Tivoli. IBM Tivoli Access Manager for e-business

IBM

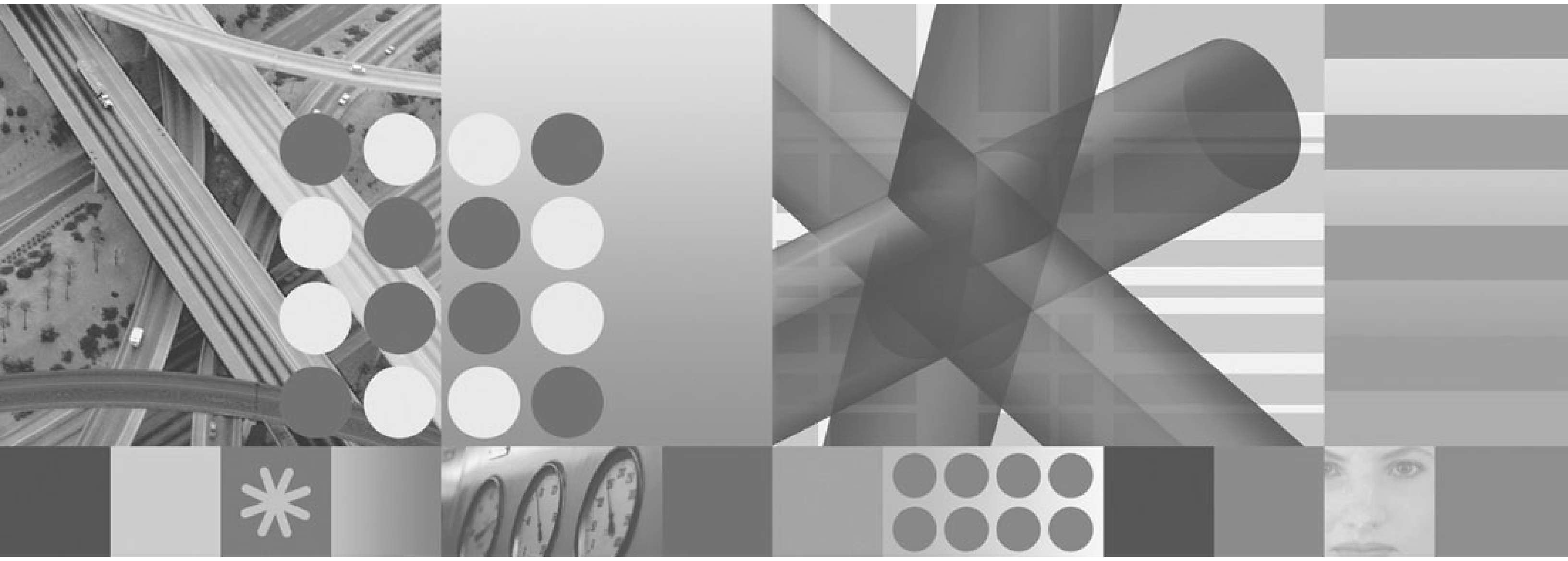
Version 5.1

Common Criteria Guide

SC32-1721-00

Tivoli® IBM Tivoli Access Manager for e-business

Version 5.1



Common Criteria Guide

SC32-1721-00

Note

Before using this information and the product it supports, read the information in "Notices" on page 29.

First Edition (June 2005)

This edition applies to version 5, 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

The *IBM® Tivoli® Access Manager for e-business Common Criteria Guide* provides information about how IBM Tivoli Access Manager, Version 5.1, with fix pack 6 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 securely control user access to protected information and resources. 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 UNIX® 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, “CC-compliant configuration files,” on page 11
- Chapter 4, “Security policy for IBM Tivoli Access Manager,” on page 13
- Chapter 5, “User requirements,” on page 17
- Chapter 6, “Evaluated security functions of IBM Tivoli Access Manager,” on page 19
- Chapter 7, “Documentation updates,” on page 21

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:

- *IBM Tivoli Access Manager for e-business: Web Security Installation Guide*, SC32-1361-00

  Provides installation, configuration, and removal instructions for the Tivoli Access Manager base software and the Web Security components.
- *IBM Tivoli Access Manager: Base Administration Guide*, SC32-1360-00

  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.
- *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*, SC32-1359-00

  Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.
- *IBM Tivoli Access Manager for e-business: Command Reference*, SC32-1354-00

  Provides information about the command line utilities and scripts provided with Tivoli Access Manager.
- *IBM Tivoli Access Manager: Administration C API Developer Reference*, SC32-1357-00

  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.
- *IBM Tivoli Access Manager for e-business: Error Message Reference*, SC32-1353-00

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

For instructions on locating a specific document in a specific version of a product, see “Accessing publications online” on page vii.

