

Access Manager
Versions 6.0, 6.1, and 6.1.1

*Apache Tomcat
Integration Guide*



Access Manager
Versions 6.0, 6.1, and 6.1.1

*Apache Tomcat
Integration Guide*



Note

Before using this information and the product it supports, read the information in Appendix B, “Notices,” on page 27

This edition applies to Version 1.0 Release ii of the Tivoli Access Manager integration with Apache Tomcat, and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2008, 2011.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	v
Who should read this book	v
Publications	v
Base Information	v
WebSEAL Information	v
Accessing Publications Online	vi
Contacting Software Support.	vi
Tivoli technical training	vi
Conventions Used in this Book.	vii
 Chapter 1. Introducing the Integration	 1
Introduction	1
Integration Product Versions and Supported Platforms	3
Integration Package Contents	3
Integration Process Flowchart.	4
Integration Checklist.	5
 Chapter 2. Integration Process	 7
Before You Start	7
Configuring Tivoli Access Manager WebSEAL	8
Creating a WebSEAL Junction	8
Virtual host Junction.	9
Transparent Path Junction	9
Standard WebSEAL Junction.	10
Configuring AMTomcatValve	10
Encoding the secretPassword	12
Configuring Apache Tomcat	12
Enabling AMTomcatValve in Tomcat	12
Enabling Application Security	13
Testing the Integration.	14
Removing the Integration.	14
Troubleshooting	15
Debug Trace in AMTomcatValve	15
DisplayHeaders JavaServer Page	15
Apache Tomcat Log Files	16
Known Exception Messages	16
 Chapter 3. Additional Considerations.	 19
ACL Considerations	19
WebSEAL Options	19
Junction Mapping Table Considerations	19
 Appendix A. Support information	 21
Searching knowledge bases	21
Searching information centers	21
Searching the Internet	21
Obtaining fixes	21
Registering with IBM Software Support	22
Receiving weekly software updates	22
Contacting IBM Software Support	23
Determining the business impact	23
Describing problems and gathering information	24
Submitting problems	24

Appendix B. Notices	27
Trademarks	29

Preface

This guide tells you how to configure and manage your IBM® Tivoli® Access Manager installation to work with Apache Tomcat.

This document assumes that both Tivoli Access Manager and Apache Tomcat are installed, configured and running on your network. This guide does not provide details on the installation and administration of these products, except where necessary to achieve integration.

Who should read this book

This guide is for those responsible for the installation, deployment and administration of IBM Tivoli Access Manager and Apache Tomcat.

Readers should be familiar with the following:

- PC and UNIX operating systems.
- Security management
- Internet protocols, including HTTP, HTTPS, TCP/IP and SSL
- Lightweight Directory Access Protocol (LDAP) and directory services
- A supported user registry
- Authentication and authorization

The reader should also be familiar with the administration of Tivoli Access Manager, Tivoli Access Manager WebSEAL and Apache Tomcat.

Publications

These publications complement the information contained in this publication:

Base Information

- *IBM Tivoli Access Manager Base Installation Guide*
Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Tivoli Access Manager Base Administrator's Guide*
Describes the concepts and procedures for using Access Manager services. Provides instructions for performing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Tivoli Access Manager WebSEAL Installation Guide*
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Tivoli Access Manager WebSEAL Administrator's Guide*
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 WebSEAL Developer's Reference*

Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli Software Library: <http://www.ibm.com/software/tivoli/library>

To locate product publications in the library, click the **Product manuals** link on the left side of the Library page. Then, locate and click the name of the product on the Tivoli Software Information Center page.

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**).

Contacting Software Support

Contact IBM Software Support by using the methods described in the *IBM Software Support Guide* at the following Web site:

<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

For more information, see Appendix A, "Support information," on page 21.

Tivoli technical training

For Tivoli technical training information, refer to the IBM Tivoli Education Web site: <http://www.ibm.com/software/tivoli/education>.

Conventions Used in this Book

The following typeface conventions are used in this book:

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.

Throughout this document, the Apache Tomcat installation directory is represented as *CATALINA_HOME*. Make substitutions based on the environment in which this integration is being configured.

The default installation directories for Tomcat 6 are:

UNIX and Linux

`/var/lib/tomcat-6/`

Windows

`C:\Program Files\Apache Software Foundation\Tomcat 6.0\`

For Apache Tomcat version 5.5, the default *CATALINA_HOME* installation directories are:

UNIX and Linux

`/var/lib/tomcat-5.5/`

Windows

`C:\Program Files\Apache Software Foundation\Tomcat 5.5\`

Note: The Apache Tomcat 5.5.26 configuration is exactly the same as the Apache Tomcat 6.0.14, however the *CATALINA_HOME/lib* directory is instead *CATALINA_HOME/server/lib*.

Chapter 1. Introducing the Integration

This chapter contains the following sections:

- “Introduction”
- “Integration Product Versions and Supported Platforms” on page 3
- “Integration Package Contents” on page 3
- “Integration Process Flowchart” on page 4
- “Integration Checklist” on page 5

Introduction

Apache Tomcat is an implementation of the Java Servlet and JavaServer Pages technologies. This integration guide describes a generic approach for integration between IBM Tivoli Access Manager (Tivoli Access Manager) and Apache Tomcat (Tomcat) to achieve single sign-on (SSO) for sites and applications hosted or deployed on Tomcat.

