Tivoli. IBM Tivoli Access Manager for e-business

IBM

Version 6.0

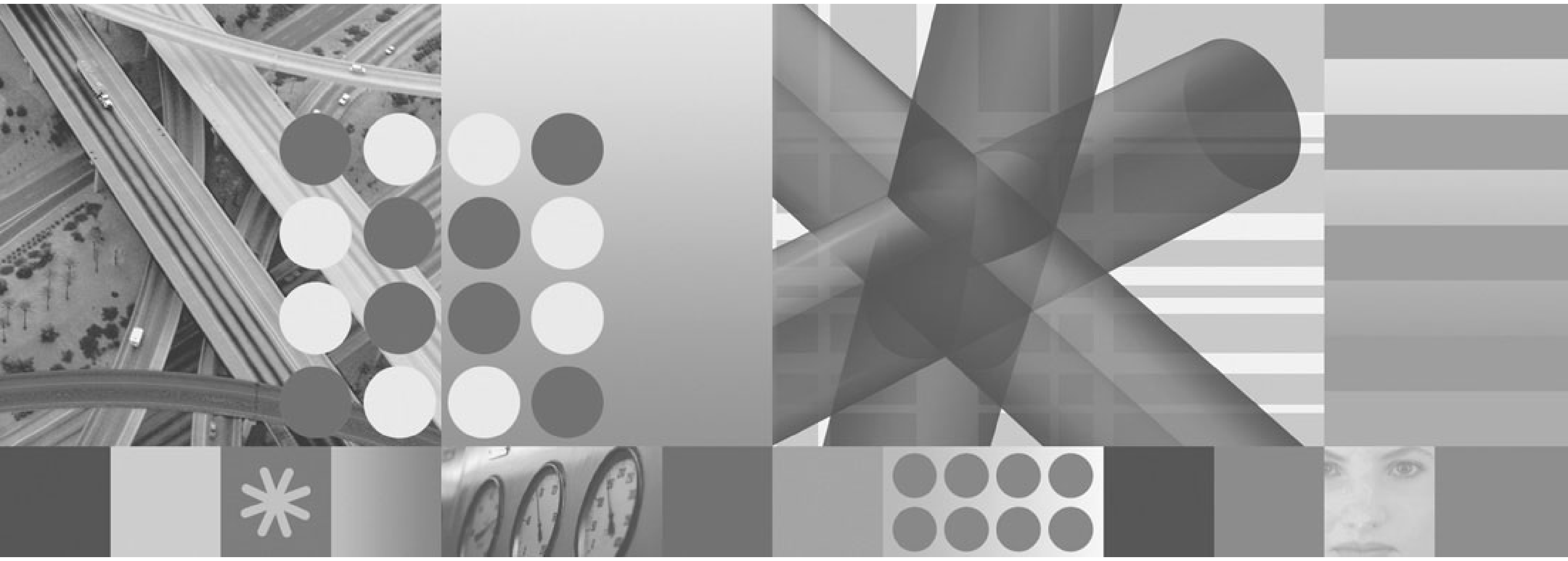
Common Criteria Guide

SC23-6138-00

Tivoli® IBM Tivoli Access Manager for e-business

IBM

Version 6.0



Common Criteria Guide

SC23-6138-00

Note

Before using this information and the product it supports, read the information in “Notices” on page 25.

First Edition (January 2007)

This edition applies to version 6, release 1, modification 0 of IBM Tivoli Access Manager (product number 5724-C08) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface . . . v

Who should read this book . . . v

What this book contains . . . v

Publications . . . vi

Accessibility . . . viii

Tivoli software training . . . viii

Contacting software support . . . viii

Conventions used in this book . . . ix

Chapter 1. Introduction . . . 1

Chapter 2. CC-compliant installation and configuration . . . 3

Verifying the integrity of Tivoli Access Manager documentation . . . 4

Installation . . . 5

Configuration . . . 6

Chapter 3. Security policy for IBM Tivoli Access Manager . . . 11

Base security policy. . . . 11

System security policy . . . 11

Tivoli Access Manager network policy . . . 13

Chapter 4. User requirements . . . 15

Chapter 5. Evaluated security functions of IBM Tivoli Access Manager . . . 17

Chapter 6. Usage guidelines . . . 19

Locking user accounts . . . 19

Specifying SSL ciphers at a host or network level on Windows . . . 19

Configuring SSL quality of protection with AES and FIPS-DES cipher limitations . . . 19

Glossary . . . 21

Notices . . . 25

Preface

The *IBM® Tivoli® Access Manager for e-business Common Criteria Guide* provides information about how IBM Tivoli Access Manager, Version 6.0 can meet the Common Criteria assurance level of EAL3+.

Tivoli Access Manager is the base software that is required to run applications in the Tivoli Access Manager product suite. It enables the integration of Tivoli Access Manager applications that provide a wide range of authorization and management solutions. Sold as an integrated solution, these products provide an access control management solution that centralizes network and application security policy for e-business applications.

Note: Tivoli Access Manager is the new name of the previously released software entitled Tivoli SecureWay® Policy Director. Also, for users familiar with the Tivoli SecureWay Policy Director software and documentation, the management server is now referred to as the policy server.

Tivoli Access Manager for e-business is a complete authorization solution for corporate Web, client/server, MQSeries®, and existing legacy applications. Tivoli Access Manager authorization allows an organization to control user access to protected information and resources in a secure manner. You use Tivoli Access Manager in conjunction with standard Internet-based applications to build highly secure and well-managed network-based applications.

Who should read this book

This guide is for system administrators who are responsible for configuring systems to meet the Common Criteria assurance level of EAL3+.

Readers should be familiar with the following:

- PC and Linux® operating systems
- Security management, including authentication and authorization
- Internet protocols, including HTTPS, FTP, TCP/IP, and Telnet
- Secure Socket Layer (SSL) and Transport Layer Security (TLS) communication protocols, key exchange (public and private), digital signatures, cryptographic algorithms, and certificate authorities
- Lightweight Directory Access Protocol (LDAP) and directory services

What this book contains

This book contains the following sections:

- Chapter 1, “Introduction,” on page 1
- Chapter 2, “CC-compliant installation and configuration,” on page 3
- Chapter 3, “Security policy for IBM Tivoli Access Manager,” on page 11
- Chapter 4, “User requirements,” on page 15
- Chapter 5, “Evaluated security functions of IBM Tivoli Access Manager,” on page 17
- Chapter 6, “Usage guidelines,” on page 19

Publications

Review the descriptions of the Tivoli Access Manager library, the prerequisite publications, and the related publications to determine which publications you might find helpful. After you determine the publications you need, refer to the instructions for accessing publications online.