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 5.2, 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 5.1.

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, Advanced Single Server Edition 5.0, 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 15408) for the assurance evaluation of IT products. Tivoli Access Manager, Version 5.1 with fix pack 6 installed, 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 means only 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 Tivoli Access Manager, Version 5.1, CC evaluated system includes the following Tivoli Access Manager systems:

Policy server (pdmgrd) with the following components installed:

- Tivoli Access Manager runtime
- Tivoli Access Manager policy server
- IBM Tivoli Directory Server client
- IBM Global Security Kit (GSKit) 7.0.3.3
- Fix pack 6

WebSEAL server (webseald) with the following components installed:

- Tivoli Access Manager runtime
- Tivoli Access Manager WebSEAL server
- IBM Tivoli Directory Server client
- IBM Global Security Kit (GSKit) 7.0.3.3
- Fix pack 6

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® 5.2
- Sun Solaris 8
- Hewlett-Packard UNIX (HP-UX) 11i
- Microsoft® Windows 2003 Enterprise Server
- SUSE LINUX Enterprise Server 8 on IBM xSeries®
- Red Hat Enterprise Linux® 3 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 *IBM Tivoli Access Manager for e-business: Web Security Installation Guide*. Additional installation and configuration requirements are as follows:

- Software *must* be downloaded directly using the Download Director applet. This requirement applies to all Tivoli Access Manager downloads including the base and Tivoli Access Manager fix packs. Using Download Director reduces the possibilities of tampering while transferring the TOE over untrusted networks.
- Ensure that you are using "clean" systems that do not have previous versions of Tivoli Access Manager installed. You are not allowed to upgrade from an older release to the current fix pack and then use this upgraded system as a basis for an evaluated configuration.
- The policy server (pdmgrd) and WebSEAL (webseald) systems must be installed on separate machines.
- Tivoli Access Manager components were evaluated using the same operating system. Mixed configurations were not evaluated, for example, both the policy server and WebSEAL were installed on AIX machines.
- It is recommended that you use installation wizards, if supported for your particular platform. If installation wizards are not supported, ensure that you follow native installation instructions and refer to the fix pack readme file for any last-minute updates.
- Web Portal Manager (WPM) is not supported in the evaluated configuration. Only the **pdadmin** command line interface and the C API are supported.
- No Application Development Kit is installed in the evaluated configuration.
- Only LDAP is supported for access to the directory server. Active Directory or other protocols are not supported.
- LDAP replicas are not supported.
- Hardware encryption devices are not supported.
- Only English language support was evaluated.
- All WebSEAL systems are configured to operate independently from each other and are connected only to the central policy server. Therefore, load balancing and failover configurations of WebSEAL systems are not supported in the evaluated configuration.
- Futhermore, self-registration, single sign-on mechanisms, the use of multi-domain (more than one domain), and the use of authorization rules are not supported in the evaluated configuration.
- Important documentation updates have been included in Chapter 7, "Documentation updates," on page 21. Refer to these updates for additional configuration changes.
- Use a **md5sum** program to verify the integrity of Tivoli Access Manager documentation and GSKit 7.0.3.3.

