:/WINNT/
   Program Files/Netegrity/SiteMinder/Reports Server ”
   name=”cgi”
   ```

   ```
   Service fn=”send_crystal_image” method=” (GET|POST):
   type=”magnus-internal/cri”
   ```

   ```
   Service fn=”CrystalReportServer” method=” (GET|POST):
   type=”magnus-internal/rpt”
   ```

3. Open the `mime.types` file from the following location:
   \<*netscape_installation*>\<*server_location*>**\https-**<*myserver*>**\config**

   For example,

   ```
   \Netscape\Suitespot\https-myorg\config
   ```

4. Remove the following lines.

   ```
   type=magnus-internal/cri exts=cri
   ```

   ```
   type=magnus-internal/rpt exts=rpt
   ```

5. Restart the Web server.

   The Reports Server uninstallation is complete.

Chapter 7. Installing Support for Registration Services

Overview

Registration Services allows administrators to add user information and users to self-register to an LDAP user directory. Registration Services simplifies the process of registering users by using customized forms to collect user profiles. Once information is entered into the form, it is sent to the Registration Services servlet. The servlet sends the information to the LDAP user directory and tells the Web Agent to redirect the user to a designated page, such as a welcome page.

Registration Services are provided for the following environments:

Configuration	Operating System	Web Server
Web Agent for NT/IIS	NT 4.0 Server or Workstation	IIS3.0 or IIS 4.0
Web Agent for NT/Netscape	NT 4.0 Server or Workstation	iPlanet Web Server Enterprise Edition 4.x or higher, or Netscape Enterprise Server 3.51 or higher
Web Agent for Solaris/Netscape	Solaris 2.5.1, 2.6, 2.7	Netscape Enterprise Server 3.51 or higher
Web Agent for Solaris/Apache	Solaris 2.5.1, 2.6, 2.7	Apache 1.3.6, Apache 1.3.9, or Apache 1.3.11

Setting up Support for Registration Services

The process of installing support for Registration Services involves the following steps:

1. Create a new instance of an LDAP directory or identify which existing LDAP directory will be used as a user directory.
2. Configure the LDAP directory in the SiteMinder Policy Server User Interface.

   Refer to *SiteMinder Policy Server Operations Guide* for more information.
3. Install and configure one of the following servlet engines:
   - New Atlanta ServletExec 2.2 (included on the SiteMinder 4.1 CD)
   - Allaire JRun 2.3.3
4. If you installed ServletExec, verify that the servlet engine is correctly installed as described in *Testing ServletExec* on page 133.
5. Install and configure the SiteMinder Web Agent, as described in the *SiteMinder Agent Operations Guide*.

Installing a Servlet Engine

Before using Registration Services, you must install a servlet engine. The servlet engine enables your server to run the Registration Services servlet.

SiteMinder supports the following servlet engines:

- New Atlanta ServletExec 2.2 (included on the SiteMinder 4.1 CD)
- Allaire JRun 2.3.3

If you are installing ServletExec, refer to one of the following sections for information:

- *Installing ServletExec on NT/Netscape* on page 111.
- *Installing ServletExec on NT/IIS* on page 115.
- *Installing ServletExec on Solaris/Netscape* on page 118.
- *Installing ServletExec on Solaris/Apache* on page 124.

For information on installing and configuring JRun, refer to Allaire's documentation.

Installing ServletExec on NT/Netscape

Before installing ServletExec, make sure the following requirements have been met:

- Windows NT Server or Workstation 4.0 is installed on your machine.
- iPlanet Web Server Enterprise Edition 4.0 or later, or Netscape Enterprise Server 3.5.1 or later is installed on your machine.
- There are no other servlet engines installed for use with a Netscape Web server installed on your machine.

☞ **Note:** If you have other servlet engines installed for use with a Netscape Web server, you must uninstall them. Refer to the servlet engine's documentation for uninstallation instructions.

- One of the following Java development kits (JDK) or runtime environments is installed:
  - Sun JDK or JRE version 1.1.x or 1.2. (You can download this software from Sun's Web site, *http://www.java.sun.com/jdk/.)*
  - IBM JDK or JRE version 1.1.x. (You can download this software from IBM's Web site, *http://www.ibm.com/developer/java.*)
  - Microsoft VM build 3186 (This software is included in Internet Explorer 4.0 or higher, which can be downloaded from Microsoft's Web site, *http://www.microsoft.com/java*.)

☞ **Note:** The JDK or JRE must be installed on your local machine. If you attempt to access a JDK or JRE located on another machine through a mapped network drive, the ServletExec will not be able to load and initialize the Java Virtual Machine.

To install ServletExec on NT/Netscape:

1. If you are running Netscape iPlanet Server 4.0, deactiviate the servlet engine:

   a. From the Netscape Administration Server home page, select the server on which you are installing ServletExec.

   b. Click the **Servlets** tab, then click the **Enable Servlets** button.

      The Netscape Enterprise Server displays the **Enable Servlets** page.

   c. Select **No** in response to **Activate the Servlet Engine?**

   d. Click **Ok**.

☞ **Note:** In earlier versions of Netscape Enterprise Server, the servlet engine is disabled by default.

2. Navigate to `\servlet-engine\nt` on the SiteMinder 4.1 CD-ROM.
3. Run **ServletExec_NSAPI_2_2c.exe**.

   The ServletExec installation checks to see which JDK or JRE is installed on your machine.

4. If you only have Microsoft VM installed on your machine, click **Yes** when asked if that is the Java environment that you want to use.
5. In the **Welcome** dialog box, click **Next**.
6. Read the **Software License Agreement**, then click **Next** if you accept.
7. Read the **READ ME** for important installation notes, then click **Next**.
8. In the **Choose Destination Location** dialog box, click **Next**.
9. In the **Select a Server** dialog box, select the server that will use ServletExec, then click **Next**.

   The ServletExec installation only installs ServletExec on one server. The installation must be run separately for each server that uses ServletExec.

10. Specify whether or not you want the installer to update `obj.conf` by clicking the **Yes** or **No** button:

    - If you select **Yes**, the installation creates a backup copy of `obj.conf`, then updates the current settings.

      Note: We recommend allowing the installation to update the `obj.conf` file.

    - If you select **No**, then you must modify the `obj.conf` file manually.

      Refer to *Editing the obj.conf file for Netscape* on page 113.

    If you selected **Yes**, the installation informs you that `obj.conf` has been updated and displays the location of the installation log file. The log file contains error messages and the location of the `obj.conf` backup file.

11. Restart your Web server.

    Note: You must restart to Web server for the ServletExec settings to take effect.

Editing the obj.conf file for Netscape

If you chose not to have the installation modify the `obj.conf` file, or you want to make changes to it, you must modify the `obj.conf` file manually.

To modify obj.conf manually:

1. Navigate to the directory in which `obj.conf` is located:

   <*netscape_installation*>\ <*location*>\<*yourserver*>`\config`

   where <*netscape_installation*> is the installed location of the Netscape, <*location*> is the installed location of the Web servers (`server4` for iPlanet Web Server 4.0 or `suitespot` for Netscape Enterprise Server 3.5x), and <*yourserver*> is the name of your Web server. For example,

   ```
   c:\Program Files\Netscape\server4\
   https-myserver\config
   ```

2. Open `obj.conf` in a text editor.

3. Add the following lines before any Init directives:

```
Init fn=load-modules shlib="<path>\ServletExec_NSAPI.dll"
  funcs= "ServletExecInit,ServletExecFilter,ServletExecService"

Init fn=ServletExecInit
```

where <*path*> is the full path to `ServletExec_NSAPI.dll`.

The Init directives that you are adding must appear before the other Init directives within the `obj.conf` file.

☞ **Note:** In Netscape Server Administation, if you activated the Java Interpreter, then deactivated it, the following lines will appear in your `obj.conf` file:

```
Init funcs="SJavaBootInit" shlib=".." fn="load-
  modules"
Init classpath=".." ldpath=".." fn="SJavaBootInit"
```

Either delete these lines or make sure that the Init directives specified above appear *before* these lines.

4. Add the following lines within the **<Object name=default>** directive:

```
NameTrans fn=ServletExecFilter root="<document root>"

Service method=(GET|HEAD|POST) type=magnus-internal/nac
fn=ServletExecService
```

where <*document root*> is the full path to the server's document root.

The **NameTrans** directive must appear before the other NameTrans directives listed in <**Object name=default**>. Similarly, the **Service method** directive must be located before the other service methods listed in <**Object name=default**>.

Once you have restarted your Web server, verify that ServletExec installed correctly. Refer to *Testing ServletExec* on page 133 for instructions.

Verifying Obj.conf Modifications (NT Only)

If you are running ServletExec on an NT machine, the `VerifyObjConf.bat` utility allows you to confirm that your `obj.conf` has been modified correctly. `VerifyObjConf.bat` checks `obj.conf` for errors, then records any errors or warnings in a log file.

To run VerifyObjConf.bat:

1. Run `VerifyObjConf.bat`.

   `VerifyObjConf.bat` is located in a subdirectory of the directory in which ServletExec is installed:

   <*netscape_installation*>\<*location*>**`\plugins\ServletExec NSAPI\<`**`yourserver`**`>`**

   where <*netscape_installation*> is the installed location of the Netscape, <*location*> is the installed location of the Web servers (`server4` for iPlanet Web Server 4.0 or `suitespot` for Netscape Enterprise Server 3.5x), and <*yourserver*> is the name of your Web server. For example,

   ```
   C:\Program Files\Netscape\server4\plugins\ServletExec
   NSAPI\https-myserver
   ```

   When `VerifyObjConf.bat` is finished, it creates `Verify.log` in the same directory in which it is located.

2. Open `Verify.log.`

What’s the next step

Once you have installed ServletExec and configured it for use with Netscape Web server, complete the following:

1. Test ServletExec to ensure it has been properly installed and configured as described in *Testing ServletExec* on page 133.
2. Install and configure the Web Agent.

   Refer to *Chapter 8, Installing Web Agents* on page 135.

3. Configure Registration Services using the Policy Server User Interface.

   Refer to the *SiteMinder Policy Server Operations Guide* for more information.

Installing ServletExec on NT/IIS

Before installing ServletExec, make sure the following requirements have been met:

- Windows NT Server or Workstation 4.0 is installed on your machine
- IIS 3.0 or IIS 4.0 is installed on your machine

- There are no other servlet engines installed for use with an IIS server installed on your machine.
- One of the following Java development kits or runtime environments is installed
  - Sun JDK or JRE version 1.1.x or 1.2. (You can download this software from Sun’s Web site, *http://www.java.sun.com/jdk/.)*
  - IBM JDK or JRE version 1.1.x. (You can download this software from IBM’s Web site, *http://www.ibm.com/developer/java.*)
  - Microsoft VM build 3186. (This software is included in Internet Explorer 4.0 or higher, which can be downloaded from Microsoft’s Web site, *http://www.microsoft.com/java.*)

☞ **Note:** The JDK or JRE must be installed on your local machine. If you attempt to access a JDK or JRE located on another machine through a mapped network drive, the ServletExec will not be able to load and initialize the Java Virtual Machine.

To install ServletExec on NT/IIS:

1. Navigate to `\servlet-engine\nt` on the SiteMinder CD-ROM.
2. Run **ServletExec_ISAPI_2_2c.exe**.
3. In the **Welcome** dialog box, click **Next**.
4. Read the **Software License Agreement**, then click **Next** if you accept.
5. Read the **READ ME** for important installation notes, then click **Next**.
6. In the **Choose Destination Location** dialog box, click **Next**.

☞ **Note:** All ServletExec files except `ServletExec_ISAPI.dll` are installed in the directory you specify. `ServletExec_ISAPI.dll` is installed in step 7.

7. In the **Choose Destination Location** dialog box, click **Next** to install `ServletExec_ISAPI.dll`.
8. Stop and re-start the **IIS Admin Service**:
   a. Open **Control Panel** in NT.
   b. Double click the **Services** icon to open the **Services** dialog box.

c. Highlight **IIS Admin Services**, then click **Stop** to stop all IIS services, including World Wide Web Publishing.

d. Highlight the **World Wide Web Publishing Service**, then click the **Start** button.

e. Click **Close** to exit the **Services** dialog box.

Once you have restarted your Web server, verify that ServletExec is installed correctly. Refer to *Testing ServletExec* on page 133 for instructions.

What's the next step

Once you have installed ServletExec on an IIS Web server, complete the following:

1. Install and configure the Web Agent.

   Refer to *Chapter 8, Installing Web Agents* on page 135.

2. Configure Registration Services using the Policy Server User Interface.

   Refer to the *SiteMinder Policy Server Operations Guide* for more information.

Installing ServletExec on Solaris/Netscape

Before installing ServletExec, make sure the following requirements have been met:

- One of the following Solaris versions and its required patches are installed on your system:

Version	Required Patches	Recommended Patches
Solaris 2.5.1	kernel update and libthread = 103640-31 C++ shared library = 106529-05	None

Solaris 2.6	kernel update = 105181-17
	C++ shared library = 105591-07
	libc = 105210-25
	libthread = 105568-14
		patchadd = 106125-08

Solaris 2.7	kernel update = 106541-08 C++ shared library = 106327-06 libthread = 106980-07	patchadd = 107171-04

- Netscape iPlanet Web Server Enterprise Edition 4.x or Netscape Enterprise Web Server 3.5x is installed on your system.

  To configure a Netscape Web server on Solaris to support Registration Services, you must install the Netscape Web server as a user other than `nobody`. The user, `nobody`, does not have sufficient permission to write to the Web server's `Config` directory.

  ☞ **Note:** For ServletExec to function properly on a Netscape iPlanet Web Server Enterprise Edition 4.0 or higher, the Java Runtime Environment must have been installed with the Netscape Server Enterprise core.

- There are no other servlet engines installed for use with a Netscape Web server installed on your machine.

  ☞ **Note:** If you have other servlet engines installed for use with a Netscape Web server, you must uninstall them. Refer to the servlet engine's documentation for uninstallation instructions.

- One of the following Java development kits or runtime environments is installed:
  - Sun JDK or JRE version 1.1.x or 1.2. (You can download this software from Sun's Web site, *http://www.java.sun.com/jdk/.)*
  - IBM JDK or JRE version 1.1.x. (You can download this software from IBM's Web site, *http://www.ibm.com/developer/java.*)
  - Microsoft VM build 3186. (This software is included in Internet Explorer 4.0 or higher, which can be downloaded from Microsoft's Web site, *http://www.microsoft.com/java.*)

To install ServletExec on Solaris/Netscape:

1. If you are running iPlanet Web Server Enterprise Edition 4.0, deactiviate the servlet engine:
   a. From the Netscape Administration Server home page, select the server on which you are installing ServletExec.
   b. Click the **Servlets** tab, then click the **Enable Servlets** button.

      The Netscape Enterprise Server displays the **Enable Servlets** page.
   c. Select **No** in response to **Activate the Servlet Engine?**
   d. Click **Ok**.

☞ **Note:** In version 3.5*x* of Netscape Enterprise Server, the Servlet engine is disabled by default.

2. Log in to the Solaris account in which you want to install Registration Services.

   You must log in as the same user as you logged into the Netscape Web Server.
3. Enter the following command to run the ServletExec installation from the SiteMinder 4.1 CD-ROM:

   ```
   sh <cdrompath>/servlet-engine/solaris/
   ServletExec_NSAPI_2_2A.sh
   ```
4. When prompted, enter the directory name of the Netscape Web server installation. For example, `$HOME/netscape/server4.`

   The ServletExec installation detects all of the Netscape Web servers.

5. Enter the name of the server on which you want to install ServletExec.
6. Enter the UNIX username used by the Netscape Server you selected.
7. Specify whether or not you want the installation to complete automatically:
   - If you specify **y**, the installation will configure the server start script and `obj.conf` file for you.

     ☞ **Note:** We recommend allowing the installation to configure the server start script and the `obj.conf`.

   - If you specify **n**, you must manually configure the server start script and `obj.conf` file after the installation, as described in *Editing the obj.conf on Solaris* on page 122.
8. Enter the base name of your Java installation.

   For example, `$HOME/JAVA1.2`
9. Restart your Web server.

What's the next step

Once you installed ServletExec, complete the following steps:

1. Modify the startup script as described in *Configuring the Netscape Startup Script* on page 120.
2. If you decided not to allow the installation to modify the `obj.conf`, you must manually configure the `obj.conf` file as described in *Editing the obj.conf on Solaris* on page 122.

Configuring the Netscape Startup Script

When you install ServletExec, the installation adds information, which you must modify, to the startup script of the Netscape Web server if you choose to allow the installation to complete automatically. If you decide to complete the installation manually, you must add information to the start script yourself.

The start script of the Web Server is located at the root of the Web Server directory. For example:

```
$HOME/netscape40/https-web-server
```

The modifications for ServletExec are located in the block of text immediately following this line:

```
# The following paths are being added for ServletExec.
```

Before using Registration Services, you must perform the three tasks listed below.

1. Verify paths in the script, or if you decided to add information manually, add paths to the script.

   Depending on the JDK version that is installed (1.1 or 1.2), the following path of the JDK libraries must be included.

   Make sure that only one path is added to the following section:

   ```
   # The following line is for the JRE 1.2 production
   release
   ```

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<$HOME/JRE/Java1.2>/
   lib/sparc;export LD_LIBRARY_PATH
   ```

   where <*$HOME/JRE/Java1.2*> is the installed location of the JDK library.

   If you decided to have the installation modify the startup script, remove any additional lines that the installation adds to the script.

   The only path defined in this section should be the path to the JDK libraries used by the ServletExec.

2. Add the path of the SiteMinder Web Agent `Lib` directory:

   Append the path of the SiteMinder Web Agent library directory to the JDK path specified above. Append the path using a colon (:).

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH: <$HOME/JRE/Java1.2>/
   lib/sparc:<$HOME/netegrity/siteminder/webagent>/lib;export
   LD_LIBRARY_PATH
   ```

   where *<$HOME/JRE/Java1.2>* is the installed location of the JDK, and **<***$HOME/netegrity/siteminder/webagent***>** is the installed location of the Web Agent.

   For example:

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH: /space/smuser/JRE/
   Java1.2/lib/sparc:/space/smuser/netegrity/siteminder/
   webagent/lib;export LD_LIBRARY_PATH
   ```

3. Verify that all Java Native Interface (JNI) versions are consistent:

   The JNI version and the JDK/JRE version referenced in the script must be the same. Make sure that the JDK version specified in the library path above match the JNI version specified in the following section:

   # The following line tells ServletExec which version of JNI to use:

   ```
   JNI_VERSION=1.2
   ```

Editing the obj.conf on Solaris

If you chose not to have the installation modify the `obj.conf` file, or you want to make changes to it, you must modify the `obj.conf` file manually.

To modify obj.conf manually:

1. Navigate to the directory in which `obj.conf` is located:

   <*netscape_installation*>/<*location*>/<*yourserver*>/`config`

   where <*netscape_installation*> is the installed location of Netscape, <*location*> is the installed location of the Netscape Web servers (`server4` for iPlanet Web Server 4.0 or `suitespot` for Netscape Enterprise Server 3.5x), and <*yourserver*> is the name of your Web server.

   For example,

   ```
   /space/smuser/netscape/server4/https-myserver/config
   ```

2. Open `obj.conf` in a text editor.
3. Add the following lines before any Init directives:

```
Init fn=“load-modules” shlib=“<path>/ServletExec_NSAPI.so”
  funcs= “ServletExecInit,ServletExecFilter,ServletExecService”

Init fn=ServletExecInit
```

   where <*path*> is the full path to `ServletExec_NSAPI.dll`.

   The Init directives that you are adding must appear before the other Init directives within the `obj.conf` file.

Note: In Netscape Server Administration, if you activated the Java Interpreter, then deactivated it, the following lines will appear in your `obj.conf` file:

```
Init funcs="SJavaBootInit" shlib=".." fn="load-
  modules"
Init classpath=".." ldpath=".." fn="SJavaBootInit"
```

Either delete these lines or make sure that the Init directives specified in step 3 appear *before* these lines.

4. Add the following lines within the **<Object name=default>** directive:

   ```
   NameTrans fn=ServletExecFilter root="<document root>"
   ```

   ```
   Service method=(GET|HEAD|POST) type=magnus-internal/nac
   fn=ServletExecService
   ```

   where <*document root*> is the full path to the server's document root.

   The **NameTrans** directive must appear before the other NameTrans directive listed in <**Object name=default**>. Similarly, the **Service method** directive must be located before the other service methods listed in <**Object name=default**>.

What's the next step

Once you have installed ServletExec and configured it for use with Netscape Web server, complete the following:

1. Test ServletExec to ensure it has been properly installed and configured as described in *Testing ServletExec* on page 133.
2. Install and configure the Web Agent.

   Refer to *Chapter 8, Installing Web Agents* on page 135.

3. Configure Registration Services using the Policy Server User Interface.

   Refer to the *SiteMinder Policy Server Operations Guide* for more information.

Installing ServletExec on Solaris/Apache

Before installing ServletExec, make sure the following requirements have been met:

- One of the following Solaris versions and its required patches are installed on your system :

Version	**Required Patches**	**Recommended Patches**
Solaris 2.5.1	kernel update and libthread = 103640-31 C++ shared library = 106529-05	

Solaris 2.6	kernel update = 105181-17
	C++ shared library = 105591-07
	libc = 105210-25
	libthread = 105568-14
		patchadd = 106125-08

Solaris 2.7	kernel update = 106541-08 C++ shared library = 106327-06 libthread = 106980-07	patchadd = 107171-04

- Apache Server version 1.3.6, 1.3.9 or 1.3.11 is installed on your system. The Apache Server must have Dynamic Shared Object (DSO) support enabled.
- There are no other servlet engines installed for use with an Apache server installed on your machine.

Note: If you must uninstall a servlet engine, make sure you remove any information regarding the servlet engine from `srm.conf` or `httpd.conf`. Refer to the servlet engines documentation for information on uninstalling a servlet engine.

- One of the following Java development kits or runtime environments is installed:
  - Sun JDK or JRE version 1.1.x or 1.2. (You can download this software from Sun’s Web site, *http://www.java.sun.com/jdk/.)*
  - IBM JDK or JRE version 1.1.x. (You can download this software from IBM’s Web site, *http://www.ibm.com/developer/java.*)

- Microsoft VM build 3186. (This software is included in Internet Explorer 4.0 or higher, which can be downloaded from Microsoft's Web site, *http://www.microsoft.com/java*.)

Overview of the Installation Procedure

To install and configure ServletExec 2.2 for an Apache Web server, you must complete the steps outlined below.

1. Install ServletExec.

   Refer to *Installing ServletExec* in the following section for instructions on installing ServletExec.

2. Recompile the Apache Web server and generate makefiles.

   Refer to *Recompiling the Apache Web Server* on page 127, for instructions.

3. Install the Web Agent.

   Refer to *Chapter 8, Installing Web Agents* on page 135 for information.

4. Edit the `httpd.conf` file to include information required to use SiteMinder and ServletExec on an Apache Web server.

   Refer to *Configuring httpd.conf* on page 128 for instructions on configuring `httpd.conf`.

5. Start ServletExec by running `runapache`.

   Refer to *Starting ServletExec Apache with runapache* on page 131 on starting ServletExec.

6. Create the required properties files as described in *Creating Properties Files* on page 132.

You will be asked for the following information during the installation:

- The Apache root document directory.
- The path of the Apache `mime.types` file.
- The path of the Apache apxs utility.
- The path of your Java executable.

To install ServletExec on an Apache Web server:

1. Navigate to `/servlet-engine/solaris` on the SiteMinder CD-ROM.

2. Run **ServletExec_Apache_2_2.sh**.

3. Enter the path where you want to install ServletExec:

   <*apache_installation*>`/ApacheServletExec`

   where <*apache_installation*> is the installed location of the Apache Web server. For example,

   `/space/smuser/apache/ApacheServletExec`

4. Enter the full path, including the filename, of the Apache `mime.types` file:

   <*apache_installation*>`/conf/mime.types`

   where <*apache_installation*> is the installed location of the Apache Web server. For example,

   `/space/smuser/apache/conf/mime.types`

5. Enter the full path name of the Apache apxs utility:

   <apacheserver-installation>`/bin/apxs`

   where <*apache_installation*> is the installed location of the Apache Web server. For example,

   `/space/smuser/apache/bin/apxs`

6. Enter the full path, including the filename, of the Java or JRE executables:

   <java_installation>/`java1.2/bin/java`

   where *<java-installation>* is the directory where the JRE or JDK is installed. For example,

   `/space/smuser/java1.2/bin/java`

   The installation script installs ServletExec, then displays the ServletExec 2.2 License Agreement.

7. If any errors occurred, follow the instructions displayed after the License Agreement.

What’s the next step?

Once you have installed ServletExec, you must recompile the Apache Web Server to include the SiteMinder and ServletExec modules. Recompiling the Apache Web server is described in the next section.

Recompiling the Apache Web Server

Once you have installed ServletExec, you must recompile the Apache Web Server to include the ServletExec module. Recompiling the Apache Web server, generates the `mod_servletexec.so` module.

To recompile the Apache Web server:

1. Add the paths of the GCC (C++ compiler) and Java executable to the environment variable PATH by entering the following command:

   ```
   export PATH=$PATH “:/<usr/local/bin>:/usr/css/bin”
   ```

   where <*usr/local/bin*> is the directory in which the GCC is located.

2. From the directory in which the Apache Web server is installed, set the following flags by entering them at the command line:

   ```
   set LDFLAGS=-lpthread
   export LDFLAGS=-lpthread
   set CFLAGS=-D_REENTRANT
   export CFLAGS=-D_REENTRANT
   ```

3. Recompile the Apache Web server with the **`enable module`** flag by entering the following command:

```
./configure ––prefix=DESTINATION_PATH_TO_APACHE_SERVER
––enable-rule=SHARED_CORE ––enable-module=so

--add-module PATH_TO_SERVLETEXEC_SRC/mod_servletexec.c –
–enable-shared=servletexec
```

☞ **Note:** The entire ./configure command must appear on one line.

4. Generate makefiles by executing **`make`**, then **`make install`**.

What’s the next step?

Once you have re-compiled the Apache Web server, you must install the SiteMinder Web Agent. Refer to *Chapter 8, Installing Web Agents* on page 135 for information on installing the Web Agent.

Configuring httpd.conf

Once you have installed and configured the Web Agent, you must modify the `httpd.conf` configuration file to enable the Web server for use with the Web Agent and ServletExec.

☞ **Note:** You may have already included the required lines in the `httpd.conf` during the Web Agent configuration.

To edit the httpd.conf file:

1. Navigate to the `conf` directory:

   For example:

   ```
   $ cd /usr/apache/conf
   ```

   where `/usr/apache/` is the installed location of the Apache Web server.

2. Open the `httpd.conf` file in a text editor.

3. In the Dynamic Shared Object (DSO) support section, add the following line:

```
LoadModule servletexec_module libexec/mod_servletexec.so
```

4. Confirm the following:

   a. **`SmInitFile`** ***/usr/apache/*****`conf/WebAgent.conf`** is in the Document Root in the main server section.

      `/usr/apache/` represents the location where the Apache Web server is installed. The path for this location cannot be a relative path.

b. The following line is in the DSO configuration section:

```
LoadModule sm_module siteminder/webagent/lib/
mod_sm.so
```

c. If your `httpd.conf` file contains the directive **ClearModuleList**, **AddModule mod_sm.c** appears at the end of the **AddModule** directive section.

☞ **Note:** If you edited the `httpd.conf` during the Web Agent configuration, the lines above should already be in `httpd.conf`. If the lines are not included, add them in the locations specified. Refer to *Chapter 8, Installing Web Agents* on page 135 for more information.

5. Confirm the following:

a. The path to the forms used by the forms authentication scheme is in the Aliases section.

The path should appear as shown below:

```
Alias /siteminderagent/forms/ “space/smuser/netegrity/
siteminder/webagent/samples/forms/”
```

```
<Directory "space/smuser/netegrity/siteminder/
   webagent/samples/forms">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

where <*space/smuser/netegrity/siteminder/webagent*> is the installed location of the SiteMinder Web Agent.

b. The path to the templates used by Registration Services is in the Aliases section.

The path should appear as shown below:

```
Alias /siteminderagent/forms/ “space/smuser/netegrity/
siteminder/webagent/samples/selfreg/”
```

```
<Directory "space/smuser/netegrity/siteminder/
   webagent/samples/selfreg">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

where <*space/smuser/netegrity/siteminder/webagent*> is the location where the SiteMinder Web Agent is installed.

Note: The Alias lines above should appear all on one line.

c. The following line appears in the AddHandler section:

```
AddHandler smformsauth-handler .fcc
```

Note: If you modified the `httpd.conf` file to include forms authentication information, the lines above should already appear in `httpd.conf`. If you did not include the forms authentication information previously in `httpd.conf`, include the lines above in the specified locations. Refer to *Chapter 8, Installing Web Agents* on page 135 for more information.

6. At the end of the file, add the following lines:

```
ServletExecInstances youripaddress:port
<Location /servlet>
SetHandler servlet-exec
</Location>
```

where *youripaddress* is IP address of the Apache Web server and *port* is the port number of the ServletExec engine.

Note: Make sure that you specify a port that is not being used by another application.

Starting ServletExec Apache with runapache

ServletExec Apache provides the `runapache` script to start the ServletExec engine. Before executing `runapache`, edit the script to include the path to the Web Agent directory, the Apache server `conf` directory and the classpaths to the Registration .jar files.

To edit the runapache file:

1. Navigate to <*ServletExec directory*>`/bin` directory.
2. Open the `runapache` script.
3. Include the path to the Web Agent after the APACHEROOT line by adding the following lines:

   `LD_LIBRARY_PATH=$LD_LIBRARY_PATH`

   *<path to Web Agent>/***`webagent/lib`**

   `; export LD_LIBRARY_PATH`
4. Include the path to the Registration .jar files and the Apache server in the CLASSPATH.

   For example:

   ```
   # Updated classpath

   #

   # ${JL}/classes.zip - this path is for JDK and JRE 1.1
   # ${JL}/rt.jar      - this path is for JRE 1.2
   # ${JRL}/rt.jar     - this path is for JDK 1.2
   #

   CLASSPATH=${JL}/classes.zip:${JL}/rt.jar:${JRL}/
   rt.jar:${NAROOT}/lib/ServletExecApache.jar:${NAROOT}/
   lib/servlet.jar:${NAROOT}/classes:${JL}/tools.jar:/
   space/smuser/netegrity/siteminder/webagent/java/
   msr.jar:/space/smuser/netegrity/siteminder/webagent/
   java/jsafe.jar:/space/smuser/netegrity/siteminder/
   webagent/java/env.jar:/space/smuser/
   apachewithservletexec3901/conf:/space/smuser/
   netegrity/siteminder/webagent/lib
   ```
5. Save the `runapache` script.

To execute runapache:

1. Navigate to the following location:

   <*ServletExec directory*>`/Bin`

   where <*ServletExec directory*> is the location where ServletExec is installed.

2. Execute **`runapache -p`**<*port number*>

   where <*port number*> is the port where ServletExec resides.

   If `runapache` completes successfully, the command prompt will not appear.

   If the command prompt appears, an error has occured during processing. `Runapache` will fail if there is a conflict between ports. Make sure that you specify a port for ServletExec that is not being used by another application. Refer to step 6 of *Configuring httpd.conf* on page 128.

