IBM® SecureWay® Policy Director

Up and Running

Version 3 Release 0

SCT6-3KNA-00

IBM® SecureWay® Policy Director

Up and Running

Version 3 Release 0

SCT6-3KNA-00

Note

Before using this information and the product it supports, read the general information under "Appendix. Notices" on page 93.

First Edition (October 1999)

This edition applies to Version 3, release 0, modification 0 of IBM SecureWay Policy Director product (SCT6-3KNA-00) and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces IBM SecureWay Global Sign-On, Version 2.0.200.

Contents

About this book

This book provides information about installing and configuring IBM® SecureWay® Policy Director (Policy Director). The Policy Director servers can be installed on the following operating systems:

- Microsoft® Windows NT®
- AIX
- Solaris

The NetSEAT client can be installed on the following operating systems:

- Windows® 95
- Windows 98
- Windows NT

Who should read this book

This book is written for the administrator who will be planning for and installing Policy Director.

The administrator should be knowledgeable in installing and configuring the IBM Distributed Computing Environment (DCE) and the IBM SecureWay Directory's lightweight directory access protocol (LDAP). The IBM SecureWay Directory and IBM Distributed Computing Environment servers are used by Policy Director and the installation software for these servers is included in the Policy Director product.

How this book is organized

This book contains the following chapters:

- "Chapter 1. Understanding Policy Director" on page 1 gives an overview of Policy Director and its components.
- "Chapter 2. System requirements" on page 15 provides information about the software and hardware requirements that your operating environment must meet.
- "Chapter 3. Planning for Policy Director" on page 19 provides information to help you plan, organize, and manage Policy Director.
- "Chapter 4. Installing and configuring IBM SecureWay Directory" on page 27 provides information on the installation and configuration of the IBM SecureWay Directory Version 3.1.1 (LDAP) Client SDK and server when you choose the LDAP user registry. You must install and configure

the LDAP server before installing Policy Director. Also, the LDAP server must be running before installing Policy Director.

- "Chapter 5. Installing Policy Director for Windows" on page 41 describes the installation and configuration of Policy Director on the Windows NT operating system.
- "Chapter 6. Installing Policy Director for AIX" on page 55 describes the installation and configuration of Policy Director on the IBM AIX operating system.
- "Chapter 7. Installing Policy Director for Solaris" on page 73 describes the installation and configuration of Policy Director on the Sun Solaris operating system.
- "Chapter 8. Related documentation" on page 87 tells you where to find other documentation for Policy Director and documentation for related products.

What is new in this release

Policy Director includes these new features in this release:

- Support for the IBM SecureWay Directory for the storage of user and group credential information.
- The latest updates to the Authorization application programming interfaces (API) specification from the Open Group.
- Ability to define and edit IBM Firewall proxy user credentials using the Policy Director Management Console.
- A Policy Director Credentials Acquisition Service (Policy Director CAS) that provides support for the use of external authentication services.
- Support for client-side certificate-based authentication using the new Policy Director Credentials Acquisition Service.
- The ability to write your own customized credentials acquisition service using the Interface Definition Language (IDL) interface between WebSEAL and the Policy Director CAS. Policy Director also provides the general server framework that handles Policy Director CAS server functions, such as startup, server registration, and signal handling.
- The choice of using a secure sockets layer (SSL) tunneling mechanism in addition to generic security services (GSS) tunneling.
- Use of the Policy Director command-line interface to manage login and password policies.
- Use of the Policy Director Management Console, or command-line interface, to manage single sign-on users, groups, and resources.
- A Web-based single sign-on resource password management tool.
- An integrated installation process.

Year 2000 readiness

These products are Year 2000 ready. When used in accordance with their associated documentation, they are capable of correctly processing, providing, and/or receiving date data within and between the twentieth and twenty-first centuries, provided that all products (for example, hardware, software, and firmware) used with the products properly exchange accurate date data with them.

Service and support

Contact IBM for service and support for all the products included in the IBM SecureWay FirstSecure offering. Some of these products may refer to non-IBM support. If you obtain these products as part of the FirstSecure offering, contact IBM for service and support.

Conventions

This book uses the following typographical conventions:

Convention	Meaning
bold	User interface elements such as check boxes, buttons, and items inside list boxes.
`monospace`	Syntax, sample code, and any text that the user must type.
Italic	Emphasis and first use of special terms that are relevant to Policy Director.
→	Shows a series of selections from a menu. For example, click **File** → **Run** means click **File**, and then click **Run**.

Web information

Information about last-minute updates to Policy Director is available at the following Web address:

`http://www.ibm.com/software/security/policy/library`

Information about updates to other IBM SecureWay FirstSecure products is available by starting at the following Web address:

`http://www.ibm.com/software/security/firstsecure/library`

Chapter 1. Understanding Policy Director

IBM SecureWay Policy Director (Policy Director) is available either as a component of IBM SecureWay FirstSecure or as a standalone product.

What is IBM SecureWay FirstSecure?

IBM SecureWay FirstSecure (FirstSecure) is part of the IBM integrated security solution. FirstSecure is a comprehensive set of integrated products that help your company:

- Establish a secure e-business environment.
- Reduce the total cost of security ownership by simplifying security planning.
- Implement security policy.
- Create an effective e-business environment.

The IBM SecureWay products include:

Policy Director
IBM SecureWay Policy Director (Policy Director) provides authentication, authorization, data security, and Web resource management.

Boundary Server
IBM SecureWay Boundary Server (Boundary Server) provides:

- The critical firewall functions of filtering, proxy, and circuit level gateway
- A virtual private network (VPN) connection to the IBM Firewall
- The components needed for Internet security
- A mobile code security solution

A configuration graphical user interface (GUI) ties together the Policy Director's proxy user function with the Boundary Server's Firewall product.

Intrusion Immunity
Intrusion Immunity provides intrusion detection and antivirus protection.

Trust Authority

IBM SecureWay Trust Authority (Trust Authority) supports public key infrastructure (PKI) standards for cryptography and interoperability. Trust Authority provides support for issuance, renewal, and revocation of digital certificates. These certificates provides a means to authenticate users and to ensure trusted communications.

Toolbox

The IBM SecureWay Toolbox (Toolbox) is a set of application programming interfaces (API) with which application programmers can incorporate security into their software. You can obtain the Toolbox as part of FirstSecure. Both Policy Director and the Toolbox include the Policy Director API library and documentation.

Because each IBM SecureWay FirstSecure product can be installed independently, you can plan a controlled move toward a secure environment. This capability reduces the complexity and cost of securing your environment and speeds deployment of Web applications and resources.

See the FirstSecure *Planning and Integration* documentation for more information about the FirstSecure components and for a list of all the IBM SecureWay products' documentation.

What is IBM SecureWay Policy Director?

Policy Director is a standalone authorization and security management solution that provides end-to-end security of resources over geographically dispersed intranets and *extranets*. An *extranet* is a virtual private network (VPN) that uses access control and security features to restrict the use of one or more intranets attached to the Internet to selected subscribers.

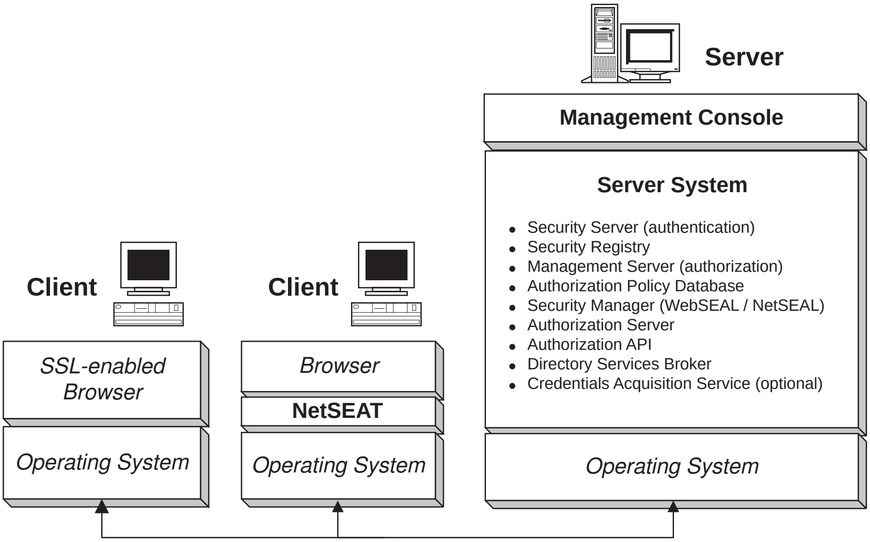
Policy Director provides authentication, authorization, data security, and resource-management services. You can use Policy Director in conjunction with standard Internet-based applications to build secure and well-managed intranets and extranets.

Policy Director runs on the Windows NT, AIX, and Solaris operating systems.

Policy Director components

Policy Director includes the following components:

- IBM SecureWay Directory's lightweight directory access protocol (LDAP) and IBM Distributed Computing Environment (DCE) clients and servers
- Policy Director Base
- Management server
- Security Manager, consisting of WebSEAL and NetSEAL
- Credential Acquisition Service (CAS)
- Authorization server
- Authorization API
- NetSEAT client
- Management Console
- Directory Services Broker (DSB)


Server
Management Console
Server System
• Security Server (authentication)
• Security Registry
• Management Server (authorization)
• Authorization Policy Database
• Security Manager (WebSEAL / NetSEAL)
• Authorization Server
• Authorization API
• Directory Services Broker
• Credentials Acquisition Service (optional)
Operating System
Client
SSL-enabled Browser
Operating System
Client
Browser
NetSEAT
Operating System

Before you install Policy Director, you must determine what security and management capabilities your network requires. Use the following sections to decide which Policy Director components you need.

IBM SecureWay Directory and DCE servers

The IBM SecureWay Directory and IBM Distributed Computing Environment servers are used by Policy Director and are included with the Policy Director product.

Policy Director can use either an LDAP user registry or a DCE user registry. You are prompted to select the user registry type during Policy Director installation.

If you plan to use an LDAP user registry, you must install an LDAP client and configure an LDAP server before installing Policy Director. Follow the instructions in “Chapter 4. Installing and configuring IBM SecureWay Directory” on page 27. If you plan to use a DCE user registry, you can skip the section on installing and configuring LDAP.

IBM SecureWay Directory server

SecureWay Directory provides the lightweight directory access protocol (LDAP) to maintain directory information in a central location for storage, updates, retrieval, and exchange. When you use LDAP for your user registry, Policy Director uses LDAP to grant authorization to users.

IBM Distributed Computing Environment server

Distributed Computing Environment (DCE) includes services and tools that support the creation, use, and maintenance of distributed applications in a heterogeneous computing environment. DCE forms the secure domain within which the Policy Director servers can mutually authenticate the user and securely communicate. On the Windows NT operating system, the NetSEAT client functions as the DCE client.

Policy Director Base

The Policy Director Base (IVBase) component is the common reference software used by all Policy Director components. This component is installed automatically when you install other Policy Director components, except when you install the Management Console on Windows.

For AIX, the SMIT Setup (IV.Smit) component is included as part of the IV.Base package. This package contains configuration information used by SMIT. The SMIT Setup package must be installed on all AIX servers.

Management server

The Management server (IVMgr) is the primary authorization server for the entire secure domain. The Management server controls and maintains the master authorization policy database. All data flows through the Management server.

The Management server must be installed on a computer in the secure domain before you install any Security Managers or the Authorization servers, but not necessarily on the same computer. There must be only one instance of the Management server installed in a given secure domain.

Each instance of the Management server requires that you install the following components, which includes the Management server, on the same computer:

- DCE client
- LDAP client (if you are using LDAP as your user registry)
- Policy Director Base
- Management server

Security Manager

The Security Manager (IVNet) appliesan access control policy that is based on information from a replica authorization policy database. The Security Manager includes the following components:

- WebSEAL for fine-grained Hypertext Transfer Protocol (HTTP) and Secure Sockets Layer interface (HTTPS) access control
- NetSEAL for coarse-grained Transmission Control Protocol/Internet Protocol (TCP/IP) access control

The NetSEAL and WebSEAL components are required to configure and enable these capabilities, which by default are disabled.

WebSEAL

WebSEAL (IVWeb) is the HTTP server component of the Security Manager. WebSEAL is a secure Web server that supports HTTP, HTTPS, and NetSEAT clients. WebSEAL combines with the Policy Director Credential Acquisition Service (Policy Director CAS) to support X.509 certificate-based authentication to a Policy Director user.

NetSEAL

NetSEAL (IVTrap) provides coarse-grained access control for TCP/IP servers. NetSEAL controls access to a set of configured ports on a TCP/IP server.

The Policy Director product suite provides security for client/server data exchange across the Internet and private intranets. Policy Director NetSEAL and Policy Director WebSEAL are server-side products that control and manage network data within secure domains defined by DCE.

Authorization server

The Authorization server (IVAcld) handles authorization requests from third-party applications that use the Policy Director Authorization API in remote mode. The Authorization server should be installed on at least one computer in the secure domain for third-party applications.

Authorization application programming interface

The Policy Director Authorization Application Development Kit (IVAuthADK), or Policy Director ADK component, includes the Policy Director Authorization application programming interfaces (API). These API let you build applications that use the Policy Director authorization.

The Policy Director ADK includes an authorization API server (AuthAPI) that lets developers build Policy Director security and authorization directly into corporate applications. The Policy Director authorization API provide direct access to the Policy Director Authorization Service. Use of these authorization API means that developers no longer need to write authorization code for each application.

The ADK includes C example programs.

The ADK also contains the source for the Policy Director CAS demonstration server, an external authorization service demonstration server.

NetSEAT client

The Policy Director NetSEAT client is a lightweight client for Windows 95, Windows 98, or Windows NT. NetSEAT provides secure communication channels to Policy Director servers.

The NetSEAT client software lets clients join secure domains and use the advanced security services that are offered by WebSEAL and NetSEAL servers. NetSEAT secures all of a client's network communications, allowing end-to-end encryption of all Web-based as well as client and server traffic.

NetSEAT provides the ability to secure a client's TCP/IP traffic, such as the traffic generated by services like Telnet and POP3. NetSEAT allows a system administrator to exercise coarse-grained control over a workstation's network activities. This control results from the use of the secure domain's ability to authenticate users and attach authorization privileges to users and resources.

Management Console

The Management Console (IVConsole) is a Java™-based graphical application that is used to manage security policy for the Policy Director secure domain. Using the Management Console, you can perform administrative tasks on the account registry and the primary authorization policy database. The Management Console requires a DCE client to log in to the secure domain and perform secure management remote procedure calls (RPCs) to the Policy Director Management servers. The Management Console uses lightweight DCE services (runtime services) provided by the NetSEAT client on Windows 95, Windows 98, or Windows NT.

Directory Services Broker

The Directory Services Broker (DSB) is distributed as part of the Management server component. The Management Console and NetSEAT clients require a DSB in the secure domain when running on a Windows 95, Windows 98, or Windows NT workstation. The DSB typically requires no administration or configuration after initial installation.

Credentials Acquisition Service (optional)

The Policy Director Credentials Acquisition Service (Policy Director CAS) is an optionally configured component.

Credential acquisition is the process of transforming, or mapping, specific identity information provided by an authentication mechanism into a common, domain-wide representation of the client's identity. This common representation is called the *client's credentials*.

When you need credentials acquisition or mapping, you must configure the Policy Director CAS to be used with the Policy Director WebSEAL server. Policy Director users are automatically mapped to credentials by WebSEAL.