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
   ```
3. Compare your output from the command with the following sums. The two sums should match to ensure download integrity.

   Base Installation Guide
   586b855d5eee0c12fa95e6736b05d286 *am51_install.pdf

   Web Security Installation Guide
   bff44712049fe95a60ec936dca678c3b *am51_webinstall.pdf

   Global Security Kit Secure Sockets Layer Introduction and iKeyman User's Guide 1f1dd9fafda20c39e2454e550ebc1daf *ss7aumst.pdf

   Base Administration Guide
   695debdf5dc73a086315be8881983a27 *am51_admin.pdf

   WebSEAL Administrator's Guide
   a739555e9cca5d5c307834b4136c3ad5 *am51_webseal_guide.pdf

   Administration C API Developer's Reference
   f5466b2df7d2de89a44d15710378ca16 *am51_adminC_devref.pdf

   Command Reference
   78d69dadf355be4eadc6feffeb6f0161 *am51_cmdref.pdf

   Error Message Reference
   9665e7bb0b8b202da6ffd53f4fceea73 *am51_error_ref.pdf

   Problem Determination Guide
   0452f583270b2651c83403fffc260b76 *am51_pdg.pdf

Verify the integrity of GSKit 7.0.3.3

In the evaluated configuration, the integrity of the GSKit 7.0.3.3 binaries that have been downloaded from IBM Service must be ensured. Verifying the integrity of GSKit can be accomplished by running the **md5sum** command against the downloaded binaries and comparing the output to the sums that are documented here.

Typically, you can verify the binaries as follows:

1. Ensure that the platform that you have downloaded the GSKit package to has an **md5sum** program available. It does not need to be the same architecture as the GSKit packages that you are checking.
2. To generate the MD5 sum for the package that you received from IBM Service, run:

   ```
   md5sum GSKit_install_file
   ```
3. Compare your output from the command with the following sums. The two sums should match to ensure binary integrity.

AIX - 32-bit
70f973cc682965c5baba0387fd15b644 *gskta.rte

AIX - 64-bit
ee1a4327ccc4e6ab5c0b1867d131000c *gsksa.rte

HP-UX
b8fdf578b571fba452d4ebe3fc6eeac8 *gsk7bas.tar.Z

Linux on xSeries
c796ed3941e06c366edc79355e9cf518 *gsk7bas-7.0-3.3.i386.rpm

Solaris
7923cb842fae07a143cea17328c9e439 *gsk7bas.tar.Z

Windows
c769c73b8646c70dd92c696bb8fd03a9 *gsk7bas.exe

Installing IBM Tivoli Access Manager

To obtain a CC-compliant installation of Tivoli Access Manager, use the *IBM Tivoli Access Manager for e-business: Web Security Installation Guide*. For CC-compliant installation the WebSEAL component, use Chapter 18, “Setting up a WebSEAL server,” in the *IBM Tivoli Access Manager for e-business: Web Security Installation Guide*.

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

Attention: The steps described are specified as a *delta* to the installation default configuration of the Tivoli Access Manager components. If *any other changes* to the default configuration are made, the system *no longer maintains the evaluated configuration*.

Determining version numbers of Tivoli Access Manager components 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, refer to the AIX documentation.

Relevant packages

Relevant packages include:

- 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     7.0.3.3  COMMITTED  AIX Certificate and SSL Base
                                  Runtime ACME Toolkit
PD.RTE        5.1.0.6  COMMITTED  Access Manager Runtime
PD.Mgr        5.1.0.6  COMMITTED  Access Manager Policy Server
```

```
PDWeb.RTE     5.1.0.6  COMMITTED  Access Manager Web Security
                                  Runtime Environment
PDWeb.Web     5.1.0.6  COMMITTED  Access Manager WebSEAL Server
```

Securing WebSEAL

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

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

It is recommended, but not required, that WebSEAL use the standard HTTPS port as follows:

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

The evaluated configuration does not include SSL, Version 2; only SSL, Version 3, and TLS, Version 1, are supported:

```
[ssl]
disable-ssl-v2 = yes
disable-ssl-v3 = no
disable-tls-v1 = no
```

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

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

Note: Define either the `[ba]` stanza or the `[forms]` stanza to use basic authentication or forms authentication, respectively, over HTTPS.

Supported cipher suites

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

- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_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 = RC4-128
default = DES-168
```

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 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 *IBM Tivoli Access Manager: Base Administration Guide*.

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

```
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 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 *IBM Tivoli Access Manager: Base 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 more than one domain is not supported by the common criteria evaluated configuration of Tivoli Access Manager. To ensure that more than one domain is not used, execute the following command using the policy server **pdadmin** utility:

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

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

Disabling the use of authorization rules

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

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

Different from the 'multi-domain' disable, authorization rules have no directly attached ACL at `/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
pdadmin sec_master> acl mod default-rule set desc "Default Domain Authzrule"
pdadmin sec_master> acl mod default-rule set group iv-admin TcdbvaBRN
pdadmin sec_master> acl mod default-rule set group ivmgrd-servers v
pdadmin sec_master> acl mod default-rule set user sec_master TcdbsvaBRl
pdadmin sec_master> acl attach /Management/Rule default-rule
```

The following test demonstrates that the use of authorization rules is no longer an option:

```
pdadmin sec_master> authzrule create rule1 "dummy rule" -desc kfjdklfjdkslfjd

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

pdadmin sec_master>
```

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 = enable
```

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 *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide* and the *IBM Tivoli Access Manager: Base Administration Guide*.