3. Test the ServletExec engine to ensure that it started as described in *Testing ServletExec* on page 133.

Note: If you want to stop ServletExec, press CTRL + C.

Creating Properties Files

Before using Registration Services, you must create the `webagent.properties` and `ems.properties` files. These files are required for Registration Services to communicate with the SiteMinder Web Agent.

To create the webagent.properties and ems.properties files:

1. Navigate to the directory where the Web Agent is installed.
2. Execute **`apache-msr-config`**
3. Specify the full path to the Apache server file when prompted.

   For example,

   `/usr/apache`

   The script creates the `webagent.properties` and the `ems.properties` files.

What’s the next step

Once you have installed ServletExec and configured it for use with Netscape Web server, complete the following:

- Test ServletExec to ensure that it has been properly installed and configured as described in *Testing ServletExec* on page 133.
- Configure Registration Services in the Policy Server User Interface.

Refer to the *SiteMinder Policy Server Operations Guide* for more information.

Testing ServletExec

Once you have installed ServletExec, made any necessary manual modifications, and restarted your Web server, you can test to see if ServletExec is working properly.

To test ServletExec, open the following URLs in your Web browser:

- **`http://<yourserver.com:port>/servlet/DateServlet`**
- **`http://<yourserver.com:port>/servlet/TestServlet`**

where ***`<yourserver.com:port>`*** is the name of your Web server including the port.

Using JRun for Registration Services

Before using JRun to support Registration Services, install and configure JRun 2.3.3 for the Web server on which the SiteMinder Web Agent will run.

Refer to Allaire’s documentation for information on installing JRun and configuring it for the appropriate Web server.

If you want to use JRun to support Registration Services on an Apache Web Server, you must complete the additional steps described in *Configuring JRun for Solaris Apache*, in the following section.

Configuring JRun for Solaris/Apache

Before configuring JRun to support Registration Services on an Apache Web server, you must have the Web Agent installed and configured. Once the Web Agent is installed and configured, create `webagent.properties`, `and ems.properties,` and modify `jsm.properties` files. These files are required for Registration Services to communicate with the SiteMinder Web Agent.

To create the webagent.properties and ems.properties files:

1. Navigate to the directory where the Web Agent is installed.
2. Execute **`apache-msr-config`**
3. Specify the full path to the Apache server file when prompted.

   For example,

   `/usr/apache`

   The script creates the `webagent.properties` and the `ems.properties` files.

To modify the jsm.properties file:

1. Navigate to the directory where `smwa-install` was untarred.
2. Execute **`apache-jrun-config`**
3. Specify the full path to the location where JRun is installed when prompted:

   For example,

   `/space/smuser/jrun/`

4. Specify the installation path of the SiteMinder Web Agent when prompted:

   For example,

   `/smuser/netegrity/`

5. Specify the full path to the Apache server file when prompted:

   For example,

   `/usr/apache`

   The script creates a new `jsm.properties` and creates a backup of the original `jsm.properties` file called `jsm.properties.presm`.

Chapter 8. Installing Web Agents

Overview

In SiteMinder 4.1, cookie providers, SSL credential collectors, and forms credential collectors function as extensions of the Web Agents. By functioning as Web Agent components, they can receive dynamic Agent Key information from the Policy Server. Agent keys allow SiteMinder Web Agents, cookie providers, SSL credential collectors and forms credential collectors to encrypt and decrypt cookies containing SiteMinder information. All SiteMinder components must have the same Agent Key to share information stored in SiteMinder cookies. (Refer to the *SiteMinder Policy Server Operations Guide* for detailed information about Agent Keys.)

A SiteMinder 4.1 Web Agent can be configured to protect a resource in addition to functioning as a cookie provider, SSL credential collector, and forms credential collector, or perform a subset of these functions. A Web Agent can also be configured to perform just one of these functions.

This chapter describes the steps involved in installing, configuring, and uninstalling the following SiteMinder Web Agents:

- Web Agent NT/IIS
- Web Agent NT/Netscape
- Web Agent UNIX/Netscape
- Web Agent UNIX/Apache

Before you begin, make sure you have one of the following supported configurations installed.

Configuration	**Operating System**	**Web Server**
Web Agent for NT/IIS	NT 4.0 Server with Service Pack 3, 4, or 5	IIS 3.0 or IIS 4.0
Web Agent for NT/Netscape	NT 4.0 Server or Workstation with Service Pack 3, 4, or 5	iPlanet Web Server, Enterprise Edition 4.0 or later, or Netscape Enterprise Server 3.51 or higher
Web Agent for HP-UX/Netscape	HP-UX 10.20	iPlanet Web Server, Enterprise Edition 4.0 or later, or Netscape Enterprise Server 3.51 or higher
Web Agent for Solaris/Netscape	Solaris 2.5.1, 2.6, or 2.7	iPlanet Web Server, Enterprise Edition 4.0 or later, or Netscape Enterprise Server 3.51 or higher
Web Agent for Solaris/Apache	Solaris 2.5.1, 2.6, or 2.7	Apache 1.3.6, 1.3.9, or 1.3.11

Installing the Web Agent on NT

This section describes how to install the SiteMinder Web Agent on the Windows NT platform. After you have installed the Web Agent, you must configure it for use with Microsoft IIS and/or Netscape Web Servers.

Before You Begin

Check that the following prerequisites have been met:

- NT Server or Workstation 4.0 with Service Pack 3, 4, or 5 is installed on the system
- IIS 3.0 or 4.0, Netscape Enterprise Server 3.51 or higher, or iPlanet Web Server Enterprise Edition 4.0 or higher is installed on the system
- You are logged into an account with Local Administrator privileges

- If you want to provide Registration Services on the Web Agent you are installing, ensure one of the following servlet engines is installed on your local machine:
  - New Atlanta ServletExec 2.2, which is included on the SiteMinder 4.1 CD-ROM
  - Allaire JRUN 2.3.3

☞ **Note:** Refer to *Chapter 7, Installing Support for Registration Services* on page 109 for instructions on installing ServletExec. Refer to Allaire's documentation for information on installing and configuring JRun.

To install the Web Agent on NT:

1. Exit all applications that are running, then insert the SiteMinder CD-ROM.
2. Run the setup program:
   a. Navigate to the `nt` folder.
   b. Double-click `Web-Agent-4.1-nt.exe`.

   SiteMinder prepares the Web Agent Installation Wizard.
3. In the **Welcome** dialog box, click **Next**.
4. Read the Software License Agreement and click **Yes** if you accept the agreement.
5. Read the Release Notes, then click **Next**.
6. In the **Choose Destination Location** dialog box, accept the default installation location or select a different location and click **Next**.
7. In the **Select Program Folder** dialog box, select the Program Folder where SiteMinder will place program icons, then click **Next**.
8. In the **Start Copying Files** dialog box, click **Next**.

   The Web Agent Setup copies files to the specified location.

9. In the **Setup Complete** dialog box, confirm that you want to configure the Web Agent when the installation is complete by ensuring the **Launch the Web Agent Configuration Wizard now** check box is selected.

Note: You may be required to reboot your machine once the installation is complete. If you are required to reboot, you will have to start the **Web Agent Configuration Wizard** manually. Refer to *Configuring the Web Agent for IIS* on page 138 or *Configuring the Web Agent for Netscape* on page 142 for instructions.

10. Click **Finish**.

SiteMinder prepares the **Web Agent Configuration Wizard**. Refer to one of the following sections for information on configuring the Web Agent:

- For IIS, refer to *Configuring the Web Agent for IIS* on page 138.
- For Netscape, refer to *Configuring the Web Agent for Netscape* on page 142.

Configuring the Web Agent for IIS

Once you have a Web Agent installed, you must configure the Web Agent.

SiteMinder Web Agents installed on IIS Web servers are automatically configured as forms credential collectors and SSL credential collectors. Additionally, IIS Web Agents can be configured as cookie providers.

Note: Refer to *SiteMinder Agent Operations Guide* for information on how to configure a Web Agent as a cookie provider.

To configure the Web Agent on IIS:

1. If necessary, open the **Web Agent Configuration Wizard** by completing the following steps:

   a. Navigate to <*webagent_installation*>`\Config`

   where <*webagent_installation*> is the installed location of the SiteMinder Web Agent.

   b. Double click **Setup.exe**.

If you indicated that you wanted to configure the Web Agent after the installation, SiteMinder automatically opens the **Web Agent Configuration Wizard** for you.

2. In the **Select Web server(s)** dialog box, select the Web server(s) that you want to configure as Web Agents, then click **Next**.

   If you select multiple Web servers, the configuration wizard will configure the first Web server, then display the current settings for the next selected Web server. If you want to modify these settings, click **Configure** and repeat steps 4-10 of this procedure.

3. In the **Web Agent Configuration for <*yourserver*>** dialog box, SiteMinder displays the configuration information for the Web server you selected.

   - To configure a new Web Agent, click **Configure**.
   - To change the configuration settings, click **Configure**.
   - To accept the configuration settings, click **Next**.

     Skip to step 10 of this procedure.

!

Warning: Clicking **Configure** resets all of the configuration settings including the settings you configured in the IIS Web Agent Management Console to default settings. You must enable the Web Agent, as described in the *SiteMinder Agent Operations Guide*, before it protects your resources again.

4. In the **Primary Policy Server on <*yourserver*>** dialog box, complete the following:

   a. Enter the IP address of the Policy Server that you want the Web Agent to connect and communicate with first. The default IP address is the address of the local machine.

   b. Click **Next**.

5. In the **Default Agent Name on <*yourserver*>** dialog box, complete the following:

    a. Enter the Agent Name (case-sensitive). Typically, the Agent is assigned the same name as the Web server on which it is installed.

    > **Tip:** Take note of the Agent name. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface. The Agent name is case-sensitive.

    b. Click **Next**.

6. In the **Default Cookie Domain on <*yourserver*>** dialog box, complete the following:

    a. Enter the domain of the Web server, using two periods. For example: `.myorg.org`. For additional information about cookie domains, refer to the *SiteMinder Agent Operations Guide*.

    b. Click **Next**.

7. In the **IIS Proxy Username and Proxy Password on <*yourserver*>** dialog box, complete the following:

    a. Specify the Proxy Username and Password.

    The proxy account must have read or execute privileges to access the files protected by the Web Agent. The account's password must be at least 6 characters long.

    b. Confirm the NT password by entering it again in the **Confirm NT Password** field.

    c. Click **Next**.

8. In the **Shared Secret on <*yourserver*>** dialog box, complete the following:

    a. Enter an alphanumeric Secret that will be shared with the Policy Servers that communicate with the Agent. The Secret must consist of 6 to 24 alphanumeric characters and cannot contain spaces.

    > **Tip:** Take note of the Shared Secret you entered. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface.

   b. Confirm the Shared Secret by entering it again in the **Confirm Shared Secret** field.

   c. Click **Next**.

9. Complete one of the following:

   - If you have a servlet engine installed on the selected Web server, specify one of the following options for Registration in the **Select Servlet Engine for Registration on <yourserver>** dialog box, then click **Next**:

     - If you want to use New Atlanta ServletExec for running Registration Services, select **New Atlanta Servlet Exec 2.2**.
     - If you want to use Allaire JRUN 2.3.3 for running Registration Services, select **Allaire JRUN 2.3.3**.
     - If you do not want to configure this Web Agent for Registration Services, select **This Web Agent will not be providing registration**.

   Note: A servlet engine is required to run Registration Services from the Web Agent you are configuring.

   - If you do not have a servlet engine installed, proceed to step 10.

     Note: If the Web Agent Configuration Wizard does not detect a servlet engine, the **Select Servlet Engine for Registration on <yourserver>** dialog box is not displayed.

10. Confirm that the configuration settings are correct by clicking **Next**.

   Note: If you are not satisfied with the Web Agent configuration, click **Configure,** then repeat steps 4-10.

SiteMinder examines the configuration settings, then displays the **Confirm Configuration Selections** dialog box.

If you are also configuring Netscape Web Agents, SiteMinder displays the default settings for the next selected Web server. Refer to *Configuring the Web Agent for Netscape* on page 142 for instructions on how to configure the Web Agent for Netscape.

11. Confirm that SiteMinder is configuring the correct Web server as a Web Agent, then click **Next**.
12. Click **Finish** to complete the configuration.

☞ **Note:** You may be required to reboot your machine once the installation is complete. If you are required to reboot, you will have to start the **Web Agent Configuration Wizard** manually. Refer to *Configuring the Web Agent for IIS* on page 138 or *Configuring the Web Agent for Netscape* on page 142 for instructions.

What's the next step?

Now that you've finished configuring the Web Agent for IIS, complete the following:

1. Configure the Web Agent(s) in the SiteMinder Policy Server User Interface, as described in the *SiteMinder Policy Server Operations Guide*.

2. Enable the Web Agent(s), as described in the *SiteMinder Agent Operations Guide*.

Configuring the Web Agent for Netscape

Once you have a Web Agent installed, you must configure the Web Agent for Netscape.

SiteMinder Web Agents installed on Netscape Web servers are automatically configured as forms credential collectors. Additionally, you can configure the Web Agents to function as SSL credential collectors and cookie providers.

To configure the Web Agent to act as an SSL credential collector, specify an SSL configuration option when prompted during the configuration.

To configure the Web Agent as a cookie provider, refer to *SiteMinder Agent Operations Guide*.

To configure the Web Agent on Netscape:

1. If necessary, open the **Web Agent Configuration Wizard** by completing the following steps:

   a. Navigate to <*webagent_installation*>`\Config`

      where <*webagent_installation*> is the installed location of the SiteMinder Web Agent.

   b. Double click **Setup.exe**.

   If you indicated that you wanted to configure the Web Agent after the installation, SiteMinder automatically opens the **Web Agent Configuration Wizard** for you.

2. In the **Select Web server(s)** dialog box, select the Web server(s) that you want to configure as Web Agents, then click **Next**.

   If you select multiple Web servers, the configuration wizard will configure the first Web server, then display the current settings for the next selected Web server. If you want to modify these settings, click Configure and repeat steps 3-10 of this procedure.

3. In the **Web Agent Configuration for <*yourserver*>** dialog box, SiteMinder displays the current configuration for the Web server you selected.

   - To configure a new Web Agent, click **Configure**.
   - To change the configuration settings, click **Configure**.
   - To accept the configuration settings, click **Next**.

     Skip to step 10 of the this procedure.

! **Warning:** Clicking **Configure** resets all of the configuration settings including the settings you configured in the `WebAgent.conf` file to default settings. You must enable the Web Agent, as described in the *SiteMinder Agent Operations Guide*, before it protects your resources again.

4. In the **Primary Policy Server on <https-yourserver>** dialog box, complete the following:

   a. Enter the IP address of the Policy Server that you want the Web Agent to connect and communicate with first. The default IP address is the address of the local machine.

   b. Click **Next**.

5. In the **Default Agent Name on <https-yourserver>** dialog box, complete the following:

   a. Enter the Agent Name (case-sensitive). Typically, the Agent is assigned the same name as the Web server on which it is installed.

   Tip: Take note of the Web Agent name. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface. The Agent name is case-sensitive.

   b. Click **Next**.

6. In the **Default Cookie Domain on <https-yourserver>** dialog box, complete the following:

   a. Enter the domain of the Web server, using two periods. For example: `.myorg.org`. For additional information about cookie domains, refer to the *SiteMinder Agent Operations Guide*.

   b. Click **Next**.

7. In the **Shared Secret on <https-yourserver>** dialog box, complete the following:

   a. Enter an alphanumeric Secret that will be shared with the Policy Servers that communicate with the Agent. The Secret must be between 6 and 24 alphanumeric characters long.

   Tip: Take note of the Shared Secret you entered. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface.

   b. Confirm the Shared Secret by entering it again in the **Confirm Shared Secret** field.

   c. Click **Next**.

8. In the **Select SSL Configuration on <https-yourserver>** dialog box, select one of the following options for advanced authentication, then click **Next**.

   - HTTP Basic over SSL
   - X509 Client Certificate
   - X509 Client Cert + HTTP BASIC over SSL
   - X509 Client Cert or HTTP Basic
   - This web agent will not be providing advanced authentication.

   For additional information about advanced authentication options, refer to the *SiteMinder Policy Server Operations Guide*.

9. Complete one of the following:

   - If you have a servlet engine installed on the selected Web server, specify one of the following options for Registration in the **Select Servlet Engine for Registration on <yourserver>** dialog box, then click **Next**:
     - If you want to use New Atlanta ServletExec for running Registration Services, select **New Atlanta Servlet Exec 2.2**.
     - If you want to use Allaire JRUN 2.3.3 for running Registration Services, select **Allaire JRUN 2.3.3**.
     - If you do not want to configure this Web Agent for Registration Services, select **This Web Agent will not be providing registration**.

   Note: The servlet engine is required to run Registration Services from the Web Agent you are configuring.

   - If you do not have a servlet engine installed, proceed to step 10.

     Note: If the Web Agent Configuration Wizard does not detect a servlet engine, the **Select Servlet Engine for Registration on <yourserver>** dialog box is not displayed.

10. Confirm that the configuration settings are correct by clicking **Next**.

Note: If you are not satisfied with the Web Agent configuration, click **Configure,** then repeat steps 4-10.

SiteMinder examines the configuration settings, then displays the **Confirm Configuration Selections** dialog box.

If you are configuring multiple Web Agents, SiteMinder displays the default settings for the next selected Web server. To modify the settings, click **Configure**, then repeat steps 3-10 of the configuration procedure.

11. Confirm that SiteMinder is configuring the correct Web server as a Web Agent, then click **Next**.
12. Click **Finish** to complete the installation.

What's the next step?

Now that you've finished configuring the Web Agent for Netscape, complete the following:

1. Configure the Web Agent(s) in the SiteMinder Policy Server User Interface, as described in the *SiteMinder Policy Server Operations Guide*.
2. Enable the Web Agent(s), as described in the *SiteMinder Agent Operations Guide*.

Reinstalling a Web Agent on NT

Reinstall a Web Agent to restore missing application files. To change Web Agent settings or to configure a Web Agent for a different Netscape Web Server, configure the Web Agent using the **Web Agent Configuration Wizard**.

To reinstall a Web Agent on NT:

1. Exit all applications that are running, then insert the SiteMinder CD-ROM.
2. Run the setup program:
    a. Navigate to the `nt` folder on the SiteMinder CD-ROM.
    b. Double-click `Web-Agent-4.1-NT.exe`.

SiteMinder detects the previous installation of the Web Agent on your system.

3. In the **Welcome** dialog box, click **Next**.
4. Read the Software License Agreement and click **Yes** if you accept the agreement.
5. Read the Release Notes, then click **Next**.
6. In the **Confirm Reinstallation** dialog box, select **Continue with reinstallation**.
7. In the **Start Copying Files** dialog box, click **Next**.

   The Web Agent Setup copies files to the specified location.
8. In the **Setup Complete** dialog box, click **Finish**.

   You should not run the **Web Agent Configuration Wizard** after reinstalling a Web Agent if you want the preserve your Web Agent configuration.

   If you want to reconfigure a Web Agent, access the **Web Agent Configuration Wizard**, as described in the following sections:

   - For IIS, refer to *Configuring the Web Agent for IIS* on page 138.
   - For Netscape, refer to *Configuring the Web Agent for Netscape* on page 142.

Note: You may be required to reboot your machine once the installation is complete.

Uninstalling a Web Agent from NT

1. Open the Control Panel.
2. Double click **Services**, and complete one of the following:

   - For Netscape, stop the Enterprise service, then close the **Services** dialog box. Make sure you are stopping the server on which the Web Agent is installed.
   - For IIS 3.0, stop the **World Wide Web Publishing Service**, then close the **Services** dialog box.

- For IIS 4.0, stop the **World Wide Web Publishing Service** and the **Content Index Service** (if it exists), then close the **Services** dialog box.

3. Double click **Add/Remove Programs** from the Control Panel.
4. Select **SiteMinder Web Agent v4.1** as the program for uninstallation, then follow the instructions on the screen.
5. Click **OK** when the uninstallation is complete and close the **Add/Remove Programs** dialog box. The uninstall is now complete.

Installing a Web Agent on UNIX

This section describes how to install the SiteMinder Web Agent on HP-UX or Solaris.

Once you install the Web Agent on UNIX, you can configure multiple Web Agents for each Netscape and/or Apache Web server installed on your system.

Before You Begin

Verify that the system meets one of the following requirements:

- HP-UX 10.20 is installed on the system, along with Netscape Enterprise Server 3.51 or higher.
- Solaris 2.5, 2.6, or 2.7 and the following patches are installed on the system:

Version	Required Patches	Recommended Patches
Solaris 2.5.1	kernel update and libthread = 103640-31 C++ shared library = 106529-05	None

Solaris 2.6	kernel update = 105181-17
	C++ shared library = 105591-07
	libc = 105210-25
	libthread = 105568-14
		patchadd = 106125-08

Solaris 2.7	kernel update = 106541-08 C++ shared library = 106327-06 libthread = 106980-07	patchadd = 107171-04

- If you are installing on a Netscape Web Server, Netscape Enterprise Server 3.51 or higher or iPlanet Web Server Enterprise Edition 4. or higher is installed on the system.
- If you are installing on an Apache Web server, Apache Web Server 1.3.6, 1.3.9, or 1.3.11 is installed with `mod_so` enabled (in the `httpd.conf` file).
- You are logged into the account in which the Web Server is installed.

☞ **Note:** If you are configuring Web Agents for Netscape and Apache Web servers on the same system, the Netscape and Apache Web server must exist in the same account.

- If you want to provide Registration Services on the Web Agent you are installing, ensure one of the following servlet engines is installed on your local machine:
  - New Atlanta ServletExec 2.2, included on the SiteMinder 4.1 CD
  - Allaire JRUN 2.3.3

☞ **Note:** Refer to *Chapter 7, Installing Support for Registration Services* on page 109 for instructions on installing ServletExec. For information on installing JRun, refer to Allaire’s documentation.

For all install questions in this section, the default entry is displayed on the screen in brackets ([ ]).

To install the Web Agent on UNIX:

1. Navigate to the `hp` or `solaris` directory on the SiteMinder CD.
2. Untar the agent installation file by typing:
   - For HP-UX, **`tar -xvf smwa-4.1-hp.tar`**
   - For Solaris, **`tar -xvf smwa-4.1-so.tar`**

   Untarring these files creates a `smwa-install` directory which contains `./smwa-install`.
3. Run **`./smwa-install`** from the Web Agent files directory.

   The installation script prepares the Release Notes.

4. Press ENTER to read the Release Notes for important information about installing SiteMinder 4.1.
5. Enter **y** to confirm that you want to continue with the installation.
6. Confirm that you have read the Software License Agreement, then enter **Y** to continue.
7. Specify a directory for installation.

   The default SiteMinder installation directory is `$HOME/netegrity/siteminder`.

   The Web Agent installation creates a subdirectory called `webagent` in the specified directory.

☞ **Note:** If you specified a directory called `webagent`, the installation does not create a new subdirectory. It installs the Web Agent in the `webagent` directory you specified.

8. If you have a Netscape Web server on your system and want to configure a Web Agent for Netscape, enter **y** when asked if the system has a Netscape Web server.

☞ **Note:** If you are installing a Web Agent for Apache or you do not want to configure a Web Agent for Netscape at this point, enter **n**, then specify the Web server during configuration.

9. Complete one of the following:
   - If you specified **y** in step 8, enter the server root for Netscape:

     <netscape_installation>/*<server_directory>*

     where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape servers.

     For example:

     `/usr/netscape/server4`.
   - If you specified **n** in step 8, proceed to step 10.

The installation program displays the installation path you entered. If you specified a Netscape server root, the installation program displays that, as well.

10. Enter **y** to confirm that the installation path and server root are correct.

    The installation is complete. You must configure the Web Agent before enabling it. Refer to *Configuring Web Agents on Netscape* on page 151 or *Configuring Web Agents for Apache* on page 155 for instructions.

What's the next step?

Now that you've installed the Web Agent for UNIX, complete the following:

1. Configure the Web Agent as described in one of the following sections:
   - For Netscape, refer to *Configuring Web Agents on Netscape* on page 151.
   - For Apache, refer to *Configuring Web Agents for Apache* on page 155.
2. Configure the Web Agent(s) in the SiteMinder Policy Server User Interface, as described in the *SiteMinder Policy Server Operations Guide*.
3. Enable the Web Agent(s), as described in the *SiteMinder Agent Operations Guide*.

Configuring Web Agents on Netscape

Once you have installed a Web Agent on UNIX, you must configure it using the configuration script installed in the same directory as the Web Agent.

SiteMinder Web Agents installed on Netscape Web servers are automatically configured as forms credential collectors. Additionally, you can configure the Web Agents to function as SSL credential collectors and cookie providers.

To configure a Web Agent to act as an SSL credential collector, specify an SSL authentication scheme when prompted during the configuration.

To configure the Web Agent as a cookie provider, refer to *SiteMinder Agent Operations Guide*.

To configure a Web Agent on Netscape:

1. Navigate to the directory where the Web Agent is installed to run the configuration.

   Note: You can also run the configuration from the same directory you ran the installation.

2. Enter ./**`smwebagent-config`** to run the configuration script.
3. At the prompt to configure a Netscape Web server, enter **`Y.`**
4. If you did not specify the Netscape server root during installation, enter the server root when prompted:

   <netscape_installation>/*<server_directory>*

   where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape servers.

   For example:

   `/usr/netscape/server4`

   The configuration script detects and lists the installed Netscape Web servers.

5. Select the appropriate Web server from the menu by entering the number listed next to the detected Web server.
6. Enter the SiteMinder Policy Server IP address. The default IP address is the IP address of the local machine.

   This server is the SiteMinder Policy Server that you want the Web server to connect and communicate with first (for example: **`123.123.12.12`**).

7. Enter the Web Agent Name (case-sensitive). Typically, the Agent is assigned the same name as the Web server on which it is installed.

   Tip: Take note of the Agent name. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface. The Agent name is case-sensitive.

8. Enter the cookie domain in which the Web Agent will be located.

   The domain must contain two periods, such as **`.myorg.org`**. For additional information about cookie domains, refer to the *SiteMinder Agent Operations Guide*.

9. Enter the Shared Secret that will be shared between the Web Agent and all Policy Servers that communicate with the Web Agent.

   The secret must be between 6 and 24 characters long.

   Note: If you try to cancel the installation while entering the Shared Secret (for example, if you press `Control + C`), at the next prompt enter **`stty echo`**, then press `ENTER` to restore the echo function. To provide optimal security, the echo function is off for this part of the install.

10. Confirm the Shared Secret by entering it again at the next prompt.

    Tip: Take note of the Shared Secret. You will need this secret when configuring the Agent in the SiteMinder Policy Server User Interface.

11. Specify the authentication scheme you want to use by entering the number next to it in the displayed list.

    The authentication scheme determines how SiteMinder authenticates users. Refer to *SiteMinder Policy Server Operations Guide* for more information about authentication schemes.

    The configuration script displays the values you entered.

12. If the configuration values are correct, enter **Y**.
13. Restart the Web server.

What's the next step?

Now that you've configured the Web Agent for Netscape, complete the following:

1. Configure the Web Agent(s) in the SiteMinder Policy Server User Interface, as described in the *SiteMinder Policy Server Operations Guide*.
2. Enable the Web Agent(s), as described in the *SiteMinder Web Agent Operations Guide*.

Reconfiguring Web Agents on Netscape

Reconfigure a Web Agent for the following reasons:

- You have upgraded the Web Agent and now you need to update the configuration
- You need to change the configuration settings previously defined for a Web Agent
- You need to remove the configuration settings from the Web Agent without uninstalling the entire Web Agent (you would need to configure the Web Agent again at a later time)

To reconfigure a Web Agent on Netscape:

1. Navigate to the `netegrity/siteminder/` directory.
2. Enter **`smwebagent-config`** to run the configuration script.
3. At the prompt to configure a Netscape Web server, enter **Y**.
4. If you did not specify the Netscape server root during installation, enter the server root when prompted:

   <netscape_installation>/*<server_directory>*

   where *<netscape_installation>* is the installed location of Netscape and <*server_directory>* is the installed location of the Netscape servers.

   For example:

   `/usr/netscape/server4`

   The configuration script detects and lists the installed Web servers.

5. Select the appropriate Web server by entering the corresponding number from the list of servers.

   The configuration script provides you with the following options:

   ```
   (o)verwrite the configuration with new settings you
   specify
   
   (p)reserve settings but update the configuration
   
   (r)emove the configuration, or
   
   (l)eave the webserver configured as it is and cancel
   the configuration
   ```

6. Complete one of the following:

   - To change the existing configuration settings, enter **`O`** and complete steps 5-12 of *Configuring Web Agents on Netscape* on page 151.
   - To update the configuration of a Web Agent that you upgraded and retain the configuration settings that were initially defined for it, enter **`p`** and at the prompt, confirm the settings. The configuration is now upgraded.
   - To remove the configuration settings from the Web Agent, enter **`r`** and at the prompt, confirm the removal. Before you use the Web Agent again, you must configure it, as described on page 151.
   - To exit the configuration script without changing the configuration settings, enter **`l`**.

Configuring Web Agents for Apache

Once you have installed a Web Agent, you must configure the Web Agent for the Apache Web server.

If you want to configure the Web Agent to additionally serve as a cookie provider, SSL credential collector, or forms credential collector, you must edit the `httpd.conf` file as described in following procedure.

Configuring a Web Agent on Solaris/Apache involves the following steps:

1. Run the configuration script.
2. Edit the `httpd.conf` file.
3. Restart the Web server.

To run the Web Agent configuration script on Apache:

1. Navigate to the directory where the Web Agent is installed.
2. Enter ./**`smwebagent-config`** to run the configuration script.
3. If prompted to configure a Netscape Web server, enter **`N`**.
4. At the prompt to configure an Apache Web server, enter **`Y`**.
5. Enter the server root for Apache. For example,

   `/usr/apache`

6. Enter the SiteMinder Policy Server IP address. The default IP address is the IP address of the local machine.

   This server is the SiteMinder Policy Server that you want the Web server to connect and communicate with first (for example: **`123.123.12.12`**).

7. Enter the Web Agent name (case-sensitive). Typically, the Agent is assigned the same name as the Web server on which it is installed.

   Tip: Take note of the Agent name. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface. The Agent name is case-sensitive.

8. Enter the cookie domain in which the Web Agent will be located.

   The domain must contain two periods, such as **`.myorg.org`**. For additional information about cookie domains, refer to the *SiteMinder Agent Operations Guide*.

9. Enter the Shared Secret that will be shared between the Web Agent and all Policy Servers that communicate with the Web Agent.

   The secret must be between 6 and 24 characters long.

   Note: If you try to cancel the installation while entering the Shared Secret (for example, if you press `Control + C`), at the next prompt enter **`stty echo`**, then press `ENTER` to restore the echo function. To provide optimal security, the echo function is off for this part of the install.

10. Confirm the Shared Secret by entering it again at the next prompt.

☞ **Note:** Take note of the Shared Secret. You will need this secret when configuring the Agent in the SiteMinder Policy Server User Interface.

11. Specify whether or not you want to provide Registration Services on the Web Agent you are configuring:
    - If you specify **y**, proceed to step 12.
    - If you specify **n**, proceed to step 13.
12. Specify the location of the servlet engine that you want to use to run Registration Services. For example, enter `$HOME/apache/ApacheServlet/Exec`.
13. If the configuration values displayed are correct, enter **Y**.