Clients accessing Policy Director using client-side X.509 certificates can have *certificate* information mapped to Policy Director identities through the Policy Director CAS, or by writing your own credentials acquisition service.

If you have users defined in some other external registry, the user names can be mapped to Policy Director identities through the use of a customized CAS server. You can write and customize your own CAS server to provide a specific solution for the secure domain and to process authentication information, such as: client certificates, user names, or tokens. The Policy Director Credentials Acquisition Service developer or designer determines entirely the specifics of this authentication and mapping service.

Policy Director stores mapping rules in a database external to Policy Director. Policy Director provides the Interface Definition Language (IDL) interface between WebSEAL and the Policy Director CAS. Policy Director also provides the general server framework that handles Policy Director CAS server functions such as startup, server registration, and signal handling. It is the Policy Director CAS developer's responsibility to extend the credentials acquisition service's framework to carry out the identity mapping functions that are required by the particular application.

For more information about each of the Policy Director components, refer to the *Policy Director Administration Guide*.

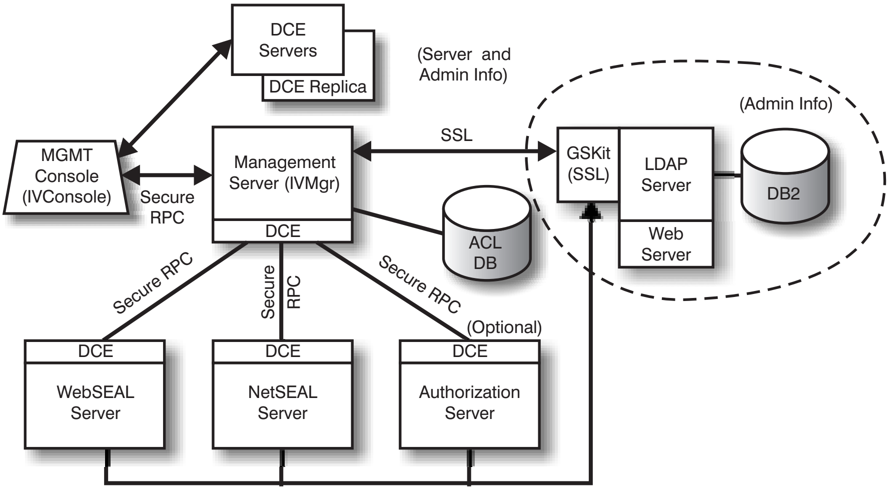
How does Policy Director work?

The following sections show four scenarios that demonstrate typical uses of Policy Director:

- An administrator using the Management Console
- A user accessing protected Web resources from a Web browser
- A user accessing a protected TCP/IP server using a NetSEAT client
- A user accessing a protected third-party server

Administrator using the Management Console

The following figure shows how data flows when an administrator is using the Management Console to manage Policy Director. The LDAP components, which are shown in the dotted line, are required only if you use LDAP as your user registry.



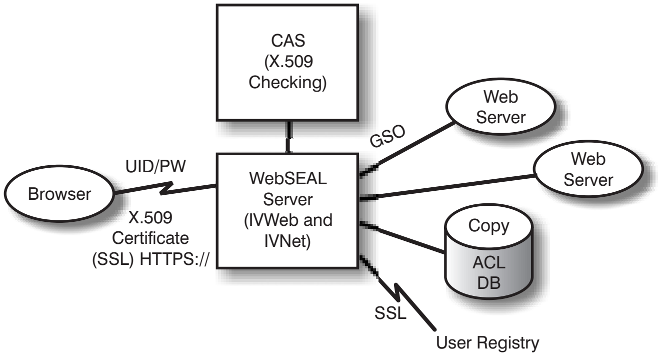
An administrator at the Management Console authenticates to the secure domain and receives credentials.

When the administrator manages users or groups from the Management Console, the Management Console sends requests over a secure RPC to the Management server. The Management server sends the corresponding changes to the LDAP server over an SSL connection that was previously established using the Management server's distinguished name (DN) and password.

When the administrator adds, modifies, or applies an access control list (ACL), the Management Console sends the data over a secure RPC to the Management server. The Management server then stores the changes in the local copy of the ACL database. When the required ACL database is modified, the Management server notifies all other servers through a secure RPC that the ACL database has changed. The WebSEAL, NetSEAL, and Authorization servers also check with the Management server periodically for updates in the ACL database.

User accessing protected Web resources from a Web browser

The following figure shows how data flows when a user is accessing protected Web resources from a Web browser.



When the user tries to access a protected Web page, the SSL-enabled browser contacts the WebSEAL server. If WebSEAL is configured for client certificate-based authentication, WebSEAL requests an X.509 certificate from the browser. When WebSEAL receives the certificate from the browser, it passes the certificate to the CAS server. The CAS attempts to map the received certificate to a user identity understood by Policy Director. Within the CAS's configuration file, the Policy Director administrator can create a table that is used to associate a certificate DN with the DN of a Policy Director user. When the CAS is called by WebSEAL with a certificate, it first extracts the DN from the certificate and searches the table for a match. If a match is found, the CAS returns the associated Policy Director user DN to WebSEAL. WebSEAL then uses this DN to identify the Policy Director user. If a match is not found, the CAS returns the DN from the certificate to WebSEAL. In this case the DN in the certificate is used to identify the Policy Director user. The WebSEAL server uses the returned DN to retrieve the user's credentials.

For more information on X.509 certificates, see the following Web address:

`http://www.ietf.org`

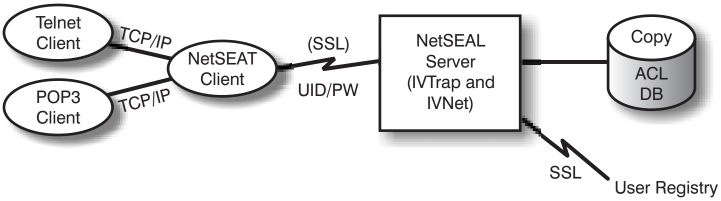
When WebSEAL successfully completes the authentication of the user, WebSEAL uses the local replica of the ACL database to decide whether the user is authorized to access the Web object in the requested manner.

If the connection between the WebSEAL server and the back-end server that contains the Web resource being accessed is a Global Sign-On (GSO) junction, WebSEAL looks up the GSO credentials for that junction in LDAP and passes the username and password to the Web server.

For information about managing GSO resources and GSO resource groups, see the Management Console information in the *Policy Director Administration Guide*.

User accessing a protected TCP/IP server using a NetSEAT client

The following figure shows how data flows when a user is accessing a protected TCP/IP server using a NetSEAT client.



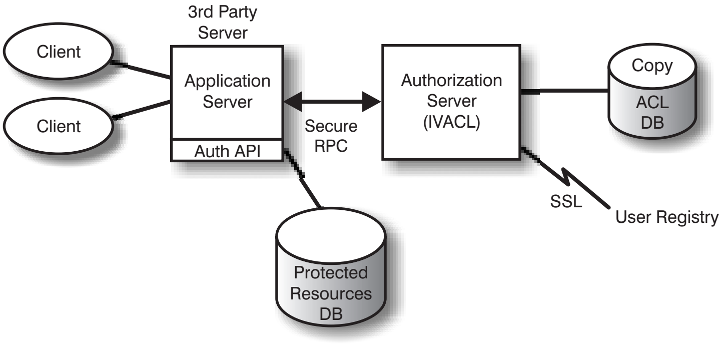
The user at the Telnet client telnets to a NetSEAL-protected server, which identifies that the user is asking for access. NetSEAL asks for the username and password and verifies the user’s identity by providing the user information and comparing it to the value stored in the user registry. NetSEAL verifies that the user can access the computer over the specified port.

NetSEAT transparently redirects requests to secure Policy Director servers, sending the information through a secure SSL tunnel. NetSEAT uses its configuration information to recognize requests to a secure server from generic TCP/IP applications such as Telnet, POP3, or HTTP. NetSEAT uses basic authentication over SSL to establish the NetSEAT user’s identity and credentials. After authorization is established, secure SSL encapsulates and completes the requested transaction according to the applicable security settings.

For example, when a Web browser requests access to a service or resource that is secured by Policy Director Security Manager, NetSEAT transparently intercepts the request and routes it to the appropriate server. If this is the first request to Policy Director and requires authentication, NetSEAT prompts the user with a login dialog box. When a user has been authenticated, Policy Director transparently attaches the appropriate credentials to each future request for information. This process enables a single sign-on environment for all Winsock applications managed by Policy Director. Additionally, Policy Director uses these credentials to determine whether the user can access the requested Policy Director protected resource.

User accessing a protected third-party server

The following figure shows how data flows when a user is accessing a protected third-party server.



When a client tries to access protected data on a third-party protected server, the third-party server authenticates the user and maps the user to a Policy Director user. The application server passes the Policy Director user information to the Authorization server, which contacts LDAP (or another product, such as DCE, that is used for the user registry) and retrieves the user's credentials. The application server then passes the credentials, the name of the object that the user wants to access, and the operation the user wants to perform to the Authorization server. The Authorization server returns an indication of whether the operation should be allowed. The application server then allows or denies the access.

What does the Policy Director package contain?

The IBM SecureWay Policy Director product, Version 3.0, is delivered on five CDs. The titles and contents of the CDs are shown in the following table.

CD Title	Contents
IBM SecureWay Policy Director Version 3.0	• IBM Policy Director Version 3.0
IBM SecureWay Policy Director Security Services	• IBM DCE for AIX Version 2.2 • IBM DCE for Windows NT Version 2.2 • Transarc DCE for Solaris Version 2.0
IBM SecureWay Directory Version 3.1.1 for AIX	• IBM SecureWay Directory Version 3.1.1 • IBM DB2 Version 5.2 with Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit Version 3.0.1 (GSKit)
IBM SecureWay Directory Version 3.1.1 for NT	• IBM SecureWay Directory Version 3.1.1 • IBM DB2 Version 5.2 with Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit Version 3.0.1 (GSKit)
IBM SecureWay Directory Version 3.1.1 for Solaris	• IBM SecureWay Directory Version 3.1.1 • IBM DB2 Version 5.2 with Fix Pack 8 • IBM Global Security Kit SSL Runtime Toolkit Version 3.0.1 (GSKit)

Chapter 2. System requirements

Your operating environment must meet the software and hardware requirements that are discussed in the following sections. For the latest information about system requirements, see the Policy Director README file. The README file contains information that supersedes the product publications.

To obtain the most current README file, access the library page of the IBM SecureWay Policy Director Web site.

```
http://www.ibm.com/software/security/policy/library
```

Before you install the Policy Director DCE, LDAP, NetSEAT, and server components, be sure you have the necessary hardware and software, listed in the sections that follow.

Hardware requirements

Memory usage, buffer and cache management, and control structures are scalable. However, the underlying requirements of your base operating system, the requirements of the prerequisite DCE and LDAP clients, and the requirements of your client applications dictate the minimum requirements for disk space and memory for your configuration.

The hardware requirements for the Policy Director server are as follows:

Platform	Minimum Disk Space	Minimum Memory
Windows NT server, with Intel® or Intel-compatible 80486 133 MHz or higher	16MB	64MB
AIX server, hardware that runs AIX 4.3.1	16MB	64MB
Solaris server, with hardware that runs Solaris 2.6	16MB	64MB

The hardware requirements for the Policy Director client are as follows:

Platform	Minimum Disk Space	Minimum Memory
Windows NT client, with Intel or Intel-compatible 80486 133 MHz or higher	16MB	32MB
AIX server, hardware that runs AIX 4.3.1	16MB	32MB
Solaris server, with hardware that runs Solaris 2.6	16MB	24MB

Software requirements

While planning your Policy Director installation, be sure that you have the correct versions of the operating systems and other prerequisite software, that are shown in the following sections. Following are the operating system requirements for Policy Director servers, the NetSEAT client, and the Management Console:

Policy Director servers

The Policy Director servers can be installed on the following operating systems:

- Windows NT Server Version 4.0 with Service Pack 4 or higher
- AIX Version 4.3.1 or higher
- Sun Solaris Version 2.6

NetSEAT clients

Policy Director NetSEAT clients can be installed on the following operating systems:

- Windows NT Version 4.0 with Service Pack 4 or higher
- Windows 98
- Windows 95

Management Console

The Policy Director Management Console can be installed on the following operating systems:

- Windows NT server, Version 4.0, with Service Pack 4 or higher
- Windows NT, Windows 95, or Windows 98
- AIX Version 4.3.1 or higher, including Java Runtime 1.1.6 or higher
- Sun Solaris Version 2.6

Other software requirements

Policy Director requires a DCE server and, if you are using LDAP as your user registry, an LDAP server. One server (either LDAP or DCE) must be on at least one computer in the secure domain. The DCE and LDAP clients and servers are provided as part of the Policy Director product. You must install DCE and LDAP before you install Policy Director. Or, you can use an existing installation of DCE and LDAP that is at the correct level.

Windows NT and AIX

On the Windows NT and AIX platforms, Policy Director servers require the following software:

- IBM DCE for Windows NT Version 2.2 or higher for Windows NT servers, or IBM DCE for AIX Version 2.2 or higher for AIX servers
- IBM SecureWay Directory Version 3.1.1 (LDAP), which includes DB2 Version 5.2, Fix Pack 7. LDAP is required only if you are using LDAP for your user registry.
- Secure Sockets Layer (SSL) Version 3.0 or higher.
- Policy Director CAS and WebSEAL require one of the following Web browsers:
  - Microsoft Internet Explorer Version 4 or higher
  - Netscape Communicator Version 4.5 or higher
  - Netscape Navigator Version 4.5 or higher
- For Policy Director clients on Windows 95 only, you must have Winsock Version 2.0 or higher.

Solaris

On the Solaris platform, Policy Director servers require the following software:

- Transarc DCE Version 2.0.
- IBM SecureWay Directory (LDAP) Version 3.1.1, which includes DB2 Version 5.2, Fix Pack 8. LDAP is required only if you are using LDAP for your user registry.
- Secure Sockets Layer Version 3.0 or higher.
- Policy Director CAS and WebSEAL require one of the following Web browsers:
  - Microsoft Internet Explorer Version 4 or higher
  - Netscape Communicator Version 4.5 or higher
  - Netscape Navigator Version 4.5 or higher

Chapter 3. Planning for Policy Director

The following sections provide the information you need to prepare and plan for the installation and configuration of Policy Director. Be sure to read "Chapter 1. Understanding Policy Director" on page 1 and decide which components of Policy Director you need before you plan your installation.

Common configurations

The configurations shown in this section can help you determine the appropriate configuration for your network. Use the table in "Components required for common configurations" on page 20 to determine the components you require for your configuration. Then select these components during Policy Director installation. Note that WebSEAL and NetSEAL can be installed on any computer. Some common Policy Director component configurations are shown in the following list:

Management server only
A server running the single instance of the Management server for the secure domain. In this scenario, the Management server resides by itself on its own system. The Management server maintains the master authorization database for the secure domain, replicates this database throughout the secure domain, and maintains location information about other Policy Director server computers in the secure domain.

Security Manager with WebSEAL server
Two components form WebSEAL—the Security Manager (IVNet) and WebSEAL (IVWeb). A WebSEAL server protects a Web space. WebSEAL supports back-end servers for high availability and fault tolerance through junctions known as *smart junctions*.

Security Manager with NetSEAL server
Two components form NetSEAL—the Security Manager (IVNet) and NetSEAL (IVTrap). A NetSEAL server secures a virtual private network (VPN) and provides access control for legacy and third-party network services.

Security Manager with WebSEAL and NetSEAL server
A combination WebSEAL and NetSEAL server.