Other WebSEAL functions

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 setting 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 that is necessary for an attacker to conduct a brute force password attack.

To maintain a CC configuration when WebSEAL security settings are not modified from the values specified in this appendix, it is recommended to not add more than four WebSEAL instances.

For more information on WebSEAL security settings, see the *IBM Tivoli Access Manager for e-business: 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. The security status of the keys, that are generated by the Tivoli Access Manager utilities (**mgrsslcfg**, **bassslcfg**, and **svrsslcfg**), were verified. Note that user-generated certificates (for example, for the WebSEAL server certificate) must have at least a key length of 1024 bits. For more information about WebSEAL certificate management, see the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*.

Chapter 3. 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 *IBM Tivoli Access Manager: Base Administration Guide*. For the `webseald-default.conf` file, consult the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*.

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

Chapter 4. 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.

Following is a non-exclusive list of security policy statements, that must be fulfilled to operate Tivoli Access Manager in a way compatible with the CC.

- Only users who are 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.
- Administrators must be trustworthy and diligent and work according to the guidance that is provided by the system documentation.
- Passwords that are generated for users of the system by administrators must be transmitted in a secure fashion to the users.
- An administrator who is using a remote terminal or remote workstation to connect to the policy server for administration needs to ensure that the remote terminal or workstation is in a secured environment and is managed securely. Management is performed by setting up a secured connection to communicate with the operating system on the policy server. There, the administrator calls the **pdadmin** command line interface and authenticates himself.

System security policy

In addition to the base security policy that is described in the “Base security” policy in the *IBM Tivoli Access Manager: Base 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 non-essential for running, managing, and administering Tivoli Access Manager.
- The operating system must be configured by trained and trustworthy personnel.
- The operating system must provide an exact time to the Tivoli Access Manager applications.
- Tivoli Access Manager configuration files and log/audit files must be protected using operating system access control mechanisms.
- LDAP access must be performed using SSL, Version 3, or 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 that is 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 that 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 Manager policy server) or the administrator can check for failed replication of the security policy database in the WebSEAL logs.