To edit the httpd.conf file:

Once you have run the configuration script, you must modify the `httpd.conf` configuration file to enable the Web server for use with the Web Agent.

1. Navigate to the `conf` directory:

   `$ cd` */usr/apache/*`conf`

   where */usr/apache/* is the installed location of the Apache Web server.
2. Open the `httpd.conf` file.
3. Add **`SmInitFile /`***usr/apache***`/conf/WebAgent.conf`** to the main server section.

   Do not use a relative path for this location.
4. Add the following line to the DSO configuration section:

   `LoadModule sm_module <`*libexec***`>/mod_sm.so`**

   where **<***libexec***>** is the location of the Web Agent `lib` directory.

The modified sections of the file should resemble the sample text below:

```
# Dynamic Shared Object (DSO) Support
#

# To be able to use the functionality of a module which was built as a DSO
# you have to place corresponding ‘LoadModule’ lines at this location so
# the directives contained in it are actually available _before_ they are
used. Please read the file README.DSO in the Apache 1.3 distribution for
#more details about the DSO mechanism and run ‘httpd -l’ for the list of
#already built-in (statically linked and thus always available) modules
#in your httpd binary.
#
# Note: The order in which modules are loaded is important.  Don’t change
# the order below without expert advice.
#

# Example:
# LoadModule foo_module libexec/mod_foo.so
LoadModule sm_module usr/siteminder/webagent/lib/mod_sm.so

# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/usr/apache/htdocs"
SmInitFile /usr/apache/conf/WebAgent.conf
```

5. If your `httpd.conf` file contains the directive **ClearModuleList**, then add **AddModule mod_sm.c** to the bottom of the **AddModule** directive section of your `httpd.conf`.

   The modified section of the file should resemble the text below:

   ```
   #Dynamic Shared Object (DSO) Support
   ClearModuleList
   AddModule mod_env.c
   AddModule mod_log_config.c
   AddModule mod_mime.c

   AddModule mod_negotiation.c
   AddModule mod_status.c
   AddModule mod_include.c
   AddModule mod_autoindex.c
   AddModule mod_dir.c
   AddModule mod_cgi.c
   AddModule mod_asis.c
   AddModule mod_imap.c
   AddModule mod_actions.c
   AddModule mod_userdir.c
   AddModule mod_alias.c
   AddModule mod_access.c
   AddModule mod_auth.c
   AddModule mod_so.c
   AddModule mod_setenvif.c
   AddModule mod_servletexec.c
   # Siteminder
   AddModule mod_sm.c
   ```

6. If you want to use Password Services, specify the following paths to the **Aliases** section:

   - **Alias /siteminderagent/pwcgi/ "***<siteminder_installation>/* **webagent/pw/"**

     where *<siteminder_installation>* is the installed location of SiteMinder.

     The path should appear as shown below:

     ```
     ### Siteminder Virtual Directory Mappings ##
     ```

     Alias /siteminderagent/pwcgi/ "space/smuser/netegrity/siteminder/webagent/pw"

     ```
     <Directory "space/smuser/netegrity/siteminder/
          webagent/pw/">
        Options Indexes MultiViews ExecCGI
        AllowOverride None
        Order allow,deny
        Allow from all
     </Directory>
     ```

   - **Alias /siteminderagent/pw/ "***<siteminder_installation>/* **webagent/pw"**

     where *<siteminder_installation>* is the installed location of SiteMinder.

     The path should appear as shown below:

     ```
     ### Siteminder Virtual Directory Mappings ##
     ```

     Alias /siteminderagent/pw/ "space/smuser/netegrity/siteminder/webagent/pw/"

     ```
     <Directory "space/smuser/netegrity/siteminder/
          webagent/pw/">
        Options Indexes MultiViews ExecCGI
        AllowOverride None
        Order allow,deny
        Allow from all
     </Directory>
     ```

☞ **Note:** Each Alias line above should appear all on one line.

7. If you want to use forms authentication, specify the following path to the form templates in the **Aliases** section:

   Alias /siteminderagent/forms/ "*<siteminder_installation>/* **webagent/samples/forms/"**

   where *<siteminder_installation>* is the installed location of SiteMinder.

The path should appear as shown below:

```
### Siteminder Virtual Directory Mappings ##

    Alias /siteminderagent/forms/ “/space/smuser/netegrity/
    siteminder/webagent/samples/forms/”

    <Directory "space/smuser/netegrity/siteminder/
         webagent/samples/forms">
       Options Indexes MultiViews
       AllowOverride None
       Order allow,deny
       Allow from all
    </Directory>
```

☞ **Note:** The Alias line above should appear all on one line.

8. If you want Basic over SSL, X509 Client Cert, X509 Client Cert or Basic, or X509 Client Cert and Basic authentication, add the following aliases to the **Aliases** section:

   - To use Basic over SSL authentication, add the following line:

     Alias/siteminderagent/nocert/"/*<siteminder_installation>*/ **webagent**

   - To use X509 Client Cert or X509 Client Cert and Basic authentication, add the following line:

     Alias/siteminderagent/cert/"/*<siteminder_installation>*/ **webagent**

   - To use X509 Client Cert or Basic authentication, add the following line:

     Alias/siteminderagent/certoptional/ "/*<siteminder_installation>*/**webagent**

     where *<siteminder_installation>* is the installed location of SiteMinder.

9. In the AddHandler section, add the following lines:

   - To use Password Services, add:

     AddHandler cgi-script .exe

   - To use forms authentication, add:

     AddHandler smformsauth-handler .fcc

- To use SSL, add:

  AddHandler smadvancedauth-handler .scc

- To use cookie providers, add:

  AddHandler smcookieprovider-handler .ccc

The modified section should appear as follows:

```
##SITEMINDER .exe ##
AddHandler cgi-script .exe

##SITEMINDER .fcc ##
AddHandler smformsauth-handler .fcc

##SITEMINDER .scc ##
AddHandler smadvancedauth-handler .scc

##SITEMINDER .ccc ##
AddHandler smcookieprovider-handler .ccc
```

10. If you are using X509 Client Cert, X509 Client Cert and Basic, or X509 Client Cert or Basic authentication, uncomment the **SSLOptions** line in Section 3 of the appropriate virtual host (if multiple hosts are defined) and make sure that **+ExportCertData +StdEnvVars** are included.

    The text should appear as follows:

    ```
    SSLOptions +ExportCertData +StdEnvVars
    ```

11. Save the modified `httpd.conf` file.
12. Restart the Web server.
13. Optimize the Apache Web Agent as described in *Optimizing an Environment for Apache* on page 163.

Reconfiguring Web Agents on Apache

Reconfigure a Web Agent on Apache for the following reasons:

- You need to change the configuration settings previously defined for a Web Agent.
- You need to remove the configuration settings from the Web Agent without uninstalling the entire Web Agent (you would need to configure the Web Agent again at a later time).

To reconfigure a Web Agent on Apache:

1. Navigate to the `netegrity/siteminder/agents` directory.
2. Enter ./**`smwa-config`** to run the configuration script.
3. If you are prompted to configure a Netscape Web server, enter **`N`**.
4. At the prompt to configure an Apache Web server, enter **`Y.`**
5. Enter the server root for Apache. For example,

   `/usr/apache`

   The configuration script detects and lists the installed Web servers.
6. Select the appropriate Web server by entering a number from the list of servers.

   The configuration script provides you with the following options:

   ```
   (o)verwrite the configuration with new settings you
   specify
   ```

   ```
   (p)reserve settings but update the configuration
   ```

   ```
   (r)emove the configuration, or
   ```

   ```
   (l)eave the webserver configured as it is and cancel
   the configuration
   ```
7. Complete one of the following:
   - To change the existing configuration settings, enter **`O`** and complete steps 5 - 13 of *Configuring Web Agents for Apache* on page 155.
   - To remove the configuration settings from the Web Agent, enter **`R`** and at the prompt, confirm the removal. Before using the Web Agent again, you will need to reconfigure it, as described on page 155.
   - To exit the configuration script without changing the configuration settings, enter **`l`**.

Optimizing an Environment for Apache

If you have installed an Apache Web Agent, optimize your system to improve the Apache Web Agent performance by completing the following two procedures:

- Tune Solaris for the Apache Web Agent
- Modify the Apache `httpd.conf` file

Tuning Solaris for the Apache Web Agent

Improve the performance of the Apache Web Agent by increasing shared memory segments in your Solaris environment. The variables that control shared memory segments are defined in the system specification file and include:

Variable Name	**Description**	**Required**	**Recommended**
shmsys:shminfo_shmmax	Maximum shared memory segment size. Controls the maximum size of your APACHE agent Resource Cache and Session Cache.	You may adjust the setting accordingly.	33554432 (32 mb) for busy sites with a need for large cache size settings.
semsys:seminfo_semmni	The maximum number of semaphore sets in the system.	10 for every instance of the APACHE agent that you will run the system.	100
semsys:seminfo_semmns	The maximum number of semaphores in the system.	10 for every instance of the APACHE agent that you will run the system	100
semsys:seminfo_semmnu	Number of processes using the undo facility.	For optimal performance, SEMMNU should be greater than the number of Apache child processes running on your system at any one time.	200 or greater than the "MaxClients" setting on your Apache.
shmsys:shminfo_shmseg	The maximum number of shared memory segments per process	6	24

To increase shared memory segments:

1. Open the `/etc/system` file, using the editor of your choice.
2. Add the variables listed above and define the variables using the recommended settings:

   ```
   set shmsys:shminfo_shmmax=33554432
   set semsys:seminfo_semmni=100
   set semsys:seminfo_semmns=100
   set semsys:seminfo_semmnu=200
   set shmsys:shminfo_shmseg=24
   ```

3. Exit the file, saving changes.
4. Reboot the system.
5. Verify the shared memory value changes:

   ```
   $ sysdef -i
   ```

Modifying the Apache httpd.conf file

Improve server performance by modifying the default configuration settings defined in the `httpd.conf` file. This file is located in the *$APACHE_ROOT*/`conf` directory. Edit the contents of the file using a text editor.

For low-traffic Web sites, define the following directives:

- Set MaxRequestsPerChild>1000 or Set MaxRequestsPerChild=0
- MinSpareServers >5
- MaxSpareServers>10
- StartServers=MinSpareServers>5

For high-traffic Web sites, define the following directives:

- Set MaxRequestsPerChild>3000 or Set MaxRequestsPerChild=0
- MinSpareServers >10

- MaxSpareServers>15
- StartServers=MinSpareServers>10

☞ **Note:** For all Web sites (low and high traffic), `mod_sm` must be assigned a higher priority level than other auth or access modules installed on your Apache configuration.

Reinstalling a Web Agent on UNIX

Reinstalling a Web Agent enables you to restore lost files.

To reinstall a Web Agent on UNIX:

1. Run **`./smwa-install`** from the Web Agent files directory.
2. Confirm that you have read the Software License Agreement, then enter **Y** to continue.
3. If you have a Netscape installation on your system and want to configure a Web Agent for Netscape, enter **y** when asked if the system has a Netscape Web server.

   ☞ **Note:** If you are installing a Web Agent for Apache or you do not want to configure a Web Agent for Netscape at this point, enter **n**, then specify the Web server during configuration.

4. Complete one of the following:
   - If you specified **y** in step 3, enter the server root for Netscape:

     <netscape_installation>/<*server_directory*>

     where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape servers.

     For example:

     `/usr/netscape/server4`.
   - If you specified **n** in step 3, proceed to step 5.

The installation program displays the installation path you entered. If you specified a Netscape server root, the installation program displays that, as well.

5. Enter an installation root for the Web Agent, such as `/home/myroot` or press ENTER to accept the default location of `/opt.`

   The installation program displays the installation root you entered.

6. If this information is correct, enter **Y**. The installation is complete.

Uninstalling a Web Agent from UNIX

1. Stop the Web server.
2. Log into the UNIX system with root privileges.
3. Navigate to the `netegrity/siteminder/agents` directory.
4. Run **`./smagent-uninstall`**.
5. At the prompt to continue the uninstall, enter **Y**.

   The uninstall script lists the location of the Web Agents and the location of the installed Web servers.

6. At the prompt to continue the uninstall, enter **Y**.

   The `netegrity/siteminder/agents` directory is removed. The Web Agent is no longer functional on the system. The `obj.conf` file(s) is restored and the `WebAgent.conf` file(s) is removed.

7. Restart the Web server(s).

   The SiteMinder Web Agent uninstallation is complete.

8. Change to your home directory (the current directory has been deleted).

Chapter 9. Installing Affiliate Agents

Overview

An Affiliate Agent is an Agent that resides outside of a SiteMinder installation. It securely collects user information from the SiteMinder Policy Server at the portal with which the affiliate is associated. Affiliate Agents can use this information to personalize the content of their own site for the user.

This chapter describes how to install and configure Affiliate Agents on NT and UNIX machines.

📖 For detailed information about configuring Affiliate Agents, refer to the *SiteMinder Agent Operations Guide*.

📖 For information about deploying Affiliate Agents, refer to the *SiteMinder Deployment Guide*.

Installing an Affiliate Agent on NT

This section describes how to install the SiteMinder Affiliate Agent on the Windows NT platform. After you have installed the Affiliate Agent, you must configure it for use with Microsoft IIS and/or Netscape Web Servers.

Before you Begin

Before installing the Affiliate Agent on NT, make sure that the following prerequisites have been met:

- NT 4.0 Server or Workstation is installed on your system along with Service Pack 3, 4, or 5
- One of the following Web servers is installed on your system:
  - iPlanet Web Server Enterprise Edition 4.0 or higher
  - Netscape Enterprise Web Server 3.51 or higher
  - IIS 3.0 or higher, or IIS 4.0 or higher.

- The SiteMinder Policy Server is installed at the portal site and the Affiliate Agent is configured in the SiteMinder Policy Server User Interface.
- You have received the following information from the SiteMinder Administrator:
  - Affiliate Agent name, as specified in the Policy Server User Interface
  - Shared Secret, as specified in the Policy Server User Interface
  - IP address or domain name of the Policy Server
  - The SiteMinder target, which is the location of SiteMinder cookie provider at the portal site

☞ **Note:** You cannot install an Affiliate Agent on a Web server that has a SiteMinder Web Agent installed on it.

To install an Affiliate Agent on NT:

1. Exit all applications that are running, then insert the SiteMinder CD-ROM.
2. Run **AffiliateAgent-4.1-NT.exe** from the `nt` directory on the SiteMinder CD-ROM:
3. In the Welcome dialog box, click **Next**.
4. Read the Software License Agreement and click **Yes** if you accept the agreement.
5. Read the Release Notes, then click **Next**.
6. In the **Choose Destination Location** dialog box, accept the default installation location or select a different location and click **Next**.
7. In the **Select Program Folder** dialog box, select the Program Folder where SiteMinder will place program icons, then click **Next**.
8. In the **Start Copying Files** dialog box, click **Next**.

   The Affiliate Agent Setup copies the files to the specified location.
9. In the **Setup Complete** dialog box, confirm that you want to configure the Affiliate Agent when the installation completes by ensuring the **Launch the Agent Configuration now** check box is selected.
10. Click **Finish**.

SiteMinder prepares the **Affiliate Agent Configuration Wizard**. Refer to *Configuring an Affiliate Agent on NT* on page 169 for instructions on configuring an Affiliate Agent.

Configuring an Affiliate Agent on NT

Once you have installed an Affiliate Agent, you must configure it to communicate with the SiteMinder Policy Server at the main portal site.

Complete the following procedure to configure an Affiliate Agent for an IIS or Netscape Web server.

To configure an Affiliate Agent:

1. If necessary, open the **Affiliate Agent Configuration Wizard** by completing the following steps:

   a. Navigate to <*affiliateagent_installation*>`\Config`

      where <*affiliateagent_installation*> is the installed location of the SiteMinder Affiliate Agent.

      For example,

      ```
      C:\Program Files\Netegrity\SiteMinder\Affiliate
      \config
      ```

   b. Double click **Setup.exe**.

   If you indicated that you wanted to configure the Affiliate Agent after installation, SiteMinder automatically opens the **Affiliate Agent Configuration Wizard** for you.

2. In the **Select Web server(s)** dialog box, select the Web server(s) that you want to configure as Affiliate Agents, then click **Next**.

   SiteMinder displays the configuration settings for the Web server you selected.

☞ **Note:** If you are configuring the Affiliate Agent for the first time, the configuration settings are undefined.

3. In the **Confirm Configuration Selections** dialog box, review the configuration settings for the first Web server you selected.

   - To configure new settings, click **Configure**.
   - To change the configuration settings, click **Configure**.
   - To accept the configuration settings, click **Next**.

     If you are satisfied with the current configuration settings, skip to step 13 of this procedure.

   !

   Warning: Clicking **Configure** resets all of the configuration settings including the settings you configured in the `Affiliate.conf` file to default settings. You must enable the Affiliate Agent, as described in the *SiteMinder Agent Operations Guide*, before it protects your resources again.

4. In the **Affiliate Name** field, enter the affiliate name provided by the portal administrator, then click **Next**.

   The affiliate name is case-sensitive. Make sure that you define the affiliate name exactly as it is defined in the Policy Server User Interface.

5. In the **Shared Secret** and **Confirm Shared Secret** fields, enter the shared secret, then click **Next**.

   The shared secret is used to communicate with the Policy Server. The secret must match the shared secret for the Affiliate Agent specified in the SiteMinder Policy Server User Interface.

6. In the **Portal Name** field, enter the company name of the portal, then click **Next**.

7. Enter the following portal information, then click **Next**.

   - In the **Portal** field, specify the IP address and port or fully qualified URL for the portal.

     For example,

     ```
     http://www.myorg.org
     ```

- In the **Target** field, specify the target of the portal server.

  The target of the portal server is the relative path to the SiteMinder cookie provider at the portal site. The cookie provider enables information to pass between the portal and the affiliate.

  For example,

  `/siteminderagent/smprofile.ccc`

  The target is appended to the portal URL to specify the exact location of the cookie provider at the portal site.

  For example,

  `http://www.myorg.org/siteminderagent/smprofile.ccc`

Note: The portal administrator must provide these values.

8. In the **Affiliate Resource** field, specify the resource in your Web site that, when accessed, will cause the Affiliate Agent to contact the portal for user information by specifying one of the following, then click **Next**.

   - Realm—Specify the relative path to the realm that contains the resources at the affiliate site that use information gathered from the portal.

     For example,

     `/realma`

   - Application—Specify the hook character (?) and a name/value pair:

     ?<*name/value pair*>

     For example,

     `?affiliate=on`

Note: Refer to the *SiteMinder Agent Operations Guide* for more information about the affiliate resource.

9. In the **Cookie Domain** field, enter the cookie domain of the affiliate Web server, then click **Next**.

   The cookie domain must be specified with two periods. For example, `.myorg.org`.

10. Specify whether or not anonymous and unknown users can access the specified resources by selecting **Yes** or **No**, then click **Next**.

    If you select **Yes**, users who were not authenticated (unknown users) or authorized (anonymous users) at the portal site will be able to gain access to the affiliate resources at your Web site. If you select **No**, users can be redirected to a No Access URL, defined in the next step, when they attempt to access a resource.

11. In the **No Access URL** field, specify a fully qualified URL to which users who are denied access to the specified resources are redirected, then click **Next**.

    If you do not specify a redirection URL, users who are denied access to resources will be redirected to a default error page.

    Note: For detailed information on allowing anonymous and unknown users to access resources associated with the Affiliate Agent, refer to *SiteMinder Agent Operations Guide*.

    The **Affiliate Agent Configuration Wizard** displays the settings you selected.

12. Confirm the configuration settings by clicking **Next**.

13. Click **Next** to confirm that you want to update the Affiliate Agent configuration for the Web server displayed.

14. Click **Finish** to complete the setup.

Reinstalling an Affiliate Agent on NT

Reinstall an Affiliate Agent to restore missing application files. To change Affiliate Agent settings or to configure an Affiliate Agent for a different Netscape or IIS Web Server, configure the Affiliate Agent using the **Affiliate Agent Configuration Wizard**.

To reinstall an Affiliate Agent on NT:

1. Exit all applications that are running, then insert the SiteMinder CD-ROM.
2. Run the setup program:
    a. Navigate to the `nt` folder on the SiteMinder CD-ROM.
    b. Double-click `AffiliateAgent-4.1-NT.exe`.

        SiteMinder detects the previous installation of the Affiliate Agent on your system.
3. In the **Welcome** dialog box, click **Next**.
4. Read the Software License Agreement and click **Yes** if you accept the agreement.
5. Read the Release Notes, then click **Next**.
6. In the **Confirm Reinstallation** dialog box, select **Continue with reinstallation**.
7. In the **Start Copying Files** dialog box, click **Next**.

    The Affiliate Agent Setup copies files to the specified location.
8. In the **Setup Complete** dialog box, click **Finish**.

    You should not run the **Agent Configuration Wizard** after reinstalling a Web Agent if you want the preserve your Affiliate Agent configuration.

    If you want to reconfigure an Affiliate Agent, access the **Agent Configuration Wizard**, as described in *Configuring an Affiliate Agent on NT* on page 169.

☞ **Note:** You may be required to reboot your machine once the installation is complete.

Uninstalling an Affiliate Agent from NT

1. Open the Control Panel.
2. Double click **Services**, and complete one of the following:
   - For Netscape, stop the Enterprise service, then close the **Services** dialog box. Make sure you are stopping the server on which the Affiliate Agent is installed.
   - For IIS 3.0, stop the **World Wide Web Publishing Service**, then close the **Services** dialog box.
   - For IIS 4.0, stop the **World Wide Web Publishing Service** and the **Content Index Service** (if it exists), then close the **Services** dialog box.
3. Double click **Add/Remove Programs** from the Control Panel.
4. Select **SiteMinder Web Agent v4.1** as the program for uninstallation, then follow the instructions on the screen.
5. Click **OK** when the uninstallation is complete and close the **Add/Remove Programs** dialog box. The uninstall is now complete.

Installing an Affiliate Agent on UNIX

This section describes how to install the SiteMinder Web Agent on a UNIX platform. After you have installed the Affiliate Agent, you must configure it for use with Microsoft IIS and/or Netscape Web Servers.

Before you Begin

If you are installing the Affiliate Agent on UNIX, make sure that the following prerequisites have been met:

- HP-UX 10.20 is installed on the system.
- One of the following Solaris versions and the required/recommended patches are installed on your system:

Version	Required Patches	Recommended Patches
Solaris 2.5.1	kernel update and libthread = 103640-31 C++ shared library = 106529-05	None

Solaris 2.6	kernel update = 105181-17
	C++ shared library = 105591-07
	libc = 105210-25
	libthread = 105568-14
		patchadd = 106125-08

Solaris 2.7	kernel update = 106541-08 C++ shared library = 106327-06 libthread = 106980-07	patchadd = 107171-04

- One of the following Web servers is installed on your system:
  - iPlanet Web Server Enterprise Edition 4.0 or higher
  - Netscape Enterprise Server 3.51 or higher
  - Apache 1.3.6, 1.3.9, or 1.3.11
- The SiteMinder Policy Server is installed at the portal site and the Affiliate Agent is configured in the SiteMinder Policy Server User Interface
- You have received the following information from the SiteMinder Administrator:
  - Affiliate Agent name, as specified in the Policy Server User Interface
  - Shared Secret, as specified in the Policy Server User Interface

- IP address or domain name of the Policy Server
- The SiteMinder target, which is the exact location of SiteMinder cookie provider at the portal site

To install an Affiliate Agent on UNIX:

1. Exit all applications that are running, then insert the SiteMinder CD-ROM.
2. Navigate to the directory in which you want to install the Affiliate Agent.
3. Untar the appropriate Affiliate Agent installation file located in the `/hp` or `/solaris` directory on the SiteMinder CD-ROM:
   - For HP-UX, **`tar -xvf smwf-4.1-so.tar`**
   - For Solaris, **`tar -xvf smwf-4.1-hp.tar`**
4. From the `smwf-install` directory, run **`./smwf-install`**.

   The installation script prepares the Release Notes.
5. Press ENTER to read the Release Notes for important information about installing the Affiliate Agent.
6. Enter **`y`** to confirm that you want to continue with the installation.
7. Confirm that you have read the Software License Agreement, then enter **`Y`** to continue.Enter **`y`** to continue with the installation.
8. Confirm that you have read the license agreement contained in `license.txt,` then enter **`y`** to continue.
9. Specify the directory where the Affiliate Agent will be installed.

   The default location is **`$HOME/netegrity/siteminder.`**

   The installation creates a subdirectory called `Affiliate` in the directory you specify.
10. If you have a Netscape installation on your system and want to configure an Affiliate Agent for Netscape, enter **`y`** when asked if the system has a Netscape Web server.

Note: If you are installing an Affiliate Agent for Apache or you do not want to configure an Affiliate Agent for Netscape at this point, enter **`n`**, then specify the Web server during configuration.

11. Complete one of the following:

    - If you specified **y** in step 10, enter the server root for Netscape:

      <netscape_installation>/*<server_directory>*

      where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape servers.

      For example:

      `/usr/netscape/server4`.

    - If you specified **n** in step 6, proceed to step 12.

    The installation program displays the installation path you entered. If you specified a Netscape server root, the installation program displays that, as well.

12. Enter **y** to confirm that the installation path and server root are correct.

The SiteMinder Affiliate Agent installation is complete. To use the Affiliate Agent with the Siteminder Policy Server, you must configure the Affiliate Agent. Refer to *Configuring the Affiliate Agent for UNIX* on page 177 for instructions.

Configuring the Affiliate Agent for UNIX

Once you have installed the Affiliate Agent, you must configure it for use with a Netscape or Apache Web server.

To configure the Affiliate Agent:

1. Run **`./smaffiliate-config`** from the directory in which the Affiliate Agent is installed.

2. Complete one of the following:

   - If you want to configure an Affiliate Agent for a Netscape Web server, enter **y** when prompted.

   - If you want to configure an Affiliate Agent for Apache, enter **n** when asked if you want to configure an Affiliate Agent for Netscape. Then, enter **y** when asked if you want to configure an Affiliate Agent for Apache.

3. Specify the Web server to configure as an Affiliate Agent by completing one of the following:

   - If you want to configure an Affiliate Agent for Netscape and you specified the Netscape root during the installation, select the Web server that you want to configure from the list of available servers, then enter its corresponding number when prompted.
   - If you want to configure an Affiliate Agent for Netscape and you did not specify the Netscape root during the installation, enter the Netscape root when prompted.

     For example,

     /usr/netscape/server4
   - If you are configuring the Affiliate Agent for an Apache Web server, enter the Apache server root when prompted:

     For example,

     /usr/apache

☞ **Note:** You cannot install an Affiliate Agent on a Web server that already has a SiteMinder Web Agent installed on it. If you select a Web server that is running a Web Agent, the installation prompts you to select another Web server.

4. Enter the Affiliate Name when prompted.

   The affiliate name is a unique identifier between the Affiliate Agent and the portal. The portal administrator should provide the affililate name.

   The affiliate name is case-sensitive. Make sure that it is defined during the installation exactly as it is defined in the Policy Server User Interface at the portal site.

5. Enter and confirm a Shared Secret for the Affiliate Agent.

   The Shared Secret must match the Shared Secret specified for the Affiliate Agent in the Policy Server User Interface at the portal site. The SiteMinder administrator at the portal site should provide this information.

   The Affiliate Agent configuration displays the settings you selected.

6. When prompted, enter the IP address and port or the fully qualified domain name for the portal.

   For example,

   `http://www.myorg.org`

7. Enter the target of the portal server.

   The target of the portal server is the relative path to the SiteMinder cookie provider at the portal site. The cookie provider enables information to pass between the portal and the affiliate.

   For example,

   `/siteminderagent/smprofile.ccc`

   The target is appended to the URL of the portal to specify the exact location of the cookie provider at the portal site.

   For example,

   `http://www.myorg.org/siteminderagent/smprofile.ccc`

8. Specify the resource in the affiliate site that, when accessed, causes the Affiliate Agent to contact the portal for user information by specifying one of the following:

   - Realm—Specify the relative path to the realm that contains the resources associated with the Affiliate Agent.

     For example,

     `/realma`

   - Application—Specify the hook character (?) and a name/value pair:

     ?<*name/value pair*>

     For example,

     `?affiliate=on`

Note: For more information about the Affiliate Resource, refer to *SiteMinder Agent Operations Guide*.

9. When prompted, enter the name of the portal.

10. Enter the cookie domain of the Affiliate Web server.

    The cookie domain must contain two periods.

    For example,

    `.myorg.org`

11. Specify whether or not unknown or anonymous users can access the specified resources by entering one of the following:

    - **Y**—Allows users who were not authenticated (unknown users) or unauthorized (anonymous users) by the portal to access the resource at your site.
    - **N**—Prevents users who were not authenticated or authorized by the portal from accessing the resources at your site.

      If you specify **N**, enter the URL for a page to which users who are denied access are redirected when prompted.

12. Specify the fully qualified URL to which users who are denied access to affiliate resources are redirected.

    For example,

    `http://www.myorg.org/realma/index.html`

    If you do not specify a redirection URL, users who are denied access to resources will be redirected to a default error page.

    Note: For detailed information on allowing anonymous and unknown users to access resources associated with the Affiliate Agent, refer to *SiteMinder Agent Operations Guide*.

    The configuration script displays the installation root and Web server target.

13. Confirm that the displayed settings are correct by entering **`y`** when prompted.

14. If you are configuring the Affiliate Agent for an Apache Web server, configure the `httpd.conf` file as described in *Configuring the Apache httpd.conf File for Apache Servers* on page 181.

15. Restart the Web server.

Configuring the Apache httpd.conf File for Apache Servers

To enable the Affiliate Agent for Apache servers, you must edit the `httpd.conf` as follows:

To edit the httpd.conf file:

Once you have run the configuration script, you must modify the `httpd.conf` configuration file to enable the Web server for use with the Affiliate Agent.

1. Navigate to the `conf` directory:

   `$ cd /`*<apache_installation>*`/conf`

   where *<apache_installation>* is the installed location of the Apache Web server.

2. Open the `httpd.conf` file.
3. Add **`SmAffiliateInitFile`** *<apache_installation>***`/conf/Affiliate.conf`** to the main server section.

   where *<apache_installation>* is the installed location of the Apache Web server. Do not use a relative path for this location.

4. Add the following line to the Dynamic Shared Object (DSO) configuration section

   `LoadModule sm_module libexec/mod_smaffiliate.so`

   The modified sections of the file should resemble the sample text below:

```
# Dynamic Shared Object (DSO) Support
#

# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Please read the file README.DSO in the Apache 1.3 distribution for more
# details about the DSO mechanism and run 'httpd -l' for the list of already
# built-in (statically linked and thus always available) modules in your httpd
# binary.
#
# Note: The order is which modules are loaded is important.  Don't change
# the order below without expert advice.
#
# Example:
# LoadModule foo_module libexec/mod_foo.so
LoadModule sm_module libexec/mod_sm.so
LoadModule sm_module libexec/mod_smaffiliate.so
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/usr/apache/htdocs"
SmAffiliateInitFile /usr/apache/conf/Affiliate.conf
```

5. If your `httpd.conf` file contains the directive **`ClearModuleList`**, then add **`AddModule mod_smaffiliate.c`** to the bottom of the AddModule directive section of your `httpd.conf`.
6. Save the modified `httpd.conf` file.
7. Restart the Apache Web server.