Authorization server
A server that provides access to the Policy Director authorization service for third-party applications that use the Policy Director Authorization API.

Authorization server and ADK
A server that provides a development environment for developers who want to build third-party applications that use the Policy Director Authorization API to call the authorization service.

Management Console
A Java-based graphical application that is used to manage security policy for the Policy Director secure domain. IVBase is not required for the Management Console on Windows.

All components
A server providing the combined services of all the above configurations.

Components required for common configurations

The Policy Director configurations that are described in “Common configurations” on page 19 are listed in the following table. The table shows which components must be installed for each configuration. When read from left to right, the indicated components are in the correct installation order.

Note that two components form both WebSEAL and NetSEAL:

WebSEAL	Security Manager (IVNet) and WebSEAL (IVWeb)
NetSEAL	Security Manager (IVNet) and NetSEAL (IVTrap)

Notes for IVBase:

- IVBase is not required for the Management Console on Windows.
- IV.Smit is automatically installed with IV.Base on AIX.

Scenarios	Installation Packages							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
Single instance of Management server only	X	X						
Security Manager with WebSEAL	X	X***	X	X				
Security Manager with NetSEAL	X	X***	X		X			
Security Manager with WebSEAL and NetSEAL	X	X***	X	X	X			
Authorization server	X	X***				X		
Authorization server and ADK	X	X***				X	X	
Management Console	X							X
All components	X	X***	X	X	X	X	X	X

*** If this is the first or only computer in the secure domain, you must install the Management server (IVMgr). If this is an additional computer in an existing secure domain with an existing Management server, you should not install another Management server. There must be only one Management server in any given secure domain.

Information required before installing

Before you begin to install Policy Director, make a note of the system information that is required for installing the Policy Director software.

Policy Director servers

- User name for cell administrator (cell_admin)
- Password for cell administrator (cell_admin)
- WebSEAL: HTTP port (default)
- WebSEAL: Web document root directory

NetSEAT client (Windows only)

- Cell name
- Security server host name
- Time server host name
- Directory Services Broker host name

Tunnel mechanisms

Policy Director supports the following protocols for transmitting encrypted data:

- Secure Sockets Layer (SSL) tunneling
- Generic Security Services (GSS) tunneling

WebSEAL supports data integrity and data privacy that are provided by the SSL-encrypted tunnel. WebSEAL and NetSEAL support RPCs. Use of integrity and timestamps with RPC provides protection against *playback attacks*. A playback attack occurs when a user's data is captured as it flows between that user's client and the server. That data is then replayed or presented back to the server as a means of impersonating that first user.

SSL tunneling: The SSL protocol allows the exchange of signals to set up communications between two workstations. This protocol provides security and privacy over the Internet. SSL works by using public key for authentication and secret key to encrypt data that is transferred over the SSL connection.

Enable SSL when using SSL tunneling to Policy Director NetSEAL servers. This configuration is used when a NetSEAT client serves as an SSL client to a Policy Director NetSEAL server that is securing specific ports (for example, the port used by Telnet).

Policy Director WebSEAL supports SSL Versions 2 and 3.

GSS tunneling: The GSS interface (GSS API) is a standard way to allow applications to access security services. GSS tunneling is used over secure RPCs. Enable this option when installing the NetSEAT client as a support module to either Policy Director for Microsoft Windows NT or Policy Director Management Console.

GSS tunneling provides security services to callers in a generic fashion. It is supportable with a range of underlying mechanisms and technologies. It allows source-level portability of applications to different environments. GSS tunneling enables control over the level of protection on traffic traveling in both directions independently of each other. For example, data traveling from the client to the server might be fully protected with bulk data encryption while data traveling from the server to the client might be unprotected.

Installation requirements for the secure domain

Policy Director is a highly distributed security system whose components can be installed in a variety of configurations on one or more computers. The following list shows what components must be installed on the secure domain.

- DCE services
- A user registry. (IBM SecureWay Directory is required only if you are using LDAP for your user registry)
- Policy Director servers
- Policy Director Management Console
- Policy Director Authorization ADK

If you are using an existing installation of DCE or LDAP, be sure that the existing installation is at the correct level. For the correct levels, see “Other software requirements” on page 16.

Observe the following dependencies before you install the Policy Director product.

Distributed computing environment services

Each Policy Director secure domain (DCE cell) requires a full DCE services installation on at least one computer to secure the communications between Policy Director servers. DCE services can reside on the same host as the Policy Director servers or can be located on a remote host on the network.

For information about installing DCE, see the installation and administration manuals and technical support resources for your required platforms. See “IBM Distributed Computing Environment documentation” on page 88 for a list of DCE documentation.

Use the following guidelines when installing DCE:

- If you are creating a new Policy Director secure domain on a single host system, perform a full DCE server installation.
- If the DCE servers are located on a remote host, create a new secure domain by installing Policy Director on a local host.
- If you are installing Policy Director for Windows NT in an existing Policy Director secure domain, use the NetSEAT client to provide access to the required DCE services. Install the NetSEAT client on the same host as the Policy Director for Windows NT servers.

User registry

Policy Director can use either the IBM SecureWay Directory (LDAP) user registry or the DCE user registry as its user registry.

If you use LDAP as the user registry, you must have an LDAP server installed and configured before installing Policy Director, and you must also install an LDAP client on each Policy Director computer. See “Chapter 4. Installing and configuring IBM SecureWay Directory” on page 27, or refer to *IBM SecureWay Directory Installation and Configuration Version 3.1.1* for complete LDAP installation information. See “IBM SecureWay Directory documentation” on page 89 for the location of this LDAP documentation.

Or, see the DCE product information, listed in “IBM Distributed Computing Environment documentation” on page 88, for information about installing DCE.

Policy Director servers

The following requirements apply to installing the Policy Director servers.

- To communicate properly, all Policy Director Windows NT servers require the Policy Director NetSEAT client.
- All Policy Director server installations require the base component, which is automatically installed.
- If you are installing the *first* or *only* computer in the secure domain, you must install the Management server on the computer.
- If you are installing an *additional* computer in an existing secure domain that has an existing Management server, do not install another Management server. There must be only one instance of the Management server in any given secure domain.
- WebSEAL, NetSEAL, and third-party Authorization server components are optional.
- The Security Manager combines with WebSEAL to provide the WebSEAL HTTP server component and fine-grained HTTP access control, and combines with NetSEAL to provide the NetSEAL coarse-grained TCP/IP access control component.
- All Policy Director servers on AIX and Solaris require a full DCE client and, if you are using LDAP as your user registry, an LDAP client.

Management Console

The Management Console requires that the secure domain and the Management server be installed and configured. The Management Console also requires a DCE client and, if it is on a Windows computer, the NetSEAT client.

Authorization ADK

Install the Policy Director authorization ADK on the application development computer. The Authorization ADK can be used to develop applications that allow users to access protected third party servers. The Authorization ADK requires the base component, which is automatically installed when the Authorization ADK is installed.

The secure domain in which the application runs must have an Authorization server installed on at least one computer. A typical development environment includes the Authorization server on the same system as the Authorization ADK.

Step-by-step Policy Director installation overview

Installation of the Policy Director requires the following steps:

1. If you have a previous version of IBM SecureWay Policy Director installed, and you want to migrate your installation, refer to the migration information on the Policy Director Web page (see “Web information” on page vii).
2. Verify that your operating system supports Policy Director.

   See “Policy Director servers” on page 16 for information about supported operating systems.
3. Determine which server components best fit your requirements and on which computers to install these components.

   See “Common configurations” on page 19 for assistance.
4. Decide if the secure domain will use SSL tunneling or GSS tunneling.

   See “Tunnel mechanisms” on page 22 for more information.
5. Install and configure a DCE infrastructure, if one does not exist.

   See “Distributed computing environment services” on page 23 for an overview of the required DCE services.
6. Decide if the secure domain will use an LDAP user registry or a DCE user registry. If you are using the IBM SecureWay Directory (LDAP) for your user registry and if you are not using an existing LDAP, install and configure LDAP.

   See “Chapter 4. Installing and configuring IBM SecureWay Directory” on page 27 for instructions about installing and configuring LDAP.
7. Install the DCE and LDAP clients on the computers to be used for the Policy Director servers.

   See the DCE product information, listed in “IBM Distributed Computing Environment documentation” on page 88, for information about installing DCE.

8. Install the Policy Director server components.

   See the installation chapter for the operating system platform you will be using. Use one of the following:

   - "Chapter 5. Installing Policy Director for Windows" on page 41
   - "Chapter 6. Installing Policy Director for AIX" on page 55
   - "Chapter 7. Installing Policy Director for Solaris" on page 73

9. Configure the Credentials Acquisition Service if you will be using the Policy Director CAS for client certificate authentication.

   See "Configuring the Credentials Acquisition Service" for information about the Policy Director CAS.

10. Install the Management Console.

    See the installation chapter for the operating system platform you will be using. Use one of the following:

    - For Windows NT, see "Installing the Management Console on Windows" on page 50.
    - For AIX, see "Installing the Management Console" on page 68.

      To configure the Management Console, see "Configuring and starting the Management Console" on page 60 if you are using the LDAP user registry, or see "Configuring and starting the Management Console" on page 66 if you are using the DCE user registry.
    - For Solaris, see "Installing and starting the Management Console" on page 84.

Reinstalling Policy Director

If you need to reinstall any package, you must first remove the existing package, and then reinstall the desired package. See "Removing Policy Director" on page 69 for instructions.

Configuring the Credentials Acquisition Service

The Policy Director Credentials Acquisition Service (Policy Director CAS) is a customizable component of Policy Director that you can use to extend the standard authentication mechanisms that are supported by WebSEAL.

The Policy Director CAS is installed automatically. If you want to use Policy Director CAS as your credentials acquisition service, you must configure it. See Chapter 2 and Chapter 13 in the *Policy Director Administration Guide* for information on understanding and configuring the Policy Director CAS.

Chapter 4. Installing and configuring IBM SecureWay Directory

If you plan to use a DCE user registry, you can skip this section on installing and configuring IBM SecureWay Directory (LDAP).

During Policy Director installation, you are asked to choose either an LDAP user registry or a DCE user registry.

- If you choose LDAP, you must install an IBM SecureWay Directory Version 3.1.1 (LDAP) Client SDK and server, and then configure the LDAP server before installing Policy Director.
- If you use SSL to access the LDAP server, the LDAP client must be configured also.

Installing the LDAP server and client

Policy Director requires an LDAP server and client if you are using LDAP as your user registry.

An LDAP server must be on at least one computer in the secure domain. The software for the LDAP client and server is provided as part of the Policy Director product. You must install this software before you install Policy Director, or you can use an existing installation of LDAP that is at the correct level.

During the installation of LDAP, choose to install **SecureWay Directory and Client SDK**.

For more information about the installation and configuration of LDAP, see the *IBM SecureWay Directory Installation and Configuration Version 3.1.1* documentation. There is a separate version of this book in HTML format for each of the supported operating systems on the appropriate CD. See “IBM SecureWay Directory documentation” on page 89 for information on how to access the documentation.

Installing the LDAP client only

If you are using LDAP as your user registry, you must install the LDAP client on each system that will run Policy Director. The LDAP client software is provided as part of the Policy Director product. Install the LDAP client before you install Policy Director.

During the installation of LDAP, choose to install **SecureWay Client SDK** only if you already have an existing installation of the LDAP server that is at the correct level already installed and configured for Policy Director.

Configuring the LDAP server

If you are using LDAP as your user registry, you must configure the LDAP server before installing the first Policy Director server. After configuring the LDAP server for the first Policy Director system, you do not need to reconfigure the LDAP server when you add additional Policy Director servers.

If you enabled SSL access to the LDAP server during the LDAP server configuration, you will need to copy a client and server key ring pair to each additional computer that uses SSL access. See "Enabling SSL access (optional)" on page 32 for more information.

To configure the LDAP server, you must complete the configuration steps in the following list one time only for each secure domain:

1. Add necessary suffixes. See "Adding suffixes" on page 29 for instructions.
2. Install security schema objects and attributes. See "Installing security schema objects and attributes" on page 29.
3. Enable LDAP access control. See "Enabling LDAP access control" on page 39 for instructions.
4. Enable SSL access. See "Enabling SSL access (optional)" on page 32 for instructions.

If you enabled SSL access, complete the steps in "Setting up the LDAP client for SSL access" on page 36 every time you add an LDAP client (Policy Director server) that uses SSL to access the LDAP server.

Note: LDAP administrators can specify password encryption settings in the LDAP database. LDAP permits passwords to be stored as clear text, which could pose a security risk. See your LDAP documentation for instructions on setting user password attributes to the appropriate encryption level.

Adding suffixes

In the IBM SecureWay Directory, create a new suffix by completing the following steps:

1. Using a Web browser, access the IBM SecureWay Directory Server Web Administration tool at Web address

   ```
   http://servername/ldap
   ```

   Log in through the Web interface as the LDAP administrator (for example, `cn=root`).
2. Click: **Suffixes → Add a suffix**.
3. In the **Suffix DN** field, you must add the suffix:

   ```
   secAuthority=Default
   ```

   The object for `secAuthority=Default` is created during configuration of the Management server.
4. Click the **Add a new suffix** button.
5. To add another suffix, click the **Add a suffix** link to return to the previous window.
6. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix. For example:

   ```
   o=IBM,c=US
   ```

   You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization's abbreviated name, and where `c=` is the country.

   This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.
7. Click the **Add a new suffix** button.
8. Repeat the procedure for each new suffix you want to add and required for your organization.
9. Click **restart the server** link on the current LDAP Administration tool Web page to restart the LDAP server when you are finished adding suffixes.

Installing security schema objects and attributes

Policy Director uses a set of LDAP objects and attributes to maintain user credentials within the LDAP server.

Use the IBM SecureWay Directory Management Tool (DMT) to determine if the security objects and attributes are installed. Install them if they are not already present. The DMT is installed as part of the IBM SecureWay Directory package.

To determine if the Policy Director security objects and attributes are installed, complete the following steps:

1. Start the Directory Management Tool on an LDAP client.

   Note: If you receive a message that there is no entry for the secAuthority=Default suffix, you can safely proceed. The object for the secAuthority=Default suffix is created during configuration of the Management server.
2. Click **Schema** → **Object classes** → **View object classes**.
3. Verify the presence of all of the following Policy Director objects and attributes:

   Object classes
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser
4. Click **Schema** → **Attributes** → **View attributes**
5. Verify the presence of all of the following Policy Director objects and attributes:

   Attributes
   secUUID
   secLoginType
   secAuthority
   secAcctValid
   secPwdValid
   secDN
   secPwdMgmtBind
   secAcctExpires
   secAcctInactivity
   secAcctLife
   secPwdAlpha
   secPwdSpaces
   secPwdFailures
   secPwdLastChanged
   secPwdLastUsed

6. Perform one of the following based on the findings in step 3 on page 30 and step 5 on page 30.
   - If all of the objects are present, no further action is needed. Continue to “Enabling SSL access (optional)” on page 32.
   - If *some*, but not all, of the objects are present, go to step 7.
   - If *none* of the objects are present, go to step 8.
7. If some, but not all, of the Policy Director objects and attributes are found, remove the existing Policy Director objects and attributes.

   In the DMT, click:

   Schema → **Object classes** → **Delete object classes** and remove the object classes.