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

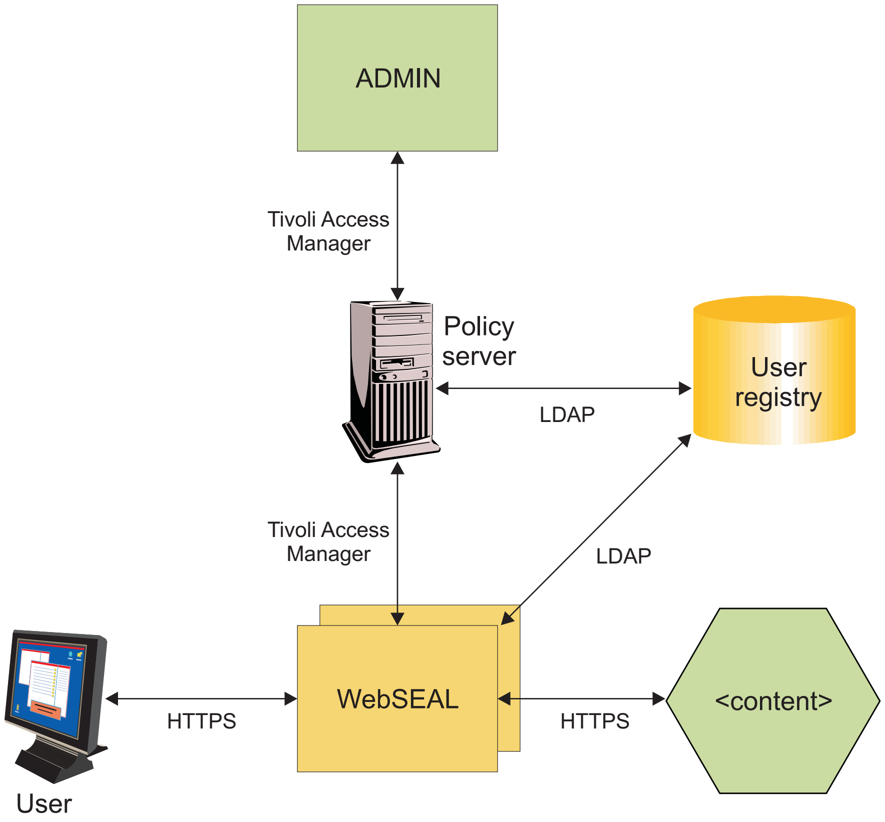
Tivoli Access Manager network policy

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. This configuration means that there is no other way for a user to access resources that are 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 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 would be a company internal network with a known and controlled user and client community that is protected against unauthorized access from external networks.

Chapter 5. 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:

- Cryptographic key generation on the client side is performed securely, thereby yielding strong cryptographic keys.
- The user's private keys that are used for authentication and key exchange with Tivoli Access Manager are stored securely and are protected against unauthorized use and access.
- Users are not hostile and are not trying to deliberately attack the security functions (that is, they are not trying to circumvent the system's policy). They also carefully protect their authentication information within their operating environment.

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 6. 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:
  - Chapter 17 through chapter 20 of the *IBM Tivoli Access Manager: Base Administration Guide*
- Authentication of users and systems:
  - Chapter 11 and chapter 12 of the *IBM Tivoli Access Manager: Base Administration Guide*
  - Chapter 6 of the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*
  - Chapter 1 of the *IBM Tivoli Access Manager for e-business: Command Reference*
- Authorization of users and systems:
  - Chapter 3 of the *IBM Tivoli Access Manager: Base Administration Guide*
  - Chapter 5 of the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*
  - Chapter 1 of the *IBM Tivoli Access Manager for e-business: Command Reference*
  - *IBM Tivoli Access Manager: Administration C API Developer Reference*
- Management of users and systems:
  - Chapter 3 and chapter 5 through chapter 13 of the *IBM Tivoli Access Manager: Base Administration Guide*
  - Chapter 2 and chapter 3 of the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*
  - Chapter 1 of the *IBM Tivoli Access Manager for e-business: Command Reference*
  - *IBM Tivoli Access Manager: Administration C API Developer Reference*
  - *IBM Tivoli Access Manager for e-business: Error Message Reference*
- Secure communication between users and systems:
  - Chapter 2 through chapter 8 of the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide*

Chapter 7. Documentation updates

The following documentation updates apply to the published Tivoli Access Manager, Version 5.1 documents.

Base Administration Guide

Update 1

In Appendix A of the *IBM Tivoli Access Manager: Base Administration Guide*, section [ldap] stanza for ldap.conf, under LdapSSLKeyFile, it states:

> The file name and location value represents an alphanumeric, case-insensitive string

This statement is incorrect. Case-insensitive is only for Windows systems. On UNIX systems, the file is case-sensitive. The following information should be added to the documented statement:

> For Linux and UNIX operating systems, path and file names are case-sensitive.

Update 2

In Appendix A of the *IBM Tivoli Access Manager: Base Administration Guide*, the difference between specifying the LdapSSL parameter in the ldap.conf file rather than specifying the ssl-enabled parameter in ivmgrd.conf in the [ldap] stanza is unclear and requires some clarification.

Both the ssl-enable and LdapSSL are used to enable SSL, but they are each defined in different configuration files for different servers. The ssl-enable entry is defined in the [ldap] stanza of the configuration files for the policy server (ivmgrd.conf), policy proxy server (pdmgrproxyd.conf), and authorization server (ivacld.conf) and enables those servers to communicate with the LDAP server using SSL. The LdapSSL entry is defined in the [ldap] stanza of the configuration file for the LDAP server (ldap.conf) and enables the LDAP server to use SSL.

The changes to the documentation are as follows:

- The ssl-enable entry indicates whether the Tivoli Access Manager server uses SSL to communicate with the LDAP server. If ssl-enable = yes, the LdapSSL entry in the ldap.conf file must be set to useSSL.
- The LdapSSL entry indicates whether SSL is enabled on the LDAP server. If the LDAP server is not SSL enabled, any Tivoli Access Manager server that is SSL enabled cannot communicate with the LDAP server.

Update 3

In Appendix A of the *IBM Tivoli Access Manager: Base Administration Guide*, the [ldap] stanza does not include the ssl-keyfile-pwd parameter, but the the *IBM Tivoli Access Manager for e-business: WebSEAL Administration Guide* includes this information.