IBM Tivoli provides a WebSEAL solution to achieve SSO between Tivoli Access Manager and Apache Tomcat. The integration consists of:

- a light weight identity assertion module, and
- documentation which describes the steps required to configure Single Sign On from an IBM Tivoli Access Manager WebSEAL to Tomcat.

Multiple configuration options are available as part of the integration.

Note: This solution is a generic approach providing Single Sign On to sites and applications hosted or deployed on Tomcat. This solution does not cater for individual or specific Independent Software Vendor (ISV) solutions or custom applications. Such applications cannot be supported due to the complex nature of filtering and identity and role requirements.

This integration passes the Tivoli Access Manager WebSEAL's authenticated user identity to the Apache Tomcat server, where the identity is established within Apache Tomcat using a custom Valve. A Valve is a filter that is inserted into Tomcat's request processing pipeline. The custom Valve supplied with this integration creates a Principal for the user and adds roles according to the Valve's configuration.

The integration uses WebSEAL as a reverse-proxy. A WebSEAL junction is created and connected to Web application(s) deployed on Tomcat. Users access and authenticate to WebSEAL, and their authenticated user ID is passed through the junction to Tomcat. A Valve is configured on Tomcat to read the user ID and create a Principal, which is used by the Web application (running on Tomcat) in order to achieve SSO.

The Valve does not verify that the user ID in the HTTP header exists in the Tomcat user registry. The Valve's configuration options contain methods for ensuring that only requests authenticated by WebSEAL are processed by the Valve. For more information, see “Configuring AMTomcatValve” on page 10 and “Configuring Tivoli Access Manager WebSEAL” on page 8.

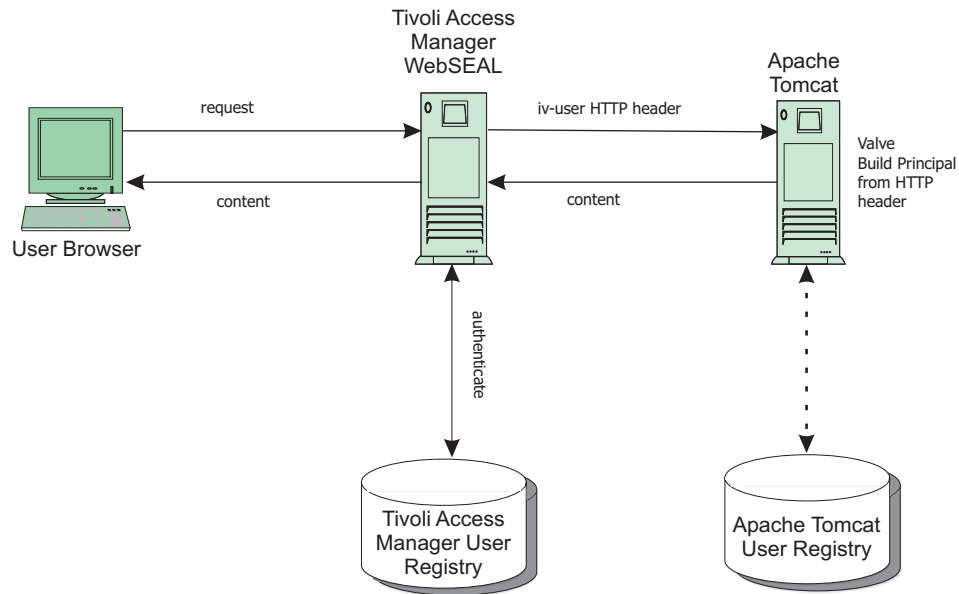


Figure 1. Tivoli Access Manager integration with Apache Tomcat process flow

The process flow is as follows:

1. A browser request to a Tomcat Web Site or Web Application is submitted through WebSEAL.
2. WebSEAL intercepts the request, authenticates and authorizes the user as required.
3. WebSEAL forwards the request to Tomcat along with the authenticated user ID in a HTTP header, called `iv-user`, as well as other optional configuration items.
4. A Valve intercepts the request and optionally establishes trust with the WebSEAL server.
5. The Valve reads the `iv-user` HTTP header and generates a Principal for the user ID contained in the header.
6. The Valve adds roles to the Principal based on the configuration, or assigns a default role.
7. The Valve passes control to the next Valve in the configuration.
8. The target application is executed using the Principal generated by the Valve.
9. Tomcat returns the requested content, based on user ID in the Principal and their roles.
10. The content is returned to the browser. WebSEAL performs filtering as appropriate for the junction method.

The **AMTomcatValve** extends **org.apache.catalina.valves.ValveBase** and implements **org.apache.catalina.Authenticator** and **org.apache.catalina.Lifecycle**. The Valve functions as follows:

1. When Tomcat is started, the Valve's **start** method is called, and configuration is read and set in the Valve.
2. Tomcat accepts a request and control is passed to the Valve, calling its **invoke** method.
3. The configuration parameters determine debug logging and establish trust via a Basic Authentication Header and Trusted Server Name.