Additional information about the Tivoli Access Manager for e-business product itself can be found at:

> http://www.ibm.com/software/tivoli/products/access-mgr-e-bus/

This document references the following documents in the Tivoli Access Manager for e-business library:

- Tivoli Access Manager for e-business Version 6.0 Release Notes

  Provides late-breaking information, such as software limitations, workarounds, and documentation updates.
- *Tivoli Access Manager for e-business Version 6.0: Installation Guide*, SC32-1684-00

  Provides installation, configuration, and removal instructions for the Tivoli Access Manager base software and the Web Security components.
- *Tivoli Access Manager for e-business Version 6.0: Administration Guide*, SC32-1686-00

  Describes the concepts and procedures for using Tivoli Access Manager services. Provides instructions for performing tasks from the Web Portal Manager interface and by using the **pdadmin** command.
- *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide*, SC32-1687-00

  Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.
- *Tivoli Access Manager for e-business Version 6.0: Auditing Guide*, SC32-2202-00

  Provides information about configuring and managing audit events using the native Tivoli Access Manager approach and the Common Auditing and Reporting Service.
- *Tivoli Access Manager for e-business Version 6.0: Administration C API Developer's Reference*, SC32-1692-00

  Provides reference information about using the administration API to enable an application to perform Tivoli Access Manager administration tasks. This document describes the C implementation of the administration API.
- *Tivoli Access Manager for e-business Version 6.0: Authorization C API Developer's Reference*, SC32-1694-00

  Provides reference material that describes how to use the Tivoli Access Manager authorization C API and the Tivoli Access Manager service plug-in interface to add Tivoli Access Manager security to applications.
- *Tivoli Access Manager for e-business Version 6.0: Command Reference*, SC32-1697-00

  Provides information about the command line utilities and scripts provided with Tivoli Access Manager.
- *Tivoli Access Manager for e-business Version 6.0: Error Message Reference*, SC32-1696-00

  Provides explanations and recommended actions for the messages produced by Tivoli Access Manager.

- *Tivoli Access Manager for e-business Version 6.0: Problem Determination Guide*, SC32-1701-00

  Provides problem determination information for Tivoli Access Manager.

For instructions on locating a specific document in a specific version of a product, see "Accessing publications online" on page viii.

Related products

This section lists the IBM products that are related to and included with a Tivoli Access Manager solution.

IBM Global Security Kit

Tivoli Access Manager provides data encryption through the use of the IBM Global Security Kit (GSKit), Version 7.0.3.3. The GSKit package provides the iKeyman key management utility, **gsk7ikm**, which is used to create key databases, public-private key pairs, and certificate requests.

IBM Tivoli Directory Server

IBM Tivoli Directory Server, Version 6.0, is included on the *IBM Tivoli Access Manager Directory Server* CD for the desired operating system.

Note: IBM Tivoli Directory Server is the new name for the previously released software known as:

- IBM Directory Server (Version 4.1 and Version 5.1)
- IBM SecureWay Directory Server (Version 3.2.2)

IBM Directory Server, Version 4.1, IBM Directory Server 5.1, and IBM Tivoli Directory Server, Version 5.2, are all supported by Tivoli Access Manager, Version 6.0.

Additional information about IBM Tivoli Directory Server can be found at the following Web address:

http://www.ibm.com/software/network/directory/library

IBM DB2 Universal Database

IBM DB2 Universal Database™ Enterprise Server Edition is included on the *IBM Tivoli Access Manager Directory Server* CD and is installed with the IBM Tivoli Directory Server software. DB2® is required when using IBM Tivoli Directory Server, z/OS® LDAP servers as the user registry for Tivoli Access Manager. For z/OS LDAP servers, you must separately purchase DB2.

Additional information about DB2 can be found at the following Web address:

http://www.ibm.com/software/data/db2

IBM WebSphere Application Server

IBM WebSphere® Application Server, Version 6.0, Fix Pack 2, is included on the *IBM Tivoli Access Manager Web Administration Interfaces* CD for the desired operating system. WebSphere Application Server enables the support of both the Web Portal Manager interface, which is used to administer Tivoli Access Manager, and the Web Administration Tool, which is used to administer IBM Tivoli Directory Server.

Additional information about IBM WebSphere Application Server can be found at the following Web address:

http://www.ibm.com/software/webservers/appserv/infocenter.html

Accessing publications online

The publications for this product and many other Tivoli products are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli Software Library. The Tivoli Software Library provides a variety of Tivoli publications such as white papers, data sheets, demonstrations, Redbooks, and announcement letters. The library is located at the following Web address:

http://publib.boulder.ibm.com/tividd/td/tdprodlist.html

To locate product publications in the library, click the first letter of the product name or scroll until you find the product name. Then click the name of the product. Product publications include release notes, installation guides, user's guides, administrator's guides, and developer's references.

Note: To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe Acrobat Print window (which is available when you click **File** → **Print**).

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from many IBM products in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/ibm/terminology

Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You also can use the keyboard instead of the mouse to operate all features of the graphical user interface.

Tivoli software training

For Tivoli software training information, refer to the IBM Tivoli Education Web site at the following Web address:

http://www.ibm.com/software/tivoli/education

Contacting software support

Before contacting IBM Tivoli Software Support with a problem, refer to the IBM Tivoli Software Support site by clicking the **Tivoli support** link at the following Web site:

http://www.ibm.com/software/support/

If you need additional help, contact software support by using the methods described in the *IBM Software Support Guide* at the following Web address:

http://techsupport.services.ibm.com/guides/handbook.html

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers, depending on the country in which you are located
- A list of information you should gather before contacting customer support

Conventions used in this book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface conventions

The following typeface conventions are used in this reference:

Bold Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java classes, and objects are in **bold**.

Italic Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

`Monospace`
Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in `monospace`.

Operating system differences

This book uses the UNIX convention for specifying environment variables and for directory notation. When using the Windows command line, replace `$variable` with `%variable%` for environment variables and replace each forward slash (/) with a backward slash (\) in directory paths. If you are using the bash shell on a Windows operating system, you can use the UNIX conventions.

Chapter 1. Introduction

A Common Criteria evaluated system is a system that has been evaluated according to the Common Criteria (CC), an internationally recognized ISO standard (ISO/IEC 15408) for the assurance evaluation of IT products. IBM Tivoli Access Manager, Version 6.0, contains the technology to meet the requirements of the CC assurance level EAL3+. The system configuration that meets these requirements is referred to as a CC-evaluated system in this guide.

The evaluation was performed on the specific configuration described in this section. Changing this configuration leads to a non-evaluated system. This, however, does not mean that the security of the system is reduced. It only means that this customized configuration is not covered by the evaluation.