   Then click **Schema** → **Attributes** → **Delete attributes** and remove the attributes.
8. If none of the Policy Director objects and attributes are found, insert the *IBM SecureWay Policy Director Version 3.0* CD.
9. At a command prompt, use **ldapmodify** to load the schema file. For example, type:

   UNIX®:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/secschema.def
   ```

   Windows:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\secschema.def
   ```

   where *x:* is the drive letter of your Windows CD-ROM drive.
10. If you plan to use Policy Director to manage SecureWay Boundary Server users, you must also add the objects and attributes from the Policy Director schema file:

    Use the **ldapmodify** command at a command prompt to load the schema file. For example, type:

    UNIX:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/puschema.def
    ```

    Windows:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\puschema.def
    ```

    where *x:* is the drive letter of your Windows CD-ROM drive.

Enabling SSL access (optional)

If SSL access to your LDAP server is not required, skip this section. Go to "Enabling LDAP access control" on page 39.

If SSL access is required by your LDAP server, continue with this section. This procedure only needs to be done the first time SSL communication is set up between the LDAP server and the LDAP client.

You can optionally enable the use of SSL to protect communications between the Policy Director servers and the LDAP server.

The IBM Global Security Kit (GSKit) SSL Runtime Toolkit Version 3.0.1 is installed during the installation of LDAP. GSKit provides two versions of a Key Management Tool—one version is a windowed version **ikmguiw** and the other version is nonwindowed **ikmgui**. You can use either version whenever **ikmguiw** is called out in the following procedures.

Complete instructions on how to use this tool can be found in the LDAP documentation. See "IBM SecureWay Directory documentation" on page 89.

Or, you can follow these abbreviated procedures to specifically enable Policy Director for SSL access.

Creating the key database file and the certificate

To enable SSL support on the LDAP sever, the server must have a certificate that identifies it and that it can use as a *personal certificate*. This personal certificate is the certificate that the server sends to the client to allow the client to authenticate the server. The certificates and the public and private key pair are stored in a key database file. A customer normally acquires a *signed certificate* from a Certificate Authority (CA), such as VeriSign.

However, you can also use a *self-signed* certificate. If using a self-signed certificate, the machine on which the certificate is generated becomes the CA.

Use the GSKit's Key Management Tool (**ikmguiw**) to create the key database file and the certificate. To create the key database file and certificate (self-signed or signed):

1. Ensure that the IBM Global Security Kit (GSKit) SSL Runtime Toolkit Version 3.0.1 and the Java-based Key Management Tool are installed on both the LDAP server and any LDAP clients that will be using SSL.

   Windows: `C:\Program Files\IBM\GSK\bin\ikmguiw.exe`

   Solaris: `/opt/IBM/GSK/bin/ikmguiw`

   AIX: `/usr/lpp/ibm/gsk/bin/ikmguiw`
2. Start the IBM Key Management tool (**ikmguiw**).

3. Click **Key Database File → New**.
4. Verify that the **CMS key database file** is the selected key database type.
5. Type the information in the **File Name** and **Location** fields where you want the key database file to be located. A key database file's extension is *.kdb*.
6. Click **OK**.
7. Enter the key database file password, and confirm it.

   Remember this password because it is required when the key database file is edited.
8. Accept the default expiration time, or change it to your organization's requirements.
9. If you wish the password to be masked and stored into a stash file, click **Stash the password to a file**.

   A stash file can be used by some applications so that the application does not have to know the password to use the key database file. The stash file has the same location and name as the key database file, and has an extension of *.sth*.
10. Click **OK**.

This completes the creation of the key database file. There is a set of default signer certificates. These signer certificates are the default Certificate Authorities that are recognized.

Creating a Personal Certificate

If you plan to use a certificate from a Certificate Authority (such as VeriSign), you must request the certificate from the CA and then receive in after it has been completed. Complete the steps in "Receiving the certificate".

Receiving the certificate: If you are using a certificate from a Certificate Authority (such as VeriSign) instead of a self-signed certificate, complete these steps:

1. Use **ikmguiw** to request a certificate from a CA and then receive the new certificate into your key database file.
2. Click the **Personal Certificate Requests** section of the key database file.
3. Click **New**.
4. Fill in all the information to produce a request that can be sent to the Certificate Authority.
5. Click **OK**.
6. After the CA returns the certificate, you can install it into your key database file by clicking the **Personal Certificates** section, and then clicking **Receive**.
7. After you have the LDAP server's certificate in the key database file, you can configure the LDAP server to enable SSL.

If your certificate is not already recognized, copy the CA's certificate to the client machine.

If your certificate is generated by a CA that is already recognized (such as VeriSign), no further action is required. Go to "Configuring the LDAP server to enable SSL" on page 35.

Creating a self-signed certificate: If you plan to use a certificate from a Certificate Authority (such as VeriSign) instead of a self-signed certificate, complete these steps."Receiving the certificate" on page 33.

To create a new self-signed certificate and store it into the key database file:

1. Click **Create → New Self-Signed Certificate**.
2. Type a name in the **Key Label** field that GSKit can use to identify this new certificate in the Key Database.

   For example, the label can be the machine name of the LDAP server.
3. Accept the defaults for the **Version** field, which is X509 V3, and for the **Key Size** field.
4. Either accept the default machine name, or enter a different distinguished name in the **Common Name** field for this certificate.
5. Enter a company name in the **Organization** field.
6. Complete any optional fields or leave them blank.
7. Either accept the defaults for the **Country** field and 365 for the **Validity Period** field, or change them to suit your own organization's requirements.
8. Click **OK**.

   GSKit generates a new public and private key pair and creates the certificate.

   If you have more than one personal certificate in the key database file, GSKit queries if you want this key to be the default key in the database. You can accept one of them as the default. The default certificate is used at runtime when a label is not provided to select which certificate to use.

This completes the creation of the LDAP server's personal certificate. It should appear in the Personal Certificates section of the key database file. Use the middle bar of the Key Management Tool to select between the types of certificates kept in the key database file.

Next, you must extract your LDAP server's certificate to a Base64-encoded ASCII data file.

Extracting the self-signed certificate

If your certificate is self-signed, you must extract the signer certificate from the key database file. Continue with this extraction procedure.

This extraction is used to set up the client machine. If you created a self-signed certificate in "Creating a self-signed certificate" on page 34, it also appears in the `Signer Certificates` section of the key database file because it is a self-signed certificate. When you are in the Signer Certificates section of the Key Database, verify that the new certificate is there.

To extract the signer certificate:

1. Use **ikmguiw** to extract your LDAP server's certificate to a Base64-encoded ASCII data file. This file will be used in the procedure in "Setting up the LDAP client for SSL access" on page 36.
2. Highlight the self-signed certificate that you just added in "Creating a self-signed certificate" on page 34.
3. Click **Extract Certificate**.
4. Click **Base64-encoded ASCII data** as the data type.
5. Type a certificate file name for the newly extracted certificate. The certificate file's extension is *.arm*.
6. Type the location where you want to store the extracted certificate.
7. Click **OK**.
8. Copy this extracted certificate to the LDAP client machine.
9. You can configure the LDAP server to enable SSL.

Configuring the LDAP server to enable SSL

To configure the LDAP server to enable SSL:

1. Make sure that the LDAP server is installed and running if you will be using LDAP as the user registry. See "Chapter 4. Installing and configuring IBM SecureWay Directory" on page 27 for complete instructions
2. Use the Web-based LDAP administration tool with the following URL:

   ```
   http://servername/ldap
   ```

   Where *servername* is the name of the LDAP server machine.
3. Log on as the LDAP administrator (for example, cn=root) if you are not already logged on.
4. Click **Server → SSL**.
5. Click either **SSL On**, which is for SSL and non-SSL enablement, or click **SSL Only** for the SSL status you want to set.

6. Click **Server Authentication** for the type of authentication method.
7. Type a port number, or accept the default port number of 636.
8. Type in the key database path and file name that you specified in step 5 in Creating the key database file and the certificate.

   The key database file's extension is *.kdb*
9. Type the name in the **Key Label** field that you used to identify it when you stored the LDAP server's certificate into the Key Database. For example, the label might be the machine name of the LDAP server.
10. Enter the key database file password and confirm it. Or, you can leave the password field blank if you want the LDAP server to use the stash file.
11. Click **Apply**.
12. Click **restart the server** link to restart the LDAP server and allow this change to take effect.

Testing the SSL access: To test that SSL has been enabled, type the following command from a LDAP server command line:

```
ldapsearch -h servername -Z -K keyfile -P key_pw -b "" -s base \
objectclass=*
```

The backslash (\) in this command is only required when the command cannot be entered on one line.

Where:

servername	The DNS host name of the LDAP server.
keyfile	The fully qualified path name of the generated key ring.
key_pw	The password of the generated key ring.

This command returns the LDAP base information, which includes the suffixes on the LDAP server.

The server SSL setup is now complete. Next, set up the LDAP client for SSL access.

Setting up the LDAP client for SSL access

After setting up the LDAP server for SSL access, you must set up the LDAP clients for SSL access.

Creating a key database file: Ensure that GSKit is installed on the client, and then create a new key database file using the IBM Key Management Tool as described in “Creating the key database file and the certificate” on page 32.

In order for the client to be able to authenticate the LDAP server, the client must recognize the Certificate Authority (signer) that created the LDAP server’s certificate. If the LDAP server is using a self-signed certificate, then the client must be enabled to recognize the machine that generated the LDAP server’s certificate as a trusted root (Certificate Authority).

Adding a signer certificate: To add a signer certificate after the key database file has been created:

1. Ensure that the certificate which was extracted from the key database file in “Extracting the self-signed certificate” on page 35 has been copied to the client machine. If it has not been copied, copy it now.
2. Click the **Signer Certificates** section of the client’s CMS key database file.
3. Click **Add**.
4. Click **Base64-encoded ASCII data** to set the data type.
5. Indicate the certificate’s file name and its location. The certificate file’s extension is *.arm*.
6. Click **OK**.
7. Type a label for the signer certificate that you are adding. For example, you might want to use the machine name of the LDAP server for the label.
8. Click **OK**.

   The self-signed certificate appears in the client’s Key Database as a signer certificate.
9. Highlight the newly added signer certificate, and click **View/Edit**.
10. Ensure that it is marked as a trusted root by making sure **Set the certificate as a trust root** is selected.

    If the LDAP server’s certificate was generated by a regular Certificate Authority, be sure that the Certificate Authority is listed as a signer certificate and marked as a trusted root. If it is not, then add the Certificate Authority’s certificate as a signer certificate and then indicate that it is a trusted root.

At this point, the client should be able to establish an SSL session with the LDAP server.

Testing SSL enablement: To test that SSL has been enabled, enter the following command from a command line on the LDAP client:

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -b "" \
-s base objectclass=*
```

The backslash (\) in this command is only required when the command cannot be entered on one line.

Where:

servername	The DNS host name of the LDAP server.
client_keyfile	The fully qualified path name of the generated key ring.
key_pw	The password of the generated key ring.

This command returns the LDAP base information, which includes the suffixes on the LDAP server.

The SSL setup is now complete.

Using LDAP server and client authentication type (optional)

This configuration section is optional:

1. Complete the procedure as described in "Configuring the LDAP server to enable SSL" on page 35. However, instead of configuring the LDAP server for **Server Authentication**, select to perform both **Server and Client Authentication**.

   In this case, after the server has sent its certificate to the client and has been authenticated by the client, the server requests the client's certificate. If the LDAP server is configured for both, then a certificate needs to be established for the client machine also.
2. On the client machine, establishing a certificate for the client machine is done as described in these procedures:
   - "Creating the key database file and the certificate" on page 32
   - "Creating a self-signed certificate" on page 34 if your certificates is a self-signed certificate, or "Receiving the certificate" on page 33 if the certificate is a signer certificate.
   - "Extracting the self-signed certificate" on page 35
   - "Configuring the LDAP server to enable SSL" on page 35
3. On the LDAP server, after the client's personal certificate has been created and added to the client's key database file, the Certificate Authority that created that client certificate must be recognized as a signer certificate (trusted root). The Certificate Authority certificate is added to the LDAP server's Key Database as described in "Adding a signer certificate" on page 37.

Testing the SSL access: After the LDAP server recognizes the Certificate Authority that created the client's personal certificate, the setup can be tested using the following command:

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -N client_label \
-b "" \ -s base objectclass=*
```

The backslash (\) in this command is only required when the command cannot be entered on one line.

Where:

servername
The DNS host name of the LDAP server.

client_keyfile
The fully qualified path name of the generated client key ring.

key_pw
The password of the generated key ring.

client_label
The label associated with the key, if any. This field is optional and is only needed if the LDAP server is configured to perform both server and client authentication.

This command returns the LDAP base information, which includes the suffixes on the LDAP server. Notice that the **-N** parameter indicates the label that was specified when the client's personal certificate was added to the client's key database file.

Do not specify the LDAP server's signer certificate label. The **-N** parameter indicates to GSKit which client certificate is sent to the server when requested. If no label is specified, then the default personal certificate is sent when the server requests the client's certificate.

The SSL setup is now complete.

Enabling LDAP access control

To complete the integration of Policy Director security with the LDAP user registry, update the LDAP ACLs that control the user registry by completing the following steps:

1. Start the Directory Management Tool from either the LDAP client or the LDAP server by clicking **Start → Programs → IBM SecureWay Directory → Directory Management Tool**.
2. Rebind the server:
   a. Click **Server → Rebind**.
   b. Click **Authenticated**.
   c. Type the user DN (for example, cn=root).
   d. Type your password.
   e. Click **OK**.

3. Click **OK** or close the warning message window for each warning message that appears.
4. Give the Policy Director security daemon group full control on the suffixes you created under “Adding suffixes” on page 29.
   a. Click **Entries → Add Entry**.
   b. Type the suffix for your Policy Director users and GSO users database in the **Entry RDN**. For example:

      ```
      o=IBM,c=US
      ```

   c. Click **Organization**.
   d. Click **Next**.

      The Create an LDAP Entry windows appears.
   e. Add the appropriate information for your organization, and then click the **Create** button.
   f. Click the **Tree → Refresh tree**, and the new entry should now appear in the Browse directory tree.
5. Give the Policy Director security daemon group full control by adding the following to the list of owners of each controlling LDAP ACL:

   ```
   cn=SecurityGroup,secAuthority=Default
   ```

   by clicking the **ACL** tab.

   The **Edit an LDAP ACL** window appears.
   a. Type cn=SecurityGroup,secAuthority=Default in the DN field, and then click **group** from the drop down list.
   b. Click the **Add** button.
   c. Select all the check boxes under Granted Rights for Add, Delete, and Class.
   d. When completed, click **Change**, and cn=SecurityGroup,secAuthority=Default should now appear in the list of ACLs for your suffix DN.
   e. Repeat the procedure for each suffix if you have more than one to add to the list of owners.

You have now completed the LDAP configuration.

Chapter 5. Installing Policy Director for Windows

The sections in this chapter tell you how to install and configure Policy Director on supported Windows and Windows NT platforms.

Before you begin the Policy Director installation, make sure you have reviewed the information in “Before installing Policy Director for Windows”.

Before installing Policy Director for Windows

Before you begin to install NetSEAT and Policy Director, read the following information:

- Before you install NetSEAT and Policy Director, you must initially install and configure the Windows NT server.
- You must know the passwords for the Windows NT domain administrator and for the secure domain administrator (for example, the cell_admin account). Be sure to obtain administrator privileges.
- If you are creating a new DCE cell when installing the Policy Director servers on the Windows NT operating system:
  - You must also install and configure a DCE server.
  - If you are using LDAP for your user registry, you must also install and configure an LDAP server.
- Be familiar with all information pertaining to Policy Director deployment, as described in “Installation requirements for the secure domain” on page 23.