Starting with Tivoli Access Manager, Version 5.1, the ssl-keyfile-pwd entry was deprecated (along with the GsoSuffix entry). Although deprecated, the configuration file might contain this entry.

WebSEAL Administration Guide

Update 1

In Chapter 5 and in Appendix A of the *IBM Tivoli Access Manager for e-business: Web Security Installation Guide*, the `[authentication-levels]` stanza of the WebSEAL configuration file incorrectly lists values for the `level` entry. The following table lists the available settings.

Table 1. Setting for the `level` entry in the `[authentication-levels]` stanza

Authentication method	Configuration file entry
None	`level = unauthenticated`
Basic authentication	`level = password`
Forms authentication	`level = password`
Token authentication	`level = token`
Certificate authentication	`level = ssl`

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.

access permission. The access privilege that applies to the entire object.

action. An access control list (ACL) permission attribute. See also *access control list*.

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.

attribute list. A linked list that contains extended information that is used to make authorization decisions. Attribute lists consist of a set of *name = value* pairs.

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. See also *multi-factor authentication*, *network-based authentication*, and *step-up authentication*.

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*.

authorization service plug-in. A dynamically loadable library (DLL or shared library) that can be loaded by the Tivoli Access Manager authorization API runtime client at initialization time in order to perform operations that extend a service interface within the Authorization API. The service interfaces that are currently available include Administration, External Authorization, Credentials modification, Entitlements and PAC manipulation interfaces. Customers may develop these services using the authorization ADK.

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.

bind. To relate an identifier to another object in a program; for example, to relate an identifier to a value, an address or another identifier, or to associate formal parameters and actual parameters.

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

business entitlement. The supplemental attribute of a user credential that describes the fine-grained conditions that can be used in the authorization of requests for resources.

C

CA. See *certificate authority*.

CDAS. See *Cross Domain Authentication Service*.

CDMF. See *Cross Domain Mapping Framework*.

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.

CGI. See *common gateway interface*.

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

common gateway interface (CGI). An Internet standard for defining scripts that pass information from a Web server to an application program, through an HTTP request, and vice versa. A CGI script is a CGI program that is written in a scripting language, such as Perl.

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.

container object. A structural designation that organizes the object space into distinct functional regions.

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.

credentials modification service. An authorization API runtime plug-in which can be used to modify a Tivoli Access Manager credential. Credentials modification services developed externally by customers are limited to performing operation to add and remove from the credentials attribute list and only to those attributes that are considered modifiable.

cross domain authentication service (CDAS). A WebSEAL service that provides a shared library mechanism that allows you to substitute the default WebSEAL authentication mechanisms with a custom process that returns a Tivoli Access Manager identity to WebSEAL. See also *WebSEAL*.

cross domain mapping framework (CDMF). A programming interface that allows a developer to customize the mapping of user identities and the handling of user attributes when WebSEAL e-Community SSO function are used.

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.

directory schema. The valid attribute types and object classes that can appear in a directory. The attribute types and object classes define the syntax of the attribute values, which attributes must be present, and which attributes may be present for the directory.

distinguished name (DN). The name that uniquely identifies an entry in a directory. A distinguished name is made up of *attribute:value* pairs, separated by commas.

digital signature. In e-commerce, data that is appended to, or is a cryptographic transformation of, a data unit and that enables the recipient of the data unit to verify the source and integrity of the unit and to recognize potential forgery.

DN. See *distinguished name*.

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

EAS. See *External Authorization Service*.

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.

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.

external authorization service. An authorization API runtime plug-in that can be used to make application or environment specific authorization decisions as part of the Tivoli Access Manager authorization decision chain. Customers may develop these services using the authorization ADK.

F

file transfer protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses Transmission Control Protocol (TCP) and Telnet services to transfer bulk-data files between machines or hosts.

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. See also *single sign-on*.

GSM. Global system for mobile communication.

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. See *Hypertext Transfer Protocol*.

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

I

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).

interprocess communication (IPC). (1) The process by which programs communicate data to each other and synchronize their activities. Semaphores, signals, and internal message queues are common methods of interprocess communication. (2) A mechanism of an operating system that allows processes to communicate with each other within the same computer or over a network.

IP. See *Internet protocol*.

IPC. See *interprocess communication*.