This document explains the constraints of a system that has to meet the requirements of a CC evaluation. The IBM Tivoli Access Manager, Version 6.0, CC-evaluated system (target of evaluation, or TOE) includes the following Tivoli Access Manager systems:

Policy server (pdmgrd) with the following components installed:

- Tivoli Access Manager Runtime 6.0.0.3 (fixpack 3)
- Tivoli Access Manager Policy Server 6.0.0.3 (fixpack 3)
- IBM Directory client 6.0.0.2
- IBM Global Security Kit (GSKit) 7.0.3.17

WebSEAL server (webseald) with the following components installed:

- Tivoli Access Manager Runtime 6.0.0.3 (fixpack 3)
- Tivoli Access Manager WebSEAL server 6.0.0.3 (fixpack 3)
- IBM Directory client 6.0.0.2
- IBM Global Security Kit (GSKit) 7.0.3.17

The policy server and WebSEAL within an evaluated configuration use the same operating system platform (but run on different machines). Those platforms will be one of the following:

- IBM AIX® 5.3
- Sun Solaris 9
- Microsoft® Windows 2003 Enterprise Server
- SuSE LINUX Enterprise Server 9 on IBM xSeries®
- Red Hat Enterprise Linux® 4 on IBM xSeries

The following sections describe the way that these components and the operational environment must be configured to attain a CC-compliant system.

Chapter 2. CC-compliant installation and configuration

The CC evaluation covers security configuration options listed only in this document. To set up the evaluated configuration that is compliant with the following information, the user needs to follow the guidance that is provided in the *Tivoli Access Manager for e-business Version 6.0: Installation Guide*. Read this chapter in its entirety before installation to ensure proper installation of the TOE.

- The policy server component of the TOE is installed and operated on a dedicated system that communicates via a network connection to the WebSEAL server.
- The Resource Manager and Authorization Evaluator are installed and operated on the same system. They communicate with each other via a library interface, the aznAPI. They communicate with the policy server via a network connection with a dedicated application layer protocol running over Transport Layer Security (TLS) Version 1.

  Note that the evaluated configuration does not include Authorization Evaluator components running on a machine separate from the Resource Manager that uses them.
- The evaluated configuration has one policy server and one or more WebSEAL server systems. All WebSEAL server systems operate independently from each other and are only connected to the central policy server. Load balancing and failover configurations of WebSEAL server systems are therefore not supported in the evaluated configuration.
- The policy server and all the WebSEAL servers use the same operating system as a basis. Configurations using different operating system platforms for different components of the TOE are not part of the evaluated configuration.
- The TOE is required to run in FIPS mode.
- Communication between client systems and the TOE, the Web server systems and the TOE, and the LDAP server and the TOE is protected using the TLS v1 or SSL v3 protocol with one of the ciphersuites defined in this guide. Communication between the policy server and the Resource Manager/Authorization Evaluator systems (WebSEAL) is protected using **only** the TLS v1 protocol with one of the ciphersuites defined in this guide. The use of unencrypted communication is disabled in the TOE. Also, the use of version 2 of the SSL protocol is disabled for communication to client systems and target systems. Within the TOE, all components are configured to use TLS v1 only. The external LDAP server also needs to support TLS v1 and be configured to use TLS v1 as its preferred protocol.
- No hardware encryption device is used. The cryptographic services are fully provided by the software implementation of the GSKit component.
- The TOE is configured to use password-based authentication and SSL client certificate-based authentication for the authentication of users. Other authentication mechanisms for user authentication are disabled.
- The TOE is configured to use password-based authentication for administrators that request access to the TOE via the pdadmin interface or the C API.
- The use of the Web Portal Manager component for the administration of the TOE is **not** supported. Instead, only the command line interface of pdadmin and the C API are supported in the evaluated configuration.
- No Application Development Kit is installed in the evaluated configuration.

- Only LDAP is supported for the access to the directory server in the evaluated configuration. Active Directory or other directory servers are not supported. LDAP replicas are also not supported.
- The TOE uses only the English language pack.
- The TOE does not support the process of "self-registration" by which a user can register to become an IBM Tivoli Access Manager user, without the administrator’s involvement. Moreover, self-registration is a function of the Web Portal manager and controlled by the administrator.
- Single sign-on mechanisms are not supported in the evaluated configuration.
- Multiple domains are not supported by the TOE, and only the default domain is used.
- Authorization rules are not supported in the evaluated configuration.
- "Session Cookies" is excluded from the evaluated configuration.
- "Credential attribute entitlement" is not supported in the evaluated configuration.
- The Java API is not supported in the evaluated configuration.
- The policy server proxy is not supported in the evaluated configuration.
- Integration with the IBM Tivoli Identity Manager is not supported in the evaluated configuration.
- The use of Access Manager Session Management Server (SMS) is not supported in the evaluated configuration.
- The use of the Common Auditing and Reporting Service (CARS) is not supported in the evaluated configuration.
- The transparent path junction option for WebSEAL is not supported in the evaluated configuration.
- Export and import of security policy (POPs, ACLs, authorization rules, and objects) to other Tivoli Access Manager domains is not supported in the evaluated configuration.
- WebSEAL support for maintaining session state using HTTP headers as session keys is not supported in the evaluated configuration.
- Only the “minimal” LDAP data format (selected during the installation of the policy server) is supported in the evaluated configuration.
- IPv6 POP-based network authentication is not supported in the evaluated configuration.

Verifying the integrity of Tivoli Access Manager documentation

To ensure the integrity of the Tivoli Access Manager documentation downloaded from the Tivoli software information center, the **md5sum** checksums are provided for the PDF versions of the documentation. These sums can be checked in the following manner:

1. Ensure that you have a **md5sum** program available. It should be available on most platforms.
2. To generate the MD5 sum for the PDF file that you have downloaded, run:

   ```
   md5sum PDF file
   ```

   where *PDF file* is the is the filename of the PDF.
3. Compare your output from the command with the following sums. The two sums should match to ensure download integrity.
   - *Tivoli Access Manager for e-business Version 6.0: Installation Guide*

  bce0d29af9b12cb1a22f828f0242ab11 *am60_install.pdf

- *Tivoli Access Manager for e-business Version 6.0: Administration Guide*

  762756e45571ac5bb5485b95d94e1298 *am60_admin.pdf
- *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide*

  47bc934eadc2497ba9388ce458669761 *am60_webseal_admin.pdf
- *Tivoli Access Manager for e-business Version 6.0: Auditing Guide*

  e25646b787cde5f82009e7856fbbd076 *am60_audit.pdf
- *Tivoli Access Manager for e-business Version 6.0: Administration C API Developer's Reference*

  f4c7f70be7c0a56bae18c7f0afc4cd42 *am60_adminc_devref.pdf
- *Tivoli Access Manager for e-business Version 6.0: Command Reference*

  730bc1d84c551629c4950550dbdd5423 *am60_cmdref.pdf
- *Tivoli Access Manager for e-business Version 6.0: Error Message Reference*

  c500dcf0109a5cb504c0ee2b589a23a9 *messages.pdf
- *Tivoli Access Manager for e-business Version 6.0: Problem Determination Guide*

  0df7eb847f9cdda91d577bf551c7d63e *am60_problem.pdf

Installation

To obtain a CC-compliant installation of Tivoli Access Manager for e-business, use the *Tivoli Access Manager for e-business Version 6.0: Installation Guide*, except for the deviations and additional configuration that are described in this guide.