4. The configured user identity header is retrieved, the authenticated user ID is extracted, and an **org.apache.catalina.realm.GenericPrincipal** is created.
5. The configured role assignments are compiled and assigned to the user Principal.
6. Control is passed to the next Valve in the chain.
7. Tomcat handles the original request, using the Principal generated by the Valve.
8. Tomcat returns the requested content for the Principal.

Integration Product Versions and Supported Platforms

The integration information provided in this guide has been tested on, and is supported for, the following product versions:

- Apache Tomcat versions 5.5.26, 6.0.14, 6.0.30, and 6.0.32
- One of the following combinations:
 - IBM Tivoli Access Manager Base Version 6.0 and IBM Tivoli Access Manager WebSEAL 6.0
 - IBM Tivoli Access Manager Base Version 6.1 and IBM Tivoli Access Manager WebSEAL 6.1
 - IBM Tivoli Access Manager Base Version 6.1.1 and IBM Tivoli Access Manager WebSEAL 6.1.1

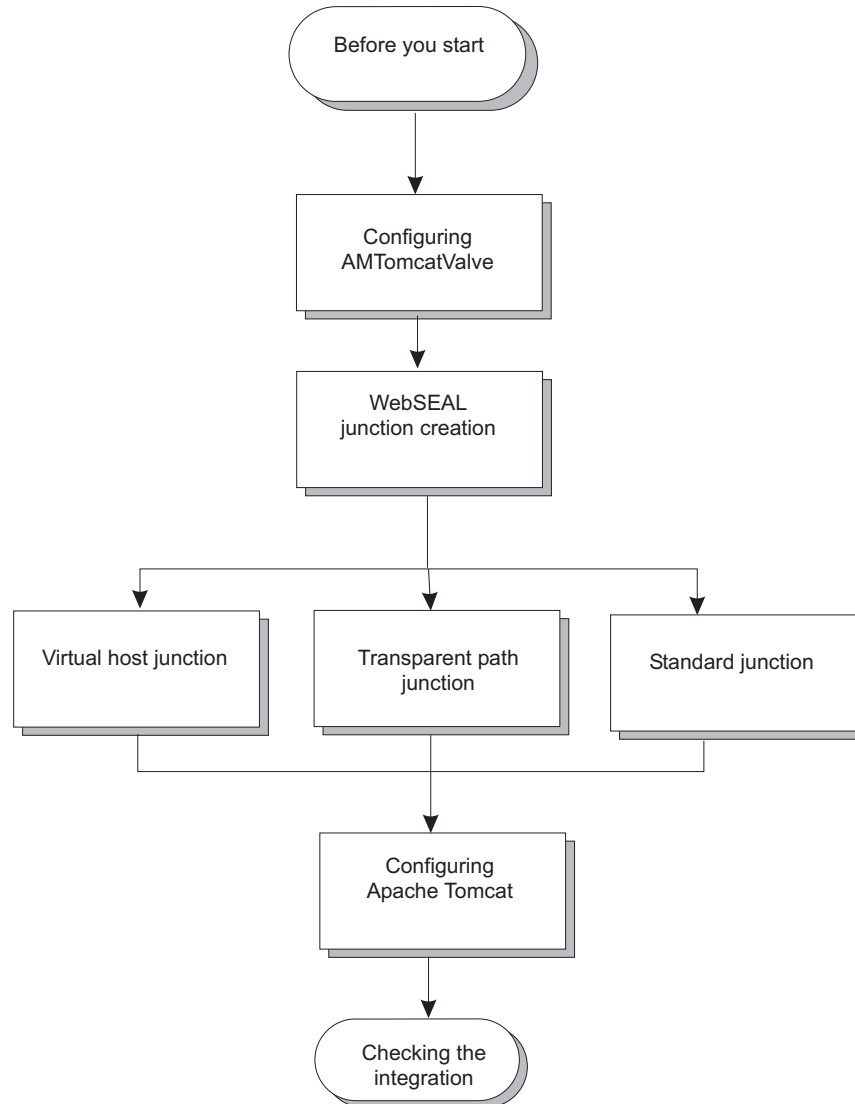
Integration Package Contents

The integration solution is packaged as a .zip file which contains the following:

File Name	Description
x.x.x-IF-AM-TOMCAT.README	The Release Notes applicable to the version.
am_tomcat_int_guide.pdf	This integration guide.
AMTomcatValve.jar	Component for providing SSO to Apache Tomcat environments protected by Tivoli Access Manager's WebSEAL.
samples/ssoAMTomcatTest.jsp	SSO test JavaServer Page to display the Principal.
samples/displayHeaders.jsp	Troubleshooting JavaServer Page to display the request HTTP headers.

Integration Process Flowchart

The diagram below illustrates the steps that must be followed through this document in order to achieve integration. Each task is detailed fully in Chapter 2, “Integration Process,” on page 7.



Integration Checklist

The following tables can be used as a checklist to help you work through the integration process. A list of each major task heading is provided, with a check box next to it. Each task is detailed fully in Chapter 2, “Integration Process,” on page 7.