Reinstalling an Affiliate Agent on UNIX

Reinstalling an Affiliate Agent enables you to restore lost files.

To reinstall a Web Agent on UNIX:

1. Run **`./smwf-install`** from the Affiliate Agent files directory.

   The installation script prepares the Release Notes.

2. Press ENTER to read the Release Notes for important information about SiteMinder 4.1.
3. Enter **y** to confirm that you want to continue with the installation.

   The installation script displays the prerequisites for installing SiteMinder Policy Server 4.1.

4. Confirm that you have read the Software License Agreement, then enter **Y** to continue. Confirm that you have read the Software License Agreement, then enter **y** to continue.
5. If you have a Netscape installation on your system and want to configure a Web Agent for Netscape, enter **y** when asked if the system has a Netscape Web server.

Note: If you are installing a Web Agent for Apache or you do not want to configure a Web Agent for Netscape at this point, enter **n**, then specify theWeb server during configuration.

6. Complete one of the following:

   - If you specified **y** in step 5, enter the server root for Netscape:

     <netscape_installation>/<server_directory>

     where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape servers.

     For example:

     `/usr/netscape/server4`.

   - If you specified **n** in step 5, proceed to step 7.

   The installation program displays the installation path you entered. If you specified a Netscape server root, the installation program displays that, as well.

7. Enter an installation root for the Web agent, such as `/home/myroot` or press ENTER to accept the default location of `/opt.`

   The installation program displays the installation root you entered.

8. If this information is correct, enter **y**. The installation is complete.

Uninstalling an Affiliate Agent from UNIX

1. Stop the Web server.
2. Log into the UNIX system with root privileges.
3. Navigate to the `netegrity/siteminder/affiliate` directory.
4. Run **`./smwf-uninstall`**.
5. At the prompt to continue the uninstall, enter **y**.

   The uninstall script lists the location of the Affiliate Agents and the location of the installed Web servers.

6. At the prompt to continue the uninstall, enter **y**.

   The `netegrity/siteminder/agents` directory is removed. The Affiliate Agent is no longer functional on the system. The `obj.conf` file(s) is restored and the `WebAgent.conf` file(s) is removed.

7. Restart the Web server(s).

   The SiteMinder Affiliate Agent uninstallation is complete.

8. Change to your home directory (the current directory has been deleted).

Chapter 10. Upgrading to SiteMinder 4.1

Overview

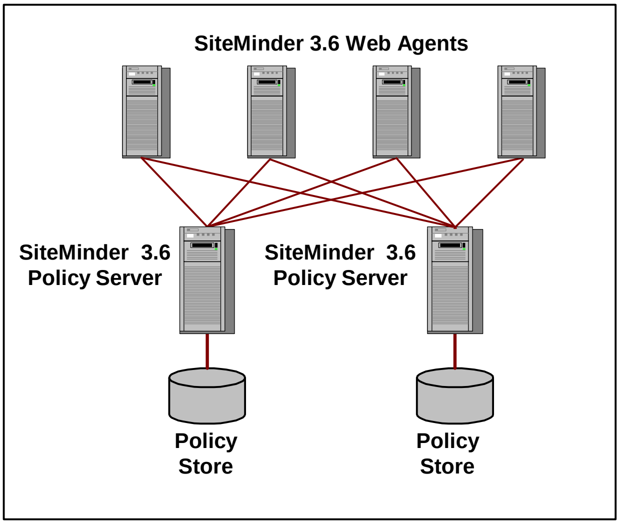
Upgrading a SiteMinder 3.6x deployment to SiteMinder 4.1 involves upgrading each SiteMinder component separately. Upgrading each component separately allows you to complete the upgrade procedure without shutting SiteMinder down if you have multiple Policy Servers and Web Agents in your deployment.

Note: If your SiteMinder 3.6x environment includes only one Policy Server, you must shut SiteMinder down during the upgrade procedure. To avoid shutting down SiteMinder you can install a backup Policy Server and configure it for failover. For information about upgrading a single Policy Server, refer to *Upgrading SiteMinder in a Single Policy Server Environment* on page 192.

To upgrade a SiteMinder deployment without shutting SiteMinder down, remove one of the Policy Servers and Web Agents from the SiteMinder environment. While those components are being upgraded, the remaining Policy Servers and Web Agents continue to protect your resources. Continue removing and upgrading SiteMinder components until you are ready to switch to the SiteMinder 4.1 deployment. Once you have enabled SiteMinder 4.1, you can upgrade the final SiteMinder components.

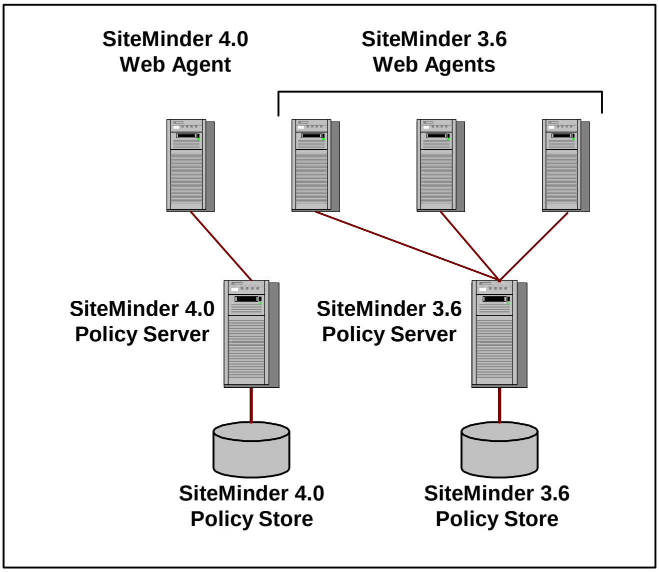
Upgrading SiteMinder in a Multiple Policy Server Environment

To upgrade your SiteMinder production environment to SiteMinder 4.1 without having to shut down SiteMinder, you must have multiple Policy Servers and Web Agents running, as shown below.


SiteMinder 3.6 Web Agents
SiteMinder 3.6 Policy Server
SiteMinder 3.6 Policy Server
Policy Store
Policy Store

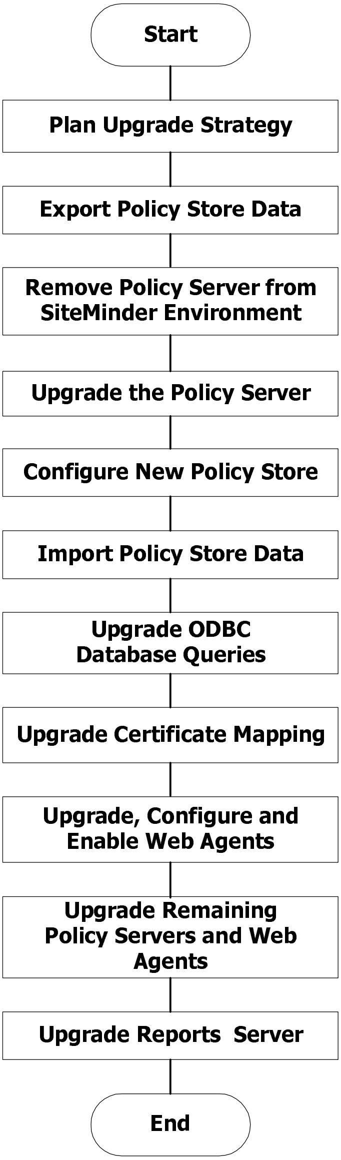
At minimum, you must have two Policy Servers and two Web Agents.

During the upgrade procedure, each SiteMinder component is removed from the production environment and upgraded separately to prevent shutting SiteMinder down, as shown below.



Tip: You should upgrade your production environment when your site receives the least amount of traffic. Even though SiteMinder does not need to be shut down, performance may be affected as you remove SiteMinder components.

The following steps are required to upgrade your SiteMinder environment. Each step is described in detail later in this chapter.


Start
Plan Upgrade Strategy
Export Policy Store Data
Remove Policy Server from SiteMinder Environment
Upgrade the Policy Server
Configure New Policy Store
Import Policy Store Data
Upgrade ODBC Database Queries
Upgrade Certificate Mapping
Upgrade, Configure and Enable Web Agents
Upgrade Remaining Policy Servers and Web Agents
Upgrade Reports Server
End

1. Decide which of the Policy Servers and Web Agents you want to upgrade first, as shown in the diagram on page 187. The remaining Policy Servers and Web Agents will continue to serve the site as you upgrade the initial Policy Servers and Web Agents.
2. Export the policy store data, as described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198. From this point on, no policy changes should be allowed until the upgrade is complete.
3. Remove the first Policy Server that you are upgrading from the SiteMinder environment, as described in *Upgrading SiteMinder in a Single Policy Server Environment* on page 192.
4. Upgrade the Policy Server to SiteMinder 4.1, as described in *Upgrading the Policy Server to SiteMinder 4.1* on page 199.
5. Configure all the new policy stores for SiteMinder 4.1, as described in the following chapters:
   - To configure a policy store on NT, refer to *Chapter 3, Setting up the Policy Store on NT* on page 47.
   - To configure a policy store on Solaris, refer to *Chapter 4, Setting up the Policy Store on Solaris* on page 75.
   - To configure an NDS policy store on Novell, refer to *Chapter 5, Setting up a Policy Store on Novell Netware* on page 91.
6. Import the SiteMinder 3.6 SP 1 policy store data into the SiteMinder 4.1 policy store using `smobjimport` (version 4.1), as described in *Importing Policy Store Data* on page 204.
7. If you are using an ODBC database as a user directory, migrate the queries to the SiteMinder 4.1 policy store, as described in *Upgrading an ODBC User Directory Schema* on page 205.
8. If you are using certificate mapping, upgrade the certificate mapping as described in *Upgrading Certificate Mapping* on page 208.

9. Upgrade the Web Agent you selected in step 1, and during the configuration, specify the SiteMinder 4.1 Policy Server as the Policy Server, as described in *Upgrading Web Agents, Cookie Providers and Advanced Authentication Schemes* on page 218.

   ☞ **Note:** If this Web Agent provides additional services, such as serving as the cookie providers, or providing advanced authentication to SiteMinder 4.1, upgrade these services, as well.

10. If you changed the Agent name, IP address, or Shared Secret when configuring Web Agents for SiteMinder 4.1, configure those Web Agents in the SiteMinder Policy Server User Interface, as described in the *SiteMinder Policy Server Operations Guide*.

11. Enable the SiteMinder 4.1 Web Agent.

12. Repeat steps 5-10 for the remaining 3.6 Policy Server and Web Agents.

    ☞ **Note:** If you want to remove the SiteMinder 3.6 policy store from an LDAP directory, you must remove the policy store data before upgrading your final Policy Server to SiteMinder 4.1. Removing the SiteMinder 3.6 policy store data requires the 3.6 version of `smldapsetup`. Refer to *Removing SiteMinder 3.6 Policy Store Data* on page 231 for instructions.

13. Enable round robin load balancing in the Web Agents, if required. Refer to the *SiteMinder Agent Operations Guide* for more information.

14. If you have a SiteMinder 3.6 Reports Server installed, upgrade the Reports Server as described in *Upgrading the Reports Server* on page 228.

15. Optionally, remove the SiteMinder 3.6 policy store data and schema as described in *Removing the SiteMinder 3.6 Policy Store* on page 230.

☞ **Note:** If you have custom components in your SiteMinder deployment, contact your Netegrity Professional Services representative for information on how to upgrade these components.

Maintaining Single Sign-on Between 3.6x and 4.1 Web Agents

In a large SiteMinder deployment that receives heavy traffic, you may not be able to quickly install new Policy Servers and Web Agents throughout your enterprise. Using SiteMinder 3.6 Service Pack 2 (SP2) Policy Servers in conjunction with SiteMinder 4.1 Policy Servers, you can upgrade SiteMinder components while maintaining single sign-on across all 3.6x and 4.1 Web Agents.

To upgrade with single sign-on support between 3.6x and 4.1 Web Agents:

1. Install SiteMinder 3.6 SP 2 on your existing SiteMinder 3.6 Policy Servers. For information, refer to the `readme.txt` file that shipped with SiteMinder 3.6 SP 2 software.
2. In the SiteMinder Policy Server Management Console for each 3.6 SP 2 Policy Server, complete the following:
   a. Select the **Advanced** tab.

   b. Select the **Enable SSO across multiple policy stores** check box.

   c. Restart the SiteMinder services.
3. In the SiteMinder Policy Server User Interface for each SiteMinder 4.1 Policy Server, complete the following:
   a. From the menu bar, select **Tools | Global Settings**.

   The SiteMinder Global Settings dialog box appears.

   b. Select the **SiteMinder 3.6 SP2+ Compatibility Mode** check box.

   c. Click **OK**.

   For more information, refer to the *SiteMinder Policy Server Operations Guide*.
4. In the SiteMinder Policy Server User Interface for each SiteMinder 4.1 Policy Server, complete the following:
   a. From the menu bar, select **Tools | Manage Keys**.

   The SiteMinder Key Management dialog box appears.

   b. Set up a static key using the value of the Agent key for your SiteMinder 3.6x Agents.

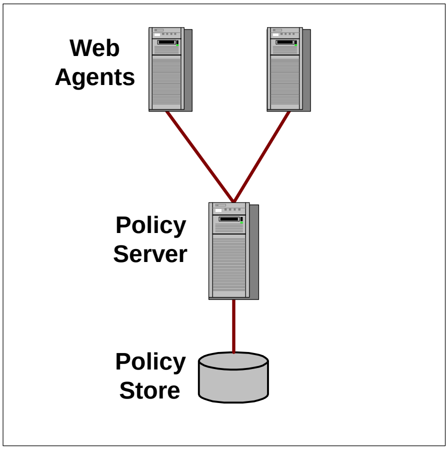
For details about setting Agent keys, refer to the *SiteMinder Policy Server Operations Guide*.

☞ **Note:** SiteMinder Policy Server versions 3.6 SP 2 and 4.1 can communicate with all SiteMinder 3.6x and 4.1 Web Agents.

Upgrading SiteMinder in a Single Policy Server Environment

If your SiteMinder 3.6 deployment consists of a single Policy Server, shown below, you must install a secondary Policy Server and Web Agent (if you only have one installed) on a separate server or shut down your site to upgrade to SiteMinder 4.1.

SiteMinder Deployment



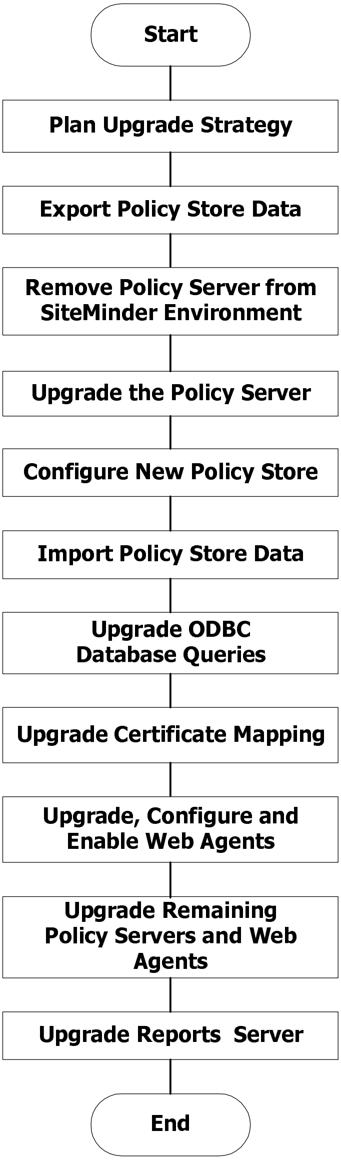
To install a second Policy Server, refer to one of the following chapters:

- *Chapter 1, Installing the Policy Server on NT* on page 15.
- *Chapter 2, Installing the Policy Server on Solaris* on page 29.

To install a second Web Agent, refer to *Chapter 8, Installing Web Agents* on page 135.

☞ **Note:** If you install a secondary Policy Server, complete the upgrade procedure described in *Upgrading SiteMinder in a Multiple Policy Server Environment* on page 186.

If you do not want to install a secondary Policy Server, the following steps are involved in upgrading to SiteMinder 4.1:


Start
Plan Upgrade Strategy
Export Policy Store Data
Remove Policy Server from SiteMinder Environment
Upgrade the Policy Server
Configure New Policy Store
Import Policy Store Data
Upgrade ODBC Database Queries
Upgrade Certificate Mapping
Upgrade, Configure and Enable Web Agents
Upgrade Remaining Policy Servers and Web Agents
Upgrade Reports Server
End

1. Determine when your site receives the least amount of traffic and plan to upgrade at that time. Users who attempt to access your site during the upgrade procedure will not be able to access your site until SiteMinder 4.1 is enabled if you have not installed a secondary Policy Server.
2. Export the policy store data, as described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198. From this point on, no policy changes should be allowed until the upgrade is complete.
3. Upgrade the Policy Server to SiteMinder 4.1, as described in *Upgrading the Policy Server to SiteMinder 4.1* on page 199.

☞ **Note:** If you want to remove the SiteMinder 3.6 policy store from an LDAP directory, you must remove the policy store data before upgrading the Policy Server to SiteMinder 4.1. Removing SiteMinder 3.6 policy store data requires the 3.6 version of `smldapsetup`. Refer to *Removing SiteMinder 3.6 Policy Store Data* on page 231 for instructions.

4. Create and configure all the new policy stores for SiteMinder 4.1, as described in the following chapters:
   - To configure a policy store on NT, refer to *Chapter 3, Setting up the Policy Store on NT* on page 47.
   - To configure a policy store on Solaris, refer to *Chapter 4, Setting up the Policy Store on Solaris* on page 75.
   - To configure an NDS policy store on Novell, refer to *Chapter 5, Setting up a Policy Store on Novell Netware* on page 91.
5. Import the SiteMinder 3.6 SP 1 policy store data into all of the SiteMinder 4.1 policy stores using `smobjimport` (version 4.1), as described in *Importing Policy Store Data* on page 204.
6. If you are using an ODBC database as a user directory, migrate the queries to the SiteMinder 4.1 policy store as described in *Upgrading an ODBC User Directory Schema* on page 205.
7. If you are using certificate mapping, upgrade the certificate mapping as described in *Upgrading Certificate Mapping* on page 208.

8. Upgrade the Web Agent(s), and during the configuration, specify the SiteMinder 4.1 Policy Server as the Policy Server, as described in *Upgrading Web Agents, Cookie Providers and Advanced Authentication Schemes* on page 218.

   Note: If this Web Agent provides additional services, such as serving as the cookie providers, or providing advanced authentication to SiteMinder 4.1, upgrade these services, as well.

9. If you changed the Agent name, IP address, or Shared Secret when configuring the Web Agent(s) for SiteMinder 4.1, reconfigure the Web Agent in the SiteMinder Policy Server User Interface, as described in the *SiteMinder Policy Server Operations Guide*.
10. Enable the SiteMinder 4.1 Web Agent.
11. If you have a SiteMinder 3.6 Reports Server installed, upgrade the Reports Server as described in *Upgrading the Reports Server* on page 228.
12. Optionally, remove the SiteMinder 3.6 policy store data and schema as described in *Removing the SiteMinder 3.6 Policy Store* on page 230.

Note: If you have custom components in your SiteMinder deployment, contact your Netegrity Professional Services representative for information on how to upgrade these components.

Removing a Policy Server From the SiteMinder Environment

To remove a Policy Server from a SiteMinder 3.6 environment that includes multiple Policy Servers, all of the Web Agents that communicate with that Policy Server must be configured to communicate with a different SiteMinder 3.6 Policy Server. Pointing the Web Agents to another Policy Server allows them to continue protecting resources during the upgrade procedure.

To remove a Policy Server from an environment that uses only one Policy Server, you must shut down the Web Servers hosting the Web Agents. This ensures that no unauthorized user can access the resources while you upgrade the Policy Server.

Configuring a Netscape or Apache Web Agent

To configure a Netscape or Apache Web Agent to point to a different Policy Server, you must modify the `WebAgent.conf` file. The `WebAgent.conf` file contains the configuration settings for your Web Agent, including the IP address and ports of the Policy Server with which the Web Agent communicates.

Note: For detailed information about configuring the `WebAgent.conf` file, refer to the *SiteMinder Agent Operations Guide*.

To configure a Netscape or Apache Web Agent to use another Policy Server:

1. Open the `WebAgent.conf` file:

   - For NT, the default location is <*netscape_installation*>\\<*serverlocation*>\https-<*hostname*>\config

     where <*netscape_installation*> is the installed location of Netscape, <*serverlocation*> is the installed location of the Netscape Web servers (`server4` for iPlanet Web Servers, `suitespot` for Netscape Enterprise Servers) and <*hostname*> is the name of the server.

     For example,

     ```
     C:\Netscape\Server4\https-myserver\config
     ```

   - For UNIX, the default location is /<*server*>/<*confdirectory*>

     where <*server*> is the installed location of Netscape or Apache Web server on which the Web Agent is installed, and <*confdirectory*> is the name of the directory where that Web server’s configuration files are stored.

     For example:

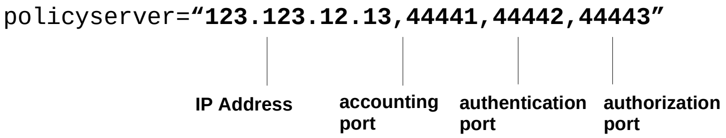
     - For Apache:

       ```
       /usr/apache/conf
       ```

     - For Netscape:

       ```
       /usr/netscape/server4/https-myserver/config
       ```

2. Edit the `policyserver` line to reflect the IP address and port numbers of the SiteMinder 3.6 Policy Server to which the Web Agent will point. For example,



```
policyserver="123.123.12.13,44441,44442,44443"
```

3. If multiple Policy Servers are listed, delete the entire `policyserver` line that corresponds to the Policy Server that you are upgrading first.
4. Save `WebAgent.conf`.
5. Stop and start the Web Server to apply the changes.

Configuring an IIS Web Agent

To configure an IIS Web Agent to point to a new Policy Server, you must configure the new Policy Server in the IIS Web Agent Management Console. The IIS Web Agent Management Console allows you to modify the configuration settings for your Web Agent, including the IP address and ports of the Policy Server with which the Web Agent communicates.

Note: For detailed information about using the IIS Web Agent Management Console, refer to the *SiteMinder Agent Operations Guide*.

To configure an IIS Web Agent to use another Policy Server:

1. Access the Web Agent IIS Management Console from the Start menu by selecting **Programs** | **SiteMinder** | **SiteMinder Web Agent NT IIS Management Console**.
2. In the Console, select the **Servers** tab to move it to the front.
3. In the Policy Server list, select the Policy Server entry you want to remove and click **Remove**.

   SiteMinder removes the Policy Server from the list.
4. Click **OK** to save your changes and exit the Console.
5. From the Services control panel, stop and restart the Web server.

Exporting SiteMinder 3.6 Policy Store Data

To upgrade to a SiteMinder 4.1 policy store and retain the data from SiteMinder 3.6, you must first export the data from the 3.6 policy store. The `smobjexport` utility allows you to export policy store data to a text file in SiteMinder Data Interchange Format (SMDIF). SMDIF standardizes SiteMinder data so you can later import the exported data to a policy store in a different version of SiteMinder.

☞ **Note:** Although you must import policy data using `smbojimport` tool included with SiteMinder 4.1, you must export the data using `smobjexport` tool included with SiteMinder 3.6.

SiteMinder provides a number of arguments for `smobjexport` that enable you to supply information required to export the policy store data. For a complete listing of `smobjexport` arguments, refer to *Chapter 11, Policy Server Tools* on page 235.

☞ **Note:** If arguments contain spaces, use double quotes around the entire argument. For example, if the name of the SiteMinder Administrator is *SiteMinder Admin*, the argument for `smobjexport` would be **`“-dSiteMinder Admin”`**.

To export data from a policy store:

1. From the command line, access the directory in which `smobjexport` is located.

   - For NT, `smobjexport` is located in <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     c:\Program Files\Netegrity\SiteMinder\Bin
     ```

   - For UNIX, `smobjexport` is located in <*siteminder_installation*>`/siteminder/bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     $HOME/siteminder/bin
     ```

2. Export the policy store data by executing `smobjexport` and its appropriate arguments as follows:

   ```
   smobjexport -o<filename>
   ```

   For example,

   ```
   smobjexport -opstore.txt
   ```

   Tip: From the command line, specify **`smobjexport -help`** to view the syntax and arguments available for **`smobjexport`**.

3. Create a backup of the exported file.

Upgrading the Policy Server to SiteMinder 4.1

Once you have removed a Policy Server from your SiteMinder environment by removing it from the list of Policy Servers with which the SiteMinder 3.6 Web Agents communicate, you can upgrade your Policy Server.

Important: If you want to remove SiteMinder 3.6 policy store data stored in an LDAP directory, you must remove the policy store data before you upgrade all of the SiteMinder 3.6 Policy Servers to SiteMinder 4.1. You must use the SiteMinder 3.6 Policy Server tools to remove the policy store data. For instructions on removing policy store data from an LDAP directory, refer to *Removing the 3.6 Policy Store From an LDAP Directory* on page 230.

Upgrading the Policy Server on NT

Before upgrading the Policy Server, create a backup copy of the policy store data by exporting it, as described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198.

To upgrade the Policy Server:

1. Exit all applications that are running.
2. Insert the SiteMinder 4.1 CD-ROM into the drive.

3. Run the SiteMinder Policy Server setup program:

   a. Navigate to the `nt` folder on the SiteMinder CD-ROM.

   b. Double-click `PolicyServer-4.1-NT.exe`.

      Setup verifies the following prerequisites:

      - You are logged into an account with local administrator privileges.
      - NT 4.1 with Service Pack 3, 4, or 5 is installed.
      - IIS 3.x or later, iPlanet Web Server Enterprise Edition 4.1 or later, or Netscape Enterprise Web Server 3.5.1 or later is installed.
      - The computer has necessary free disk space.

   SiteMinder prepares the Setup Wizard which will guide you through installing the Policy Server. This step may take a few moments.

4. Read the Welcome message and click **Next**.

5. Read the Software License Agreement and click **Yes** if you accept the agreement.

6. Read the Release Notes, then click **Next**.

7. In the **User Information** dialog box, enter your name and company name and click **Next**.

8. In the **Policy Store Data Upgrade Reminder** dialog box, select **Continue with Upgrade** if you have exported your SiteMinder 3.6 policy store data and created a backup.

   Note: If you have not exported your SiteMinder 3.6 data, exit the upgrade and follow the procedure described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198.

   The upgrade detects the Web servers installed on your machine and displays them in the **Configure Additional Web Servers** dialog box.

9. In the **Configure Additional Web Servers** dialog box, select any additional Web servers to configure for the Policy Server, then click **Next**.

Note: If there is a check mark to the right of a Web server in the list, that Web server has already been configured for the Policy Server.

10. In the **Preserve Server Settings Options** dialog box, select one of the following:

    - **Preserve existing settings**—Retains Policy Server settings that were configured using the SiteMinder Policy Server Management Console.

      To complete the upgrade after selecting **Preserve existing settings**:

      a. In the **Start Copying Files** dialog box, click **Next**.

      b. In the **Setup Complete** dialog box, click **Finish**.

    - **Install default settings**—Replaces the Policy Server settings that were configured using the SiteMinder Policy Server Management Console. The existing SiteMinder policy store, encryption key, and Super User account password are preserved.

      To complete the upgrade after selecting **Install default settings**:

      a. In the **Select Program Folder** dialog box, select the program folder and click **Next**.

      b. In the **Setup Complete** dialog box, click **Finish**.

11. If prompted, reboot your computer.

Upgrading the Policy Server on Solaris

Before upgrading the Policy Server, create a backup copy of the policy store data by exporting it, as described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198.

To upgrade a Policy Server on Solaris:

1. Log in to the account where the Policy Server is installed.
2. Copy `smps-4.1-so.tar` from the SiteMinder CD-ROM.

3. Untar the `smps-4.1-so.tar` file.
4. Change to the `smps-install` directory.
5. Run the `./smps-upgrade` shell script.

   The upgrade script checks to see if the required/recommended patches are installed and prepares the Release Notes.

6. Press ENTER to read the Release Notes for important information about upgrading to SiteMinder 4.1.
7. Enter **`y`** to confirm that you want to continue with the upgrade.

   The upgrade script displays the prerequisites for installing SiteMinder Policy Server 4.1.

8. Specify a directory path under which the SiteMinder upgrade directory will be created or press ENTER to use your current location.
9. To view the License Agreement, press ENTER when prompted.

   The installation script displays the License Agreement.

10. If you have read the License Agreement and agree with the terms, enter **`y`** to continue the installation.
11. If you have exported your SiteMinder 3.6 policy store data, enter **`y`** to continue with the upgrade.

Note: If you have not exported your SiteMinder 3.6 data, exit the upgrade and follow the procedure described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198.

The upgrade script creates a `siteminder` directory in the specified location. For example, if you specify `/opt`, then this product will be installed in `/opt/siteminder`. If the `siteminder` installation directory already exists make sure that the account you logged into has proper file permissions to create a subdirectory. If available disk space is found, the installation extracts the files to the chosen directory. This may take a few moments.

12. Enter the path to the Netscape server directory:

    <netscape_installation>/*<server_directory>*

    where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape Web servers.

    For example,

    ```
    /usr/netscape/server4
    ```

    The upgrade script searches the Netscape Server directory and displays a list of all Web servers that are configured for the SiteMinder Policy Server.

13. Select the Web server(s) to restart by doing the following:

    - Enter the corresponding number for the Web server that you want to restart, then press ENTER.
    - Press ENTER to restart all of the Web servers displayed in the list.

    The upgrade script stops and starts the specified Web server(s).

14. Specify whether or not you want to restart additional Web servers by entering one of the following:

    - If you want to restart additional Web servers, specify **y**, then repeat steps 11 to 13 of this procedure.
    - If you have restarted all of the Web servers configured for the SiteMinder Policy Server, specify **n**.

The upgrade script displays a message that the upgrade is complete.

Importing Policy Store Data

Once you have exported the policy store data from SiteMinder 3.6, and prepared a new policy store, you can import the exported policy store data.

☞ **Note:** You must import the policy store data using the `smobjimport` tool included with SiteMinder 4.1. `Smobjimport` is installed during the upgrade procedure.

To import the policy store data, use the `smobjimport` tool and specify the following arguments:

Argument	Description
-36	This flag indicates that the file being imported is in version 3.6 format.
-i<*file-name*>	Specifies the path and filename of the input file.This should match the name of the file you exported from the old policy store.

To import the policy store data:

1. If you have not already done so, create a new policy store, as described in one of the following chapters:
   - For NT, *Chapter 3, Setting up the Policy Store on NT* on page 47
   - For Solaris, *Chapter 4, Setting up the Policy Store on Solaris* on page 75
   - For NDS, *Chapter 5, Setting up a Policy Store on Novell Netware* on page 91
2. From the command line, access the directory in which `smobjimport` is located.
   - For NT, `smobjimport` is located in <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder, such as:

     ```
     c:\Program Files\Netegrity\SiteMinder\Bin
     ```

- For UNIX, `smobjimport` is located in <*siteminder_installation*>`/bin`

  where <*siteminder_installation*> is the installed location of SiteMinder, such as:

  ```
  /$HOME/netegrity/siteminder/bin
  ```

3. Import the policy store data by executing `smobjimport` and the following arguments:

   `smobjimport -36 -i<`*filename*`>`

   For example,

   `smobjimport -36 -ipstore.txt`

☞ **Note:** Do not specify the **`-f`** switch with `smobjimport` when you import the SiteMinder 3.6 policy store data. Specifying the **`-f`** switch may overwrite data that you imported when you set up the policy store.