Determining the version of the TOE with AIX

Use the **lslpp -l** rather than the **pdversion** command to determine version numbers of components. The **lslpp -l** command will list all of the packages that are installed. For additional usage information, consult AIX guidance documentation.

Relevant packages

Relevant packages include the following:

- Access Manager Policy Server
- Access Manager Runtime
- AIX Certificate and SSL Base Runtime ACME Toolkit (GSKit)
- Access Manager Web Security Runtime Environment
- Access Manager WebSEAL Server

Sample output

The **lslpp -l** command will produce a long list of the packages installed. The list of results will look similar to the following:

```
gskta.rte     7.0.3.17 COMMITTED  AIX Certificate and SSL Base
                                  Runtime ACME Toolkit
PD.RTE        6.0.0.3  COMMITTED  Access Manager Runtime
PD.Mgr        6.0.0.3  COMMITTED  Access Manager Policy Server
PDWeb.RTE     6.0.0.3  COMMITTED  Access Manager Web Security
                                  Runtime Environment
PDWeb.Web     6.0.0.3  COMMITTED  Access Manager WebSEAL Server
```

Determining the version of the TOE (non-AIX)

To determine the version of the TOE on platforms other than AIX, run the **pdversion** command. The command output includes the current fixpack version. In the following example, the WebSEAL fixpack level is 6.0.0.3 (6.0.0-TIV-AWS-FP0003).

```
pdversion
IBM Tivoli Access Manager Runtime   6.0.0.3
IBM Tivoli Access Manager Policy Server Not Installed
IBM Tivoli Access Manager Web Portal Manager Not Installed
IBM Tivoli Access Manager Application Developer Kit Not Installed
IBM Tivoli Access Manager Authorization Server Not Installed
IBM Tivoli Access Manager Java Runtime Environment Not Installed
IBM Tivoli Access Manager Policy Proxy Server Not Installed
IBM Tivoli Access Manager WebSEAL Server 6.0.0.3
```

Configuration

After the initial installation of Tivoli Access Manager for e-business, additional configuration steps are necessary to achieve a CC-compliant state. These steps are listed in the following sections.

Note: The steps described are specified as a delta to the default initial configuration of the Tivoli Access Manager components.

CC-compliant configuration files

The following configuration files were used in the CC evaluation of Tivoli Access Manager. For descriptions of these files, including stanza and parameter information, see the *Tivoli Access Manager for e-business Version 6.0: Administration Guide*. For the webseald-default.conf file, consult the *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide*.

- ivmgrd.conf
- ldap.conf
- pd.conf
- webseald-default.conf

Selecting the LDAP data format

During the installation of the policy server, you are given the opportunity to select what LDAP data format is to be used for user and group tracking information. When prompted, the **minimal** data format must be selected. For more information on LDAP data formats, see chapter 5 of the *Tivoli Access Manager for e-business Version 6.0: Installation Guide*.

Enabling FIPS mode and HTTPS

IBM Tivoli Directory Server and the policy server: Enable Federal Information Processing Standards (FIPS) for the policy server and the IBM Tivoli Directory Server using the *Tivoli Access Manager for e-business Version 6.0: Installation Guide*.

Securing WebSEAL: The evaluated configuration supports only HTTPS access to WebSEAL. To ensure that only HTTPS access is used, the WebSEAL configuration file (webseald-default.conf by default) must be edited. Make the following configuration changes in webseald-default.conf to ensure HTTPS access:

```
[server]
http = no
https = yes
```

It is recommended, though not required, that WebSEAL uses the standard HTTPS port as follows:

```
[server]
https-port = 443
```

FIPS mode processing is disabled by default. To enable FIPS mode processing, set the following entry:

```
[ssl]
fips-mode-processing = yes
```

Note: Connections from WebSEAL to the backend servers must be SSL based (TLS Version 1 or SSL version 3). WebSEAL does not rewrite the URLs according to the junction when SSL and non-SSL is mixed.

SSL v2 must be disabled. To disable SSL v2, set the following entry:

```
[junction]
disable-ssl-v2 = yes
```

Configuring WebSEAL authentication mechanisms

The evaluated configuration restricts the use of a user authentication mechanism to the following subset:

- User ID and password-based authentication (basic authentication)
- Certificate-based authentication (forms authentication)

Therefore, one of the following configuration parameters have to be set in the `webseald-default.conf` configuration file.

Basic authentication	Forms authentication

`[ba]`
`ba-auth = https`
 	
`[forms]`
`#forms-auth = https`
	`[certificate]`
	`accept-client-certs = optional`
	
	`[authentication-mechanisms]`
	`cert-ssl =` *`client_certificate_path`*

Note: Either `[ba]` over HTTPS or `[forms]` over HTTPS can be used.

Configuring WebSEAL supported cipher suites

The following TLS Version 1 and SSL Version 3 cipher suites must be used in the evaluated configuration:

TLS Version 1 supported cipher suites:

- `TLS_RSA_WITH_DES_CBC_SHA`
- `TLS_RSA_WITH_3DES_EDE_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_256_CBC_SHA`

SSL Version 3 supported cipher suites:

- `SSL_RSA_FIPS_WITH_DES_CBC_SHA`
- `SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA`

The following parameters must be set in `webseald-default.conf`:

```
[ssl-qop]
ssl-qop-mgmt = yes

[ssl-qop-mgmt-default]
default = FIPS-DES-56
default = FIPS-DES-168
default = DES-56
default = DES-168
default = AES-128
default = AES-256
```

Configuring auditing

The event log mechanism allows various targets for the log and audit entries.

On **WebSEAL**, the following entries must be placed in the configuration file in the [aznapi-configuration] stanza:

```
logaudit=yes
logcfg = audit.azn:file path=audit_file,
         log_id=audit,
         flush_interval=1,
         rollover_size=10000000,
         buffer_size=0,
         queue_size=1,
         hi_water=1
logcfg = audit.authn:file log_id=audit
logcfg = audit.mgmt:file log_id=audit
logcfg = audit.http:file log_id=audit
```

where *audit_file* is the fully qualified path of the audit log file.

Note: The configuration directive must be entered on one line. The line breaks in this document are for readability purposes only. Also of importance, there must be no blank spaces after commas in the logcfg entry. For more information on the event logging and auditing, see the *Tivoli Access Manager for e-business Version 6.0: Administration Guide*.