Installing NetSEAT and Policy Director

Before you begin the Policy Director installation, be sure to close all applications. After you finish installing Policy Director, you must shut down and restart the computer.

Completing the Secure Domain Inventory

During the installation, you must provide the following information specific to the configuration of your secure domain:

- Your secure domain name (DCE cell), for example cell_admin.
- The names of the computers that are providing the following services:
  - Security
  - Time
  - Cell Directory Services (CDS)
  - Directory Services Broker (DSB)

Installing NetSEAT

The Policy Director NetSEAT setup file copies the NetSEAT files onto your hard disk and then automatically starts the NetSEAT configuration utility.

To install NetSEAT:

1. Log in as a user with administrator privileges.
2. Insert the *IBM SecureWay Policy Director Version 3.0* CD into the CD-ROM drive.
3. Change to the \win32\client directory on the CD.
4. Double-click the Setup.exe file, and the InstallShield program starts.
5. When the Choose Installation Language window appears, select the appropriate language.
6. Click **Next** and the Policy Director Welcome window appears.
7. Click **Next**.
8. When the Choose Components to Install window appears, click **Client for Policy Director server products**.
9. Click **Next**.
10. When the Choose Setup Type window appears, click **Typical**.

    The default location for a typical installation is:

    ```
    c:\Program Files\ibm\netseat\
    ```

    Or if you click **Custom** specify the drive and directory where you want NetSEAT installed.

    The Choose Destination Location window appears.
11. Click **Next**.

    The NetSEAT files are copied to the default NetSEAT location of your hard disk. The NetSEAT Configuration window appears.

Configuring NetSEAT

The NetSEAT configuration tasks provide NetSEAT with information about the secure domain, such as DCE server names, locations, and services.

After all NetSEAT files have been copied to the hard drive, the NetSEAT Configuration window (**Secure Domains** tab) appears.

To configure NetSEAT:

1. To add an entry for a new secure domain, click **Add**.

   The New Secure Domain window appears.
2. Type the name of the secure domain (DCE cell) to which NetSEAT will belong, such as cell_admin.
3. Select either the **Enable GSS** or the **Enable SSL** check box.
4. Click **OK**.

   The Secure Domain Properties window appears.
5. To add a DCE server and the services it will provide, click **Add**.

   The Add a DCE Server window appears.

   Use this window to inform NetSEAT of existing DCE servers in the secure domain and the services that are provided by each. You might need to add more than one DCE server. All services could be on one computer or divided among several computers.

   Possible scenarios include:

   - **New Secure Domain (one host system)**

     If you are creating a new secure domain that consists of one host system only, your host system provides all the DCE services. Type the name of your host system in the **Machine Name** field. Select one or more of the services. Select the DSB even though it is not installed yet.
   - **New Secure Domain (more than one host)**

     If you are creating a new secure domain, and the DCE services are located on another host, your local host will provide only the DSB service. In this case, first add the DCE server that is providing the DCE services (Security, Time, CDS). Then, add another DCE server that is named `localhost` to represent your local system, and select the DSB check box. You can select the DSB even though it is not installed yet.
   - **Existing Secure Domain**

     If you are adding Policy Director in an existing secure domain, add the name of the DCE server that provides Security, Time, and CDS. Then, add the name of the DCE server that includes the Policy Director Management server that automatically has the DSB installed. Select the DSB check box for this system. In this scenario all services, including the DSB, could be located on the same host system.

6. For each server, type the fully DN machine name of an existing server in the secure domain (for example, SFF98732.austin.ibm.com).
7. For each server, select one or more of these services for the server:
   - Security
   - DSB
   - Time
   - CDS
8. Click **OK**.

   The Secure Domain Properties window displays the new entry.
9. As required, repeat step 5 on page 43 to step 8 to add additional servers and services.
10. From the Secure Domain Properties window, accept the default advanced login configuration of **DCE Login only**.

    The integrated login area of the Secure Domains Properties window is not used in this NetSEAT installation.
11. Click **OK**.

    The NetSEAT Configuration window appears.
12. Click **OK**.

    The System Restart Required window appears.
13. Click **Yes** to restart the computer.
14. Click **OK**.

    When the computer restarts, NetSEAT automatically starts. A NetSEAT icon appears in the Windows task bar.

    The NetSEAT installation and configuration are now complete.

Verifying NetSEAT client configuration

Before installing Policy Director server, verify that the NetSEAT client is successfully configured into the specified secure domain. Use **netseat_ping** to determine if the following services are available:

- Security Service
- Time Service
- Cell Directory Service
- Directory Services Broker (DSB)

To verify that the NetSEAT client can communicate with the necessary services, complete the following steps:

1. Click **Start → Programs → NetSEAT → NetSEAT Login** to log in as cell_admin.

   Or, you can use the **netseat_login** command at the command line to log in.
2. Do not select PKI Login unless it is specifically required for your configuration.
3. Type the Policy Director Administrator user name and password.
4. Click **OK**.
5. At the command line, use the **netseat_ping** command to obtain configuration status.

   For example, if a NetSEAT client configures into a secure domain that is called ″redback,″ obtain status by typing this command at the DOS prompt:

   ```
   netseat_ping -C redback
   ```

   Information similar to the following output would appear:

   ```
   /.../redback:
          SecurityServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          CdsServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          TimeServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          DsbServers:
                       ncacn_ip_tcp:redback[ ] not available
                       ncacn_ip_udp:redback[ ] not available
   ```

   However, note that the DSB will not be running yet if you plan to create a new secure domain. In this case, the **netseat_ping** output for the DSB will read `not available`. This reading is the expected output for this scenario. You can safely proceed with the Policy Director installation because the installation of the Policy Director Management server component will automatically install, configure, and start the DSB. If the DSB is already running, the output for the DSB will read `is available (v3.1)`.
6. If any services other than the DSB are not available, resolve the problem before installing the Policy Director servers.

Installing Policy Director servers

Before you begin to install the Policy Director servers, be sure you know the user name and password of an administrator.

To install Policy Director server components:

1. Make sure that the LDAP server is installed and running if you will be using LDAP as the user registry. See “Chapter 4. Installing and configuring IBM SecureWay Directory” on page 27 for complete instructions
2. Insert the *IBM SecureWay Policy Director Version 3.0* CD in the CD-ROM drive.
3. Change to the \win32\server directory on the CD.
4. Click the Setup.exe file, and the InstallShield program starts.
5. When the Choose Installation Language window appears, select the appropriate language.
6. Click **Next** and the Policy Director Welcome window appears.
7. Click **Next**.

   The Choose Destination Location window appears.
8. Accept the default directory location for the program files or click the **Browse** button to create or select another directory.

   The default location is: `C:\Program Files\IBM\`

   If you installed NetSEAT in a non-default location, install the Policy Director servers in the same location.
9. Click **Next**.

   The Select Components window appears.
10. Select the appropriate Policy Director server components. For assistance with your selection, see “Common configurations” on page 19.

    There should be only one instance of the Policy Director Management server (IVMgr) in the secure domain.
11. Click **Next**.
12. If you did not select WebSEAL, go to 14 on page 47.

    If you selected the WebSEAL (IVWeb) component, the Choose Web Document Root Location window appears. This windows asks you for the location of the root directory of your Web space. All resources belonging to your Web site reside under this directory.
13. Accept the default root directory location, or click the **Browse** button to create or select another directory. The default location is:

    ```
    C:\...\IBM\Policy Director\www\docs
    ```

The Policy Director files now copy from the CD to your hard drive. The secure domain Administrator Login window appears. This step is necessary to establish security credentials and complete the configuration process.

14. Complete the DCE Cell Administrator name and password.
15. If you selected the Management server component (IVMgr), you are prompted to select **LDAP Registry** or **DCE Registry**.

    If you did not select the Management server, the User Registry type for the existing secure domain is automatically detected:

    - If an LDAP user registry is detected, the installation continues as described in “Using an LDAP user registry”.
    - If a DCE user registry is detected, the installation continues as described in “Using a DCE user registry” on page 48.
16. Click one of the following for your user registry:
    - If you selected **LDAP Registry**, go to “Using an LDAP user registry”.
    - If you selected **DCE Registry**, go to “Using a DCE user registry” on page 48.

Using an LDAP user registry

If your Policy Director secure domain uses an LDAP user registry, or if you are installing IVMgr and have selected **LDAP Registry**, the LDAP Server Information window appears.

1. Type the required information for the LDAP server configuration:
   - LDAP Host Name
   - Port Number
   - SSL Port Number (required only if using SSL to access the LDAP server)
   - LDAP DN for GSO Database (for example, o=ibm,c=us)
2. Click **Next**.

   The Communication with the LDAP Server window appears.
3. Choose to enable or disable SSL communication between Policy Director and the LDAP server. Click **Yes** to enable SSL communication or click **No** to disable SSL communication.

   On Windows NT, SSL communication is enabled one time between all Policy Director servers on the host system and the LDAP server.

   If you have enabled SSL communication, go to step 4 on page 48.

   If you have disabled SSL communication, go to step 5 on page 48.

4. Provide values for the following prompts:
   - SSL Key File location
   - SSL File DN (key label)
   - SSL Key File password

   See “Creating the key database file and the certificate” on page 32 for information.
5. Click **Next**.

   The LDAP Administrator Login window appears.
6. Complete the LDAP Administrator name (for example, cn=root) and password information, and click **OK**.

   The servers are configured and start up. This might take several minutes. The System Information windows appears and displays the status of the servers, including registration information.
7. Click **Next**.

   The Policy Director Setup Complete window appears.
8. Click **Yes** to restart.

   If you checked **No** to the restart option, you must restart Windows NT later to complete the configuration process. This completes the Policy Director installation.
9. Click **Finish**.

   You are prompted to restart your system.

Using a DCE user registry

If your Policy Director secure domain uses a DCE user registry, or if you are installing IVMgr and have selected **DCE Registry**, the installation continues as follows:

1. If you selected the WebSEAL (IVWeb) component, the Choose Web Document Root Location window appears. This windows requests the location of the root directory of your Web space. All resources belonging to your Web site reside under this directory.

   If you did not select WebSEAL, go to 3.
2. Accept the default root directory location, or click the **Browse** button to create or select another directory. The default location is:

   ```
   C:\Program Files\IBM\Policy Director\www\docs
   ```
3. Click **Next**.

   The Policy Director files now copy from the CD to your hard drive. The secure domain Administrator Login window appears.

4. Complete the LDAP Administrator name and password information, and then click **OK**.

   The servers are configured and start up. This might take several minutes. The System Information windows appears and displays the status of the servers, including registration information.
5. Click **Next**.

   The Policy Director setup complete window appears.
6. Click **Finish**.

   You are prompted to restart your system.
7. Click **Yes** to restart.

   If you checked **No** to the restart option, you must restart Windows NT later to complete the configuration process. This completes the Policy Director installation.

Configuring the Credentials Acquisition Service

The Policy Director CAS is installed automatically. If you want to use CAS for your credentials acquisition service, you must configure it. See the information about configuring a credentials acquisition service in the *Policy Director Administration Guide* for instructions.

Using NetSEAL Trap on Windows NT

Policy Director NetSEAL (IVTrap) traps requests made to specific ports. To use the NetSEAL trap, you must stop and restart all applications that use the specified ports.

For more information about configuring Policy Director NetSEAL to trap specific ports, see the overview information about NetSEAL in the *Policy Director Administration Guide.*

Installing the Management Console on Windows

Policy Director provides a Management Console that manages many components of the Policy Director security system from a Windows client desktop. The Management Console can be installed on any of the following operating systems:

- Windows 95
- Windows 98
- Windows NT Version 4.0, with Service Pack 4 or higher

Each Windows operating system that runs Policy Director requires the Policy Director NetSEAT client.

The NetSEAT client can be configured as either a DCE runtime client or as a client to a Policy Director server. Although either configuration is acceptable for the Management Console, the Policy Director servers require the full client to the Policy Director server.

If you need to reinstall any components, you must remove the existing component before reinstalling it.

Installing the Management Console with server components

After the Policy Director server components have been installed and configured in “Installing Policy Director servers” on page 46, complete the following steps:

1. Insert the *IBM SecureWay Policy Director Version 3.0* CD in the CD-ROM drive.
2. Change to the \win32\Console directory.
3. Double-click the Setup.exe file, and the InstallShield program starts.
4. When the Choose Installation Language window appears, select the appropriate language.
5. Click **Next** and the Policy Director Welcome window appears.
6. Click **Next** and the Choose Destination Location window appears.
7. Indicate a location where you want the files installed.

   The files are copied to their proper locations on the Windows computer. An information window appears indicating a successful installation.
8. If queried whether you want to restart Windows, click **yes**.
9. Click **OK**.
10. Go to “Starting the Management Console” on page 51.

Installing the Management Console without server components

To enable administration of Policy Director security from additional Windows systems, you can install the Management Console on Windows systems that do not have the Policy Director server components installed. When you install the Management Console in this way, the NetSEAT client can be configured as either a DCE runtime client or as a client to a Policy Director server.

To install the Management Console without the server components, go to the Windows desktop system and complete the following steps:

1. Verify that the Windows operating system is a supported platform. See "Policy Director servers" on page 16.
2. Install Policy Director NetSEAT Client. Follow the instructions in "Installing NetSEAT" on page 42.
3. Verify that the NetSEAT client is properly configured into the secure domain in which you will run the Management Console. See "Verifying NetSEAT client configuration" on page 44.
4. Insert the *IBM SecureWay Policy Director Version 3.0* CD into the CD-ROM drive.
5. Change to the \win32\Console directory
6. Double-click the Setup.exe file, and the InstallShield program starts.
7. When the Choose Installation Language window appears, select the appropriate language.
8. Click **Next** and the Policy Director Welcome window appears.
9. Click **Next** and the Choose Destination Location window appears
10. Indicate a location where you want the files installed.

    The files are copied to their proper locations on the Windows computer. An information window appears indicating a successful installation.
11. Click **OK** to complete the installation
12. To start the Management Console, go to "Starting the Management Console".

Starting the Management Console

To start the Management Console:

1. Make sure that the Policy Director servers are installed and running.
2. Click **Start** → **Programs** → **Policy Director** → **Management Console.**

   The Policy Director Management Console window appears.
3. Log in to the Management Console as a user with administrator privileges, such as cell_admin.

Removing Policy Director

To remove Policy Director components be sure to log on as administrator. Log in to the Windows domain as a user with administrator credentials. For example:

```
dce_login cell_admin password
```

If you attempt to remove a component without the proper secure domain credentials, an Authorization Failure message window appears.

You must remove Policy Director components in exactly the reverse order of installation. Use the **Add/Remove Programs** icon from the Control Panel to remove Policy Director.

To uninstall an entire Policy Director installation, perform the following procedures in the order shown:

1. Remove the Management Console.
2. Remove the server components.
3. Remove the NetSEAT client.

Removing the Management Console

To remove the Management Console:

1. If the Management Console is running, close it.
2. Go to **Add/Remove Programs** in the Control Panel, and then click **Policy Director Management Console.**
3. Click the **Add/Remove** button.
4. When queried, click **yes** to confirm that you want to remove the program.
5. Click **OK**.

Removing the server components

To remove the Policy Director server components, you must obtain privileges and credentials, and then remove the components.

To remove server components:

1. Make sure that the Policy Director servers are installed and running.
2. Go to **Add/Remove Programs** in the Control panel, and then select the first Policy Director server component you want to remove.