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*.

key database file. See *key ring*.

key file. See *key ring*.

key pair. In computer security, a public key and a private key. When the key pair is used for encryption, the sender uses the public key to encrypt the message, and the recipient uses the private key to decrypt the message. When the key pair is used for signing, the signer uses the private key to encrypt a representation of the message, and the recipient uses the public key to decrypt the representation of the message for signature verification.

key ring. In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

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

management domain. The default domain in which Tivoli Access Manager enforces security policies for authentication, authorization, and access control. This domain is created when the policy server is configured. See also *domain*.

management server. Obsolete. See *policy server*.

metadata. Data that describes the characteristics of stored data.

migration. The installation of a new version or release of a program to replace an earlier version or release.

multi-factor authentication. A protected object policy (POP) that forces a user to authenticate using two or more levels of authentication. For example, the access control on a protected resource can require that the users authenticate with both user name/password and user name/token passcode. See also *protected object policy*.

multiplexing proxy agent (MPA). A gateway that accommodates multiple client access. These gateways are sometimes known as Wireless Access Protocol (WAP) gateways when clients access a secure domain using a WAP. Gateways establish a single authenticated channel to the originating server and tunnel all client requests and responses through this channel.

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

PAC. See *privilege attribute certificate*.

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.

privilege attribute certificate. A digital document that contains a principal's authentication and authorization attributes and a principal's capabilities.

privilege attribute certificate service. An authorization API runtime client plug-in which translates a PAC of a predetermined format in to a Tivoli Access Manager credential, and vice-versa. These services could also be used to package or marshall a Tivoli Access Manager credential for transmission to other members of the secure domain. Customers may develop these services using the authorization ADK. See also *privilege attribute certificate*.

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*.

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

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.

resource object. The representation of an actual network resource, such as a service, file, and program.

response file. A file that contains a set of predefined answers to questions asked by a program and that is used instead of entering those values one at a time.

role activation. The process of applying the access permissions to a role.

role assignment. The process of assigning a role to a user, such that the user has the appropriate access permissions for the object defined for that role.

routing file. An ASCII file that contains commands that control the configuration of messages.

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

scalability. The ability of a network system to respond to increasing numbers of users who access resources.

schema. The set of statements, expressed in a data definition language, that completely describe the structure of a database. In a relational database, the schema defines the tables, the fields in each table, and the relationships between fields and tables.

Secure Sockets Layer (SSL). 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.

security management. The management discipline that addresses an organization's ability to control access to applications and data that are critical to its success.

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.

silent installation. An installation that does not send messages to the console but instead stores messages and errors in log files. Also, a silent installation can use response files for data input. See also *response file*.

single sign-on (SSO). The ability of a user to logon once and access multiple applications without having to logon to each application separately. See also *global sign-on*.

SSL. See *Secure Sockets Layer*.

SSO. See *single Signon*.

step-up authentication. A protected object policy (POP) that relies on a preconfigured hierarchy of authentication levels and enforces a specific level of authentication according to the policy set on a resource. The step-up authentication POP does not force the user to authenticate using multiple levels of authentication to access any given resource but requires the user to authenticate at a level at least as high as that required by the policy protecting a resource.

suffix. A distinguished name that identifies the top entry in a locally held directory hierarchy. Because of the relative naming scheme used in Lightweight Directory Access Protocol (LDAP), this suffix applies to every other entry within that directory hierarchy. A directory server can have multiple suffixes, each identifying a locally held directory hierarchy.

T

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (2) In local area networks (LANs), a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

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

U

uniform resource identifier (URI). The character string used to identify content on the Internet, including the name of the resource (a directory and file name), the location of the resource (the computer where the directory and file name exist), and how the resource can be accessed (the protocol, such as HTTP). An example of a URI is a uniform resource locator, or URL.

uniform resource locator (URL). A sequence of characters that represent information resources on a computer or in a network such as the Internet. This sequence of characters includes the abbreviated name of the protocol used to access the information resource and the information used by the protocol to locate the information resource. For example, in the context of the Internet, these are abbreviated names of some protocols used to access various information resources: http, ftp, gopher, telnet, and news.

URI. See *uniform resource identifier*.

URL. See *uniform resource locator*.

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

user registry. See *registry*.

V

virtual hosting. The capability of a Web server that allows it to appear as more than one host to the Internet.

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

SC32-1721-00