On the **policy server**, the following entries must be placed in the configuration file (pd.conf) in the [aznapi-configuration] stanza:

```
logaudit=yes
logcfg = audit.azn:file path=audit_file,
         log_id=audit,
         flush_interval=1,
         rollover_size=10000000,
         buffer_size=0,
         queue_size=1,
         hi_water=1
logcfg = audit.authn:file log_id=audit
logcfg = audit.mgmt:file log_id=audit
logcfg = audit.http:file log_id=audit
```

where *audit_file* is the fully qualified path of the audit log file.

Note: The configuration directive must be entered on one line. The line breaks in this document are for readability purposes only. Also of importance, there must be no blank spaces after commas in the logcfg entry. For more information on the event logging and auditing, see the *Tivoli Access Manager for e-business Version 6.0: Administration Guide*.

These examples send all audit events from all the audit categories to one audit log file. This file will grow up to 10,000,000 bytes before a new log file is created. A timestamp is appended to the old file.

The administrator needs to ensure that there is always enough space in the file system into which the audit trail is written. These examples create an audit trail for all of the subclasses that support auditing.

Disabling multi-domains

The use of multiple domains is not supported by the CC-evaluated configuration of Tivoli Access Manager. To ensure that no more than one domain is used, execute the following command using the policy server **pdadmin** utility:

```
pdadmin –a admin_id –p admin_password acl modify default-domain set group iv-admin TcdbvaBRN
```

Note: In order to enforce the "single domain" rule, the above changes can be made to the ACLs to protect the management objects. These changes *cannot* completely disable the function in question, but they will hinder accidental usage.

Disabling the use of authorization rules

The use of authorization rules is *not supported* by the CC-evaluated configuration of Tivoli Access Manager.

Note: In order to enforce this rule, the following changes can be made to the ACLs to protect the management objects. These changes *cannot* completely disable the function in question, but they will hinder accidental usage. Entering the pdadmin commands below *cannot* completely disable the function in question, but they will hinder accidental usage.

Unlike the "single domain" rule, authorization rules have no ACL directly attached to `/Management/Rule`. To disable authorization rules, a default-rule ACL (minus the m bit) must be created. Then the ACL must be attached to the `/Management/Rule`. To disable the use of authorization rules, perform the following pdadmin commands:

```
pdadmin -a admin_id -p admin_password
acl create default-rule
acl mod default-rule set desc "Default Domain Authzrule"
acl mod default-rule set group iv-admin TcdbvaBRN
acl mod default-rule set group ivmgrd-servers v
acl mod default-rule set user admin_id TcdbsvaBRl
acl attach /Management/Rule default-rule
```

To verify that the use of authorization rules is disabled, issue the following command:

```
authzrule create rule1 "dummy rule" -desc kfjdklfjdkslfjd
```

This should result in the following error message:

```
Could not perform the administration request
Error: HPDAC1050E   Operation is not authorized. (status 0x1005b41a)
```

Enabling polling for security policy database updates

To enable polling for updates of the security policy database, set the following parameter in the `[aznapi-configuration]` stanza of the `webseald-default.conf` file:

```
cache-refresh-interval = 600
```

This parameter ensures that WebSEAL polls for potential updates of the security policy database every 600 seconds and, subsequently, replicates the security policy database if changes occur. For more information on WebSEAL security settings and security policy database replication, see the *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide* and the *Tivoli Access Manager for e-business Version 6.0: Administration Guide*.

Disabling the LTPA cache

To ensure that any unwanted functionality is switched off, the following parameters must be changed:

```
[ltpa]
ltpa-cache-enabled = no
```

Login policy

To conform to the CC requirements, use the **pdadmin** command to change the default login policy for user and administrative IDs as follows:

```
policy set max-login-failures 3
```

This ensures that the login policy is applied after three consecutive failed attempts and not after ten attempts (the default). Note that you do not need to change the default penalty of 180 seconds.

Note: More than one WebSEAL server instance can be configured at one time. Each instance presents an additional entry point through which an attacker can guess passwords. When a large number of instances are configured, care must be taken to maintain optimal levels of password security. In these cases, other WebSEAL security settings should be adjusted. For example, increasing the default penalty for consecutive failed attempts greatly extends the time necessary for an attacker to conduct a brute force password attack.

To maintain a CC-evaluated configuration using the WebSEAL security settings specified in this guide, it is recommended that no more than four WebSEAL instances be configured.

For more information on WebSEAL security settings, see the *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide*.

Password policy

To conform to the CC requirements, use the **pdadmin** command to change the default password policy as follows:

```
policy set password-spaces no
```

Cryptographic key management

The evaluation of Tivoli Access Manager also covers the cryptographic key generation process. This means that the security status of the keys generated by the Tivoli Access Manager utilities (**mgrsslcfg**, **bassslcfg**, and **svrsslcfg**) was verified. Note that user-generated certificates (for example, for the WebSEAL server certificate) must have a key length of at least 1024 bits. For more information about WebSEAL certificate management, see the *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide*.

Chapter 3. Security policy for IBM Tivoli Access Manager

The CC configuration of Tivoli Access Manager is based on a security policy that must be respected to achieve and maintain a secure operation.

Base security policy

The systems must be installed and operated in access-controlled facilities that only authorized administrators have access to. The platforms that Tivoli Access Manager server components run on must be secured accordingly, allowing access only to authorized administrators.

The following is a all-inclusive list of security policy statements, that must be fulfilled to operate Tivoli Access Manager in a CC-compliant manner.

- Only users authorized to work with the information on the systems are granted user IDs on the system.
- Administrators and users must use high-quality passwords (as random as possible and not affiliated with the user or the organization).
- Users and administrators must not disclose their passwords to others.
- Passwords that are generated for users of the system by administrators must be transmitted in a secure fashion to the users.

System security policy

In addition to the base security policy that is described in the "Default security policy" in the *Tivoli Access Manager for e-business Version 6.0: Administration Guide*, the systems and networks that are used for operating Tivoli Access Manager need to fulfill additional policy statements as follows:

- The machines on which Tivoli Access Manager is deployed must be dedicated Tivoli Access Manager machines. (Tivoli Access Manager applications must be the only applications running on the underlying operating systems.)

  Note: All operating system services must be switched off, especially networked services that are nonessential for running, managing, and administering Tivoli Access Manager.
- The operating system must provide an accurate system time to the Tivoli Access Manager applications.
- The operating system within the IT environment must provide protection of the configuration files against unauthorized access.
- The Directory Server must provide access control mechanisms to prohibit unauthorized access to directory entries. This access control must also be enforced when importing and exporting data.
- The Directory Server must identify and authenticate users that request access to directory entries.
- LDAP access must be performed using TLS Version 1.
- The LDAP server must perform user identification and authentication in addition to performing access control on the entries it provides.
- To ensure that the security policy enforced by WebSEAL is up to date, the network between the Tivoli Access Manager Policy Server and WebSEAL must be active. If the network goes down, a security administrator might update the

security policy on the Tivoli Access Manager Policy Server, but that updated policy will not be delivered to WebSEAL. If the administrator believes the network is not functioning correctly, the administrator can use network management or routing tools (for example, using the TCP/IP ping command from the WebSEAL server to the Tivoli Access Management Policy Server) or the administrator can check for failed replication of the security policy database in the WebSEAL logs.