3. Remove the Policy Director server components in exactly the reverse of the order in which they were installed.

   For example, if you install all components, remove them in the following order:

   - Authorization ADK (IVAuthADK)
   - Authorization server (IVAcld).
   - NetSEAL (IVTrap).
   - WebSEAL (IVWeb).
   - Security Manager (IVNet).
   - Management server (IVMgr).
   - Base (IVBase). This component is always automatically installed.

   The Policy Director Management Console can be removed at any time. For more information on the order in which you install components, see "Step-by-step Policy Director installation overview" on page 25.
4. Click the **Add/Remove** button.
5. Enter the LDAP Administrator username and password when requested.
6. Repeat step 2 on page 52 to step 5 for each Policy Director server component.
7. Click **OK** when finished.

Removing the NetSEAT client

You must have Windows NT administrator privileges to remove Policy Director NetSEAT components.

1. Go to **Add/Remove Programs** in the Control panel, and then click the **Install/Uninstall** tab.
2. From the list window of the tab, click **Policy Director NetSEAT Client**.
3. Click **Add/Remove**.
4. Click **OK**.

Chapter 6. Installing Policy Director for AIX

The sections in this chapter tell you how to install and configure Policy Director on the AIX operating system.

Before you begin the Policy Director installation, make sure you have reviewed the information in “Before installing Policy Director for AIX”.

Before installing Policy Director for AIX

Before you begin to install NetSEAT and Policy Director, read the following information:

- If you are creating a new DCE cell when installing the Policy Director servers:
  - You must also install and configure a DCE server.
  - If you are using LDAP for your user registry, you must also install and configure an LDAP server.
- Be familiar with all information pertaining to Policy Director deployment, as described in “Installation requirements for the secure domain” on page 23.

Installing the Management Console

Policy Director provides a Management Console that can be used to manage all components of the Policy Director system. Administrators can choose to install the Management Console on an AIX system, a Windows system, or both.

The Management Console for AIX is distributed as an package named IV.Console. Use SMIT to install and configure the package.

Installing Policy Director

To install Policy Director on AIX, use the following instructions:

1. Make sure that the LDAP server is installed and running if you will be using LDAP as the user registry. See “Chapter 4. Installing and configuring IBM SecureWay Directory” on page 27 for complete instructions
2. Log in as root.
3. Insert the *IBM SecureWay Policy Director Version 3.0* CD into the CD-ROM drive.
4. Start SMIT.
5. Click **Software Installation and Maintenance**.

   The Software Installation and Maintenance menu appears.
6. Click **Install and Update Software**.

   The Install and Update Software menu appears.
7. Click **Install and Update Software by Package Name**.

   The Install and Update Software by Package Name window appears.
8. Type the name of the device from which you are installing the software.

   For example:
   - If you are installing from a CD device, you might type: `/dev/cd0`
   - If you are installing from a directory on a mounted server, you might type: `/mnt/user/lpp/IV`

     After you type the device name, a Multi-select List window appears.
9. Click **IV**.

   A Multi-select List window displays the list of Policy Director software packages.
10. Select the packages you want to install.
    - To install all of the Policy Director packages click the entry **IV**.
    - When installing only some of the Policy Director packages, be sure to observe the installation dependencies that are described in “Installation requirements for the secure domain” on page 23.
11. Click **OK**.

    The SMIT menu Install and Update Software by Package Name window appears.
12. Click **yes** for the field that is labeled:

    ```
    AUTOMATICALLY install requisite software?
    ```

    This step ensures that the Policy Director base (IV.Base) and SMIT setup (IV.smit) packages are installed. These packages are prerequisite software for the other Policy Director packages. If you choose to set this field to **no**, return to the package selection menu. Ensure that you have selected IV.Base and IV.Smit.

13. Set other fields to values appropriate to your installation.
14. Click **OK**.

    SMIT displays status messages, including:

    - Pre-installation verification of Policy Director software packages.
    - The name of each package during extraction of the package's files.
    - Creation of configuration menus for each package.
    - A status message that indicates success on completion of file extraction.
15. When file extraction is complete, configure the Policy Director packages, using the information in "Configuring Policy Director with an LDAP user registry". Or, see "Configuring Policy Director with a DCE user registry" on page 64 if you are using the DCE registry.

Configuring Policy Director with an LDAP user registry

You must install the Policy Director software packages before you can configure them. If you have not already installed the Policy Director packages, see "Installing Policy Director" on page 56.

If you installed Policy Director with a DCE user registry, go to "Configuring Policy Director with a DCE user registry" on page 64.

You must configure each installed Policy Director package, with the exception of the SMIT Setup. Configure the packages one at a time. Some of the Policy Director packages require the administrator to respond to screen prompts during configuration.

To configure the Policy Director packages:

1. Start SMIT.

   The System Management menu appears.
2. Click **Communications Applications and Services**.

   A list of installed software packages appears. For example:

   - TCP/IP
   - NFS
   - DCE (Distributed Computing Environment)
   - Policy Director

3. Click **Policy Director**.

   The Policy Director menu appears with the following options:

   - Policy Director Configuration
   - Policy Director Unconfiguration

4. Click **Policy Director Configuration**.

   A list of installed Policy Director packages appears, such as:

   - Policy Director Base Configuration
   - Policy Director Management Server Configuration
   - Policy Director Management Console Configuration
   - Policy Director Security Manager Configuration
   - Policy Director WebSEAL Configuration
   - Policy Director Authorization Server Configuration
   - Policy Director NetSEAL Configuration
   - Policy Director Authorization ADK Configuration

5. Click each package to configure, one at a time.

   You must configure the Policy Director packages in the order in which they are presented on the Policy Director configuration list. Select each package in turn, from the top item to the bottom item.

You must now configure the Policy Director packages you have selected using the appropriate configuration instructions in the following sections.

Configuring the Base package

The Base package is installed on a computer whenever you install any of the other packages. To configure the Base package, click **Policy Director Base** in the Policy Director configuration list.

The Policy Director Base package configuration completes without any user input.

Configuring the Management server

To configure the Management server:

1. Click **Policy Director Management Server** in the Policy Director configuration list.

   A prompt appears requesting you to choose a user registry type.

2. If you are using LDAP as your user registry, type 2 for LDAP user registry.

   A prompt appears requesting the DCE Cell Administrator name and password.

3. When prompted, type the DCE Cell Administrator account name and password.

   If you are using LDAP as your user registry, a series of prompts appears to configure communication between the Management server and the LDAP server.
4. Type the required information for the LDAP server configuration:
   - LDAP server host name
   - LDAP server port number
   - LDAP server SSL port number (optional)
5. Type the username and password for the LDAP administrative user (for example, `cn=root`). Policy Director security information is now registered with the LDAP server.
6. Choose to enable or disable SSL communication between Management server and the LDAP server.

   Note: You can individually enable or disable SSL communication between each server and the LDAP server. In this case, you are setting SSL communication between the Management Server (IVMgr) and the LDAP server.
7. If you disabled SSL communication, go to step 8. If you have enabled SSL communication, provide values for the following prompts:
   - SSL Key Ring File Location
   - SSL Key Label
   - Password for SSL Key
8. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix, which you added in “Adding suffixes” on page 29. For example:

   ```
   o=IBM,c=US
   ```

   This prompt does not appear when either the Policy Director Management server, or the Authorization server, has been configured previously.

   You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization’s abbreviated name, and where `c=` is the country.

   This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.

After GSO database access is configured, the Policy Director Configuration Manager automatically configures a Directory Services Broker. A series of messages lists each automated step as it completes.

A message appears indicating that the IVMgr package installation was successful.

The list of available packages reappears.

Configuring and starting the Management Console

To configure the Management Console, click **Policy Director Management Console** in the Policy Director configuration list.

The Policy Director Management Console configuration completes without any user input.

To start the AIX version of the Management Console:

1. Make sure that the Policy Director servers are installed and running.
2. Type the following command:

```
$ /opt/intraverse/bin/ivconsole
```

Or, if you are using the Windows client version of the Management Console, follow the instructions in “Starting the Management Console” on page 51.

Configuring the Security Manager

To configure the Security Manager (IVNet):

1. Click **Policy Director Security Manager** in the Policy Director configuration list.

   A series of prompts appear in order to integrate the Security Manager with the LDAP server.
2. If prompted, type the required information for the LDAP server configuration:
   - LDAP server host name
   - LDAP server port number
   - LDAP server SSL port number (optional)

   These prompts do not appears when either the Policy Director Management server, or the Authorization server, has been configured previously.
3. Type the username and password for the LDAP administrative user. Policy Director security information is now registered with the LDAP server.

4. Choose to enable or disable SSL communication between Security Manager and the LDAP server.

   Note: You can individually enable or disable SSL communication between each Policy Director server and the LDAP server. In this case, you are setting SSL communication between the Security Manager (IVNet, for use by WebSEAL and NetSEAL) and the LDAP server.
5. If you disabled SSL communication, go to step 6. If you have enabled SSL communication, provide values for the following prompts:
   - SSL Key Ring File Location
   - SSL Key Label
   - Password for SSL Key
6. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix, which you added in "Adding suffixes" on page 29. For example:

   ```
   o=IBM,c=US
   ```

   This prompt does not appear when either the Policy Director Management server, or the Authorization server, has been configured previously.

   You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization's abbreviated name, and where `c=` is the country.

   This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.

   A prompt appears requesting the DCE Cell Administration name and password.
7. When prompted, type the DCE Cell Administrator account name and password.

   The Security Manager is configured and started. The CAS server is also started.

   A message appears indicating that the Security Manager package installation is successful.

Configuring Policy Director WebSEAL

To configure Policy Director WebSEAL (IVWeb):

1. Click **Policy Director WebSEAL** in the Policy Director configuration list.

   The Policy Director WebSEAL configuration menu appears with values that confirm the following:

   - HTTP and HTTPS client access
   - Required Transmission Control Protocol (TCP) ports
   - The default Web document root directory

2. Confirm the current configuration values:

   ```
   Please check Web Server configuration:
   1. Enable TCP HTTP?                 Yes
   2. HTTP Port                        80
   3. Enable HTTPS?                    Yes
   4. HTTPS Port                       443
   5. Web document root directory      /opt/Policy Director/www/docs
   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```

3. Type a to accept the configuration and continue the installation, or enter the number of a value to change.

   The Policy Director Security Manager configuration prompts for the DCE Cell Administrator name and password.

4. Type the DCE Cell Administrator account name and password.

   The Policy Director Security Manager restarts.

   The installation configures and enables Policy Director WebSEAL on the computer.

Configuring the Policy Director Authorization server

To configure the Policy Director Authorization server (IVAcld):

1. Click **Policy Director Authorization Server** in the Policy Director configuration list.

   One or more prompts appear in order to integrate the Policy Director Authorization server with the LDAP server.

2. If prompted, type the required information for the LDAP server configuration:

   - LDAP server host name
   - LDAP server port number
   - LDAP server SSL port number (optional)

   These prompts do not appears when either the Policy Director Management server, or the Authorization server, has been configured previously.

3. Type the username and password for the LDAP administrative user. Policy Director security information is now registered with the LDAP server.
4. Choose to enable or disable SSL communication between Security Manager and the LDAP server.

   Note: You can individually enable or disable SSL communication between each Policy Director server and the LDAP server. In this case, you are setting SSL communication between the Authorization server (IVAcld) and the LDAP server.
5. If you disabled SSL communication, go to step 6. If you have enabled SSL communication, provide values for the following prompts:
   - SSL Key Ring File Location
   - SSL Key Label
   - Password for SSL Key
6. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix, which you added in "Adding suffixes" on page 29. For example:

   ```
   o=IBM,c=US
   ```

   This prompt does not appear when either the Policy Director Management server, or the Authorization server, has been configured previously.

   You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization's abbreviated name, and where `c=` is the country.

   This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.

   A prompt appears requesting the DCE Cell Administration name and password.
7. When prompted, type the DCE Cell Administrator account name and password.

   The Authorization Server is configured and started.

   A message appears indicating that the Authorization server package installation is successful.

Configuring Policy Director NetSEAL

To configure Policy Director NetSEAL:

1. Click **Policy Director NetSEAL** in the Policy Director configuration list.

   A prompt appears requesting the DCE Cell Administrator name and password.

2. Type the username and password for the LDAP administrative user. Policy Director security information is now registered with the LDAP server.

   The Policy Director NetSEAL Package configuration completes.

Policy Director NetSEAL traps requests that are made to specific ports. To use the NetSEAL trap, you must stop and restart all applications that use the specified ports. For more information on using Policy Director NetSEAL, see “Using NetSEAL Trap on AIX” on page 69.

Configuring the Policy Director Authorization ADK

To configure the Policy Director Authorization ADK, click **Policy Director Authorization ADK** in the Policy Director configuration list.

The Policy Director Authorization package configuration completes without any user input.

Configuring the Policy Director Credentials Acquisition Service

The Policy Director CAS is installed automatically. If you want to use the Policy Director CAS for your credentials acquisition service, you must configure it. See information about the Policy Director CAS and how to configure it for the WebSEAL server in the *Policy Director Administration Guide*.

Configuring Policy Director with a DCE user registry

You must install the Policy Director software packages before you can configure them. If you have not already installed the Policy Director packages, see “Installing Policy Director” on page 56 first.

If you installed Policy Director with an LDAP user registry, go to “Configuring Policy Director with an LDAP user registry” on page 57.

You must configure each installed Policy Director package, with the exception of the SMIT Setup. Configure the packages one at a time. Some of the Policy Director packages require the administrator to respond to screen prompts during configuration.

To configure the Policy Director packages:

1. Start SMIT.

   The System Management menu appears.
2. Click **Communications Applications and Services**.

   A list of installed software packages appears. For example:
   - TCP/IP
   - NFS
   - DCE (Distributed Computing Environment)
   - Policy Director
3. Click **Policy Director**.

   The Policy Director menu appears with the following options:
   - Policy Director Configuration
   - Policy Director Unconfiguration
4. Click **Policy Director Configuration**.

   A list of installed Policy Director packages appears, such as:
   - Policy Director Base Configuration
   - Policy Director Management Server Configuration
   - Policy Director Management Console Configuration
   - Policy Director Security Manager Configuration
   - Policy Director WebSEAL Configuration
   - Policy Director Authorization Server Configuration
   - Policy Director NetSEAL Configuration
   - Policy Director Authorization ADK Configuration
5. Click each package to configure, one at a time.

   You must configure the Policy Director packages in the order in which they are presented on the Policy Director configuration list. Select each package in turn, from the top item to the bottom item.

You must now configure the Policy Director packages you have selected using the appropriate configuration instructions in the following sections.

Configuring the Base package

The Base package is installed on a computer whenever you install any of the other packages. To configure the Base package, click **Policy Director Base** in the Policy Director configuration list.

The Policy Director Base package configuration completes without any user input.

Configuring the Management server

To configure the Management server:

1. Click **Policy Director Management Server** in the Policy Director configuration list.

   A prompt appears requesting the DCE Cell Administrator name and password.

2. When prompted, type the DCE Cell Administrator account name and password.

   The installation configures and starts the Management server.

Configuring and starting the Management Console

To configure the Management Console, click **Policy Director Management Console** in the Policy Director configuration list.

The Policy Director Management Console configuration completes without any user input.

To start the AIX version of the Management Console:

1. Make sure that the Policy Director servers are installed and running.
2. Type the following command:

   ```
   $ /opt/intraverse/bin/ivconsole
   ```

Configuring the Security Manager

To configure the Security Manager (IVNet):

1. Click **Policy Director Security Manager** in the Policy Director configuration list.
2. When prompted, type the DCE Cell Administrator account name and password.

The installation configures and starts the Security Manager.

Configuring Policy Director WebSEAL

To configure Policy Director WebSEAL (IVWeb):

1. Click **Policy Director WebSEAL** in the Policy Director configuration list.

   The Policy Director WebSEAL configuration menu appears with values that confirm the following:

   - HTTP and HTTPS client access
   - Required Transmission Control Protocol (TCP) ports
   - The default Web document root directory

2. Confirm the current configuration values:

   ```
   Please check Web Server configuration:
   1. Enable TCP HTTP?                  Yes
   2. HTTP Port                         80
   3. Enable HTTPS?                     Yes
   4. HTTPS Port                        443
   5. Web document root directory       /opt/Policy Director/www/docs
   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```

3. Type a to accept the configuration and continue the installation, or enter the number of a value to change.

   The Policy Director Security Manager configuration prompts for the DCE Cell Administrator name and password.