Upgrading an ODBC User Directory Schema

To use a proprietary ODBC database as a user directory for authentication and/or authorization, SiteMinder 3.6 uses a file (`smdsquery.ini`) which allows it to access user and user group information. The `smdsquery.ini` file is comprised of a number of SQL queries, which tell SiteMinder how to find information within the ODBC database.

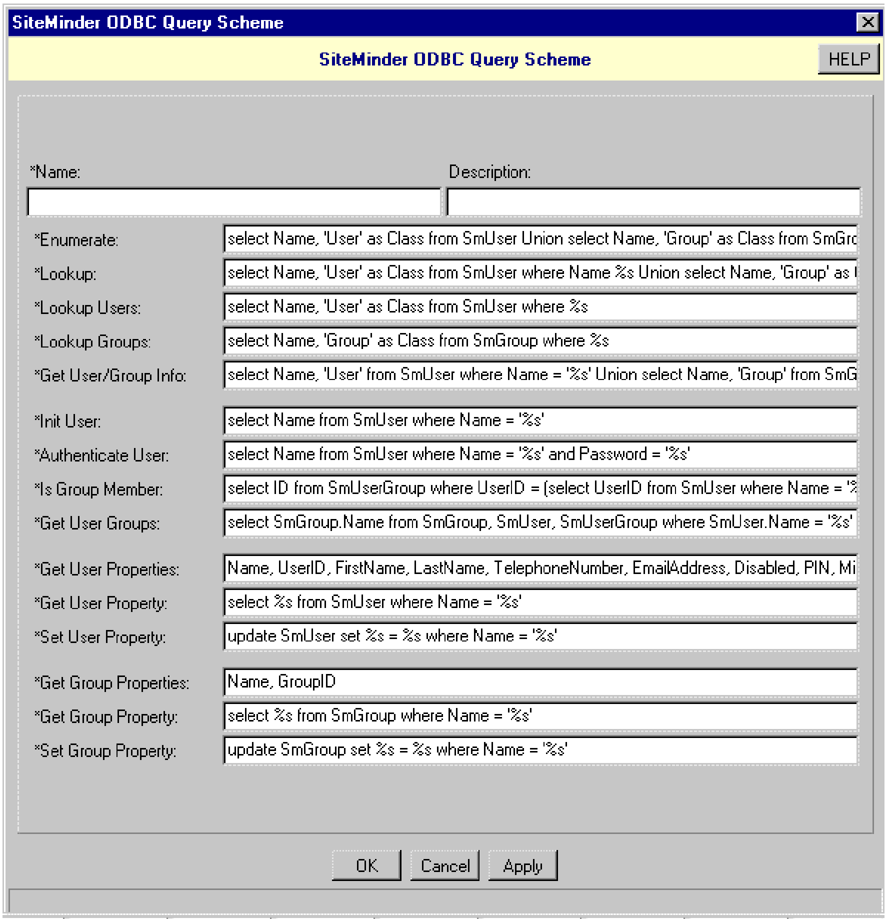
In the SiteMinder 4.1 Policy Server User Interface, you can easily create the same type of SQL queries to access user and user group information. The queries are stored directly in the policy store instead of `smdsquery.ini`. (SiteMinder 4.1 no longer uses `smdsquery.ini`.)

To use the SQL queries created in SiteMinder 3.6 in SiteMinder 4.1, you must migrate the queries stored in `smdsquery.ini` to the policy store using the SiteMinder Policy Server User Interface.

To migrate queries from a 3.6x to a 4.1 policy store:

1. In SiteMinder 4.1, log in to the SiteMinder Policy Server User Interface.
2. From the menu bar, select **Edit | System Configuration | Create ODBC Query Scheme**.

The system displays the **SiteMinder ODBC Query Scheme** dialog box as shown below. Mandatory fields are indicated by an asterisk preceding the field name.



*Name:	
Description:	
*Enumerate:	select Name, 'User' as Class from SmUser Union select Name, 'Group' as Class from SmGro
*Lookup:	select Name, 'User' as Class from SmUser where Name %s Union select Name, 'Group' as
*Lookup Users:	select Name, 'User' as Class from SmUser where %s
*Lookup Groups:	select Name, 'Group' as Class from SmGroup where %s
*Get User/Group Info:	select Name, 'User' from SmUser where Name = '%s' Union select Name, 'Group' from SmG
*Init User:	select Name from SmUser where Name = '%s'
*Authenticate User:	select Name from SmUser where Name = '%s' and Password = '%s'
*Is Group Member:	select ID from SmUserGroup where UserID = (select UserID from SmUser where Name = '%
*Get User Groups:	select SmGroup.Name from SmGroup, SmUser, SmUserGroup where SmUser.Name = '%s'
*Get User Properties:	Name, UserID, FirstName, LastName, TelephoneNumber, EmailAddress, Disabled, PIN, Mi
*Get User Property:	select %s from SmUser where Name = '%s'
*Set User Property:	update SmUser set %s = %s where Name = '%s'
*Get Group Properties:	Name, GroupID
*Get Group Property:	select %s from SmGroup where Name = '%s'
*Set Group Property:	update SmGroup set %s = %s where Name = '%s'

3. In the **Name** field, enter a name for the new query.

4. In the **Description** field, enter a brief description of the new query.

5. With the **SiteMinder ODBC Query Scheme** dialog box open, open `smdsquery.ini` in another window.

    ☞ **Note:** `Smdsquery.ini` is preserved when the SiteMinder Policy Server is upgraded.

    `Smdsquery.ini` is located in one of the following locations:

    - For NT, <*siteminder_installation*>`\Bin`

      where <*siteminder_installation*> is the installed location of SiteMinder.

      For example,

      `C:\Program Files\Netegrity\SiteMinder\Bin`

    - For UNIX, <*siteminder_installation*>`/bin`

      where <*siteminder_installation*> is the installed location of SiteMinder.

      For example,

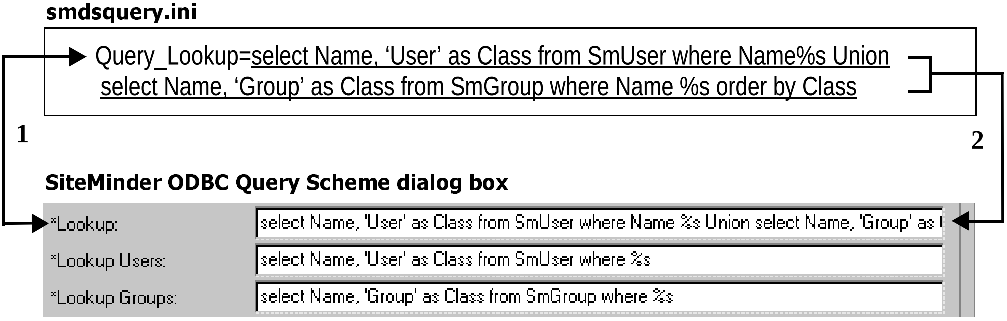
      `/usr/siteminder/Bin`

6. In `smdsquery.ini`, locate the line that begins "**Query_Enumerate=**" and copy all of the text following the equal sign (=) to the end of the line.

7. In the **SiteMinder ODBC Query Scheme** dialog box, place your cursor in the **Enumerate** field and paste the text you copied from `smdsquery.ini`.

8. Continue copying the queries from `smdsquery.ini` and pasting them into the corresponding field in the **SiteMinder ODBC Query Scheme** dialog box until you have populated all of the required fields.

    In `smdsquery.ini`, each field name is preceded by "**Query_**". For example, in `smdsquery.ini`, **Lookup** appears as "**Query_Lookup=**". To copy the query into the **SiteMinder ODBC Query Scheme** dialog box, copy all of the text on the current line following the equal sign (=) and paste it into the Lookup field (refer to the following figure).



smdsquery.ini

```
Query_Lookup=select Name, ‘User’ as Class from SmUser where Name%s Union
 select Name, ‘Group’ as Class from SmGroup where Name %s order by Class
```

SiteMinder ODBC Query Scheme dialog box

*Lookup:	select Name, 'User' as Class from SmUser where Name %s Union select Name, 'Group' as t
*Lookup Users:	select Name, 'User' as Class from SmUser where %s
*Lookup Groups:	select Name, 'Group' as Class from SmGroup where %s

1. The **Lookup** field is represented in **smdsquery.ini** as **Query_Lookup=.**
2. The underlined text represents the information you copy, then paste into the **Lookup** field.

9. Click **OK** to save the new query and return to the SiteMinder Policy Server User Interface.

Upgrading Certificate Mapping

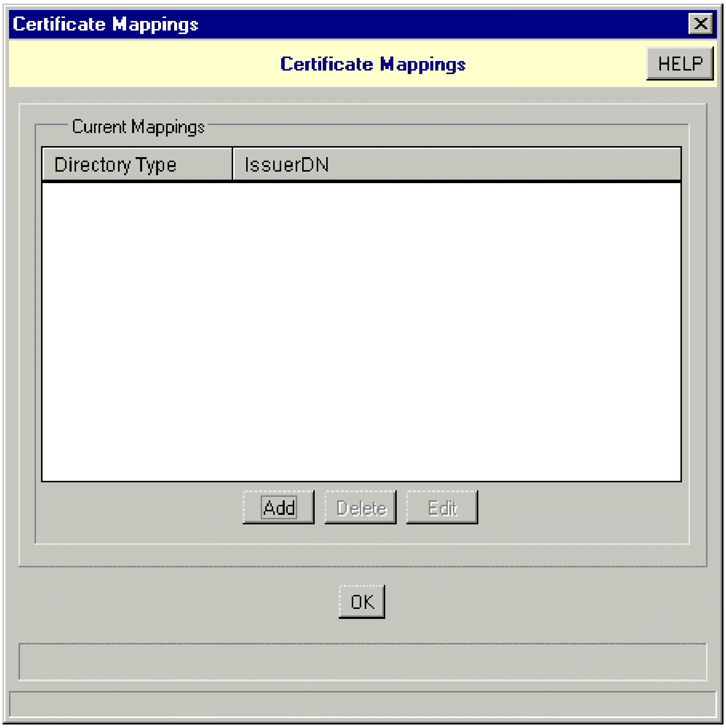
Certificate mapping is required for all authentication schemes that involve certificates. It links certificate information to a user entry in a user directory. Certificate Mapping defines how data in the certificate is mapped to form a user Distinguished Name (DN). This user DN is then used by the Policy Server to authenticate the user.

In previous versions of SiteMinder, Certificate Mapping was stored in the `smcertmap.ini` file. In SiteMinder 4.1, Certificate Mapping is configured in the Policy Server User Interface and stored in the policy store. To use Certificate Mappings configured prior to SiteMinder 4.1, you must complete the following procedure:

To migrate certificate mapping from SiteMinder 3.6x to 4.1:

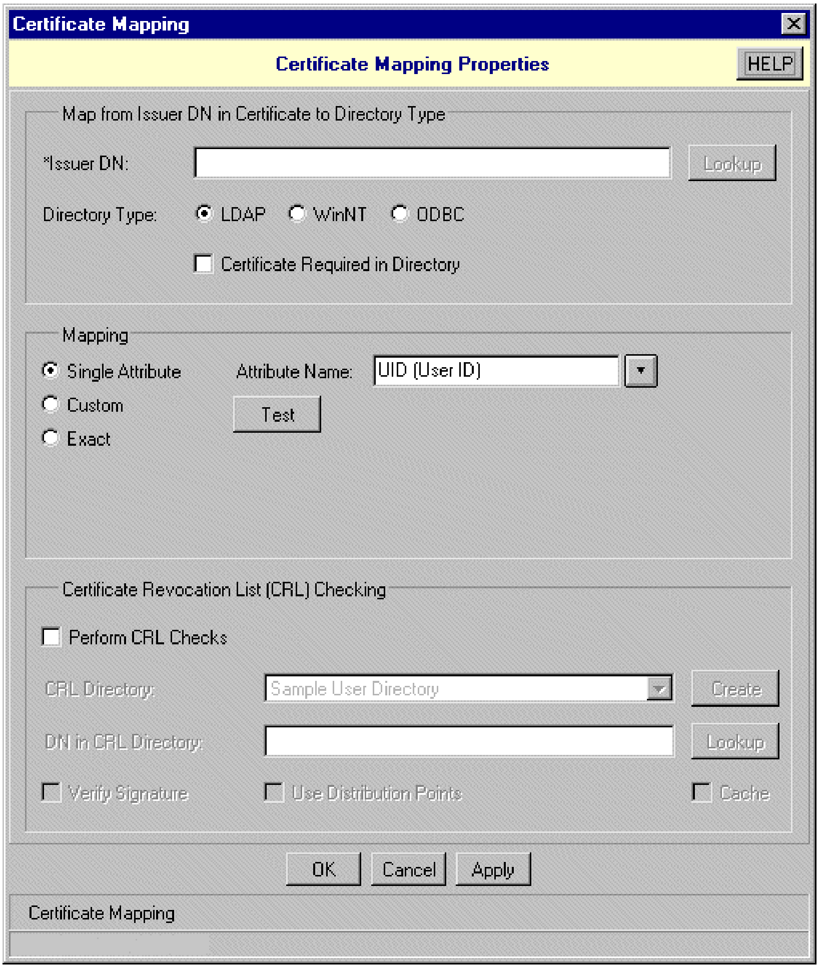
1. In SiteMinder 4.1, log in to the SiteMinder Policy Server User Interface.
2. From the menu bar, select **Advanced | Certificate Mapping**.

The system displays the **Certificate Mappings** dialog box as shown below.



3. Click **Add**.

   SiteMinder displays the **Certificate Mapping Properties** dialog box:



Certificate Mapping

Certificate Mapping Properties

Map from Issuer DN in Certificate to Directory Type

*Issuer DN:

Directory Type: ● LDAP ○ WinNT ○ ODBC

□ Certificate Required in Directory

Mapping

● Single Attribute ○ Custom ○ Exact

Attribute Name: UID (User ID)

Certificate Revocation List (CRL) Checking

□ Perform CRL Checks

CRL Directory: Sample User Directory

DN in CRL Directory:

□ Verify Signature □ Use Distribution Points □ Cache

Certificate Mapping

4. With the **SiteMinder Certificate Mapping Properties** dialog box open, open `smcertmap.ini` in another window.

Note: `Smcertmap.ini` is preserved when the SiteMinder Policy Server is upgraded.

`Smcertmap.ini` is located in one of the following locations:

- For NT, <*siteminder_installation*>`\Bin`

  where <*siteminder_installation*> is the installed location of SiteMinder.

  For example,

  `C:\Program Files\Netegrity\SiteMinder\Bin`

- For UNIX, <*siteminder_installation*>`/bin`

  where <*siteminder_installation*> is the installed location of SiteMinder.

  For example,

  `/usr/siteminder/bin`

5. In `smcertmap.ini`, locate the line that begins “**IssuerDN=**” and copy all of the text following the equal sign (=) to the end of the line. Do not include the initial or final quotation marks (“ ”).

   The following is an example of an IssuerDN:

   ```
   IssueDN=“CN=VeriSign Class 1 CA Individual Subscriber-Persona Not Validated,
   OU=\“www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98\”,OU=VeriSign Trust
   Network, O=\”VeriSign, Inc.\”
   ```

6. In the **Certificate Mapping Properties** dialog box, place your cursor in the **IssuerDN** field and paste the text you copied from `smcertmap.ini`.
7. In the `smcertmap.ini` file, locate the line that begins “**Directory=**” and note the directory type specified.
8. In the **Directory Type** field in the **Certificate Mapping Properties** dialog box, select the directory type that corresponds to the directory type in `smcertmap.ini`.

☞ **Note:** Certificate mapping using an ODBC database is a new feature in SiteMinder 4.1. If you are upgrading existing certificate mapping, you should not select ODBC.

9. In the **Mapping** group box, select one of the following mapping options:

   - **Single Attribute**—Select this option if you are mapping a single attribute from the certificate to the user directory. You should select this option if you specified a value in the “**CertFrom=**” field in `smcertmap.ini.`

     Refer to *Configuring Single Attribute Certificate Mapping* on page 212 for instructions on configuring single attribute mapping.

   - **Custom**—Select this option if you are using complex multiple attribute mapping. You should select this option if you specified values in the “**MapToLDAP=**” field in `smcertmap.ini.`

     Refer to *Configuring Custom Certificate Mapping* on page 215 for instructions on configuring custom mapping.

   - **Exact**—Select this option if the entire subject DN of the certificate maps exactly to the DN in the user directory. You should select this option if you specified a full DN in the “**FullDN=**” field in `smcertmap.ini.`

     Refer to *Configuring Exact Certificate Mapping* on page 216 for instructions on configuring exact mapping.

10. In the `smcertmap.ini` file, locate the line that begins “**CRLCheck=**”, then complete one of the following:

    - If “**CRLCheck=**” is set to **false**, then CRL checking is not enabled and you do not need to specify any more information. Proceed to step 11 to complete the upgrade procedure.

    - If “**CRLCheck=**” is set to **true,** then CRL checking is enabled and you must configure the information in the **Certificate Revocation List (CRL) Checking** group box before completing the upgrade procedure. Refer to *Upgrading CRL Checking* on page 217 for instructions on upgrading CRL checking *before* proceeding to step 11.

11. Click **OK** to save the new certificate map and return to the SiteMinder Policy Server User Interface.

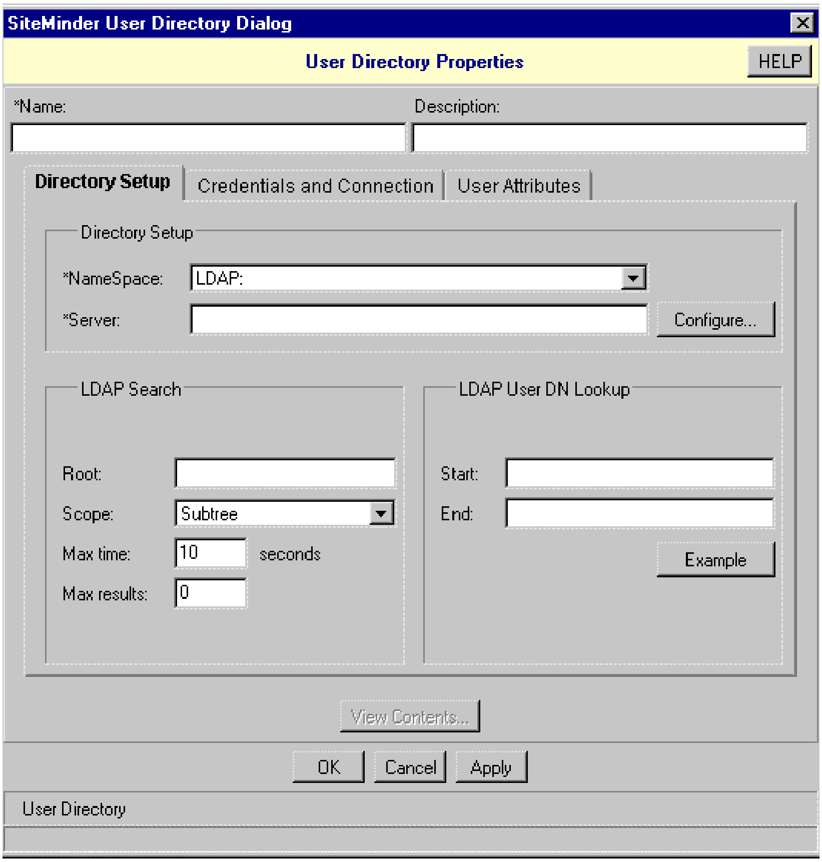
Configuring Single Attribute Certificate Mapping

1. Complete steps 1-8 of the procedure described in *Upgrading Certificate Mapping* on page 208.

2. Select the **Single Attribute** mapping option in the **Mapping** group box.
3. From the **Attribute Name** drop-down list, select the attribute that matches the value specified in **CertFrom** field in `smcertmap.ini`.

   This attribute is the attribute in the certificate that maps to an attribute in the user directory.

   If you are using an NT directory for certificate authentication, you must map the certificate attribute to the UID. If you are using an LDAP directory, the certificate attribute maps to the values specified in the **Start** and **End** fields in the **User Directory Properties** dialog box:



*NameSpace: LDAP:

*Server:

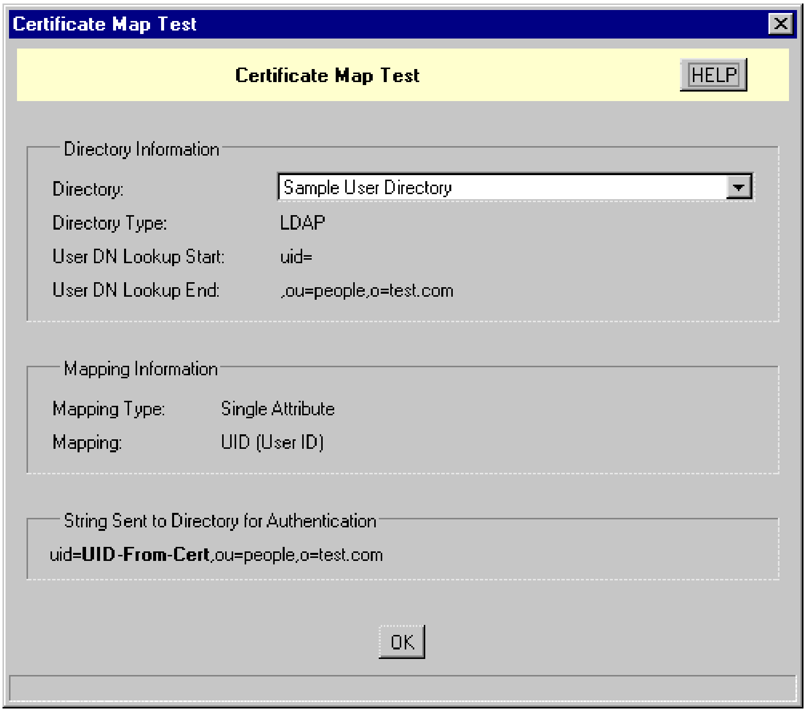
Scope: Subtree

Max time: 10 seconds

Max results: 0

4. Once you have specified an attribute, click **Test**.

SiteMinder displays the **Certificate Map Test** dialog box:



Directory Information

Directory: Sample User Directory

Directory Type: LDAP

User DN Lookup Start: uid=

User DN Lookup End: ,ou=people,o=test.com

Mapping Information

Mapping Type: Single Attribute

Mapping: UID (User ID)

String Sent to Directory for Authentication

uid=**UID-From-Cert**,ou=people,o=test.com

5. In the **Certificate Map Test** dialog box, select the user directory that you are using for certificate authentication from the **Directory** drop-down list, then click **OK**.

6. Complete one of the following:

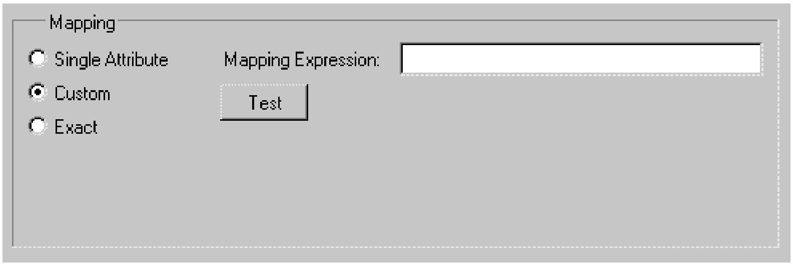
   - Upgrade CRL checking as described in *Upgrading CRL Checking* on page 217.
   - Click **OK** to return to the **Certificate Mappings** dialog box, if you have completed your certificate mapping upgrade.

Configuring Custom Certificate Mapping

1. Complete steps 1-8 of the procedure described in *Upgrading Certificate Mapping* on page 208.

2. Select the **Custom** mapping option in the **Mapping** group box.

   The **Mapping** group box changes, as shown below:



Mapping

○ Single Attribute

● Custom

○ Exact

Mapping Expression:

3. In `smcertmap.ini`, locate the line that begins “**MapToLDAP=**” and copy all of the text following the equal sign (=) to the end of the line.

4. In the **Mapping Expression** field**,** paste the text you copied from `smcertmap.ini`.

5. Click **Test**.

   SiteMinder displays the **Certificate Map Test** dialog box.

6. In the **Certificate Map Test** dialog box, select the user directory that you are using for certificate authentication from the **Directory** drop-down list, then click **OK**.

7. Complete one of the following:

   - Upgrade CRL checking as described in *Upgrading CRL Checking* on page 217.

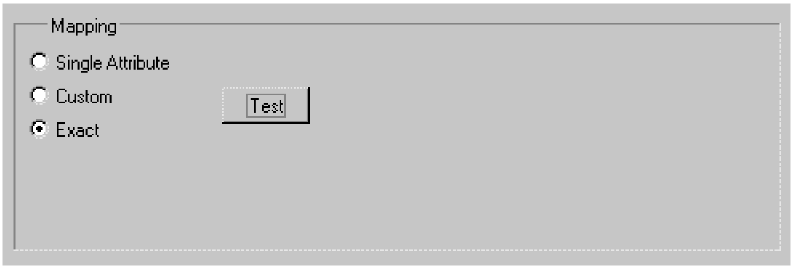
   - If you have completed your certificate mapping upgrade, click **OK** to return to the **Certificate Mappings** dialog box.

Configuring Exact Certificate Mapping

1. Complete steps 1-8 of the procedure described in *Upgrading Certificate Mapping* on page 208.

2. Select the **Exact** mapping option the **Mapping** group box.

   SiteMinder displays changes the **Mapping** group box as shown below:



Mapping

○ Single Attribute

○ Custom

● Exact

3. Click **Test**.

   SiteMinder displays the **Certificate Map Test** dialog box.

4. In the **Certificate Map Test** dialog box, select the user directory that you are using for certificate authentication from the **Directory** drop-down list, then click **OK**.

5. Complete one of the following:

   - Upgrade CRL checking as described in *Upgrading CRL Checking* on page 217.

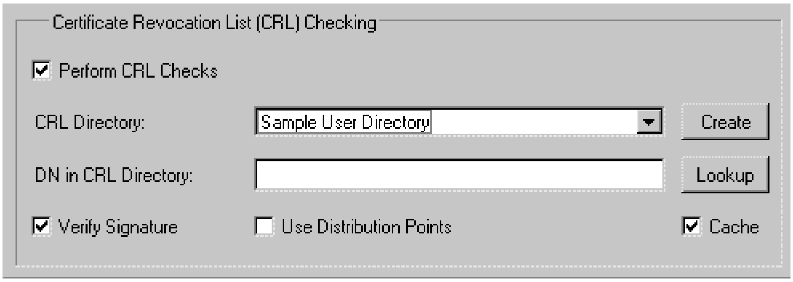
   - If you have completed your certificate mapping upgrade, click **OK** to return to the **Certificate Mappings** dialog box.

Upgrading CRL Checking

1. Complete steps 1-9 in the procedure described in *Upgrading Certificate Mapping* on page 208.

2. Select the **Perform CRL Checks** check box.

   The fields within the **Certificate Revocation List (CRL) Checking** group box are activated:



Certificate Revocation List (CRL) Checking

☑ Perform CRL Checks

CRL Directory: Sample User Directory

DN in CRL Directory:

☑ Verify Signature ☐ Use Distribution Points ☑ Cache

3. In the **CRL Directory** field, select the directory where the CRL is located.

4. Optionally, if the DN of the CA in the CRL directory differs from the IssuerDN specified in the certificate, specify that DN in the **DN in CRL Directory** field.

5. Locate the **VerifySignature** field in `smcertmap.ini`.

   - If **VerifySignature=true,** select the **Verify Signature** check box in the **Certificate Revocation List (CRL) Checking** group box.

   - If **VerifySignature=false,** make sure the **Verify Signature** check box in the **Certificate Revocation List (CRL) Checking** group box is not selected.

6. Locate the **UseDistPts** field in `smcertmap.ini`.

   - If **UseDistPts=true,** select the **Use Distribution Points** check box in the **Certificate Revocation List (CRL) Checking** group box.

   - If **UseDistPts=false,** make sure the **Use Distribution Points** check box in the **Certificate Revocation List (CRL) Checking** group box is not selected.

7. Locate the **CacheCRLs** field in `smcertmap.ini`.
   - If **CacheCRLs=true,** select the **Cache** check box in the **Certificate Revocation List (CRL) Checking** group box.
   - If **CacheCRLs=false,** make sure the **Cache** check box in the **Certificate Revocation List (CRL) Checking** group box is not selected.
8. Click **OK** to save the new certificate map and return to the **Certificate Mappings** dialog box.

Upgrading Web Agents, Cookie Providers and Advanced Authentication Schemes

Once you have upgraded and configured a SiteMinder 4.1 Web Agent, it can no longer communicate with a SiteMinder 3.6 Policy Server. However, it can communicate with a SiteMinder 3.6 SP 2 Policy Server (refer to *Maintaining Single Sign-on Between 3.6x and 4.1 Web Agents* on page 191).

☞ **Note:** If you want to configure the Web Agent that you are upgrading to perform Registration Services, you must install a servlet engine before completing the upgrade procedure. Refer to *Chapter 7, Installing Support for Registration Services* on page 109.

Upgrading Cookie Providers and Advanced Authentication Schemes

In SiteMinder 4.1, cookie providers, SSL credential collectors and forms credential collectors function as extensions of the Web Agents. By functioning as Web Agent components, they can receive dynamic Agent Key information from the Policy Server. Agent keys allow SiteMinder Web Agents, cookie providers, SSL credential collectors and forms credential collectors to encrypt and decrypt cookies containing SiteMinder information. All SiteMinder components must have the same Agent Key to share information stored in SiteMinder cookies. (Refer to the *SiteMinder Policy Server Operations Guide* for detailed information about Agent Keys.)

A SiteMinder 4.1 Web Agent can be configured to protect a resource in addition to functioning as a cookie provider, SSL credential collector, and forms credential collector, or perform a subset of these functions. A Web Agent can also be configured to perform just one of these functions.

Cookie providers, SSL collectors, and forms collectors are upgraded and configured like Web Agents. The following procedure upgrades a 3.6 Web Agent installed on IIS or Netscape for NT. If that Web Agent was installed with a cookie provider, SSL credential collector or forms credential collector, the additional components are automatically upgraded, as well.

You must complete the upgrade procedure, then configure the Web Agent for SiteMinder 4.1.

To upgrade Agents on NT:

1. Exit all applications that are running, then insert the SiteMinder CD-ROM.
2. Run the setup program:
   a. Navigate to the `nt` folder.
   b. Double-click `WebAgent-4.1-NT.exe`.
3. In the **Welcome** dialog box, click **Next**.
4. Read the Software License Agreement and click **Yes** if you accept the agreement.
5. Read the Release Notes, then click **Next**.

   The upgrade wizard locates and displays the SiteMinder 3.6 SP 1 Web Agents, cookie providers, SSL credential collector, and forms credential collectors installed on your machine.