- Only those users who have been authorized to access Web resources protected by the TOE may access those resources after they have been successfully authenticated (unless a protected Web resource is defined to be accessible by unauthenticated users, in which case no prior authentication is required).
- Only administrators authorized for access to defined management resources of the TOE may access those resources after they have been successfully authenticated.
- The system must allow to limit the access to, modification of, and destruction of the information in protected Web resources to those authorized users which have a "need to know" for that information.
- The administrators of the system shall be held accountable for their actions within the system.
- Specific administration tasks as well as management operations to defined subsets of the Web resources protected by the TOE may be delegated to administrators that are only allowed to perform the management tasks within their defined area of responsibility and are not able to extend this area themselves.
- Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives.
- Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack, which might compromise IT security objectives.
- Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner which maintains IT security objectives.
- The operating system of the machines running the TOE is assumed to be configured and maintained such that it provides a reliable basis for the operation of the TOE software. The operating system is configured such that no unauthorized access to functions provided by the operating system software (including network daemons) is possible either locally or via any network connection. Any machine used to run all or a part of the TOE software is used solely for this purpose and is not used to run other application software except those required for the management and maintenance of the underlying operating system and hardware.
- Those responsible for the TOE must ensure that the TOE is integrated into the overall system in a way that prohibits direct access to resources to be protected by the TOE in a way that bypass the TOE and its security functions.
- Those responsible for the TOE shall control the user community that can request access to resources protected by the TOE. This includes a configuration where the client systems allowed to submit requests to the TOE are controlled (e. g. a company internal network with a known and controlled user community protected against unauthorized access from external networks).

Additional management and administration issues and mechanisms of the underlying operating systems are outside the scope of this document.

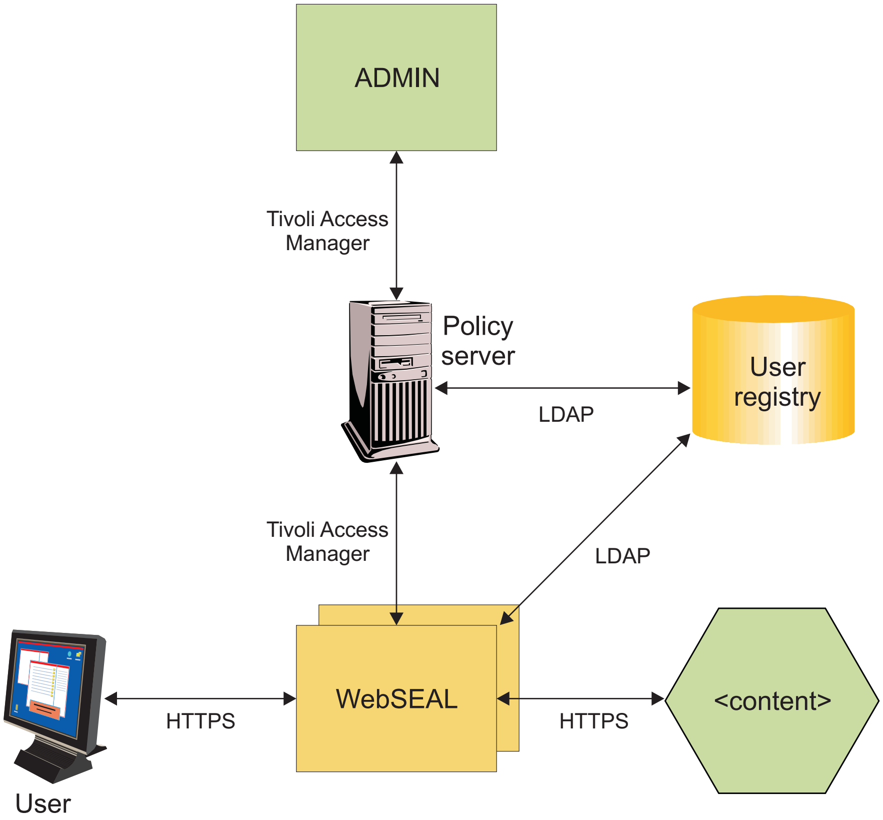
Tivoli Access Manager network policy

The following list describes the communication profile of each component. This communication profile must be enforced by the network environment to operate Tivoli Access Manager in a secure way.

Generally, the networks have to be configured in a way that WebSEAL is the enforcement point for the resource access policy. That means that there is no other way for a user to access the resources protected by Tivoli Access Manager. Management and administration mechanisms of the operating system must be in line with this rule.

- Policy server (pdmgrd)
  - Tivoli Access Manager communication
  - LDAP to the registry
- WebSEAL server (webseald)
  - For external users, HTTPS only
  - HTTPS to back-end resources
  - Tivoli Access Manager communication for authentication, authorization, database replication, management, and auditing
  - LDAP to the registry

The following diagram gives an overview of the network policy:



Note: This policy does not imply any particular network setup. According to best practices, internal and external networking interfaces must be clearly separated, yielding HTTPS access for external users only. Any other network service must not be accessible from external networks.

The implemented network security policy must restrict client access to the HTTPS port to a controlled client community. An example of proper restrictions is a company internal network with a known and controlled user and client community that is protected against unauthorized access from external networks.

Chapter 4. User requirements

Each secure system has areas in which its security is based on an assumption (and therefore trust). The security of Tivoli Access Manager is based on the following assumptions regarding the behavior of external users:

- It has to be ensured that protected resources can not be accessed in a way that bypasses the TOE. All internal and external access attempts to protected resources have to be channeled through the TOE.
- Users have to administer and protect private keys of their client system used for authentication and key exchange with the TOE in a secure way. This includes the secure generation of strong keys as well as the protection of private keys against any kind of unauthorized access and use.
- Users and administrators have to protect their passwords used for authentication to the TOE such that no unauthorized access to them is possible.
- Cryptographic key generation on the client side is performed securely, thus yielding strong cryptographic keys.
- The machines running the TOE software need to be protected against unauthorized physical access and modification. All machines running parts of the TOE software require this protection.
- Any machine used to run all or a part of the TOE software are assumed to be used solely for this purpose and are not used to run other application software except those required for the management and maintenance of the underlying operating system and hardware.
- The operating system of the machines running the TOE are assumed to be configured and maintained by trained and trustworthy personnel such that the operating system provides a reliable basis for the operation of the TOE software. Especially it is assumed that the operating system is configured such that no unauthorized access to functions provided by the operating system software (including network daemons) is possible either locally or via any network connection.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation. They will perform administration activities from a secure environment using terminals and/or workstations they trust via secured connections to the policy server.
- Users are not hostile and trying to deliberately attack the security functions (that is, they are trying to circumvent the system's policy). They also carefully protect their authentication information within their operating environment.
- The directory server used by the TOE provides protection mechanism against unauthorized access to TSF data stored in the directory. This includes the requirement for authentication when accessing user entries and the configuration to use TLS v1 as the preferred protocol to protect the communication links.