4. Type the DCE Cell Administrator account name and password.

   The Policy Director Security Manager restarts.

   The installation configures and enables Policy Director WebSEAL on the computer.

Configuring the Policy Director Authorization server

To configure the Policy Director Authorization server (IVAcld):

1. Click **Policy Director Authorization Server** in the Policy Director configuration list.

   A prompt appears requesting the DCE Cell Administration name and password.

2. Type the DCE Cell Administrator account name and password.

   The Authorization Server is configured and started.

Configuring Policy Director NetSEAL

To configure Policy Director NetSEAL:

1. Click **Policy Director NetSEAL** in the Policy Director configuration list.

   A prompt appears requesting the DCE Cell Administrator name and password.

2. Type the username and password for the LDAP administrative user. Policy Director security information is now registered with the LDAP server.

   The Policy Director NetSEAL configuration completes.

Policy Director NetSEAL traps requests that are made to specific ports. To use the NetSEAL trap, you must stop and restart all applications that use the specified ports. For more information on using Policy Director NetSEAL, see “Using NetSEAL Trap on AIX” on page 69.

Configuring the Policy Director Authorization ADK

To configure the Policy Director Authorization ADK, click **Policy Director Authorization ADK** in the Policy Director configuration list.

The Policy Director Authorization package configuration completes without any user input.

Configuring the Policy Director Credentials Acquisition Service

The Policy Director CAS is installed automatically. If you want to use the Policy Director CAS for your credentials acquisition service, you must configure it. See information about the Policy Director CAS and how to configure it for the WebSEAL server in the *Policy Director Administration Guide*.

Installing the Management Console

Policy Director provides a Management Console that manages many components of the Policy Director security system from a Windows client desktop. The Management Console can be installed on any of the following operating systems:

- Windows 95
- Windows 98
- Windows NT Version 4.0, with Service Pack 4 or higher
- AIX Version 4.3.1.0 or higher

Each Windows operating system that runs Policy Director requires the Policy Director NetSEAT client.

The NetSEAT client can be configured as either a DCE runtime client or as a client to a Policy Director server. Although either configuration is acceptable for the Management Console, the Policy Director servers require the full client to the Policy Director server.

If you need to reinstall any components, you must remove the existing component before reinstalling it.

Using NetSEAL Trap on AIX

To use the Policy Director NetSEAL trap, the NetSEAL daemon Security Manager (secmgrd) must start before any applications that access secured (trapped) ports. Use /etc/inittab entries to ensure that secmgrd starts before the applications during the startup process.

Use the NetSEAL trap with networking applications, such as Telnet, RLOGIN, and POP3. The **inetd** daemon controls these applications. The Policy Director startup script, /etc/iv/iv, starts secmgrd, and then stops and restarts the inetd daemon. This procedure ensures the successful entrapment of these applications after system startup.

If you stop and restart Policy Director, you must also stop and restart any applications that make requests to trapped ports. To automate this process, you can add code to /etc/iv/iv to stop and start the applications after secmgrd starts. Use the /etc/iv/iv script's technique for stopping and restarting **inetd** as a template for how to stop and start other applications.

For more information about configuring Policy Director NetSEAL to trap specific ports, see the information about NetSEAL in the *Policy Director Administration Guide*.

Removing Policy Director

You must unconfigure Policy Director for AIX before you can remove it.

- For information about unconfiguring Policy Director, see "Unconfiguring Policy Director packages".
- For information about removing Policy Director, see "Removing Policy Director packages" on page 70.

To remove the Windows version of the Management Console, see

Unconfiguring Policy Director packages

To unconfigure the Policy Director servers, complete the following steps:

1. Start SMIT.
2. Click **Communications Applications and Services**.

   The Communications Applications and Services menu appears.
3. Click **Policy Director**.

   The Policy Director menu appears.

4. From the menu, click **Policy Director Unconfiguration**.

   The list of configured Policy Director packages appears.

   Select the package to unconfigure. Packages that might be shown are:

   - Policy Director Authorization Server Unconfiguration
   - Policy Director Authorization ADK Unconfiguration
   - Policy Director NetSEAL Unconfiguration
   - Policy Director WebSEAL Unconfiguration
   - Policy Director Security Manager Unconfiguration
   - Policy Director Management Server Unconfiguration
   - Policy Director Management Console Unconfiguration
   - Policy Director Base Unconfiguration
   - IV Smit menu Unconfiguration
5. Packages must be unconfigured one at a time.

   Note: You must unconfigure the packages in the reverse order from which they were installed. To ensure this order, unconfigure the packages from the top of the menu down to the bottom of the menu.
6. If you are unconfiguring Policy Director packages because you want to remove all of Policy Director from the computer, click **Policy Director Smit menu Unconfiguration** after unconfiguring all other Policy Director packages.

   This step removes Policy Director package information from the SMIT database.
7. See “Removing Policy Director packages” to remove Policy Director.

Removing Policy Director packages

Before you try to remove Policy Director, first verify that the Policy Director software has been unconfigured. “Unconfiguring Policy Director packages” on page 69 gives instructions for unconfiguring.

To remove Policy Director:

1. Start SMIT.
2. Click **Software Installation and Maintenance**.

   The Software Installation and Maintenance menu appears.
3. Click **Software Maintenance and Utilities**.

   The Software Maintenance and Utilities menu appears.

4. Click **Remove Installed Software**.

   The Remove Installed Software window appears.

5. Select the Policy Director packages to remove. You can select more than one package at the same time.

   To remove all Policy Director packages, type `IV`.

The Policy Director software is removed.

Removing the Management Console and NetSEAT

The Management Console on Windows and the NetSEAT client on Windows can be removed using the InstallShield uninstall function:

- Remove the Management Console. See “Removing the Management Console” on page 52 for instructions.
- Remove the NetSEAT client. See “Removing the NetSEAT client” on page 53 for instructions.

Chapter 7. Installing Policy Director for Solaris

The sections in this chapter tell you how to install and configure Policy Director on the Solaris operating system.

Before you begin the Policy Director installation, make sure you have reviewed the information in “Before installing Policy Director for Solaris”.

Before installing Policy Director for Solaris

Before you begin to install and Policy Director, read the following information:

The installation procedure for this release of Policy Director requires the **pkgadd** command. To run the **pkgadd** command, type the following at a command prompt:

```
# pkgadd -d /cdrom/cdrom0/solaris
```

Use the **pkgadd** command to install the Policy Director software. The **pkgadd** command often displays supplementary prompts that are not indicated in the standard procedure instructions. These prompts appear in response to situations specific to your system setup and configuration. Always respond `y` to any of these prompts that occur outside of the standard procedures.

Before you install Policy Director:

- You must install a DCE client.
- If you are using LDAP for your user registry, you must also install an LDAP client.

You must enable the Transarc DCE remote administration features before you begin the installation of Policy Director. You cannot complete the Policy Director installation if the remote administration features are not enabled.

The use of some remote administration features enables the Cell Administrator to become essentially equivalent to the local root account. Transarc DCE normally disables these remote administration features. However, the Policy Director software requires these features.

Refer to Section 4.2.1 of the *Transarc Release Notes, Release 1.1* (DCE-D1002-01) for information about how to enable the remote administration features.

Installation screen output

The standard procedures in this document do not indicate all the screen output possible from the **pkgadd** command. Most undocumented screen output provides additional information about the operations you are performing. In general, the standard procedures in this documentation show only those messages that require a user response.

Installing Policy Director servers with an LDAP user registry

If you are installing Policy Director with a DCE user registry, go to "Installing Policy Director server with a DCE user registry" on page 81.

The server packages are located in the /solaris directory on the *IBM SecureWay Policy Director Version 3.0* CD.

You must be logged on as user root to install the Policy Director packages.

If you need to reinstall any package, you must first remove the existing package (**pkgrm**) before reinstalling the desired package.

To install the Management server:

1. Make sure that the LDAP server is installed and running if you will be using LDAP as the user registry. See "Chapter 4. Installing and configuring IBM SecureWay Directory" on page 27 for complete instructions.
2. Type the **pkgadd** command to list the available packages from the CD:

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   The list of available packages appears on the display.

   If you use a different CD-ROM mount point, substitute it in the command above.
3. Type the selection number for IVBase to install the Policy Director Base files, and then press Enter.

   This command extracts files from the CD and installs them where you specify on the hard disk.

   A prompt appears indicating that the IVBase package installation was successful. The list of available packages reappears.

   Before continuing to the next step, remember that there should only be one instance of the Management server (IVMgr) in the secure domain. If this is a standalone system installation, continue to the next step. If you are installing on a secondary server, be sure you have reviewed "Installation requirements for the secure domain" on page 23.

4. Type the selection number for IVMgr to install the Policy Director Management server files. Press Enter.

   This command extracts files from the CD and installs them where you specify on the hard disk.

   A prompt appears requesting you to choose a user registry type.

5. If you are using LDAP for your user registry, type 2 for LDAP user registry.

   A prompt appears requesting the DCE Cell Administrator name and password.

6. Type the required information for access to the DCE Cell Administration account.

   ```
   Enter the user name of the Cell Administrator [cell_admin]:
   Enter the password for the Cell Administrator:
   ```

   A series of prompts appears to configure communication between the Management server and the LDAP server.

7. Type the required information for the LDAP server configuration:

   - LDAP server host name
   - LDAP server port number
   - LDAP server SSL port number

8. Type the DN and password for the LDAP administrative user (for example, cn=root). The LDAP server now contains Policy Director security information.

9. Choose to enable or disable SSL communication between the Management server and the LDAP server.

   You can individually enable or disable SSL communication between each Policy Director server and the LDAP server. In this case, you are setting SSL communication between the Management server and the LDAP server.

10. If you disabled SSL communication, skip this step. If you enabled SSL communication, provide values for the following prompts:

    - SSL Key Ring File Location
    - SSL Key Label
    - Password for SSL Key

11. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix, which you added in “Adding suffixes” on page 29. For example:

    ```
    o=IBM,c=US
    ```

    This prompt does not appear when either the Policy Director Management server, or the Authorization server, has been configured previously.

    You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization’s abbreviated name, and where `c=` is the country.

    This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.

    A prompt appears requesting the DCE Cell Administration name and password.

After the GSO database access is configured, the Policy Director Configuration Manager automatically configures a DSB. A series of messages lists each automated step as it completes.

A message appears indicating that the IVMgr package installation is successful. The list of available packages reappears.

Installing the Security Manager for WebSEAL and NetSEAL

The Security Manager package (IVNet) requires resources from the Base package. Be sure that the Base component is installed before you install IVNet.

1. Type the selection number for IVNet to install the Policy Director Security Manager files, and then press Enter.

   Files are extracted from the CD and installed on the hard disk in the default directory.

   If you are using LDAP as your user registry, a series of prompts appears to integrate the Security Manager with the LDAP server.

2. If prompted, type the required information for the LDAP server configuration:

   - LDAP server host name
   - LDAP server port number
   - LDAP server SSL port number

   The above LDAP server configuration prompts appear only if communication with the LDAP server has not previously been configured for any other Policy Director packages on this system. If the Management server (IVMgr) or authorization server (IVAcld) have been configured on this system, the preceding prompts do not appear at this step.

3. Type the DN and password for the LDAP administrative user.

   The LDAP server now contains Policy Director security information.

4. Choose to enable or disable SSL communication between the Security Manager and the LDAP server.

   You can individually enable or disable SSL communication between each Policy Director server and the LDAP server. In this case, you are setting SSL communication between the Security Manager and the LDAP server.

5. If you disabled SSL communication, skip this step. If you enabled SSL communication, provide values for the following prompts:
   - `SSL Key Ring File Location`
   - `SSL Key Label`
   - `Password for SSL Key`

6. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix, which you added in “Adding suffixes” on page 29. For example:

   ```
   o=IBM,c=US
   ```

   This prompt does not appear when either the Policy Director Management server, or the Authorization server, has been configured previously.

   You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization’s abbreviated name, and where `c=` is the country.

   This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.

   A prompt appears requesting the DCE Cell Administration name and password.

7. Type the required information for access to the DCE Cell Administration account.

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   The Security Manager is configured and started.

   The CAS server is configured and started.

A prompt appears indicating that the IVNet package installation is successful. The list of available packages reappears.

Enabling the WebSEAL component

Install the WebSEAL (IVWeb) package if you want to enable the WebSEAL component. Then, to enable the WebSEAL component:

1. Type the selection number for IVWeb to install the files that are required to enable the WebSEAL HTTP server component.
2. Press Enter to continue.

   The files are extracted from the CD and installed on the hard disk.