6. In the **Select An Option** dialog box, specify whether or not you want to uninstall the displayed SiteMinder 3.6 components and continue with the upgrade by selecting one of the following:
   - **Continue with upgrade and uninstall the previous version**—Uninstalls previous versions of the Web Agents, cookie providers, SSL authentication schemes, and forms authentication schemes, then upgrades each uninstalled component.
   - **Abort the installation**—Leaves all of the SiteMinder 3.6 SP1 components and exits the upgrade procedure.
7. In the **Start Copying Files** dialog box, confirm that the displayed settings are correct, then click **Next**.

8. In the **Setup Complete** dialog box, confirm that you want to configure the Weg Agent when the upgrade is complete by ensuring the **Launch the Web Agent Configuration Wizard now** check box is selected.
9. Click **Finish**.

Note: You must configure all Web Agents, cookie providers, SSL authentication schemes and forms authentication schemes with the Web Agent Configuration Wizard before using them.

Configuring a Web Agent on NT

You must configure the Web Agent to communicate with a SiteMinder 4.1 Policy Server.

When you configure a Web Agent for IIS, the forms credential collector, and SSL credential collector are configured automatically.

When you configure a Web Agent for Netscape, the forms credential collector is configured automatically. However, you will be provided with the option to install any of the following:

- HTTP Basic over SSL
- Client Certificate
- Client Certificates + HTTP Basic over SSL
- Client Certificates or HTTP Basic

The ability to function as a cookie provider is now a feature of all Web Agents, however, you must manually configure this functionality in the Web Agent’s configuration. Refer to the *SiteMinder Agent Operations Guide*.

To configure an upgraded Web Agent:

1. If necessary, open the **Web Agent Configuration Wizard** by completing the following steps:
   a. Navigate to <*webagent_installation*>`\Config`

      where <*webagent_installation*> is the installed location of the SiteMinder Web Agent.

   b. Double click **Setup.exe**.

If you indicated that you wanted to configure the Web Agent after the installation, SiteMinder automatically opens the **Web Agent Configuration Wizard** for you.

2. In the **Select Web server(s)** dialog box, select the Web server(s) that you want to configure as Web Agents, then click **Next**.

   If you select multiple Web servers, the configuration wizard will configure the first Web server, then display the current settings for the next selected Web server.

☞ **Note:** If you are configuring a Web Agent for IIS, you can only select one IIS Web Server.

The **Web Agent Configuration for <yourserver> from version 3.6** displays the SiteMinder 3.6 configuration settings for the first Web server you selected.

3. In the **Web Agent Configuration for <*yourserver*>** dialog box, click **Next**.

! **Warning:** If you click **Configure**, all of the Web Agent configuration settings, including the settings you configured in the IIS Web Agent Management Console (for IIS) or `WebAgent.conf` (for Netscape) will be set to default. If you want to configure new settings, you must enable the Web Agent, as described in the *SiteMinder Agent Operations Guide*, before it protects your resources again.

4. In the **Primary Policy Server on <*yourserver*>** dialog box, complete the following:

   a. Enter the IP address of the SiteMinder 4.1 Policy Server that the Web Agent communicates with first. The default IP address is the address of the local machine.

   b. Click **Next**.

5. In the **Default Agent Name on <*yourserver*>** dialog box, complete the following:

   a. Enter the Agent Name (case-sensitive). The Agent name should match the Agent name specified in the SiteMinder Policy Server User Interface.

   b. Click **Next**.

6. In the **Default Cookie Domain on <*yourserver*>** dialog box, complete the following:

   a. Enter the domain of the Web server, using two periods. For example: `.myorg.org`. For additional information about cookie domains, refer to the *SiteMinder Agent Operations Guide*.

   b. Click **Next**.

7. If you are configuring a Web Agent on IIS , specify the following in the **IIS Proxy Username and Proxy Password on <*yourserver*>** dialog box:

   a. Specify the Proxy username and Password.

      The proxy account must have read or execute privileges to access the files protected by the Web Agent. The account's password must be at least 6 characters long.

   b. Confirm the Proxy password by entering it again in the **Confirm NT Password** field.

   c. Click **Next**.

8. In the **Shared Secret on <*yourserver*>** dialog box, complete the following:

   a. Enter an alphanumeric Secret that will be shared with the Policy Servers that communicate with the Agent. The Secret must consist of 6 to 24 alphanumeric characters and cannot contain spaces.

      Tip: Note the Shared Secret you entered. You will need this name when configuring the Agent in the SiteMinder Policy Server User Interface.

   b. Confirm the Shared Secret by entering it again in the **Confirm Shared Secret** field.

   c. Click **Next**.

9. If you are updating Agents on a Netscape Web Server, select one of the following options for advanced authentication in the **Select SSL Configuration on <https-yourserver>** dialog box, then click **Next**.
   - HTTP Basic over SSL
   - X509 Client Certificate
   - X509 Client Cert + HTTP BASIC over SSL
   - X509 Client Cert or HTTP Basic
   - This web agent will not be providing advanced authentication.
10. Complete one of the following:
    - If you have a servlet engine installed on the Web server, specify one of the following Registration Services options in the **Select Servlet Engine for Registration on <yourserver>** dialog box, then click **Next**:
      - If you want to use New Atlanta ServletExec for running Registration Services, select **New Atlanta Servlet Exec 2.2**.
      - If you want to use Allaire JRUN 2.3.3 for running Registration Services, select **Allaire JRUN 2.3.3**.
      - If you do not want to configure this Web Agent for Registration Services, select **This Web Agent will not be providing registration**.
    - If you do not have a servlet engine installed, proceed to step 10.

    ☞ **Note:** If you do not have a servlet engine installed on the Web server, the configuration wizard will not display the **Select Servlet Engine for Registration on <yourserver>** dialog box.

11. Confirm that the configuration settings are correct by clicking **Next**.

    SiteMinder examines the configuration settings, then displays the **Confirm Configuration Selections** dialog box.

    If you are configuring multiple Web Agents, SiteMinder displays the default settings for the next selected Web server. To modify the settings, click **Configure**, then repeat steps 3-10 of the configuration procedure.

12. Confirm that SiteMinder is configuring the correct Web server as a Web Agent, then click **Next**.
13. Click **Finish** to complete the configuration.

Upgrading Web Agents, Cookie Providers, and Credential Collectors on UNIX

To upgrade a SiteMinder 3.6 Web Agent on HP-UX or Solaris you must install the SiteMinder 4.1 Web Agent files, then configure the Web Agent.

When you configure a Web Agent, the forms credential collector is configured automatically. However, you will be provided with the option to install any of the following:

- HTTP Basic over SSL
- Client Certificate
- Client Certificates + HTTP Basic over SSL
- Client Certificates or HTTP Basic

The ability to function as a cookie provider is now a feature of all Web Agents, however, you must manually configure this functionality in the Web Agent's configuration. Refer to the *SiteMinder Agent Operations Guide*.

☞ **Note:** You must uninstall the SiteMinder 3.6 UNIX Web Agent before configuring the SiteMinder 4.1 Web Agent. If you do not uninstall the 3.6 Web Agent before configuring the 4.1 Web Agent, you will have to manually delete the 3.6 Web agent files after the configuration.

To upgrade a Web Agent on HP-UX or Solaris:

1. Navigate to the `hp` or `solaris` directory on the SiteMinder 4.1 CD-ROM:
2. Untar one of the following files:
   - For HP-UX, enter:

     ```
     tar -xvf smwa-4.1-hp.tar
     ```

   - For Solaris, enter:

     ```
     tar -xvf smwa-4.1-so.tar
     ```

3. Run **`./smwa-install`** from the Web Agent files directory.

   The installation script prepares the Release Notes.

4. Press ENTER to read the Release Notes for important information about upgrading SiteMinder 4.1.

5. Enter **`y`** to confirm that you want to continue with the upgrade.

6. Confirm that you have read the Software License Agreement, then enter **`Y`** to continue.

7. Specify a directory for installation.

   The default SiteMinder installation directory is `$HOME/netegrity/siteminder`.

   The Web Agent installation creates a subdirectory called `webagent` in the specified directory.

☞ **Note:** If you specified a directory called `webagent`, the installation does not create a new subdirectory. It installs the Web Agent in the directory you specified.

8. If you have a Netscape Web server on your system and want to configure a Web Agent for Netscape, enter **y** when asked if the system has a Netscape Web server.

☞ **Note:** If you are installing a Web Agent for Apache or you do not want to configure a Web Agent for Netscape at this point, enter **n**, then specify the Web server during configuration.

9. Complete one of the following:

   ■ If you specified **y** in step 8, enter the server root for Netscape:

   <netscape_installation>/*<server_directory>*

   where *<netscape_installation>* is the installed location of Netscape and <*server_directory*> is the installed location of the Netscape servers.

   For example:

   `/usr/netscape/server4`.

- If you specified **n** in step 8, proceed to step 11.

The upgrade program displays the installation path you entered. If you specified a Netscape server root, the upgrade program displays that, as well.

10. Enter **y** to confirm that the installation path and server root are correct.

    The installation is complete. You must configure the Web Agent before enabling it.

11. Optionally, uninstall the SiteMinder 3.6 Web Agent from the Web server, as described in *Chapter 8, Installing Web Agents* on page 135.

    You must uninstall the SiteMinder 3.6 UNIX Web Agent before configuring the SiteMinder 4.1 Web Agent. If you do not uninstall the 3.6 Web Agent before configuring the 4.1 Web Agent, you will have to manually delete the 3.6 Web agent files after the configuration.

To configure a Web Agent for Netscape or Apache:

1. Navigate to the `netegrity/siteminder/` directory.
2. Enter **`smwebagent-config`** to run the configuration script.
3. At the prompt to configure a Netscape Web server, enter one of the following:
   - To upgrade a Web Agent running on a Netscape Web server, specify **`Y,`** then complete the following steps:
     a. Enter the server root for Netscape. For example:

        `/usr/netscape/suitespot`

        The installation program displays the installation path and the server root you entered.

     b. Enter **y** to confirm that the installation path and server root are correct.
   - To upgrade a Web Agent running on an Apache Web server, specify **`n,`** then complete the following steps:
     a. Specify **Y** when asked if the system has an Apache Web server installed.

     b. Enter the server root for Apache. For example:

```
/usr/apache
```

The installation program displays the installation path and the server root you entered.

c. Enter **`y`** to confirm that the installation path and server root are correct.

The configuration script detects and lists the installed Web servers.

4. Select the appropriate configuration option by entering its corresponding number from the following list:

   ```
   (o)verwrite the configuration with new settings you
   specify

   (p)reserve settings but update the configuration

   (r)emove the configuration, or

   (l)eave the webserver configured as it is and cancel
   the configuration
   ```

5. Enter **`O`** to change the existing configuration settings.
6. Enter the IP address of a SiteMinder 4.1 Policy Server. The default provided is the IP address of the local machine.

   This server is the SiteMinder Policy Server that you want the Web server to connect and communicate with first (for example: **`123.123.12.12`**).
7. Enter the Web Agent Name (for example: *`www1`*). The default provided is the current Web server name.
8. Enter the cookie domain in which the Web Agent will be located.

   The domain must contain two periods, such as **`.myorg.org`**. For additional information about cookie domains, refer to the *SiteMinder Agent Operations Guide.*

9. Enter the Shared Secret that will be shared between the Web Agent and all Policy Servers that communicate with the Web Agent.

   The secret must be between 6 and 24 characters long.

☞ **Note:** If you try to cancel the installation while entering the Shared Secret (for example, if you press `Control + C`), at the next prompt enter **`stty echo`**, then press `ENTER` to restore the echo function. To provide optimal security, the echo function is off for this part of the install.

10. Confirm the Shared Secret by entering it again at the next prompt.

Tip: Take note of the secret. You will need this secret when configuring the Agent in the SiteMinder Policy Server User Interface.

11. Specify the authentication scheme you want to use by entering the number next to it in the displayed list.

    The authentication scheme determines how SiteMinder authenticates users. Refer to *The Policy Server Operations Guide* for more information about authentication schemes.

    The configuration script displays the values you entered.

12. If the configuration values are correct, enter **Y**.
13. Restart the Web server.

Upgrading the Reports Server

If you have a SiteMinder 3.6 Reports Server installed, complete the following procedure to upgrade it to SiteMinder 4.1.

To upgrade the Reports Server on NT:

1. From the SiteMinder 4.1 CD-ROM, run **`ReportsServer-4.1-NT.exe`** located in the `nt` folder.
2. In the **SiteMinder Reports Server NT** dialog box, click **Continue**.
3. Read the Welcome message and click **Next**.

4. Read the Software License Agreement and click **Yes** to accept the agreement.

5. In the **Reports Server Database Settings Options** dialog box, select one of the following:

   - **Preserve existing database settings**—Retains the existing Reports Server database settings. The upgrade installs the new functionality.

     In the **SiteMinder Policy Server Information** dialog box, complete the following to preserve the existing database settings:

     a. Enter the name of the system that the Policy Server was installed on, such as **`mymachine1`**.

     b. Enter the IP address of the Policy Server, such as **`123.123.12.12`**.

     c. Enter the SiteMinder Administration Server port number, such as **44444**, then click **Next**.

     d. In the **Setup Complete** dialog box, click **Finish**.

   - **Install new database settings**—Allows you to enter new Reports Server database settings. The setup will proceed with a upgrade of the new functionality. Complete the following:

     a. In the **SiteMinder Policy Server Information** dialog box, complete the following:

        1. Enter the name of the system that the Policy Server was installed on, such as **`mymachine1`**.

        2. Enter the I.P. address of the Policy Server, such as **`123.123.12.12`**.

        3. Enter the SiteMinder Administration Server port number, such as **44444**.

     b. Select the type of database that contains the logging information.

     c. If you selected Oracle Database, complete the fields in the **Oracle Database Information** dialog box:

        1. Enter the database service name in the **Service** field.

        2. Click **Next** to continue the installation.

  d. If you selected SQL Server database, enter the name of the SQL Server that hosts the database and click **Next**.

  e. In the **Setup Complete** dialog box, click **Finish**.

6. If prompted, reboot your computer.

Removing the SiteMinder 3.6 Policy Store

Upgrading your SiteMinder environment to SiteMinder 4.1 does not remove the SiteMinder 3.6 policy store. Once you have upgraded all of the SiteMinder 3.6 components to SiteMinder 4.1 and imported the SiteMinder 3.6 policy store data to a SiteMinder 4.1 policy store, you can optionally delete the SiteMinder 3.6 data and remove the policy store schema. Deleting the policy data frees system resources and ensures that the old policy data cannot be used.

☞ **Note:** Before permanently removing policy data, make sure that you have created a backup of the exported data.

Removing the 3.6 Policy Store From an LDAP Directory

SiteMinder provides a tool, called `smldapsetup`, which deletes SiteMinder 3.6 policy store data from an LDAP directory, generates an LDIF file containing information required to delete the schema, then executes the LDIF file.

☞ **Note:** For more information about `smldapsetup`, refer to *Chapter 11, Policy Server Tools* on page 235.

To remove policy store data from an LDAP directory, complete the following steps:

1. Export the SiteMinder 3.6 policy store data, as described in *Exporting SiteMinder 3.6 Policy Store Data* on page 198.

   Exporting the policy store creates a file that you can import into a SiteMinder 4.1 policy store and create a backup of your data.

2. Remove the SiteMinder 3.6 policy store data using the SiteMinder 3.6 `smldapsetup` tool, as described in *Removing SiteMinder 3.6 Policy Store Data* on page 231.

3. Complete steps 3-14 of the upgrade procedure described in *Upgrading SiteMinder in a Multiple Policy Server Environment* on page 186 or, complete steps 3-11 of the upgrade procedure described in *Upgrading SiteMinder in a Single Policy Server Environment* on page 192.
4. Remove the SiteMinder 3.6 schema, as described in *Removing the SiteMinder 3.6 Policy Store Schema* on page 232.

Removing SiteMinder 3.6 Policy Store Data

You must remove SiteMinder 3.6 policy store data before you can remove the SiteMinder 3.6 policy store schema. To remove the SiteMinder 3.6 policy store data, you must use the `smldapsetup` tool included with SiteMinder 3.6. Before upgrading your Policy Server (in a single Policy Server environment), or your final Policy Server (in a multiple Policy Server environment) to SiteMinder 4.1, complete the procedure below.

To remove the SiteMinder 3.6 LDAP policy store data:

1. In the SiteMinder 3.6 Policy Server Management Console, complete the following:
   a. Select the **LDAP** tab to bring it forward.
   b. Make sure the IP address and Root DN specified in the **Policy Store** group box correspond to the IP address and Root DN of the policy store from which you are removing data.
   c. Click **OK** to exit the Policy Server Management Console
2. Navigate to one of the following locations:
   - For NT, <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder.

     For example,

     ```
     C:\Program Files\Netegrity\SiteMinder\Bin
     ```

- For Solaris, <*siteminder_installation*>`/bin`

  where <*siteminder_installation*> is the installed location of SiteMinder.

  For example,

  ```
  /usr/netegrity/bin
  ```

3. Remove the policy store data from the SiteMinder 3.6 policy store by executing `smldapsetup remove` and the required arguments:

   ```
   smldapsetup remove -a<adminname> -b<adminpw>
   ```

   where **<*adminname*>** is the name of a SiteMinder administrator with privileges to modify the schema, and **<*adminpw*>** is the corresponding password.

   For example,

   ```
   smldapsetup remove -aAdmin -bpassword
   ```

☞ **Note:** Removing policy store data may take a few moments.

Removing the SiteMinder 3.6 Policy Store Schema

Once you have removed the SiteMinder 3.6 policy store data using the 3.6 `smldapsetup` tool, upgraded your Policy Server(s), and imported the policy store data to the SiteMinder 4.1 policy store, you can remove the SiteMinder 3.6 policy store schema.

To remove the SiteMinder 3.6 policy store schema:

1. Navigate to one of the following locations on the SiteMinder 4.1 CD-ROM:

   - For NT, `36-tools\nt`
   - For Solaris, `36-tools/solaris`

2. Complete one of the following:

   - For LDAP policy stores running on Netscape Directory Server 3.5.1 or later, execute the following command:

     ```
     smldapsetup ldgen smldap36deleteN30.ldif
     ```

- For LDAP policy stores running on iPlanet Directory Server 4.1 or later, execute the following command:

  ```
  smldapsetup ldgen smldap36deleteN40.ldif
  ```

Removing 3.6 Policy Stores, Logs, and Token Data from an ODBC Database

SiteMinder provides tools to remove the SiteMinder 3.6 policy store data, audit logs and token data from an ODBC database.

If you want to preserve SiteMinder 3.6 logs or token information, make sure you export that information prior to completing this procedure.

To remove the SiteMinder 3.6 policy store from an ODBC database:

1. Open a Command Prompt window and navigate to the one of the following locations on the SiteMinder 4.1 CD-ROM:
   - For NT, `3-6tools\nt`
   - For Solaris, `3-6tools/solaris`
2. Remove the policy store data and schema by completing the following:
   - For policy stores in Oracle databases, execute the following command:

     ```
     sm36_oracle_delete.sql
     ```

   - For policy stores in SQL databases, execute the following command:

     ```
     sm36_mssql_delete.sql
     ```

Chapter 11. Policy Server Tools

Overview

SiteMinder provides a number of tools to help administrators manage their SiteMinder environment. The following table explains the purpose of each tool:

Policy Server Tools:

Tool	Description
smobjexport	Used to export policy data from the SiteMinder policy store.
smobjimport	Used to import policy data into the SiteMinder policy store.
smldapsetup	Used to manage the SiteMinder policy store in an LDAP directory.
ODBC database tools	Used to remove SiteMinder policy store, token data, and log schemas from ODBC databases.
smpatchcheck	Checks to make sure all of the required/recommended patches are installed on your Solaris machine.
smreadclog	Used to read RADIUS log files generated by the Policy Server.
SiteMinder Test Tool	Used to interactively test SiteMinder policies without using a SiteMinder Agent.
SiteMinder Token Tool	Used to preload information about hardware tokens.

Exporting Policy Data Using Smobjexport

Using **`smobjexport`**, you can export policy store data to a text file. The resulting text file can be used to migrate, archive, or replicate policy store data. **`Smobjexport`** can export the entire policy store or a single policy domain.

`Smobjexport` exports policy store data in SiteMinder Data Interchange Format (DIF). SiteMinder DIF standardizes SiteMinder data so it can be imported to a different type of policy store. For example, you can export a SiteMinder DIF file from an ODBC database and import it to an LDAP directory.

☞ **Note:** You cannot import a single policy domain to a policy store in a different SiteMinder deployment that uses a different policy store. The policy domain is bound to authorization schemes, agents/agent groups, and user directories, which are defined uniquely within the policy store. If you define the same authorization schemes, agents, and user directories in a separate SiteMinder deployment, they will have different identifiers that the policy domain will not recognize.

`Smobjexport` uses the following arguments to supply information required to export the data:

Argument	**Description**
-o<*file-name*>	The specified path and filename of the output file. If this argument is not specified, the default output filename is stdout.txt. This filename should be a name other than the one used for **`smldapsetup ldgen -f`**<*filename*>, otherwise the export will be overwritten.
-f	Overwrites an existing output file.
-s<*domain-name*>	Exports only the specified policy domain.
-c	Exports sensitive data as clear-text. Exporting data as clear-text allows you to migrate policy data from a Siteminder deployment that uses one encryption key to another SiteMinder deployment that uses a different encryption key. To use -c, you must enter the credentials of a SiteMinder administrator who can manage all SiteMinder domain objects. (Enter credentials using the -d and -w arguments). For more information about administration privileges, refer to the *SiteMinder Policy Server Operations Guide*.
-d<*admin-name*>	Specifies the login name of a SiteMinder Administrator that can manage all SiteMinder objects in the policy store being exported.
-w<*admin-pw*>	Specifies the password of the SiteMinder Administrator specified using -d.

Argument	Description
-k	Exports Agent keys stored in the policy store.
-v	Enables verbose mode.
-t	Enables low level tracing mode. This mode can be used to troubleshoot the export process.

Note: If the arguments contain spaces, use double quotes around the entire argument. For example, if the name of the SiteMinder administrator is *SiteMinder Admin*, the argument for **`smobjexport`** would be **`“-dSiteMinder Admin"`**

To export data using smobjexport:

1. Navigate to one of the following locations:

   - On NT, <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     C:\Program Files\Netegrity\SiteMinder\Bin
     ```

   - On Unix, <*siteminder installlation*>`/bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     /$SM_HOME/netegrity/siteminder/bin
     ```

2. Enter the following command:

   ```
   smobjexport-o<file-name> -s<domain-name>
   -c -d<admin-name> -w<admin-pw> -v -t
   ```

   For example,

   ```
   smobjexport -opstore.txt -smydomain -c
   -dSiteMinder -wpassword -v -t
   ```

   Note: The **`-o`**<*filename*> argument should use a filename other than the one used for **`smldapsetup ldgen -f`**<*filename*>, otherwise the export will be overwritten.

Importing Policy Data Using Smobjimport

The **`smobjimport`** tool imports text files that contain exported policy store data in SiteMinder Data Interchange Format (DIF). You can import a SiteMinder DIF file into an ODBC or LDAP directory.

☞ **Note:** You cannot import a single policy domain to a policy store in a different SiteMinder deployment that uses a different policy store. The policy domain is bound to authorization schemes, agents/agent groups, and user directories, which are defined uniquely within the policy store. If you define the same authorization schemes, agents, and user directories in a separate SiteMinder deployment, they will have different identifiers that the policy domain will not recognize.

`Smobjimport` uses the following arguments to supply information required to import data:

Argument	**Description**
-36	Allows you to import policy store data from SiteMinder 3.6.
-i<*file-name*>	Specifies the path and filename of the input file.
-f	Indicates that duplicate information should be overwritten.
-c	Indicates that the input file contains sensitive data in clear-text. This argument allows to you import policy data from a SiteMinder deployment that uses one encryption key to another SiteMinder deployment that uses a different encryption key. This option requires the credentials of a SiteMinder administrator who can manage all SiteMinder domain objects (enter credentials using the -d and -w arguments). For more information on administration privileges, refer to the *SiteMinder Policy Server Operations Guide.*
-d<*admin-name*>	Specifies the log in name of a SiteMinder Administrator that can manage all SiteMinder objects.
-w<*admin-pw*>	Specifies the password of the SiteMinder Administrator specified in -d.
-k	Imports Agent keys stored in the policy store.

Argument	Description
-v	Enables verbose mode.
-t	Enables low level tracing mode. This can be used to troubleshoot the import process.

☞ **Note:** If any of the arguments contain spaces, use double quotes around the entire argument. For example, if the name of the SiteMinder administrator is *SiteMinder Admin*, the argument for **`smobjimport`** would be **`"-dSiteMinder Admin"`**

☞ **Note:** If the description of a SiteMinder object specified in the Policy Server User Interface is more than one line long, `smobjimport` will only import the first line of the description.

To import Policy data using smobjimport:

1. Navigate to one of the following locations:

   - On NT, <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     C:\Program Files\Netegrity\SiteMinder\Bin
     ```

   - On Unix, <*siteminder installlation*>`/bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     /$SM_HOME/netegrity/siteminder/bin
     ```

2. Enter the following command:

   `smobjimport -i<`*filename*`> -v -t`

   For example,

   `smobjimport -ipstore.txt -v -t`

Managing an LDAP Policy Store using Smldapsetup

The **`smldapsetup`** utility allows you to manage an LDAP policy store from the command line. Using **`smldapsetup`**, you can configure an LDAP policy store, generate an LDIF file, and remove policy store data and schema.

To use **`smldapsetup`**, specify a mode, which determines the action that **`smldapsetup`** will perform, and arguments, which contain the values that are used to configure the LDAP server. Refer to *Modes* on page 241 and *Arguments* on page 243 for information about the modes and arguments you can use with **`smldapsetup`**.

The following table contains the modes you can use with `smldapsetup` and the arguments each mode uses:

Modes	**Arguments**
reg	-h<*host*>, -p<*port*>, -d<*userdn*>, -w<*userpw*>, -r<*root*>, -ssl<*1/0*>, -c<*certdb*>
ldgen	-h<*host*>, -p<*port*>, -d<*userdn*>, -w<*userpw*>, -r<*root*>, -ssl<*1/0*>, -c<*certdb*> -a *<adminname>*,-b *<adminpw>*, -f<*ldif*>, -t *<tool>*,*-e*
lmod	-h<*host*>, -p<*port*>, -d<*userdn*>, -w<*userpw*>, -r<*root*>, -ssl<*1/0*>, -c<*certdb*>, -a *<adminname>*,-b *<adminpw>*, -f<*ldif*>, *-e*
remove	-h<*host*>, -p<*port*>, -d<*userdn*>, -w<*userpw*>, -r<*root*>, -ssl<*1/0*>, -c<*certdb*>,-a *<adminname>*, -b *<adminpw>*
switch	none
revert	-v
status	-v

To use smldapsetup:

1. Navigate to one of the following locations:
   - On NT, <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     C:\Program Files\Netegrity\SiteMinder\Bin
     ```
   - On Unix, <*siteminder installlation*>`/bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     /$SM_HOME/netegrity/siteminder/bin
     ```
2. Enter the following command:

   `smldapsetup` **<*mode*> <*arguments*>**

   For example,

   ```
   smldapsetup reg -hldapserver.mycompany.com “-dLDAP
   User” -wMyPassword123 -ro=security.com
   ```

Modes

The mode indicates the action that **`smldapsetup`** performs. You can specify a mode to connect to the LDAP server, generate an LDIF file, configure an LDAP policy store and remove policy data. The following table lists the modes:

Mode	Description
reg	Tests the connection to the LDAP server. If the connection succeeds, **`smldapsetup`** configures the SiteMinder LDAP server as its policy store using the **`-h<`*host*`>`**, **`-p<`*port*`>`**, **`-d<`*userdn*`>`**, **`-w<`***userpw*>, **`-r<`*root*`>`**, **`-ssl<`*1/0*`>`** and **`-c<`*certdb*`>`** arguments.
ldgen	Automatically detects supported LDAP servers and generates an LDIF file with the SiteMinder schema. The generated file is used by **`smldapsetup ldmod`** to create the SiteMinder schema. If the **`-e`** argument is specified, **`smldapsetup ldgen`** creates an LDIF file that can be used with **`ldmod`** to delete the SiteMinder schema. Use the -m switch to skip automatic detection of LDAP servers. The ldgen mode requires the -f switch unless previously configured in **`reg`** mode.

Mode	Description
ldmod	Connects to the LDAP server and the SiteMinder schema without populating the policy store with any data. It requires the **-a<*adminname*>** and **-b<*adminpassword*>** arguments; the ldapmodify program; and the LDIF file, specified with the -f<*ldif*> argument. If you specify the **-h<*host*>**, **-p<*port*>**, **-d<*userdn*>**,**-w<*userpw*>**, **-r<*root*>**, **-ssl<*1/0*>** and **-c<*certdb*>** arguments, `smldapsetup ldmod` will modify the LDAP directory specified using these arguments. If you do not specify **-h<*host*>**, **-p<*port*>**, **-d<*userdn*>**,**-w<*userpw*>**, **-r<*root*>**, **-ssl<*1/0*>** and **-c<*certdb*>,** `smldapsetup ldmod` uses the LDAP directory previously defined using `smldapsetup reg` or the Policy Server Management Console.
remove	Connects to the LDAP server, then removes all policy data stored under the SiteMinder LDAP node. Remove does not delete the SiteMinder schema. You must specify a SiteMinder administrator with privileges to modify the schema using **-a<*adminname*>** and **-b<*adminpw*>** arguments. If you specify the **-h<*host*>**, **-p<*port*>**, **-d<*userdn*>**,**-w<*userpw*>**, **-r<*root*>**, **-ssl<*1/0*>** and **-c<*certdb*>** arguments, `smldapsetup remove` will remove policy data from the LDAP directory specified by these arguments. If you do not specify **-h<*host*>**, **-p<*port*>**, **-d<*userdn*>**,**-w<*userpw*>**, **-r<*root*>**, **-ssl<*1/0*>** and **-c<*certdb*>,** `smldapsetup remove` will remove the policy data from the LDAP directory previously defined using `smldapsetup reg` or the Policy Server Management Console.
switch	Reconfigures the SiteMinder Policy Server to use LDAP rather than ODBC. It does not prepare the LDAP store or the LDAP connection parameters before making the change.
revert	Reverts to ODBC policy store from LDAP. The only argument used with this mode is **-v**.
status	Verifies that the LDAP policy store connection parameters are configured correctly. It requires the **-v** argument. If you specify the **-h<*host*>**, **-p<*port*>**, **-d<*userdn*>**, **-w<*userpw*>**, **-r<*root*>**, **-ssl<*1/0*>** and**-c<*certdb*>** arguments, **`smldapsetup status`** tests the connection to the LDAP directory specified using these arguments. If you do not specify **-h<*host*>**, **-p<*port*>**, **-d<*userdn*>**,**-w<*userpw*>**, **-r<*root*>**, **-ssl<*1/0*>** and **-c<*certdb*>,** `smldapsetup status` verifies the connection to the LDAP directory previously defined using `smldapsetup reg` or the Policy Server Management Console.

From the **LDAP** tab in the Policy Server Management Console, you can view or change the settings you configured with the **reg**, **switch** and **revert** functions using a GUI interface. You must use **smldapsetup** to perform the **ldgen**, **ldmod**, **remove**, and **status** functions.