Should any of these assumptions no longer be true, the administrator must be aware that access *on the behalf of the user in question* is possible, because any attacker can successfully impersonate that user.

Chapter 5. Evaluated security functions of IBM Tivoli Access Manager

The evaluation of Tivoli Access Manager covered the security functions shown below. Refer to the documentation listed for further information on configuration and management of these functions.

- Audit of security relevant actions:
  - *Tivoli Access Manager for e-business Version 6.0: Auditing Guide*
- Authentication of users and systems:
  - *Tivoli Access Manager for e-business Version 6.0: Administration Guide* (chapters 11 and 12)
  - *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide* (part 3)
  - *Tivoli Access Manager for e-business Version 6.0: Command Reference* (chapter 1)
- Authorization of users and systems:
  - *Tivoli Access Manager for e-business Version 6.0: Administration Guide* (chapter 3)
  - *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide* (part 6)
  - *Tivoli Access Manager for e-business Version 6.0: Command Reference* (chapter 1)
  - *Tivoli Access Manager for e-business Version 6.0: Administration C API Developer's Reference*
- Management of users and systems:
  - *Tivoli Access Manager for e-business Version 6.0: Administration Guide* (chapters 3 and 5–13)
  - *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide* (parts 1 and 2)
  - *Tivoli Access Manager for e-business Version 6.0: Command Reference* (chapter 1)
  - *Tivoli Access Manager for e-business Version 6.0: Administration C API Developer's Reference*
  - *Tivoli Access Manager for e-business Version 6.0: Error Message Reference*
- Secure communication between users and systems:
  - *Tivoli Access Manager for e-business Version 6.0: WebSEAL Administration Guide* (parts 1–7)

Chapter 6. Usage guidelines

This section contains usage guidelines on locking user accounts, specifying SSL ciphers on Windows, and configuring quality of protection using cipher limitations.

Locking user accounts

Administrators should be aware that the chance of a successful password-guessing attack increases when administrators centrally manage user IDs and passwords for multiple WebSEAL instances. Failed password counts and penalty times are local to each WebSEAL instance. Consequently, each additional WebSEAL instance increases the opportunity for potential attacks.

Rather than using a time penalty for user lockouts after the maximum number of consecutive failed login attempts is reached, it might be appropriate to lock the user account completely until an administrator can analyze the event and manually reset the account lock.

Specifying SSL ciphers at a host or network level on Windows

Specification of SSL ciphers at a host or network level does not function correctly on the Microsoft Windows version of WebSEAL 6.0 fixpack 3. The default cipher specification, `[ssl-qop-mgmt-default]`, *does* function correctly unless host or network entries are specified in `[ssl-qop-mgmt-hosts]` or `[ssl-qop-mgmt-networks]`, respectively. This issue only affects customers with `[ssl-qop] ssl-qop-mgmt = yes` and entries under `[ssl-qop-mgmt-hosts]` or `[ssl-qop-mgmt-networks]`.

Configuring SSL quality of protection with AES and FIPS-DES cipher limitations

If an AES cipher (AES-128, AES-256, or both) is specified under the WebSEAL `ssl-qop-mgmt-default` configuration parameter, both FIPS-DES ciphers (FIPS-DES-56 and FIPS-DES-168) will be available in addition to the AES cipher. To specify SSL quality of protection using only a single cipher, do not specify an AES cipher. Instead, specify any of the following: FIPS-DES-56, FIPS-DES-168, DES-56, DES-168.

Glossary

A

access control. In computer security, the process of ensuring that the resources of a computer system can be accessed only by authorized users in authorized ways.

access control list (ACL). In computer security, a list that is associated with an object that identifies all the subjects that can access the object and their access rights. For example, an access control list is a list that is associated with a file that identifies the users who can access the file and identifies the users' access rights to that file.

ACL. See *access control list*.

administration service. An authorization API runtime plug-in that can be used to perform administration requests on a Tivoli Access Manager resource manager application. The administration service will respond to remote requests from the **pdadmin** command to perform tasks, such as listing the objects under a particular node in the protected object tree. Customers may develop these services using the authorization ADK.

AES. Advanced encryption standard. A method for encrypting information.

API. Application programming interface.

authentication. (1) In computer security, verification of the identity of a user or the user's eligibility to access an object. (2) In computer security, verification that a message has not been altered or corrupted. (3) In computer security, a process that is used to verify the user of an information system or of protected resources.

authorization. (1) In computer security, the right granted to a user to communicate with or make use of a computer system. (2) The process of granting a user either complete or restricted access to an object, resource, or function.

authorization rule. See *rule*.

B

BA. See *basic authentication*.

basic authentication. A method of authentication that requires the user to enter a valid user name and password before access to a secure online resource is granted.

blade. A component that provides application-specific services and components.

C

CA. See *certificate authority*.

certificate. In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority.

certificate authority (CA). An organization that issues certificates. The certificate authority authenticates the certificate owner's identity and the services that the owner is authorized to use, issues new certificates, renews existing certificates, and revokes certificates belonging to users who are no longer authorized to use them.

cipher. Encrypted data that is unreadable until it has been converted into plain data (decrypted) with a key.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (2) The machines, devices, and programs that make up a system, subsystem, or network.

connection. (1) In data communication, an association established between functional units for conveying information. (2) In TCP/IP, the path between two protocol applications that provides reliable data stream delivery service. In the Internet, a connection extends from a TCP application on one system to a TCP application on another system. (3) In system communications, a line over which data can be passed between two systems or between a system and a device.

cookie. Information that a server stores on a client machine and accesses during subsequent sessions. Cookies allow servers to remember specific information about clients.

credentials. Detailed information, acquired during authentication, that describes the user, any group associations, and other security-related identity attributes. Credentials can be used to perform a multitude of services, such as authorization, auditing, and delegation.

D

daemon. A program that runs unattended to perform continuous or periodic system wide functions, such as network control. Some daemons are triggered automatically to perform their task; others operate periodically.

DES. Data encryption standard. A method for encrypting information.

domain. (1) A logical grouping of users, systems, and resources that share common services and usually function with a common purpose. (2) That part of a computer network in which the data processing resources are under common control. See also *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames that are separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is as400.rchland.vnet.ibm.com, each of the following is a domain name: as400.rchland.vnet.ibm.com, vnet.ibm.com, ibm.com.