Table 1. Integration checklist

Planning	Completed	Task Heading
✓ To Do	☐ Done	Configuring AMTomcatValve
✓ To Do	☐ Done	Creating a WebSEAL junction: • Virtual host junction, • Transparent junction, or • Standard junction.
✓ To Do	☐ Done	Configuring Apache Tomcat: • Enabling the AMTomcatValve • Enabling Application Security

Chapter 2. Integration Process

This chapter details the steps required to achieve the integration. This chapter has the following sections:

- “Before You Start”
- “Configuring Tivoli Access Manager WebSEAL” on page 8
- “Configuring AMTomcatValve” on page 10
- “Configuring Apache Tomcat” on page 12
- “Testing the Integration” on page 14
- “Removing the Integration” on page 14
- “Troubleshooting” on page 15

Before You Start

Before you begin this integration, review the information in Chapter 1, “Introducing the Integration,” on page 1. Determine the procedures that you will need to follow by referring to “Integration Process Flowchart” on page 4 and “Integration Checklist” on page 5.

Before beginning the integration, you should also be aware of the following:

- This solution does not cater for individual or specific Independent Software Vendor (ISV) solutions or custom applications. Such applications cannot be supported due to the complex nature of filtering and identity and role requirements.
- For applications running on Tomcat that require a user ID, a one-to-one mapping of user-ids (from Tivoli Access Manager to the applications user registry) is required.
- This integration solution does not provide authorization. The backend application must be configured for server-based security, user authentication and Role assignment.

Configuring Tivoli Access Manager WebSEAL

This section details the integration steps required for Tivoli Access Manager WebSEAL.

The required Tivoli Access Manager configuration is determined by the trust and role options configured for the **AMTomcatValve**. For details on required WebSEAL configuration to support the functionality of the **AMTomcatValve**, refer to “Configuring AMTomcatValve” on page 10.

Required Configuration

By default, the **AMTomcatValve** reads the authenticated user identity from the `iv-user` HTTP header. This header must be plain text (not encoded) and must be present during all requests. Specify the `-c iv-user` option when creating the WebSEAL junction.

Optional Trust Validation Configuration

Trust can be established using one or both of the following options.

- Basic Authentication header:
 1. Configure a complex password `[junction]basicauth-dummy-passwd` parameter in the WebSEAL configuration file (`webseal_install_dir/etc/webseald-instance.conf`).
 2. Specify the `-b supply` option when creating the WebSEAL junction.

This password must be encoded and entered in the Valve configuration in `server.xml` on the Apache Tomcat Server

- Known (trusted) server host name. The value of this key is the HTTP header the server name will be passed in. The default value is `iv_server_name`. If a different value is selected, the Valve must be configured to retrieve the server name from the correct HTTP header. Configure the `[header-names]server-name` parameter in the WebSEAL configuration file (`webseal_install_dir/etc/webseald-instance.conf`).

Optional Role Assignment Configuration

Coarse grained authorization from Tivoli Access Manager can be achieved by assigning Role names to the user Principal based on Tivoli Access Manager group memberships. Specify the `-c iv-groups` when creating the WebSEAL junction.

Creating a WebSEAL Junction

A WebSEAL junction must be created to connect WebSEAL with Tomcat. The WebSEAL junction can be configured to use either TCP or SSL (recommended), although there may be a dependency on the protocol that is configured for the Tomcat application.

There are three types of junction that can be created to achieve this:

- Virtual Host Junction,
- Transparent Path Junction, or
- Standard Junction.

The instructions for creating such junctions are detailed in the following sections. For additional junction considerations, see Chapter 3, “Additional Considerations,” on page 19.

Virtual host Junction

WebSEAL supports virtual hosting and, through virtual host junctions, can eliminate the limitations of URL filtering. Virtual host junctions allow WebSEAL to communicate with local or remote virtual hosts. WebSEAL uses the HTTP Host header in client requests to direct those requests to the appropriate document spaces located on junctioned servers or on the local machine.

Virtual hosting introduces some DNS and session management challenges. For more details on Virtual Host junctions, see the *Tivoli Access Manager WebSEAL Administration Guide*.

To create a Virtual host junction, where the Valve is configured to validate trust based on a shared secret password (basicauth-dummy-passwd) and pass the user's groups for role mapping (example command, entered as one line):

```
pdadmin> server task instance-webseald-server_name virtualhost create -t
        type -h tomcat_fqdn [-v virtualhost_fqdn] -c iv-user,iv-groups -b
        supply junction_name
```

Having created a Virtual host junction as described above, proceed to “Configuring AMTomcatValve” on page 10.

Transparent Path Junction

Links to resources located on the back end server must be filtered by WebSEAL to ensure that the user does not access it directly but rather through the WebSEAL junction. There are three sections of a URL that need to be considered:

- Protocol (http/https),
- hostname:port and
- Path.

WebSEAL 6.0 introduces the Transparent Path (TP) junction which removes the need to filter the path. A transparent path junction observes a crucial requirement: the configured junction name must match the name of a subdirectory under the root of the backend server document space. All resources accessed through this junction must be located under this subdirectory. The transparent path junction name represents the name of the actual subdirectory on the backend server.