Arguments

Arguments allow you to specify the information used by the modes to manage the LDAP policy store. If you do not specify arguments, **`smldapsetup`** uses the values configured in the SiteMinder Policy Server Management Console.

Note: **`Smldapsetup`** does not allow space between an argument and its value. For example, the **`-h`** argument should be specified as follows: **`smldapsetup ldmod -hldapserver.mycompany.com`**

The arguments you can specify in an **`smldapsetup`** call are listed in the following table:

Argument	Description
-h<host>	Specify the fully qualified name of the LDAP server (for example, **`-hldapserver.mycompany.com`**); the relative name, if the machines are in the same domain (**`-hldapserver`**); or the IP address (**`-h123.12.12.12`**). If you do not specify a host, **`smldapsetup`** uses the previously configured value as the default.
-p<*port*>	Specify a non-standard LDAP port. The LDAP port must be specified if the LDAP server is using a non-standard port or if you are moving a server to a new server that uses a different port (such as moving from a server using SSL to one that is not). If a port is not specified, the previous configuration values are used. If no previous port configuration has been specified, **`smldapsetup`** uses the default ports 389 (if SSL is not being used) or 636 (if SSL is being used).
-d<*userdn*>	Specify the LDAP user name of a user with the power to create new LDAP directory schema and entries. This is not necessarily the user name of the LDAP server administrator. If you do not specify a user name, **`smldapsetup`** uses the previously configured name as the default.
-w<*userpw*>	Specify the password for the administrator identified in the **`-d`** argument described above (for example, "**`-wMyPassword123`**"). If you do not specify a password, **`smldapsetup`** uses the previously configuration value.
-r<*root*>	Specify the distinguished name of the node in the LDAP tree where SiteMinder will search for the policy store schema (for example: **`-ro=security.com`**). If you do not specify a root, **`smldapsetup`** uses the previously configured root.
-a<adminname>	Specify the user name of a SiteMinder administrator with privileges to modify the schema. This argument is required by **`smldapsetup remove`**.
-b<adminpw>	Specify the password for the SiteMinder administrator identified in the -a argument. This argument is required by **`smldapsetup remove.`**

Argument	Description
-e	When specified with **`smldapsetup ldgen`**, generates an LDIF file that can delete the SiteMinder schema. The generated file must be used with **`smldapsetup ldmod`** to remove the schema.
-m *<n>*	Use to skip automatic detection of LDAP servers where *<n>* is one of the following: **1**—Skips automatic detection for Netscape v3 LDAP servers. **2**—Skips automatic detection for Netscape v4 LDAP servers. **3**—Skips automatic detection for Active Directory LDAP servers.
-f<*ldif*>	Specify the absolute or relative path to an LDIF file from the directory in which **`smldapsetup`** is being executed (for example, **`-f../siteminder/db/smldap.ldif`**). By default if you do not specify a path, `smldapsetup` uses the current directory as the default.
-t<*tool*>	Specify the absolute or relative path (including filename and extension) of the `ldapmodify` command line utility. `Ldapmodify` is used to configure the server schema using the LDIF format commands. LDAP servers and SiteMinder provide a copy of `ldapmodify`. If the utility is not in the default location, use this argument to specify its location (for example, **`-tC:\Netscape\SuiteSpot\bin\slapd\server\ldapmodify.exe`**)
-ssl<*1 or 0*>	Specify **`-ssl1`** to use an SSL-encrypted connection to the LDAP server, and -**`ssl0`** to use a non-SSL connection. If you do not specify a value for **`-ssl`**, **`smldapssetup`** uses the previously configured value. If the LDAP connection has not been configured before, the initial default value is 0 (*do not use SSL*).
-c<*cert*>	This argument must be specified when using an SSL encrypted (**`-ssl1`**) LDAP connection. Specify the absolute path to the SSL client certificate database (usually called **`cert7.db`** for the Netscape Navigator Web browser). The default value is the value previously specified in the SiteMinder Policy Server Management Console.
-k<*n*>	Enables you to use **`smldapsetup`** to modify the key store if you are storing key information in a different LDAP directory. If you specify **`-k`**, **`smldapsetup`** checks to see if the Policy Server is pointing to the key store before performing any functions. If the Policy Server is not pointing to the key store, **`smldapsetup`** issues a warning. If you specify **`-k1`**, **`smldapsetup`** performs the desired function without checking if the Policy Server is correctly pointing to the key store. If you do not specify **`-k`** or **`-k1`**, **`smldapsetup`** will modify the policy store.
-v	Use the **`-v`** argument to enable verbose mode for troubleshooting. With **`-v`**, **`smldapsetup`** logs its command-line arguments and configuration entries as it performs each step in the LDAP migration.
-q	Use the **`-q`** argument to enable quiet mode (no questions will be asked).

☞ **Note:** If the arguments contain spaces, you must enter double quotes around the entire argument. For example, if the name of the SiteMinder administrator is LDAP user, the argument for **`smldapsetup`** would be **`"-dLDAP user"`**

Removing the SiteMinder Policy Store using Smldapsetup

To remove the SiteMinder policy store data and schema from an LDAP directory, you must first delete the data, then remove the schema.

! **Warning:** Before removing the SiteMinder policy store data, make sure that the Policy Server is pointing to the policy store that contains the data you want to delete. `Smldapsetup remove` will remove the data from the policy store to which the Policy Server is pointing. Additionally, export the policy store data to an output file and create a backup of the file before removing the data. Refer to *Exporting Policy Data Using Smobjexport* on page 235.

To remove the policy store using smldapsetup:

1. Navigate to one of the following locations:

   - On NT, <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     C:\Program Files\Netegrity\SiteMinder\Bin
     ```

   - On Unix, <*siteminder installlation*>`/bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     /$SM_HOME/netegrity/siteminde/bin
     ```

2. Remove the policy store data by entering the following command:

   `smldapsetup remove -a<`*`name`*`> -b<`*`password`*`>`

   For example,

   ```
   smldapsetup remove -aSMAdmin -badminpassword
   ```

   ☞ **Note:** Removing the policy store data may take a few moments.

3. Generate the LDIF file you will use to delete the schema by entering the following:

   smldapsetup ldgen -e -f<*ldif*>

   where <*ldif*> is the name of the LDIF file you are generating.

   For example,

   smldapsetup ldgen -e -fdelete.ldif

4. Remove the SiteMinder schema by executing the following command:

   smldapsetup ldmod -f<*ldif*>

   where <*ldif* > is the name of the LDIF file you generated using **smldapsetup ldgen -e**.

   For example,

   smldapsetup ldmod -fdelete.ldif

Deleting SiteMinder Data in ODBC Databases

SiteMinder provides a number of tools to delete the SiteMinder schema from ODBC databases. The following table describes each tool:

Tool	Description
sm_oracle_ps_delete.sql	Removes the SiteMinder 4.1 policy store and data from an Oracle database.
sm_oracle_logs_delete.sql	Removes SiteMinder 4.1 logs stored in an Oracle database if the database was created using sm_oracle_logs.sql.
sm_oracle_token_delete.sql	Removes the SiteMinder 4.1 token data, such as Encotone Encrypta card data, and schema from an Oracle database if the database was created using sm_oracle_token.sql.
sm_mssql_ps_delete.sql	Removes the SiteMinder 4.1 policy store and data from an SQL database.

Tool	Description
sm_mssql_logs_delete.sql	Removes SiteMinder 4.1 logs stored in an SQL database if the database was created using sm_oracle_logs.sql.
sm_mssql_token_delete.sql	Removes the SiteMinder 4.1 token data, such as Encotone TeleID card data, and schema from an SQL database if the database was created using sm_oracle_token.sql.

The ODBC database tools are in the following locations:

- For NT, <*siteminder_installation*>`\Db`

  where <*siteminder_installation*> is the installed location of SiteMinder.

  For example,

  ```
  C:\Program Files\Netegrity\SiteMinder\Db
  ```

- For UNIX, <*siteminder_installation*>`/db`

  where <*siteminder_installation*> is the installed location of SiteMinder.

  For example,

  ```
  $SM_HOME/siteminder/db
  ```

Import these files into the policy store database. For information on importing schema files, refer to your database documentation.

☞ **Note:** For information on creating policy stores, token data stores, and logs for ODBC databases, refer to *Chapter 3, Setting up the Policy Store on NT* on page 47 or *Chapter 4, Setting up the Policy Store on Solaris* on page 75.

Checking Solaris Patches With Smpatchcheck

SiteMinder provides a utility, called **`smpatchcheck`**, that checks whether or not you have the Solaris patches required for the SiteMinder Policy Server and Web Agent installed on your system. **`Smpatchcheck`** can be run on Solaris 2.5.1, 2.6, and 2.7.

To use smpatchcheck

1. Navigate <*siteminder installlation*>`/bin`

   where <*siteminder_installation*> is the installed location of SiteMinder. For example:

   ```
   /$SM_HOME/netegrity/siteminder/bin
   ```

2. Enter **`smpatchcheck`**.

   `Smpatchcheck` looks for each required/recommended patch and then displays its status.

   For example:

   ```
   Testing for Required Patches:
     Testing for Patch: 106327-09 ... NOT Installed
   Testing for Recommended Patches:
     Testing for Patch: 106541-08 ... Installed
     Testing for Patch: 106980-00 ... Installed

   SiteMinder Patch Check: Failed
   ```

   `Smpatchcheck` returns one of the following messages:

   - **Failed**—One or more of the required patches is not installed.
   - **Partially Failed**—One or more of the recommended patches is not installed.
   - **Success**—All of the required and recommended patches are installed.

Reading RADIUS Log Files With Smreadclog

This tool is used to read RADIUS log files generated by the SiteMinder Policy Server. It is useful for troubleshooting the Policy Server when used as a RADIUS authentication server. Options are provided to display individual RADIUS attributes that are exchanged between NAS and SiteMinder.

`Smreadclog` uses the following arguments to supply information required to read RADIUS log files

Argument	Description
-i<input-file]	Specifies the filename of the log file.
-o<output-file>	Specifies the filename of the output file.
-s<secret>	Specifies the shared secret that can be used to decode RADIUS passwords.
-r	Indicates that a hex dump of an entire RADIUS packet be displayed.
-a	Indicates that RADIUS attributes should be displayed individually.
-d	Indicates that RADIUS attributes should be displayed according to their definition in the policy store. This option displays actual attribute names as well as attribute values formatted based on their attribute type. Without this option, only the attribute name and value are displayed (as a hex string).
-p<radius-server>	Allows you to record and replay RADIUS activity of the authentication and authorization services against your RADIUS server.
-m<authentication port>	Specifies the port used for RADIUS authentication if that port is not the default port, 1645.
-n<accounting port>	Specifies the port used for RADIUS accounting if that port is not the default port, 1646.

For information about deploying the Policy Server as a RADIUS authentication server, refer to the *SiteMinder Deployment Guide*.

To use smreadclog:

1. Navigate to one of the following locations:

   - On NT, <*siteminder_installation*>`\Bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     C:\Program Files\Netegrity\SiteMinder\Bin
     ```

   - On Unix, <*siteminder installlation*>`/bin`

     where <*siteminder_installation*> is the installed location of SiteMinder. For example:

     ```
     /$SM_HOME/netegrity/siteminder/bin
     ```

2. Enter the following command:

   ```
   smreadclog -i<input-file> -o<output-file>
   -s<secret> -r -a -d -p<radius-server> -m<port>
   -n<port>
   ```

   For example,

   ```
   smreadclog -iradiuslog.txt -oradiuslog2.txt
   -ssecret -r -a -d -p123.123.12.12
   ```

The SiteMinder Test Tool

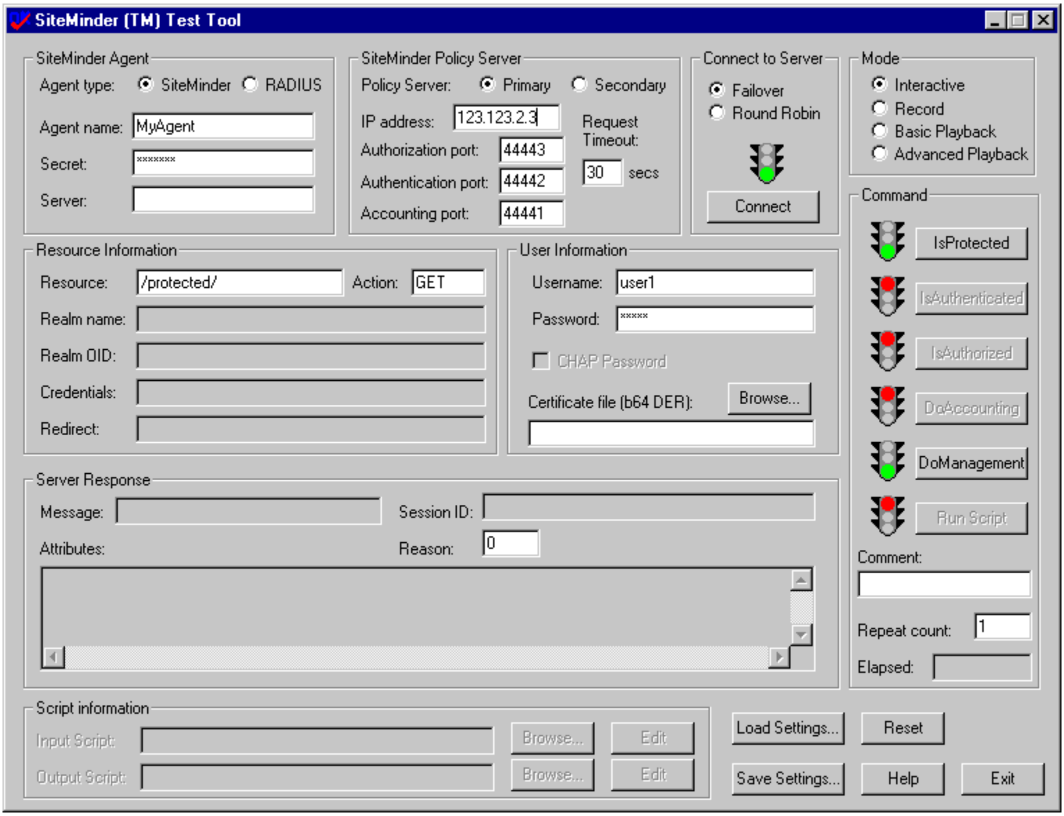
The SiteMinder Test Tool is a valuable utility that simulates the interaction between Agents and Policy Servers, allowing you to test the functionality the Policy Server. During testing, the Test Tool acts as the Agent, making the same requests to the Policy Server as a real Agent. This allows you to test your SiteMinder configuration before deploying it.

The SiteMinder Test Tool performs three types of tests:

- Functionality—Tests SiteMinder policies to ensure they are configured correctly.
- Regression—Tests whether or not changes, such as migrating a policy store or implementing a new feature, affects SiteMinder.
- Stress—Tests the performance of the Policy Server as it receives multiple requests.

About the SiteMinder Test Tool Interface

The Test Tool interface, shown below, allows you to configure a test environment, run tests and store data.



SiteMinder (TM) Test Tool

SiteMinder Agent
Agent type: ● SiteMinder ○ RADIUS
Agent name: MyAgent
Secret: *******
Server:

SiteMinder Policy Server
Policy Server: ● Primary ○ Secondary
IP address: 123.123.2.3
Authorization port: 44443
Authentication port: 44442
Accounting port: 44441
Request Timeout: 30 secs

Connect to Server
● Failover
○ Round Robin

Mode
● Interactive
○ Record
○ Basic Playback
○ Advanced Playback

Resource Information
Resource: /protected/ Action: GET
Realm name:
Realm OID:
Credentials:
Redirect:

User Information
Username: user1
Password: *****
□ CHAP Password
Certificate file (b64 DER):

Server Response
Message:
Session ID:
Attributes:
Reason: 0

Command
Comment:
Repeat count: 1
Elapsed:

Script information
Input Script:
Output Script:

The Test Tool includes the following group boxes:

- **SiteMinder Agent**—Identifies the Agent that communicates with the Policy Server during the test.
- **SiteMinder Policy Server**—Identifies the IP address and port information of the Policy Server.
- **Connect to Server**—Specifies Failover or Round Robin operation mode between two Policy Servers and allows you to establish a connection with the Policy Server from the Test Tool.

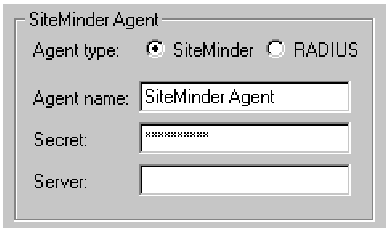
- **Mode**—Specifies Interactive, Record, Basic Playback, or Advanced Playback mode.
- **Resource Information**—Identifies the resource against which you are conducting tests.
- **User Information**—Allows you to specify user and certificate information for authorization tests.
- **Command**—Contains buttons and fields for executing tests.
- **Server Response**—Displays information about successful and failed server operations during testing.
- **Script Information**—Allows you to specify scripting information for **Record**, **Basic Playback** and **Advanced Playback** mode.

Each of these group boxes is described in detail in the following sections.

In addition to the group boxes listed above, the SiteMinder Test Tool provides buttons for saving, loading Test Tool settings, resetting the Resource Information fields, accessing Help and exiting the Test Tool.

SiteMinder Agent

The **SiteMinder Agent** group box allows you to specify information about which SiteMinder Agent or RADIUS Agent you are simulating. This group box, shown below, contains the following fields:



SiteMinder Agent

Agent type: ● SiteMinder ○ RADIUS

Agent name: SiteMinder Agent

Secret: **********

Server:

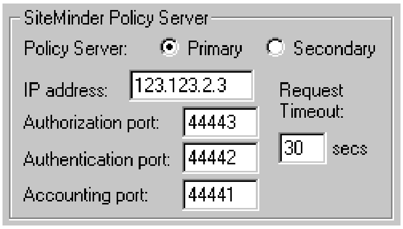
- **Agent Type**—Indicates whether the Agent is a SiteMinder Agent or a RADIUS Agent.

  If you select a SiteMinder Agent, you must specify the **Agent Name** and **Secret**. If you select a RADIUS Agent, only the **Secret** is required. Refer to the *SiteMinder Deployment Guide* for more information about testing RADIUS Agents.

- **Agent Name**—Enter the name of the Agent as it appears in the SiteMinder Policy Server User Interface.
- **Secret**—Enter the shared secret of the Agent. This must match the shared secret entered when the Agent was created.
- **Server**—Optionally, enter the full name of the server on which the Agent resides. For example, to test the Policy Server for `http://www.security.com`, enter **`www.security.com`** in this field.

SiteMinder Policy Server

The **SiteMinder Policy Server** group box identifies the Policy Server and the ports reserved for Policy Server communication. It contains the following fields:



SiteMinder Policy Server

Policy Server: ● Primary ○ Secondary

IP address: 123.123.2.3

Authorization port: 44443

Authentication port: 44442

Accounting port: 44441

Request Timeout: 30 secs

- **Policy Server**—Indicates whether you are specifying the Primary or Secondary Policy Server.
- **IP Address**—Specifies the IP address of the Policy Server. By default, this field contains the IP address of the local system.
- **Authorization Port**—Specifies the TCP port used for authorization requests. This field is populated with SiteMinder’s default authorization port.
- **Authentication Port** — Specifies the TCP port used for authentication requests. This field is populated with SiteMinder’s default authentication port.
- **Accounting Port** — Specifies the TCP port used for accounting requests. This field is populated with SiteMinder’s default accounting port.
- **Timeout** — Displays the time, in seconds, that the Test Tool should wait for a response from the Policy Server.

Connect to Server

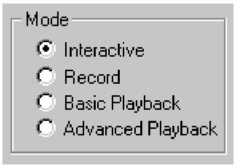
The **Connect to Server** group box allows you to initialize the connection between the Agent and the Policy Server. You must establish a connection with the Policy Server before performing any tests.

To establish a connection, specify one of the following options for how the Agent communicates with multiple Policy Servers, and click the **Connect** button.

- **Failover**—Enables failover. During failover, the Test Tool directs requests to the initial Policy Server. If the initial Policy Server fails, the Test Tool redirects requests to the secondary Policy Server. For more information on failover, see the *SiteMinder Agent Operations Guide*.
- **Round Robin**—Enables round robin load balancing. Round Robin load balancing divides requests between the primary and secondary Policy Servers. For each connection, the Test Tool alternates between Policy Servers. For more information on round robin load balancing, see the *SiteMinder Agent Operations Guide*.

Mode

The **Mode** group box determines the mode in which you run tests in the Policy Server. The following modes are available:



- **Interactive**—Allows you to enter data, run tests, and see the results displayed immediately in the Test Tool dialog box.
- **Record**—Combines Interactive operation with a script generation feature that writes test results to a plain-text script file. This file can subsequently be used as an input file to repeat the test in playback mode.

  When you select **Record**, the **Output Script** field in the **Script Information** dialog box becomes active. In this field, enter the path and filename for the text file where the test results will be stored. For example, enter **`c:\temp\script.txt`**.

You can run multiple tests and record them to the same script file. The Test Tool appends the test results to the end of the file. You can then use the script file for regression and stress testing.

Record mode writes every test performed in the specified text file. To stop recording, specify a new mode.

- **Basic Playback**—Uses script files created in the **Record** mode to automate sequential tests for regression testing.

  When you select Basic Playback, the only active fields in the Test Tool are the **Input Script** and **Output Script** fields.

  Refer to *Performing Regression Tests* on page 266 for more information.

- **Advanced Playback**—Runs multi-threaded stress tests.

  In this mode, the Test Tool reads instructions for running tests from a *thread control file*. The thread control file is a plain text file created using the Test Tool's scripting language. It can make multiple requests to the Policy Server simultaneously, which enables you to simulate continuous or intermittent multi-thread requests. These tests mimic multiple agents communicating with the Policy Server or a single Agent sending requests over multiple threads to the Policy Server simultaneously.

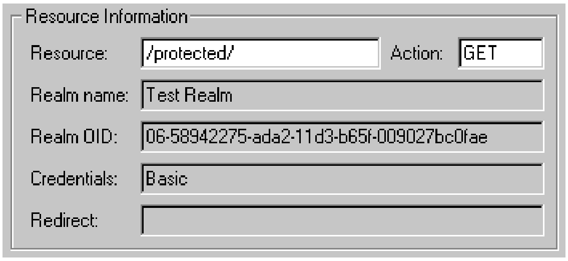
  When you select **Advanced Playback**, the only active field in the Test Tool is the **Control Script** field.

  Refer to *Performing Stress Tests* on page 267 for more information about **Advanced Playback** mode.

Resource Information

The **Resource Information** group box allows you to enter information about the resource you are using to test the Policy Server. The **Resource** and **Action** fields are required for functionality tests. The remaining fields contain test responses returned by the Policy Server.

This group box includes the following fields:



Resource Information

Resource: /protected/ Action: GET

Realm name: Test Realm

Realm OID: 06-58942275-ada2-11d3-b65f-009027bc0fae

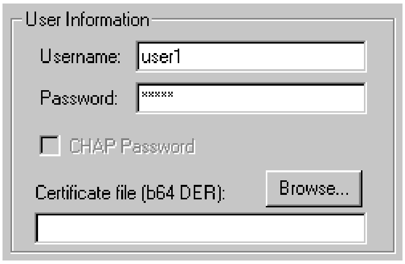
Credentials: Basic

Redirect:

- **Resource**—Enter the relative path of the resource that SiteMinder is protecting. The path is relative to the Web server's publishing directory. For example, `/protected/`.
- **Action**—Enter the Agent action, Authentication Event, or Authorization event specified in the rule that you are testing (refer to the *Policy Server Operations Guide*).
- **Realm Name**—Displays the name of the realm that contains the specified resource, returned by the Policy Server.
- **Realm OID**—Lists the realm object identifier returned by the Policy Server.
- **Credentials**—Indicates the authentication scheme used to protect the resource.
- **Redirect**—Displays a redirect string in response to the IsProtected test if the authentication scheme for the realm uses a redirect string. All certificate and HTML forms-based schemes return this string, which typically instructs the Agent where to display a form.

User Information

The **User Information** group box allows you to test a particular user against the configured policies.



Username: user1

Password: *****

□ CHAP Password

Certificate file (b64 DER):

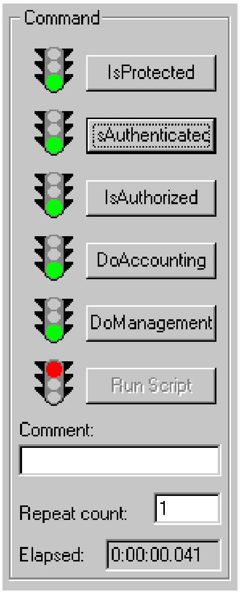
It contains the following fields:

- **User Name**—Enter the user name you want to use to access the resource.
- **Password**—Enter the password for the user entered in **User Name**.
- **CHAP Password**—If you are using a RADIUS CHAP authentication scheme, select this check box.
- **Certificate File**—If the protected resource requires certificates to authenticate users, you must provide a certificate file so that the Test Tool can simulate certificate authentication. Click **Browse** to locate the certificate file.

Command

The **Command** group box allows you to perform functionality tests on the Policy Server and add comments to output script files.

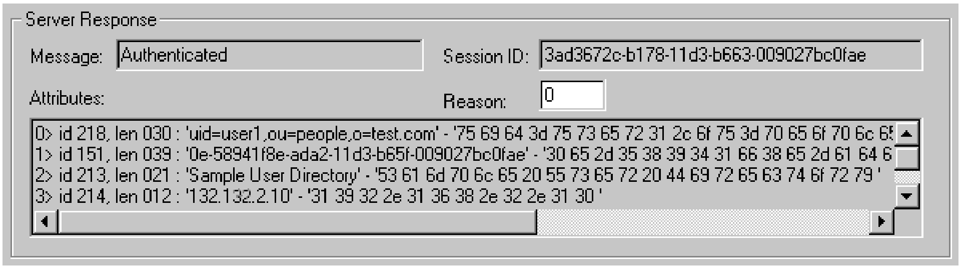
The **Command** group box contains the following fields:



- **IsProtected**—Determines if the resource is protected.
- **IsAuthenticated**—Determines if a set of credentials is authenticated.
- **IsAuthorized**—Determines if the user is authorized by SiteMinder to perform a specific action on a resource.
- **DoAccounting**—Logs accounting server transactions.
- **DoManagement**—Requests agent commands, such as cache flush commands that clear the Agent cache.
- **Run Script**—Runs scripts for Basic and Advanced Playback modes.
- **Comment**—Writes a comment to the output script file in Record mode.
- **Repeat Count**—Determines the number of times the Test Tool runs a test.

Server Responses

The **Server Response** group box displays additional Policy Server responses for executed tests. It contains the following fields:



Message: Authenticated

Session ID: 3ad3672c-b178-11d3-b663-009027bc0fae

Reason: 0

Attributes:

```
0> id 218, len 030 : 'uid=user1,ou=people,o=test.com' - '75 69 64 3d 75 73 65 72 31 2c 6f 75 3d 70 65 6f 70 6c 6
1> id 151, len 039 : '0e-58941f8e-ada2-11d3-b65f-009027bc0fae' - '30 65 2d 35 38 39 34 31 66 38 65 2d 61 64 6
2> id 213, len 021 : 'Sample User Directory' - '53 61 6d 70 6c 65 20 55 73 65 72 20 44 69 72 65 63 74 6f 72 79 '
3> id 214, len 012 : '132.132.2.10' - '31 39 32 2e 31 36 38 2e 32 2e 31 30 '
```

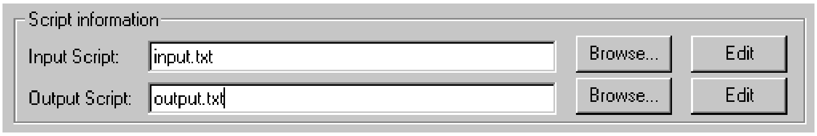
- **Message**—Indicates the result after you run a test. For example, if you run the IsProtected test, and the resource is successfully protected, the message field displays `Protected`.
- **Session ID**—Displays the ID that SiteMinder assigned to the session.
- **Attributes**—Lists additional information that is part of the response. The information varies depending on the test you run.
- **Reason**—Displays the reason code associated with the outcome of the test. This field is used to supply information to developers using the SiteMinder SDK. The reason codes are listed in `SmApi.h`.

☞ **Note:** To clear responses without removing user-supplied information, click **Reset** in the lower right corner of the dialog box.

Script Information

The **Script Information** group box is used for specifying script file names when you run tests in **Record**, **Basic Playback**, and **Advanced Playback** modes. The Test Tool displays different fields depending on the mode.

The **Script Information** group box contains the following fields:



Input Script: input.txt

Output Script: output.txt

- **Input Script**—In Basic Playback mode, enter a path and file name for the source test data against which you want to run a regression test.
- **Output Script**—In Record mode, enter a path and file name where you want to store test data.
- **Control Script**—In Advanced Playback mode, enter the path and file name for the thread control file that contains the control script for your test.

Test Tool Buttons

The following buttons are located in the lower right corner of the dialog box:

- **Load Settings**—Allows you to load test settings saved in a text file.
- **Save Settings**—Allows you to save your current test settings to a text file.
- **Reset**—Clears responses displayed in the **Attributes** field of the Server Response region without removing user-supplied information.
- **Exit**—Closes the SiteMinder Test Tool dialog box and terminates all tests.

Testing a Policy

You must configure the test environment. This includes specifying the Web Agent that you are simulating, the resource protected by the Agent, and the user credentials you are authenticating. If you perform tests in **Record**, **Basic Playback**, or **Advanced Playback** mode, you must also specify script information.

To test a policy:

☞ **Note:** This procedure assumes that you are simulating a SiteMinder Agent for testing. Refer to the *SiteMinder Deployment Guide* for information on performing RADIUS tests.

1. Access the Test Tool by completing one of the following:
   - For NT, select **Programs | SiteMinder | SiteMinder Test Tool** From the Windows **Start** menu.
   - For UNIX, enter `smtest` from the `/siteminder/bin` directory.

2. In the **SiteMinder Agents** group box, specify the following information:

    a. Select the **SiteMinder** button in the **Agent Type** field.

    b. In the **Agent Name** field, enter the name of the Web Agent as it appears in the SiteMinder Policy Server User Interface.

    c. In the **Secret** field, enter the shared secret that was defined for the Agent in the SiteMinder Policy Server User Interface.

    d. Optionally, enter the full name of the server on which the Web Agent resides in the **Server** field.

3. In the **SiteMinder Policy Server** group box, specify the following information:

    a. In the **Policy Server** field, select the **Primary** or **Secondary** Policy Server by selecting the appropriate radio button.

    b. In the **IP Address** field, enter the IP address of the Policy Server.

    c. In the **Authorization Port** field, specify the TCP port used for authorization requests.

    d. In the **Authentication Port** field, specify the TCP port used for authentication requests.

    e. In the **Accounting Port** field, specify the TCP port used for accounting requests.

    f. In the **Timeout** field, enter the time, in seconds, that the Test Tool should wait for a response from the Policy Server.

4. In the **Connect to Server** group box, do the following:

    a. Select an operation mode by selecting the **Failover** or **Round Robin** radio button.

    b. Click the **Connect** button.