   A configuration list appears with values that confirm HTTP and HTTPS client access, the required TCP ports, and the default Web document root directory.
3. Confirm the current configuration values:

   ```
   Check Web Server configuration:
   1. Enable TCP HTTP? Yes
   2. HTTP Port 80
   3. Enable HTTPS? Yes
   4. HTTPS Port 443
   5. Web document root directory /opt/Policy Director/www/docs

   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```
4. Type a to accept the configuration and continue the installation, and then press Enter.
5. Type the required information for access to the DCE Cell Administration account.

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   The installation configures and enables WebSEAL on the computer. The Security Manager restarts automatically.

Enabling the NetSEAL component

Install the NetSEAL (IVTrap) package if you want to enable the NetSEAL component. Then, to enable the NetSEAL component:

1. Type the selection number for IVTrap to install the files that are required to enable the NetSEAL coarse-grained TCP/IP access control component, and then press Enter.

   NetSEAL is configured and enabled.

   A prompt appears requesting the name and password of the DCE cell administrator.

2. Enter the required information for access to the DCE Cell Administration account.

   A message appears stating that you need to specify protected ports by using the **ivadmin** command.

   Another message appears, stating that you need to restart (reboot) the system to ensure that all protected ports are placed under NetSEAL’s control.

   A prompt appears indicating that the IVTrap package installation is successful. The list of available packages reappears.

Policy Director NetSEAL traps requests that are made to specific ports. To use the NetSEAL trap, you must stop and restart all applications that use the specified ports. For more information on configuring Policy Director NetSEAL, see the overview information about NetSEAL in the *Policy Director Administration Guide*.

Installing the Authorization server

To install the Authorization server:

1. Type the selection number for IVAcld to install the Policy Director Authorization Server files, and then press Enter.

   Files are extracted from the CD and installed on the hard disk in the default directory.

   If you are using LDAP as your user registry, a series of prompts appears to integrate the Authorization server with the LDAP server.

2. If prompted, type the required information for the LDAP server configuration:

   - LDAP server host name
   - LDAP server port number
   - LDAP server SSL port number

   The above LDAP server configuration prompts appear only if communication with the LDAP server has not previously been configured for any other Policy Director packages on this system. If the Management server (IVMgr) or Security Manager (IVNet) have been configured on this system, the preceding prompts do not appear at this step.

3. Type the DN and password for the LDAP administrative user.

   The LDAP server now contains Policy Director security information.

4. Choose to enable or disable SSL communication between the Management server and the LDAP server.

   You can individually enable or disable SSL communication between each Policy Director server and the LDAP server. In this case, you are setting SSL communication between the Management server and the LDAP server.

5. If you disabled SSL communication, skip this step. If you enabled SSL communication, provide values for the following prompts:
   - `SSL Key Ring File Location`
   - `SSL Key Label`
   - `Password for SSL Key`
6. If needed, add a suffix for your Policy Director users and Global Sign-On (GSO) data by providing the DN for the GSO database suffix, which you added in "Adding suffixes" on page 29. For example:

   ```
   o=IBM,c=US
   ```

   This prompt does not appear when either the Policy Director Management server, or the Authorization server, has been configured previously.

   You can name the suffixes as you like in a manner appropriate for your installation, where `o=` is your own organization's abbreviated name, and where `c=` is the country.

   This step creates suffixes for your GSO data and for your users and groups. These suffixes are created with the LDAP Web Administration tool.

   A prompt appears requesting the DCE Cell Administration name and password.
7. Type the required information for access to the DCE Cell Administration account.

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   The Authorization server is configured and started.

   A prompt appears indicating that the IVAcld package installation is successful. The list of available packages reappears.

Installing the Authorization API component

To Install the Authorization API for C files, type the selection number for IVAuthADK, and then press Enter.

Files are extracted from the CD and installed on the hard disk in the default directory.

A prompt appears indicating that the IVAuthADK package installation is successful. The list of available packages reappears.

Installing Policy Director server with a DCE user registry

If you are installing Policy Director with an LDAP user registry, go to "Installing Policy Director servers with an LDAP user registry" on page 74.

The server packages are located in the /solaris directory on the *IBM SecureWay Policy Director Version 3.0* CD.

You must be logged on as user root to install the Policy Director packages.

If you need to reinstall any package, you must first remove the existing package (**pkgrm**) before reinstalling the desired package.

To install the Management server:

1. Type the **pkgadd** command to list the available packages from the CD:

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   The list of available packages appears on the display.

   If you use a different CD-ROM mount point, substitute it in the command above.
2. Type the selection number for IVBase to install the Policy Director Base files, and then press Enter.

   This command extracts files from the CD and installs them where you specify on the hard disk.

   A prompt appears indicating that the IVBase package installation was successful. The list of available packages reappears.

   Before continuing to the next step, remember that there should only be one instance of the Management server (IVMgr) in the secure domain. If this is a standalone system installation, continue to the next step. If you are installing on a secondary server, be sure you have reviewed "Installation requirements for the secure domain" on page 23.
3. Type the selection number for IVMgr to install the Policy Director Management server files. Press Enter.

   This command extracts files from the CD and installs them where you specify on the hard disk.

   A prompt appears requesting you to choose a user registry type.
4. If you are using DCE for your user registry, type 1.

   A prompt appears requesting the DCE Cell Administrator name and password.
5. Type the required information for access to the DCE Cell Administration account.

   ```
   Enter the user name of the Cell Administrator [cell_admin]:
   Enter the password for the Cell Administrator:
   ```

A message appears indicating that the IVMgr package installation is successful. The list of available packages reappears.

Installing the Security Manager for WebSEAL and NetSEAL

The Security Manager package (IVNet) requires resources from the Base package. Be sure that the Base component is installed before you install IVNet.

1. Type the selection number for IVNet to install the Policy Director Security Manager files, and then press Enter.

   Files are extracted from the CD and installed on the hard disk in the default directory. A prompt appears requesting the DCE Cell Administrator name and password.

2. Type the required information for access to the DCE Cell Administration account.

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   The Security Manager is configured and started.

   A prompt appears indicating that the IVNet package installation is successful. The list of available packages reappears.

Enabling the WebSEAL component

Install the WebSEAL (IVWeb) package if you want to enable the WebSEAL component.

1. Type the selection number for IVWeb to install the files that are required to enable the WebSEAL HTTP server component.

2. Press Enter to continue.

   The files are extracted from the CD and installed on the hard disk.

   A configuration list appears with values that confirm HTTP and HTTPS client access, the required TCP ports, and the default Web document root directory.

3. Confirm the current configuration values:

   ```
   Check Web Server configuration:
   1. Enable TCP HTTP? Yes
   2. HTTP Port 80
   3. Enable HTTPS? Yes
   4. HTTPS Port 443
   5. Web document root directory /opt/Policy Director/www/docs

   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```

4. Type a to accept the configuration and continue the installation, and then press Enter.

5. Type the required information for access to the DCE Cell Administration account.

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   The installation configures and enables WebSEAL on the computer. The Security Manager restarts automatically.

Enabling the NetSEAL component

Install the NetSEAL (IVTrap) package if you want to enable the NetSEAL component.

1. Type the selection number for IVTrap to install the files that are required to enable the NetSEAL coarse-grained TCP/IP access control component, and then press Enter.

   NetSEAL is configured and enabled.

   A prompt appears requesting the name and password of the DCE cell administrator.
2. Enter the required information for access to the DCE Cell Administration account.

   A message appears stating that you need to specify protected ports by using the **ivadmin** command.

   Another message appears, stating that you need to restart (reboot) the system to ensure that all protected ports are placed under NetSEAL's control.

   A prompt appears indicating that the IVTrap package installation is successful. The list of available packages reappears.

Policy Director NetSEAL traps requests that are made to specific ports. To use the NetSEAL trap, you must stop and restart all applications that use the specified ports. For more information on configuring Policy Director NetSEAL, see the overview information about NetSEAL in the *Policy Director Administration Guide.*

Installing the Authorization server

To install the Authorization server:

1. Type the selection number for IVAcld to install the Policy Director Authorization Server files, and then press Enter.

   Files are extracted from the CD and installed on the hard disk in the default directory. A prompt appears requesting the DCE Cell Administrator name and password.
2. Type the required information for access to the DCE Cell Administration account.

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

The Authorization server is configured and started.

A prompt appears indicating that the IVAcld package installation is successful. The list of available packages reappears.

Installing the Authorization API component

To install the Authorization API for C files, type the selection number for IVAuthADK, and then press Enter.

Files are extracted from the CD and installed on the hard disk in the default directory.

A prompt appears indicating that the IVAuthADK package installation is successful. The list of available packages reappears.

Configuring the Credentials Acquisition Service

The Policy Director CAS is installed automatically. If you want to use the Policy Director CAS for your credentials acquisition service, you must configure it. See the information about configuring a credentials acquisition service in the *Policy Director Administration Guide* for instructions.

Installing and starting the Management Console

Policy Director provides a Management Console that manages many of the Policy Director components.

The Management Console for Solaris is installed using the IVConsole installation package. Use **pkgadd** to install and configure the package.

1. Log in as root.
2. Insert and mount the *IBM SecureWay Policy Director Version 3.0* CD into the CD-ROM drive of the Policy Director server system.
3. Display the list of available packages:

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```
4. Type the selection number for IVBase if it is not installed already. If IVBase is already installed, go to step 6.
5. Type y to continue.

   The list of packages appears.
6. Type the selection number for IVConsole.
7. Type y to continue.

   A prompt appears indicating a successful installation. The Management Console is now ready to start.

To start the Management Console:

1. Make sure that the Policy Director servers are installed and running.
2. Type the following command:

```
$ /opt/intraverse/bin/ivconsole
```

Removing Policy Director

Remove the Policy Director servers from the computer by using the **pkgrm** utility. Packages must be removed opposite the order followed during installation. The **pkgrm** and **pkgadd** commands are members of the same utility family and have the same user interface. The root user runs the **pkgrm** utility.

There are several methods for using this command:

- Start the **pkgrm** command with no arguments.

  A numbered list of current packages on your computer appears. Type a single selection number for the package you want to remove.
- Start the **pkgrm** command and specify a single package name as the argument to the command. For example:

  ```
  # pkgrm IVBase
  ```
- Start the **pkgrm** command and specify a sequence of package names as multiple arguments to the command. For example:

  ```
  # pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
  ```

Consult the Solaris operating system documentation for more detailed information about the **pkgrm** command.

Note: You must remove the Policy Director packages in exactly the reverse of the order that is required for installation.

To remove Policy Director:

1. Log in to the Solaris operating system as root.

   Use one of the preceding methods of starting the **pkgrm** command.
2. Policy Director components must be removed in the following order:
   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

Your computer system configuration might not include every package that is shown in the previous list. The Policy Director Management Console (IVConsole) can be removed at any time before IVBase.

Removing the Management Console

To remove the Management Console:

1. Log in as user root.
2. Type the following command:

   ```
   # pkgrm ivconsole
   ```

Chapter 8. Related documentation

You can use the documentation listed in this chapter to find more information about Policy Director Version 3.0 and related products.

Policy Director documentation

This book, *IBM SecureWay Policy Director Up and Running, Version 3.0*, in addition to being provided with the Policy Director product, is also available in a documentation pack. The Policy Director documentation pack includes this book and the Policy Director license information.

In addition to this book, the following documents contain information about Policy Director and are available in PostScript Document Format (PDF) format under the /doc subdirectory on the *IBM SecureWay Policy Director Version 3.0* CD:

- *IBM SecureWay Policy Director Administration Guide, Version 3.0*

  This book gives detailed instructions for administering Policy Director. This book provides information about IBM SecureWay Policy Director, such as:
  - Policy Director concepts such as authentication, authorization, and credentials acquisition
  - General administration tasks using the Management Console
  - WebSEAL administration
  - NetSEAL administration
  - NetSEAT administration
  - Administration resources (the **ivadmin** command)
- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

  This book discusses the Authorization API components and how to perform these tasks:
  - Building applications with the Authorization API
  - Initializing the Policy Director Authorization Service
  - Authenticating an application server or client
  - Obtaining user credentials
  - Making an authorization decision
  - Performing optional tasks
  - Cleaning up and shutting down
  - Deploying applications with the Authorization API

The Policy Director README file might contains the most up-to-date information about Policy Director information that supersedes the product publications.

To obtain the most current README file, access the library page of the IBM SecureWay Policy Director Web site.

```
http://www.ibm.com/software/security/policy/library
```

IBM SecureWay FirstSecure documentation

The following book contains information about FirstSecure:

- *IBM SecureWay FirstSecure Planning and Integration, Version 2.0 (S564-8D11–00)*

  This book describes FirstSecure and the products that make up FirstSecure, and helps you start planning to use all the IBM SecureWay products.

IBM SecureWay Policy Director (Policy Director) is available either as a component of IBM SecureWay FirstSecure or as a standalone product. If your version of Policy Director is included in the FirstSecure offering, this book is provided with FirstSecure. If your version of Policy Director was purchased as a standalone product, this book can be found at the FirstSecure Web page:

```
http://www.ibm.com/software/security/firstsecure/library
```

IBM Distributed Computing Environment documentation

The following documents describe how to install DCE and are available on the *IBM SecureWay Policy Director Security Services* CD in PDF format under /doc or at the DCE Web documentation sites.

IBM DCE for Windows NT

IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2 is available at the following Web address:

```
http://www.software.ibm.com/network/dce/library/publications/dcent.html
```

This book describes Distributed Computing Environment (DCE) for Windows NT, Version 2.2, and explains how to plan for, install, and configure the product.

The *IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2* book is also available on the *IBM SecureWay Policy Director Security Services* CD in /doc/DCE22_QuickBeginnings_NT.pdf.

IBM DCE for AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2, available at the following Web address:

```
http://www.software.ibm.com/network/dce/library/publications/dceaix.html
```

This book describes the IBM Distributed Computing Environment for AIX, Version 2.2 (DCE 2.2 for AIX), and explains how to plan for, install, and configure the product.

The *IBM Distributed Computing Environment for AIX Quick Beginnings Version 2.2* is also available on the *IBM SecureWay Policy Director Security Services* CD in /doc/DCE22_QuickBeginnings_AIX.pdf.

Transarc DCE for Solaris

The *Transarc DCE Version 2.0 Release Notes* and the *Installation and Configuration Guide* are available at the following Web address:

```
http://www.transarc.com/Library/documentation/dce/2.0/index.html
```

The *Transarc DCE Version 2.0 Release Notes* documents the following information about Transarc DCE software and documentation:

- Differences between OSF DCE and the DCE * DFS product
- Differences between Version 2.0 and Version 1.1 of DCE * DFS
- Known defects and limitations associated with DCE * DFS

The *Transarc DCE Version 2.0 Release Notes* is also available on the *IBM SecureWay Policy Director Security Services* CD in /doc/DCE20_ReleaseNotes_Solaris.pdf.

The *Installation and Configuration Guide* provides instructions for installing, configuring, and upgrading the DCE DFS 2.0 product.

The *Installation and Configuration Guide* is also available on the *IBM SecureWay Policy Director Security Services* CD in /doc/DCE20_InstallGuide_Solaris.pdf.

IBM SecureWay Directory documentation

The following book contains installation and configuration information for IBM SecureWay Directory (LDAP):

- *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*

  There is a separate version of this book in HTML format for each of the supported operating systems. The book for each operating system is on the appropriate CD at /doc/wparent.htm.

The CDs are:

- *IBM SecureWay Directory Version 3.1.1 for NT*
- *IBM SecureWay Directory Version 3.1.1 for AIX*
- *IBM SecureWay Directory Version 3.1.1 for Solaris*

After LDAP installation, the location of the installation and configuration .HTM documentation file is:

Windows:

```
C:\Program Files\IBM\LDAP\nls\html\enUS1252\config\wparent.htm
```

UNIX:

```
opt/IBM/LDAP/nls/html/enUS1252/config/wparent.htm
```

The following book in HTML file contains information on how to administer IBM SecureWay:

- *IBM SecureWay Directory Administration Guide, Version 3.1.1*
  1. Using a Web browser, access the documentation found at this Web address after a default installation of LDAP:

     ```
     C:\Program Files\IBM\LDAP\nls\html\enUS1252\config\wparent.ht
     ```

This following book in HTML format contains information about the IBM SecureWay Directory client:

- *IBM SecureWay Directory Client SDK Programming Reference, Version 3.1.1*

  This book contains links to this LDAP information:

  - The LDAP Client SDK Plugin Programming Reference information
    1. Using a Web browser, access the documentation found at this Web address after a default installation of LDAP:

       ```
       C:\Program Files\IBM\doc\progref.htm
       ```
    2. Open the *IBM SecureWay Directory Client SDK Programming Reference* documentation.
    3. Click **Appendices**.
    4. Click **LDAP Client SDK Plugin Programming Reference**

- The information on how to use the GSKit and the Key Management Tool **ikmguiw** to configure the LDAP server to support SSL access
  1. If this book is not already opened, open the *IBM SecureWay Directory Client SDK Programming Reference* documentation.
  2. Click **API categories**.
  3. Click **SSL**.
  4. Click the **LDAP_SSL API**.
  5. Locate and click the **Using IKMGUI** link to open the appropriate HTML file.

The following document is also available for IBM SecureWay Directory server:

- *IBM SecureWay Directory Server Plug-ins Reference*

Appendix. Notices

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

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

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AIX
DB2
FirstSecure
IBM
SecureWay

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape and the Netscape logos	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Index

Part Number: CT63KNA

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SCT6-3KNA-00

CT63KNA