Create a transparent path junction to each of the backend directories. The junction command is the same as for a standard junction but includes the -x option. To create a transparent path junction, where the Valve is configured to validate trust based on a shared secret password (basicauth-dummy-passwd) and pass the user's groups for role mapping (example command, entered as one line):

```
pdadmin> server task instance-webseald-server_name create -t type
        -c iv-user,iv-groups -h tomcat_fqdn [-v virtualhost_fqdn:port_no]
        -p port_no -x /junction_name
```

Transparent Path junctions do not cater for the use of regular expressions. Therefore, paths that reside at the root of the back end server must be entered into the JMT. For more details on transparent path junctions, refer to the *Tivoli Access Manager WebSEAL Administration Guide*.

Having created a Transparent Path junction as described above, proceed to “Configuring AMTomcatValve” on page 10.

Standard WebSEAL Junction

When using standard junctions, filtering challenges may be encountered due to content being returned (such as links generated on the client through use of scripts). Many of the challenges may be overcome through additional WebSEAL configuration or back end application configuration.

To create a standard junction, where the Valve is configured to validate trust based on a shared secret password (basicauth-dummy-passwd) and pass the user's groups for role mapping (example command, entered as one line):

```
pdadmin> server task webseald-server_name create -t type
-c iv-user,iv-groups -h tomcat_fqdn [-v virtualhost_fqdn:port_no]
-p port_no /junction_name
```

For more detailed instructions on WebSEAL junction creation, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*. For additional junction considerations, see Chapter 3, "Additional Considerations," on page 19.

After creating a Standard junction as described above, proceed to "Configuring AMTomcatValve."

Configuring AMTomcatValve

The **AMTomcatValve** valve provides a lightweight Single Sign On solution from IBM Tivoli Access Manager WebSEAL to applications hosted on Apache Tomcat. The valve is highly configurable allowing control over user identity headers, trust association and role assignments. The valve is configured in Tomcat's `server.xml` and configuration parameters are specified within the Valve tag. All configuration options for the valve are optional. All key and value pairs must be separated by a space character and values must be enclosed in double quotes (""). Configuration errors will be output in the Tomcat logs if the configuration is incorrect. For example:

```
<Valve className="com.ibm.tivoli.integration.am.catalina.valves.AMTomcatValve"
debugTrace="true" />
```

Without any optional parameters supplied, the Valve will not output any trace, will not attempt to associate trust, will expect the HTTP `iv-user` header to contain the user ID and will insert a default role of **AMTomcatAuthenticated**. This configuration is recommended only for testing the initial deployment or problem determination. For example, you can configure the Valve to only expect the HTTP `iv-user` header, and not perform any trust association or tracing, as follows:

```
<Valve className="com.ibm.tivoli.integration.am.catalina.valves.AMTomcatValve" />
```

All configuration items are optional. Where configuration options are not specified, the default values are applied. All configuration keys are case sensitive.

A Principal is created using the value from the `iv-user` HTTP header or other specified plain text header. Trust can optionally be established by checking any of a Basic Authentication password or WebSEAL server name (`iv_server_name`). Roles can optionally be assigned from a specified list, or from a plain text HTTP header. When **addRoles** and **groupsHeader** are not specified the **AMTomcatValve** will add a default role called **AMTomcatAuthenticated**.

Table 2. Configuration Key values

Configuration Key	Description	Default Value	Allowable Valves
debugTrace	Provides detailed trace information in the Tomcat log files. Not recommended in a production environment.	nil	Any non-null or empty string value. The value is not parsed.
userHeader	HTTP header in the request to extract the Authenticated user from. Must be plain text (not encoded). A Principal will be built using this name.	iv-user	Case sensitive string representing the HTTP header.
groupsHeader	HTTP header in the request to extract group names for role assignments. Must be plain text (not encoded). Multiple vales in the header must be comma separated and may be quoted with single or double quotes.	nil	Case sensitive string representing the HTTP header.
addRoles	Role names to add to all Principals created by the valve.	nil	Case sensitive string representing roles to add to the Principal. Comma separate entries to specify multiple roles.
secretPassword	Establish Trust association using the Basic Authorization HTTP header password.	nil	Base64 encoded basicauth-dummy-passwd parameter from WebSEAL's [junction] stanza.
ivServerName	Establish Trust association using WebSEAL's iv-server-name HTTP header.	nil	Case sensitive string representing trusted server names. Comma separate entries to specify multiple servers.
ivServerHeader	HTTP header present in the request to extract the trusted server name from. Must be plain text (not encoded). Only used when ivServerName parameter is set.	iv_server_name	Case sensitive string representing the HTTP header.

A more elaborate Valve configuration may then resemble:

```
<Valve className="com.ibm.tivoli.integration.am.catalina.valves.AMTomcatValve"
  debugTrace="true" addRoles="hr,finance" ivServerName="webseal.ibm.com"/>
```

This configuration would enable tracing, add the roles “hr” and “finance” to the Principal and verify that the requesting server name is “webseal.ibm.com”.