5. In the **Mode** group box, select the **Interactive**, **Record**, **Basic Playback**, or **Advanced Playback** radio button.

☞ **Note:** If you select **Record**, **Basic Playback**, or **Advanced Playback**, specify the required information in the **Script Information** group box.

6. In the **Resource Information** group box, do the following:

   a. Enter the path of the resource that SiteMinder is protecting in the **Resource** field.

   b. Enter the action specified in the rule in the **Action** field.

Note: The remaining fields in the **Resource Information** group box contain test results and are populated by the Test Tool.

7. In the **User Information** group box, enter the following:

   a. In the **User Name** field, enter the user name you want to use to access the resources.

   b. In the **Password** field, enter the password for the specified user.

   c. If you are using a CHAP authentication scheme, select the **CHAP Password** check box.

   d. If the protected resource requires certificates to authenticate users, manually specify a certificate file so that the Test Tool can simulate certificate authentication. Click **Browse** above the **Certificate File** field to locate the certificate file.

8. In the **Command** group box, do the following:

   a. If you specified **Record** in step 5, optionally enter a comment you want to record along with the test results in the **Comment** field.

   b. Enter the number of times you want the Policy Server to repeat the test in the **Repeat Count** field.

   c. Initiate the test that you want to run by clicking one of the following buttons:

      - **IsProtected**—Determines if the resource is protected. (Refer to *IsProtected* on page 264).

      - **IsAuthenticated**—Determines if a set of credentials is authenticated. (Refer to *IsAuthenticated* on page 264).

      - **IsAuthorized**—Determines if the user is authorized by SiteMinder to perform a specific action on a resource. (Refer to *IsAuthorized* on page 265).

Saving and Loading Configurations

To avoid re-entering user-supplied information, such as the Agent, Resource, and User Information, you can use the **Load Settings** and **Save Settings** buttons.

Use the **Save Settings** button to save the current settings to a plain text file. When you click **Save Settings**, the Test Tool prompts you to enter a file name. To retrieve this information. Click on **Load Settings**, select the file, and click **Open**. The user-configured fields are automatically filled-in with the values defined in the file. If you change any information, use the **Save Settings** button again to overwrite the existing file or create a new one.

Performing Functionality Tests

The SiteMinder Test Tool allows you to test the functionality of SiteMinder policies in a simulated real-world environment. To perform a functionality test, you must have a SiteMinder Policy Server and Web Agent configured and running, a policy domain (configured with any type of user directory), and a policy that pairs an authenticating rule with a response.

Using the Test Tool, you can ensure that a SiteMinder policy is protecting a resource, authenticating users and authorizing users to perform specified actions on a resource.

SiteMinder allows you to perform the following functionality tests:

- **IsProtected**—Determines if the resource is protected.
- **IsAuthenticated**—Determines if a set of user credentials is authenticated.
- **IsAuthorized**—Determines if the user is authorized by SiteMinder to perform a specific action on a resource.

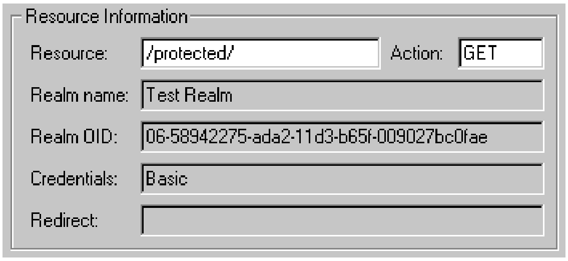
These tests must be run in the order they appear above. For example, you must run IsProtected before running IsAuthenticated. The order reflects the steps that SiteMinder uses to determine a user’s access rights.

After performing a test, the Test Tool displays the amount of time the test took to run in the **Elapsed Time** field of the **Command** group box. Because of fluctuations in the system, averaging the elapsed time of multiple tests provides more accurate results. To get an average elapsed time, specify the number of times you want to run the test in **Repeat Count** field. The Test Tool runs the test the specified number of times and then displays the total elapsed time. Divide the elapsed time by the number of times the test was run to determine the average elapsed time.

IsProtected

Running IsProtected allows you to test if a SiteMinder policy is protecting the resource you specified.

If IsProtected is successful, the Test Tool displays “`Protected`” in the Message field in the Server Response group box. Protected means that the Test Tool was able to make a successful connection to the Policy Server and a SiteMinder policy is protecting the resource. The Test Tool also populates the **Realm Name**, **Realm OID**, and **Credentials** fields with values returned by the Policy Server, as shown below:



Resource Information

Resource: /protected/

Action: GET

Realm name: Test Realm

Realm OID: 06-58942275-ada2-11d3-b65f-009027bc0fae

Credentials: Basic

Redirect:

Refer to *Resource Information* on page 256 for a description of each field.

If **IsProtected** is unsuccessful, the Test Tool displays `Error` in the Message field. If you receive an error, verify that the SiteMinder Test Tool can successfully connect to the Policy Server.

You can also check the smservalog for debugging information. For information about enabling the smservalog, refer to the *SiteMinder Policy Server Operations Guide*.

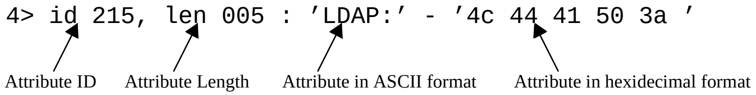
IsAuthenticated

IsAuthenticated allows you to test if a SiteMinder policy can authenticate a set of credentials.

☞ **Note:** You must run IsProtected before you can run IsAuthenticated.

If the Test Tool successfully authenticates the user, it displays `Authenticated` in the **Message** field in the Server Response group box and populates the following fields with values returned by the Policy Server:

- **Session ID—**Displays a unique SiteMinder-assigned session ID. The Policy Server uses this ID to identify the cookie where session information is stored.
- **Attributes—**Lists the attributes the Policy Server sends back in the response. For example:



```
4> id 215, len 005 : ’LDAP:’ - ’4c 44 41 50 3a ’
```

- **Reason**—Displays the reason code associated with the outcome of the test. Reason codes are listed in `SmApi.h`.

IsAuthorized

Running IsAuthorized allows you to determine if a user is authorized to perform a specific action on a resource.

If SiteMinder authorizes the user successfully, the Test Tool displays `Authorized` in the **Message** field and the SiteMinder-assigned Session ID in the **Session ID** field.

To perform a functionality test:

1. Configure the Test Tool or load previously configured settings.
   - Refer to *Testing a Policy* on page 260 for information on configuring the Test Tool.
   - Refer to *Saving and Loading Configurations* on page 263 for information on loading previously configured settings.
2. Initialize a connection between the Policy Server and the Test Tool by clicking the **Connect** button in the **Policy Server** group box.

3. In the **Mode** group box, select the radio button corresponding to one of the following options:

   a. **Interactive**—Allows you to enter data, run tests, and see the results displayed immediately in the Test Tool dialog box.

   b. **Record**—Combines interactive operation with a script generation feature that puts the test results in a plain-text script file.

4. If you selected **Record** in step 3, enter the path and filename of the output file in the **Output Script** field in the **Script Information** group box.

☞ **Note:** If you selected **Interactive** mode, the **Output Script** field is not active.

5. If desired, specify the number of times you want the Test Tool to run your test in the **Repeat Count** field in the **Command** group box.

6. Click one of the following buttons in the **Command** group box to run a functionality test:

   - **IsProtected**
   - **Is Authenticated**
   - **IsAuthorized**

   The Test Tool displays results in the Resource Information group box.

Performing Regression Tests

Regression tests allow you to test whether or not changes made to SiteMinder, such as upgrading the policy store or implementing a new feature, affect SiteMinder policies. During regression testing, you run tests before making any changes and again after you have implemented changes. By comparing the results of the tests, you can determine if the changes affect SiteMinder.

To perform a regression test:

1. Configure the Test Tool or load previously configured settings.
2. Run tests in **Record** mode.

   Note: Make sure you specify an output file in the **Output Script** field in the **Script Information** group box. The ouput script must include a file extension. For example, `output.txt`.

3. When the test is complete, select **Basic Playback** in the **Mode** group box.
4. In the **Script Information** group box, enter the name of the text file in the **Input Script** field.

   This file name should match the name of the **Output Script** file you created in **Record** mode.

5. Specify an output file name in the **Output Script** field.
6. In the **Command** group box, click **Run Script**.

   The Test Tool runs the input script and creates the output script file.

7. Compare the input and output script files.

Performing Stress Tests

The Test Tool allows you to test SiteMinder's performance when the Policy Server receives more than one request at a time. Using stress tests, you can simulate multiple Agents talking to the SiteMinder Policy Server simultaneously or a single Agent communicating with the Policy Server on multiple threads.

Stress tests are run in **Advanced Playback** mode. The Test Tool receives instructions from a *thread control file* that specifies which tests to run and how many times to run them. After executing the instructions in the thread control file, the results of the test are written to a new file. The Test Tool names the file by appending `_out1` to the end of the thread control file. For example, if the thread control file is: `c:\temp\test_data.txt`, the Test Tool names the new file `c:\temp\test_data.txt_out1`.

The thread control file is explained in detail in the next section.

Thread Control Files

A thread control file is what determines the actions of the Test Tool running in the **Advanced Playback** mode. A thread control file contains multiple instruction lines in the Test Tool's own scripting language and comments, indicated by the # symbol at the beginning of a line.

The basic instructions are in the format: <*script file name*>, <*number of script repetitions*>, <*number of threads*>. For example:

```
c:\temp\test_data.txt, 8, 6
```

This line indicates that the input script will be `c:\temp\test_data.txt`, that the Test Tool will run the script eight times, and that there will be six simultaneous threads running the script. The output of the test, by default, will be `c:\temp\test_data.txt_out1`, up to `c:\temp\test_data.txt_out6.`

The Test Tool scripting language includes the following commands to control the script file output:

Test Tool Scripting Language Commands

Command	Description
.report	Generates a final report (as an output file) summarizing the test results. The report does not include the status of each server request. This is the default.
.output	Generates a final report (as an output file) summarizing the overall results including the status of each server request.
.viewstats	Displays final statistics in a text editor.
.verbose	Generates output files containing the details of each server request.
.brief	Generates output files containing the brief results of each server request. This option is only valid when used with the .output command.
.sleep	Lets the Test Tool pause for a specified amount of time (in milliseconds). This simulates intermittent server requests.

Command	Description
.connect <*setting_file*>	Initializes the Test Tool with the information from the settings file to set up a multi-threaded test with one simulated Agent. The default multi-threaded testing is comprised of multiple simulated Agents with one simulated Agent per thread. You can also set up testing with one simulated Agent and multiple threads by using this option.
.disconnect	Un-initializes the Test Tool to indicate the end of one simulated Agent multi-threaded test.

The following is an example of a thread control script:

```
.output
.brief
c:\temp\test_data1.txt, 2, 3
.verbose
.sleep 5000
c:\temp\test_data1.txt, 2, 2
.brief
c:\temp\test_data1.txt, 3, 4
.connect smtest.ini
c:\temp\test_data1.txt, 5, 6
.disconnect
```

In addition to writing test results to a text file, Advanced Playback mode also generates a report summarizing the results. This report contains the following information:

- Time the test started and finished
- Total elapsed time
- Minimum, maximum, and average request time
- Total number of requests
- Throughput
- Tests run and their results

To run a stress test:

1. Create a thread control script.
2. In the **Mode** group box, select **Advanced Playback**.
3. In the **Script Information** group box, enter the name of the thread control script in the **Control Script** field.
4. In the **Command** group box, click **Run Script**.

   When Run Script is clicked, the Test Tool opens a DOS window and displays the thread it is running and the thread's status.

   The Test Tool also writes all of the status information to a file. The file name is the name of the thread control file with `_out#` appended to it, where # is an incremented number for the thread. For example, the thread control file, `thread.txt`, yields output files named `thread.txt_out1` and `thread.txt_out2`.

Sample Test Report

The following is a sample test report:

```
Control File:   C:\temp\control.txt
Started at:     0:02:05.481
Finished at:    0:03:22.672
Total Elapsed:  0:00:01.396

Minimum Request Time:   0:00:00.400
Maximum Request Time:   0:00:05.498
Average Request Time:   0:00:01.396

Total Requests         234
Throughput (Req/Sec):   3.241

Request              Count     Yes      No    Timeout   Error
------------------ ------------  -------  -------  ----------  --------
IsProtected            78      72      0        0        6
IsAuthenticated        78      78      0        0        0
IsAuthorized           78      72      0        6        0
------------------ ------------  -------  -------  ----------  --------
Total:                234     222      0        6        6
```

Importing Tokens Using the SiteMinder Token Tool

SiteMinder supports hardware-based security cards or tokens. Tokens use a dynamically generated password to provide an additional level of security.

All tokens require a data file provided by the vendor. Some tokens, such as ACE, access the token data file remotely on the vendor's server. Most tokens access the token database locally, through the SiteMinder Token Tool.

SiteMinder supports the following types of tokens:

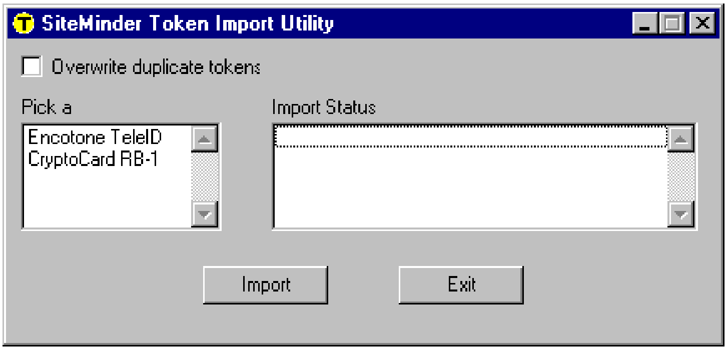
- Encotone TeleID
- CryptoCard RB-1

Before assigning tokens to users, the administrator must import a token data file. This file, provided by the token vendor, contains the identification or serial number for each token you are licensed to install.

To import the token data file:

1. From the Windows **Start** menu, select **Programs | SiteMinder | SiteMinder Test Tool**.

   The following dialog box opens:



2. Select the **Overwrite duplicate tokens** check box if you want to overwrite existing tokens.
3. Specify the type of token in the **Pick** field and click the **Import** button.

   The Token Tool displays the **Open** dialog.

4. Select the location from which to import the token data file and click the **Open** button.

   You can either import this file from your hard drive or directly from your install disk.

5. The Token Tool displays a list of all of the serial numbers installed in the database.

6. Click **Exit** to close and exit the token utility.

Index

A

about
- SiteMinder documentation, 9

accessing
- Policy Server from IE 5.0, NT, 22
- Policy Server, NT, 20
- Policy Server, Solaris, 39

Affiliate Agent
- configuring httpd.conf, 181
- configuring, IIS, 169
- configuring, NT/Netscape, 169
- configuring, Solaris/Apache, 177
- configuring, UNIX/Netscape, 177
- description, 167
- installing, NT, 168
- installing, UNIX, 176
- reinstalling, NT, 173
- reinstalling, UNIX, 182
- system requirements, NT, 167
- system requirements, UNIX, 175
- uinstalling, NT, 174
- uninstalling, UNIX, 183

Apache Affiliate Agent, Solaris
- configuring, 177
- configuring httpd.conf, 181
- installing, 176
- reinstalling, 182
- required Solaris patches, 175
- uninstalling, 183

Apache Web Agent, Solaris
- configuring, 155
- configuring after upgrade, Solaris, 226
- improving server performance, 164
- increasing shared memory segments, 163
- modifying httpd.conf, 157
- optimizing, 163
- pointing to a Policy Server, 196
- reconfiguring, 161
- reinstalling, 165
- uninstalling, 166
- upgrading, 224

audit log
- storing in an Oracle database, NT, 37
- storing in an Oracle database, Solaris, 78

B

browsers
- supported for Policy Server, NT, 15
- supported for Policy Server, Solaris, 30

C

certificate mapping
- upgrading, 208

Concepts Guide, SiteMinder, 9

conventions, 11

cookie provider
- in SiteMinder 4.0, 135
- upgrading, 218

D

Developer’s API Guide, SiteMinder, 10

documentation
- conventions, 11
- online books, 10
- online help, 10
- organization, 11
- printed, 9

release notes, 9
SiteMinder Agent Operations Guide, 9
SiteMinder Concepts Guide, 9
SiteMinder Deployment Guide, 9
SiteMinder Developer's API Guide, 10
SiteMinder Installation Guide, 9
SiteMinder Policy Server Operations Guide, 9

E

ems.properties
creating for JRUN, Solaris/Apache, 133
creating for ServletExec, Solaris/Apache, 132

F

failover
configuring, NT, 73
configuring, Solaris, 88
forms authentication schemes
in SiteMinder 4.0, 135
upgrading, 218
functionality tests
description, 263
performing, 265

H

HP-UX
configuring a Netscape Web Agent, 151
configuring an SSL credential collector, Netscape, 151
reconfiguring a Netscape Web Agent, 154
reinstalling a Netscape Web Agent, 165
uninstalling a Netscape Web Agent, 166
Web Agent system requirements, 148
httpd.conf
configuring Affiliate Agents, Solaris, 181
modifying for Web Agent, Solaris, 157
modifying to improve Apache performance, 164

I

IIS Affiliate Agent
configuring, 169
installing, NT, 168
reinstalling, 173
uninstalling, 174
IIS Web Agent
configuring, 138
configuring after upgrade, 220
installing, 136
reinstalling, 146
removing a Policy Server, 197
uninstalling, 147
upgrading, 219
Installation Guide, SiteMinder, 9
Internet Explorer 5.0
accessing the Policy Server User Interface, NT, 22

J

JRun
configuring, Solaris/Apache, 133
creating properties files, 133
jsm.properties
modifying for JRUN, Solaris/Apache, 134

K

key store
configuring SiteMinder to use LDAP, NT, 53
configuring SiteMinder to use LDAP, Solaris, 85
using an Oracle database, NT, 57
using an Oracle database, Solaris, 75

L

LDAP directory
configuring policy store, NT, 53
configuring policy store, Solaris, 34
creating a new policy store, Solaris, 80
exporting data, NT, 51

- exporting data, Solaris, 83
- migrating data, NT, 49, 51
- migrating data, Solaris, 83
- removing policy store data, 231
- removing policy store schema, 232
- removing the policy store, overview, 230
- storing policies, 48
- storing SiteMinder data, 80
- supported versions, NT, 47
- supported versions, Solaris, 30

limit parameters, Solaris
- increasing parameter values, 31

M

migrating data
- using smobjimport, 238

mime.types
- removing a Policy Server, NT/Netscape, 26

N

NDS policy store
- configuring, 91
- configuring in Policy Server Management Console, 93
- migrating data, 96
- removing data, 98
- system requirements, 91

Netscape Affiliate Agent
- configuring, NT, 169
- configuring, UNIX, 177
- installing, NT, 168
- installing, UNIX, 176
- reinstalling, NT, 173
- reinstalling, UNIX, 182
- required Solaris patches, 175
- uninstalling, NT, 174
- uninstalling, UNIX, 183

Netscape Web Agent
- configuring after upgrade, NT, 220
- configuring after upgrade, Solaris, 226
- configuring an SSL credential collector, NT, 142
- configuring an SSL credential collector, UNIX, 151
- configuring, NT, 142
- configuring, UNIX, 151
- installing, NT, 136
- installing, UNIX, 148
- pointing to a Policy Server, 196
- reconfiguring, UNIX, 154
- reinstalling, NT, 146
- reinstalling,UNIX, 165
- uninstalling, NT, 147
- uninstalling, UNIX, 166
- upgrading, NT, 219
- upgrading, Solaris, 224

Netscape Web Server
- configuring Policy Server, Solaris, 38
- uninstalling the Policy Server, NT, 26

NT
- accessing the Policy Server, 20
- configuring a Netscape Web Agent, 142
- configuring a policy store, 47
- configuring an IIS Web Agent, 138
- installing a Web Agent, 136
- installing the Policy Server, 16
- reinstalling a Web Agent, 146
- reinstalling the Policy Server, 19
- uninstalling a Web Agent, 147
- uninstalling the Policy Server, 24
- upgrading cookie providers, 219
- upgrading forms authentication schemes, 219
- upgrading SSL authentication schemes, 219
- upgrading the Policy Server, 199
- upgrading the Reports Server, 228
- upgrading Web Agents, 219
- Web Agent requirements, 136

O

obj.conf file
- editing for ServletExec, NT, 113
- editing for ServletExec, Solaris, 122
- modifying for Policy Server, Solaris, 38
- removing Policy Server, NT, 26
- removing the Policy Server, Solaris, 44

ODBC database
- adding a data source name, 45
- configuring, 44
- deleting, 246
- removing a policy store, 233
- required Oracle parameters, Solaris, 45
- upgrading user directory schema, 205

online
- books, 10
- help, 10

online help, 10

Oracle database
- configuring a policy store, NT, 60
- creating the SiteMinder schema, 60
- deleting, 246
- removing a policy store, 233
- required parameters for adding, 45
- requirements for policy store, NT, 47
- requirements for policy store, Solaris, 36
- storing SiteMinder data, Solaris, 75
- supported versions, Solaris, 30

P

Policy Server
- accessing, NT, 20
- accessing, Solaris, 39
- choosing an Oracle policy store, Solaris, 36
- configuring an LDAP key store, NT, 53
- configuring an LDAP key store, Solaris, 85
- configuring an LDAP policy store, NT, 53
- configuring an LDAP policy store, Solaris, 85
- configuring LDAP policy stores, Solaris, 34
- configuring Netscape Web server, Solaris, 38
- installing, NT, 16
- installing, Solaris, 32
- reinstalling, NT, 19
- removing from obj.conf, Solaris, 44
- removing windu files, Solaris, 43
- removing, Solaris, 43
- storing audit logs in an Oracle database, 37
- system requirements, NT, 15
- system requirements, Solaris, 29
- testing browser support, NT, 20
- testing browser support, Solaris, 39
- tools, 235
- uninstalling for Netscape Web servers, NT, 26
- uninstalling, NT, 24
- uninstalling, Solaris, 43
- upgrading certificate mapping, 208
- upgrading SQL queries, 205
- upgrading, NT, 199
- upgrading, overview, 199
- upgrading, Solaris, 201

Policy Server Management Console
- configuring an LDAP policy store, NT, 54
- configuring an ODBC database, 67
- configuring NDS policy store, 93

Policy Server Operations Guide, SiteMinder, 9

policy store
- configuring failover, NT, 73
- configuring failover, Solaris, 88
- configuring, NDS, 91
- creating an LDAP schema, Solaris, 80
- creating an NDS schema, 91
- creating an ODBC schema, NT, 60
- creating LDAP schema, NT, 49
- description, 47, 75
- exporting data for an upgrade, 198
- importing data after an upgrade, 204
- migrating data to an LDAP policy store, NT, 49
- migrating data to an LDAP policy store,

- Solaris, 85
- migrating data to an NDS policy store, 96
- migrating LDAP data, NT, 51
- removing after an upgrade, 230
- removing data from NDS, 98
- supported databases, NT, 47
- supported databases, Solaris, 75
- supported directories, NT, 47
- supported directories, Solaris, 75
- supported migrations, NT, 51
- supported migrations, Solaris, 83
- system requirements, NT, 47
- system requirements, Solaris, 76
- using an LDAP directory, 48
- using an SQL server database, 49, 57

printed documentation, 9

R

RADIUS
- reading log files, 249
- smreadclog, 249

Registration Services
- configuring JRun, Solaris/Apache, 133
- description, 109
- installing ServletExec, NT/IIS, 115
- installing ServletExec, NT/Netscape, 112
- installing ServletExec, Solaris/Apache, 124
- installing ServletExec, Solaris/Netscape, 118
- requirements for Web Agent, NT, 137
- requirements for Web Agent, UNIX, 149
- setting up, 110
- supported environments, 109
- testing ServletExec, 133

regression tests
- description, 266
- performing, 267

release notes, 9

Reports Server
- changing the redirection URL, 103
- description, 101
- installing, 102
- reinstalling, 104
- requirements, 102
- uninstalling, 105
- uninstalling, IIS Web Servers, 106
- uninstalling, Netscape 3.x, 106
- upgrading, 228

runapache, 131

S

s98sm
- configuring auto startup, Solaris, 40

schema
- creating for Oracle, 60
- creating for SQL, 60
- storing audit logs in Oracle, NT, 60
- storing audit logs in SQL, NT, 60
- storing policies in Oracle, NT, 60
- storing policies in SQL, NT, 60
- storing tokens in Oracle, NT, 60
- storing tokens in SQL, NT, 60

schmap.exe
- description, 91
- extending the NDS schema, 91
- removing policy store data, 98

screen resolution
- NT recommendations, 15
- Solaris recommendations, 30

servlet engine
- configuring JRun, Solaris/Apache, 133
- installing ServletExec, NT/IIS, 116
- installing ServletExec, NT/Netscape, 112
- installing ServletExec, Solaris/Apache, 125
- installing ServletExec, Solaris/Netscape, 119
- supported versions, 110

ServletExec
- creating properties files, Solaris/Apache, 132

- editing httpd.conf, Solaris/Apache, 128
- editing obj.conf, NT, 113
- editing obj.conf, Solaris, 122
- installing, NT/IIS, 116
- installing, NT/Netscape, 112
- installing, Solaris/Apache, 125
- installing, Solaris/Netscape, 119
- requirements, NT/IIS, 115
- requirements, NT/Netscape, 111
- requirements, Solaris/Apache, 124
- requirements, Solaris/Netscape, 118
- starting with runapache, Solaris/Apache, 131
- startup script, Solaris/Netscape, 120
- testing, 133
- verifying obj.conf, NT, 114

smcertmap.ini
- upgrading to SiteMinder 4.0, 208

smdsquery.ini
- upgrading to SiteMinder 4.0, 205

smldapsetup
- arguments, 243
- configuring a policy store, NT, 52
- configuring a policy store, Solaris, 80
- description, 240
- modes, 241
- removing a policy store, overview, 230
- removing policy store data, 231
- removing policy store schema, 232
- removing the policy store, 245
- using, 241

smobjexport, 51
- arguments, 236
- description, 235
- exporting data, 237
- exporting data for an upgrade, 198

smobjimport
- arguments, 238
- description, 238
- importing data, 238
- importing data after an upgrade, 204

smpatchcheck
- description, 248
- using, 248

smreadclog, 249
- arguments, 249
- description, 249
- using, 250

smuser account
- creating, Solaris, 30

Solaris
- checking patches, 248
- configuring a Netscape Affiliate Agent, 177
- configuring a Netscape Web Agent, 151
- configuring an Apache Affiliate Agent, 177
- configuring an Apache Web Agent, 155
- configuring an SSL credential collector, Apache, 151
- configuring an SSL credential collector, Netscape, 151
- configuring Policy Server auto startup, 40
- configuring the Policy Server to use LDAP, 85
- creating an LDAP key store, 80
- creating an LDAP policy store, 80
- creating an smuser account, 30
- increasing limit parameters, 31
- increasing shared memory segments, 163
- installing Policy Server, 32
- optimizing for an Apache Web Agent, 163
- patches required for Affiliate Agents, 175
- patches required for Policy Servers, 29
- patches required for Web Agents, 148
- reconfiguring a Netscape Web Agent, 154
- reconfiguring an Apache Web Agent, 161
- reinstalling a Web Agent, 165
- removing Policy Server, 43
- removing Policy Server windu files, 43
- storing keys in an Oracle database, 75
- storing policies in Oracle database, 75
- uninstalling a Web Agent, 166
- uninstalling the Policy Server, 41

- upgrading cookie providers, 224
- upgrading forms authentication schemes, 224
- upgrading SSL authentication schemes, 224
- upgrading the Policy Server, 201
- upgrading Web Agents, 224
- Web Agent system requirements, 148

SQL database
- configuring a policy store, NT, 60
- creating the SiteMinder schema, 60
- deleting, 246
- removing a policy store, 233
- required drivers for policy store, 58
- storing policies in, 49, 57

SSL authentication schemes
- configuring a Web Agent, NT/Netscape, 142
- in SiteMinder 4.0, 135
- upgrading, 218

startup
- configuring auto startup, Solaris, 40

stress tests
- description, 267
- performing, 270
- sample test report, 270
- thread control file, 268

support, 13

system requirements
- Affiliate Agent, NT, 167
- Affiliate Agent, UNIX, 175
- NDS policy store, 91
- Policy Server, NT, 15
- Policy Server, Solaris, 29
- policy store, NT, 47
- policy store, Solaris, 76
- Web Agent, NT, 136
- Web Agent, UNIX, 148

system_odbc.ini
- adding a data source name, 45
- description, 44
- editing for an Oracle database, Solaris, 77

T

technical support, 13

Test Tool
- configuring, 260
- description, 250
- loading configurations, 263
- performing functionality tests, 263
- performing regression tests, 266
- performing stress test, 267
- saving configurations, 263
- scripting language commands, 268
- testing a policy, 260
- using the interface, 251

thread control file
- description, 268
- example, 269

token data
- storing in an Oracle database, Solaris, 78

Token Tool
- description, 271
- importing token data files, 271

tools
- ODBC database tools, 246
- overview, 235
- smldapsetup, 240
- smobjexport, 235
- smobjimport, 238
- smpatchcheck, 248
- smreadclog, 249
- Test Tool, 250
- Token Tool, 271

U

unlimit command, 31

upgrading SiteMinder
- advanced authentication, 218
- certificate mapping, 208
- cookie providers, 218
- exporting data, overview, 198
- importing data, overview, 204
- in a multiple Policy Server environment,

186
in a single Policy Server environment, 192
ODBC user directory schema, 205
overview, 185
Policy Server, overview, 199
policy store, NT, 199
policy store, Solaris, 201
removing a Policy Server, 195
removing an ODBC policy store, 233
removing audit logs, 233
removing LDAP policy store data, 231
removing LDAP policy store schema, 232
removing token data, 233
Reports Server, 228
Web Agents, overview, 218

W

Web Agent
configuring after upgrade, NT, 220
configuring after upgrade, Solaris, 226
configuring for Apache, Solaris, 155
configuring for IIS, NT, 138
configuring for Netscape, NT, 142
configuring for Netscape, UNIX, 151
description, 135
improving Apache Server performance, Solaris, 164
increasing shared memory segments, Solaris, 163
modifying httpd.conf, Solaris/Apache, 157
optimizing for Apache, Solaris, 163
reconfiguring for Apache, Solaris, 161
reconfiguring for Netscape/UNIX, 154
reinstalling, NT, 146
reinstalling,UNIX, 165
removing a Policy Server, Apache, 196
removing a Policy Server, IIS, 197
removing a Policy Server, Netscape, 196
supported environments, 136
uninstalling, NT, 147
uninstalling, UNIX, 166
upgrading, overview, 218
Web Agent Configuration Wizard
accessing, 220
accessing, NT/IIS, 138
accessing, NT/Netscape, 143
Web Agent Operations Guide, SiteMinder, 9
Web browser
requirements, NT, 15
requirements, Solaris, 30
testing Policy Server support on NT, 20
Web server
Policy Server requirements, NT, 15
Policy Server requirements, Solaris, 30
webagent.conf
removing the Policy Server, NT, 25, 196
removing the Policy Server, Solaris, 196
webagent.properties
creating for JRUN, Solaris/Apache, 133
creating for ServletExec, Solaris/Apache, 132
windu files
removing Policy Server, Solaris, 43