E

encryption. In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

EAL. Evaluation asurance level. A numerical grade (1–7) assigned following the completion of a Common Criteria security evaluation.

entitlement. A data structure that contains externalized security policy information. Entitlements contain policy data or capabilities that are formatted in a way that is understandable to a specific application.

entitlement service. An authorization API runtime plug-in which can be used to return entitlements from an external source for a principal or set of conditions. Entitlements are normally application specific data that will be consumed by the resource manager application in some way or added to the principal's credentials for use further on in the authorization process. Customers may develop these services using the authorization ADK.

F

FIPS. Federal information processing standard.

Fully qualified path. The path from the root through the hierarchical structure to locate a folder, directory, or file.

G

global sign-on (GSO). A flexible single sign-on solution that enables the user to provide alternative user names and passwords to the back-end Web application server. Global sign-on grants users access to the computing resources they are authorized to use — through a single login. Designed for large enterprises consisting of multiple systems and applications within heterogeneous, distributed computing environments, GSO eliminates the need for users to manage multiple user names and passwords.

GSM. Global system for mobile communication.

GSKit. Global Secure ToolKit. A set of programmable interfaces that allow an application to be SSL enabled.

GSO. See *global sign-on*.

H

host. A computer that is connected to a network (such as the Internet or an SNA network) and provides an access point to that network. Also, depending on the environment, the host may provide centralized control of the network. The host can be a client, a server, or both a client and a server simultaneously.

HTTP. Hypertext transfer protocol. In the Internet suite of protocols, the protocol that is used to transfer and display hypertext documents.

HTTPS. Secure hypertext transfer protocol.

I

IEC. International Electrotechnical Commission.

Internet protocol (IP). In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

Internet suite of protocols. A set of protocols developed for use on the Internet and published as Requests for Comments (RFCs) through the Internet Engineering Task Force (IETF).

IP. See *Internet protocol*.

ISO. International Standards Organization.

ITU. International Telecommunication Union.

J

junction. An HTTP or HTTPS connection between a front-end WebSEAL server and a back-end Web application server. WebSEAL uses a junction to provide protective services on behalf of the back-end server.

K

key. In computer security, a sequence of symbols that is used with a cryptographic algorithm for encrypting or decrypting data. See *private key* and *public key*.

L

LDAP. See *Lightweight Directory Access Protocol*.

Lightweight Directory Access Protocol (LDAP). An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). Applications that use LDAP (known as directory-enabled applications) can use the directory as a common data store and for retrieving information about people or services, such as e-mail addresses, public keys, or service-specific configuration parameters. LDAP was originally specified in RFC 1777. LDAP version 3 is specified in RFC 2251, and the IETF continues work on additional standard functions. Some of the IETF-defined standard schemas for LDAP are found in RFC 2256.

Lightweight Third Party Authentication (LTPA). An authentication framework that allows single sign-on across a set of Web servers that fall within an Internet domain.

LTPA. See *lightweight third party authentication*.

M

MD5. Message-Digest algorithm 5. A cryptographic hash function with a 128-bit hash value.

N

network-based authentication. A protected object policy (POP) that controls access to objects based on the internet protocol (IP) address of the user. See also *protected object policy*.

NIST. National Institute of Standards and Technologies.

P

permission. The ability to access a protected object, such as a file or directory. The number and meaning of permissions for an object are defined by the access control list (ACL). See also *access control list*.

policy. A set of rules that are applied to managed resources.

policy server. The Tivoli Access Manager server that maintains the location information about other servers in the secure domain.

polling. The process by which databases are interrogated at regular intervals to determine if data needs to be transmitted.

POP. See *protected object policy*.

portal. An integrated Web site that dynamically produces a customized list of Web resources, such as links, content, or services, available to a specific user, based on the access permissions for the particular user.

private key. In computer security, a key that is known only to its owner. Contrast with *public key.*

protected object. The logical representation of an actual system resource that is used for applying ACLs and POPs and for authorizing user access. See also *protected object policy* and *protected object space*.

protected object policy (POP). A type of security policy that imposes additional conditions on the operation permitted by the ACL policy to access a protected object. It is the responsibility of the resource manager to enforce the POP conditions. See also *access control list*, *protected object*, and *protected object space*.

protected object space. The virtual object representation of actual system resources that is used for applying ACLs and POPs and for authorizing user access. See also *protected object* and *protected object policy*.

public key. In computer security, a key that is made available to everyone. Contrast with *private key*.

Q

quality of protection. The level of data security, determined by a combination of authentication, integrity, and privacy conditions.

R

registry. The data store that contains access and configuration information for users, systems, and software.

replica. A server that contains a copy of the directory or directories of another server. Replicas back up servers in order to enhance performance or response times and to ensure data integrity.

RSA encryption. A system for public-key cryptography used for encryption and authentication. The system's security depends on the difficulty of factoring the product of two large prime numbers.

rule. One or more logical statements that enable the event server to recognize relationships among events (event correlation) and to execute automated responses accordingly.

run time. The time period during which a computer program is executing. A runtime environment is an execution environment.

S

self-registration. The process by which a user can enter required data and become a registered Tivoli Access Manager user, without the involvement of an administrator.

service. Work performed by a server. A service can be a simple request for data to be sent or stored (as with file servers, HTTP servers, e-mail servers, and finger servers), or it can be more complex work such as that of print servers or process servers.

SSL. Secure Sockets Layer protocol. A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

T

TLS. Transport Layer Security protocol. A cryptographic protocol that provides secure communications over the Internet.

TCP. Transmission Control Protocol. TCP/IP is an Internet protocol suite containing the set of communications protocols.

TOE. Target of Evaluation.

trusted root. In the Secure Sockets Layer (SSL), the public key and associated distinguished name of a certificate authority (CA).

U

user. Any person, organization, process, device, program, protocol, or system that uses a service provided by others.

user registry. See *registry*.

W

Web Portal Manager (WPM). A Web-based graphical application used to manage Tivoli Access Manager Base and WebSEAL security policy in a secure domain. An alternative to the **pdadmin** command line interface, this GUI enables remote administrator access and enables administrators to create delegated user domains and assign delegate administrators to these domains.

WebSEAL. A Tivoli Access Manager blade. WebSEAL is a high performance, multi-threaded Web server that applies a security policy to a protected object space. WebSEAL can provide single sign-on solutions and incorporate back-end Web application server resources into its security policy.

WPM. See *Web Portal Manager*.

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 described 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 publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication 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 was exchanged, should contact:

IBM Corporation
2Z4A/101
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.

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.

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

IBM, IBM Logo, AIX, DB2, DB2 Universal Database, MQSeries, SecureWay, Tivoli, Tivoli logo, WebSphere, xSeries, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Lotus and Domino are trademarks of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Printed in USA

SC23-6138-00