During startup of the Apache Tomcat server the AMTomcatValve’s **start()** method is called which will initialize the configuration and output the settings in the Tomcat logs. For example:

```
AMTomcatValve configuration -
debugTrace: false
userHeader: iv-user
secretPassword: false
addRoles: false
groupsHeader: false
ivServerName: false
ivServerHeader: iv_server_name
AMTomcatValve.start() exit.
```

Encoding the secretPassword

The value for **secretPassword** in the valve’s configuration must be Base64 encoded. A utility is provided in the AMTomcatValve.jar file. Note that the utility uses Sun classes and will only operate in a Java Runtime with access to the `sun.misc.BASE64Encoder()` class.

Generating the encoded password will output the encoded and original password entered. For example:

```
java -classpath CATALINA_HOME/lib/AMTomcatValve.jar
com.ibm.tivoli.integration.util.Encode secretpassword
Encrypted: [c2VjcmV0cGFzc3dvcmQ=], Decrypted: [secretpassword]
```

Configuring Apache Tomcat

This section details the integration steps required on Apache Tomcat to enable and configure **AMTomcatValve**.

Enabling AMTomcatValve in Tomcat

To configure the Tivoli Access Manager for Tomcat Valve:

1. Copy the AMTomcatValve.jar file from the integration package to the following directory:

`CATALINA_HOME/lib`

2. In `CATALINA_HOME/conf/server.xml`, add the Valve definition applicable to your deployment. Generally, the Valve configuration is added within the `<Engine>` tag. For example:

```
<Server ...>
...
<Service name="Catalina">
...
  <Engine name="Catalina" defaultHost="localhost">
    ...
    <Valve className="com.ibm.tivoli.integration.am.catalina.valves.AMTomcatValve" />
    ...
  </Engine>
</Service>
</Server>
```

Note: The default configuration for the **AMTomcatValve**:

- does not produce any trace messages,
- uses the `iv-user` HTTP header,

- does not establish trust by way of a shared secret password or server name, and
- adds a default role of **AMTomcatAuthenticated**.

For additional detail on configuring the Valve, refer to “Configuring AMTomcatValve” on page 10.

Enabling Application Security

To enable container security for the Web Application:

1. Add security constraints to the application to be secured. This is done within the web.xml file in the WEB-INF directory of the application. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
...
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Application</web-resource-name>
      <url-pattern>/*</url-pattern>
      <http-method>POST</http-method>
      <http-method>GET</http-method>
    </web-resource-collection>
    <auth-constraint>
      <role-name>AMTomcatAuthenticated</role-name>
    </auth-constraint>
  </security-constraint>
...
</web-app>
```

Note: The <role-name> auth-constraints must be met for successful authorization to the application. Any roles required to access the application must be either:

- set in the **AMTomcatValve** configuration, or
 - passed as Tivoli Access Manager group memberships in the iv-groups HTTP header, or
 - set as only **AMTomcatAuthenticated** (if none of the previous options are used).
2. Add a login configuration to the application to be secured, so that authentication is handled by Apache Tomcat. This is done within the web.xml file in the WEB-INF directory of the application. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
...
  <login-config>
    <auth-method>BASIC</auth-method>
  </login-config>
...
</web-app>
```

3. *Optional:* If the role is also not present in the <security-role> element, a warning will appear in the Tomcat log.

To remove this warning, security roles can be added to the application which will enable mapping of all the roles defined in the application to users and groups defined for Tomcat. This is done within the web.xml file in the WEB-INF directory of the application. For example:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
  ...
  <security-role>
    <role-name>AMTomcatAuthenticated</role-name>
  </security-role>
  ...
</web-app>

```

After configuring Tomcat to use **theAMTomcatValve**, proceed to “Testing the Integration.”

Testing the Integration

The following example can be used to test the integration.

SsoAMTomcatTest JavaServer Page

Perform the following steps to create the ssoAMTomcatTest JavaServer Page:

1. Select a suitable application directory on the Tomcat server to copy the JSP. For example:

CATALINA_HOME/ webapps/appName

2. Copy ssoAMTomcatTest.jsp to this directory.

Once you have created the ssoAMTomcatTest JSP as shown above, test the integration as follows:

1. Open a browser and access Tomcat with the appropriate URL:

Using Virtual Host junction:

`http[s]://tomcat_fqdn/appName/ssoAMTomcatTest.jsp`

For example: `https://www.mywebsite.com/appName/ssoAMTomcatTest.jsp`

Using Transparent Path Junction:

`http[s]://webseal_fqdn/appName/ssoAMTomcatTest.jsp`

For example: `https://www.webseal.acme.com/appName/ssoAMTomcatTest.jsp`

Using Standard WebSEAL Junction:

`http[s]://webseal_fqdn/junction_name/appName/ssoAMTomcatTest.jsp`

For example: `https://www.webseal.acme.com/jct_tomcat/appName/ssoAMTomcatTest.jsp`

2. Tivoli Access Manager WebSEAL will prompt for authentication. Log in using the Tivoli Access Manager user ID and password.
3. Upon successful authentication, a page displaying the user ID of the current user Principal should be displayed.

Removing the Integration

The uninstall process is virtually a reverse of the installation process described above. To remove the integration, you only need to restore your original Apache Tomcat server settings.

Any changes made to the Web application settings should be removed, including the Valve configuration. The Valve jar file should be removed from the Tomcat library path.

Troubleshooting

This section describes how to resolve several known issues, plus further information on locating log files and tracing in the AMTomcatValve.

Debug Trace in AMTomcatValve

By default, the **AMTomcatValve** does not output any log or trace, other than the startup information when it is first loaded. To enable trace from the valve, modify the <Valve> entry in the Tomcat's `server.xml` file, adding the following:

```
debugTrace=true
```

For example:

```
<Valve className="com.ibm.tivoli.integration.am.catalina.valves.AMTomcatValve"
      debugTrace="true" />
```

All output from the valve will be redirected to Tomcat's configured Standard Out (`stdout_date.log`) file. It is recommended that **debugTrace** is only enabled for testing the initial deployment, and for problem determination, due to the large amount of messages that are generated.

DisplayHeaders JavaServer Page

To assist with configuration issues with the **AMTomcatValve** and WebSEAL, the `displayHeader.jsp` file can be deployed in Tomcat to show the request HTTP headers. This will assist in determining the presence and values of the HTTP headers that are required for the valve, including `iv-user`, `iv-groups`, `iv-server-name` and the Basic Authorization.

Perform the following steps to create the **displayHeaders** JavaServer Page:

1. Select a suitable application directory on the Tomcat server to copy the JSP. For example:
`CATALINA_HOME/webapps/appName`
2. Copy `displayHeaders.jsp` to this directory.

Once you have created the **displayHeaders** JSP as shown above, test the integration as follows:

1. Open a browser and access Tomcat with the appropriate URL:

Using Virtual Host junction:

```
http[s]://tomcat_fqdn/appName/displayHeaders.jsp
```

For example: `https://www.mywebsite.com/appName/displayHeaders.jsp`

Using Transparent Path Junction:

```
http[s]://webseal_fqdn/appName/displayHeaders.jsp
```

For example: `https://www.webseal.acme.com/appName/displayHeaders.jsp`

Using Standard WebSEAL Junction:

```
http[s]://webseal_fqdn/junction_name/appName/displayHeaders.jsp
```

For example: `https://www.webseal.acme.com/jct_tomcat/appName/displayHeaders.jsp`

2. Tivoli Access Manager WebSEAL will prompt for authentication. Log in using the Tivoli Access Manager user ID and password.
3. Upon successful authentication, a page displaying the request headers is displayed. If the page is blank, or an Unauthorized page is displayed, check the Tomcat log files for the presence of Known Exception Messages (see below) to resolve the problem.

Apache Tomcat Log Files

When errors occur in the Valve, such as missing HTTP headers or failed trust validation, it will throw an Exception that is then handled by the caller.

Check the Tomcat log directory for log entries to help diagnose the problem:

`CATALINA_HOME/logs`

Known Exception Messages

Problem:

```
java.lang.ClassNotFoundException:  
com.ibm.tivoli.integration.am.catalina.valves.AMTomcatValve
```

Resolution:

Ensure the `AMTomcatValve.jar` file has been copied to the `CATALINA_HOME/lib` directory.

Problem:

```
javax.servlet.ServletException: iv-user not found
```

Resolution:

Ensure that the `-c iv-user` option is specified when creating the required junction type.

Problem:

```
javax.servlet.ServletException: AMTomcatValve.checkBaPassword():  
Basic Authentication header not found. Unable to establish trust
```

Resolution:

Ensure that the `-b supply` option is specified when creating the required junction type, or remove `secretPassword` from the valve configuration.

Problem:

```
javax.servlet.ServletException: AMTomcatValve.checkBaPassword():  
Basic Authentication failed. Password does not match
```

Resolution:

Ensure that the value of `basicauth-dummy-passwd` specified in WebSEAL's `[junction]` stanza is encoded, and that it is copied correctly into the `secretPassword="encodedPassword"` section of the valve configuration.

Problem:

```
javax.servlet.ServletException: AMTomcatValve.checkIvServerName():  
default-webseald-fqdn not in trusted.
```

Resolution:

Ensure that the value of `server-name` from WebSEAL's `[server]` stanza is contained within the `ivServerName="webseal_server1,webseal_server2"` section of the valve configuration.
Ensure that the `server-name` value in WebSEAL's `[header-names]` stanza is

`iv_server_name`.

Ensure that the **server-name** value in WebSEAL's `[header-names]` stanza matches **ivServerHeader** in the valve configuration.

Chapter 3. Additional Considerations

When integrating Tivoli Access Manager with Tomcat, the following considerations should be taken into account.

Note: Given the broad range of Web site and application design possibilities, more specific discussion of these considerations is outside the scope of this integration guide.

ACL Considerations

In order for a back end Web application to perform its full set of functionality, an Access Control List (ACL) may need to be added for the Tomcat server. For details of ACL management, refer to the *IBM Tivoli Access Manager Base Administration Guide*. For details of plug-in specific ACL policies, refer to the *IBM Tivoli Access Manager Plug-in for Web Servers User's Guide*.

WebSEAL Options

To allow WebSEAL to filter content from Tomcat applications correctly, the `webseal_install_dir/etc/webseald.conf` file may need to be modified. WebSEAL will need to be restarted after these changes have been made.

For details of WebSEAL filtering options, refer to the *IBM Tivoli Access Manager WebSEAL Administrator's Guide*.

Junction Mapping Table Considerations

Server-relative URLs generated on the client-side by applets and scripts initially lack knowledge of the junction point. WebSEAL cannot filter the URL because it is generated dynamically on the client side. During a client request for a resource using this URL, WebSEAL can attempt to reprocess the server-relative URL using a predefined mapping table. WebSEAL will need to be restarted after these changes have been made.

For details of WebSEAL junction and JMT options, refer to the *IBM Tivoli Access Manager WebSEAL Administrator's Guide*.

Appendix A. Support information

This section describes the following options for obtaining support for IBM products:

- “Searching knowledge bases”
- “Obtaining fixes”
- “Registering with IBM Software Support” on page 22
- “Receiving weekly software updates” on page 22
- “Contacting IBM Software Support” on page 23

Searching knowledge bases

If you encounter a problem, you want it resolved quickly. You can search the available knowledge bases to determine whether the resolution to your problem was already encountered and is already documented.

Searching information centers

IBM provides extensive documentation in an information center that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Searching the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, perform the following steps:

1. Expand the product folder in the navigation frame on the left.
2. Expand **Troubleshooting and support**.
3. Expand **Searching knowledge bases**.
4. Click **Web search**.

From this topic, you can search a variety of resources, which includes the following resources:

- IBM Technotes
- IBM downloads
- IBM Redbooks®
- IBM developerWorks®
- Forums and news groups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, check the product support site by performing the following steps:

1. Go to the IBM Software Support site at the following Web address:

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

2. Under **Products A - Z**, click the letter with which your product starts to open a Software Product List.
3. Click your product name to open the product-specific support page.
4. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
5. Click the name of a fix to read the description.
6. Optional, download the fix.

Registering with IBM Software Support

Before you can receive weekly e-mail updates about fixes and other news about IBM products, you need to register with IBM Software Support. To register with IBM Software Support, follow these steps:

1. Go to the IBM Software Support site at the following Web address:

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

2. Click **Register** in the upper right-hand corner of the support page to establish your user ID and password.
3. Complete the form, and click **Submit**.

Receiving weekly software updates

After registering with IBM Software Support, you can receive weekly e-mail updates about fixes and other news about IBM products. To receive weekly notifications, follow these steps:

1. Go to the IBM Software Support site at the following Web address

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

2. Click the **My support** link to open the Sign in page.
3. Provide your sign in information, and click **Submit** to open your support page.
4. Click the **Edit profile** tab.
5. For each product about which you want to receive updates, use the filters to choose your exact interests, and click **Add products**.
6. Repeat step 5 for each additional product.
7. After choosing all your products, click the **Subscribe to email** link.
8. For each product category, use the filters and choose which updates you want to receive, and click **Update**.
9. Repeat step 8 for each additional product category.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at the following Web address:

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

Contacting IBM Software Support

IBM Software Support provides assistance with product defects. Before contacting IBM Software Support, the following criteria must be met:

- Your company has an active IBM software maintenance contract.
- You are authorized to submit problems to IBM Software Support.

The type of software maintenance contract that you need depends on the type of product that you have. Product types are one of the following categories:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2® and WebSphere® products that run on Windows, Linux, or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

Online

Go to the IBM Software Passport Advantage site at the following Web address and click **How to Enroll**:

[http://www.lotus.com/services/passport.nsf/
WebDocs/Passport_Advantage_Home](http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home)

By phone

For the phone number to call in your country, go to the IBM Software Support site at the following Web address and click the name of your geographic region:

<http://techsupport.services.ibm.com/guides/contacts.html>

- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in System z®, pSeries®, and iSeries® environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM eServer Technical Support Advantage site at the following Web address:

<http://www.ibm.com/servers/eserver/techsupport.html>

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the *IBM Software Support Handbook* at the following Web address and click the name of your geographic region for phone numbers of people who provide support for your location:

<http://techsupport.services.ibm.com/guides/contacts.html>

To contact IBM Software support, follow these steps:

1. "Determining the business impact"
2. "Describing problems and gathering information" on page 24
3. "Submitting problems" on page 24

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem that you are reporting. Use the following severity criteria:

Severity 1

The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2

The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3

The problem has *some* business impact. The program is usable, but less significant features that are not critical are unavailable.

Severity 4

The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you create the problem again? If so, what steps were performed to encounter the problem?
- Was any change made to the system? For example, were there changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online

Go to the Submit and track problems page on the IBM Software Support site at the following address, and provide your information into the appropriate problem submission tool:

<http://www.ibm.com/software/support/probsub.html>

By phone

For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at the following Web address and click the name of your geographic region:

<http://techsupport.services.ibm.com/guides/contacts.html>

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolution.

For more information about problem resolution, see “Searching knowledge bases” on page 21 and “Obtaining fixes” on page 21.

Appendix B. 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 might 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 has been 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.

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

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

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

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

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, AIX®, and Tivoli, are trademarks or registered trademarks of International Business Machines 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, other countries, or both.

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

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

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

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



Printed in USA