



# Installing and using the webScurity webApp.secure client





# Installing and using the webScurity webApp.secure client

**Note**

Before using this information and the product it supports, read the information in "Notices," on page 19.

**First Edition (August 2006)**

**© Copyright International Business Machines Corporation 2006. All rights reserved.**

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

---

## Contents

<b>About this book</b> . . . . .	<b>v</b>	<b>Chapter 6. Security</b> . . . . .	<b>11</b>
<b>Chapter 1. Overview</b> . . . . .	<b>1</b>	<b>Chapter 7. Data integrity considerations</b> . . . . .	<b>13</b>
<b>Chapter 2. Pre-requisites</b> . . . . .	<b>3</b>	<b>Chapter 8. Tuning</b> . . . . .	<b>15</b>
<b>Chapter 3. Installation.</b> . . . . .	<b>5</b>	<b>Chapter 9. Service and upgrade</b> . . . . .	<b>17</b>
<b>Chapter 4. Configuration</b> . . . . .	<b>7</b>	Obtaining updates . . . . .	17
Initialization . . . . .	8	<b>Appendix. Notices.</b> . . . . .	<b>19</b>
Testing the configuration . . . . .	8	Trademarks . . . . .	20
Backing up the configuration . . . . .	8		
<b>Chapter 5. Operation</b> . . . . .	<b>9</b>		
User interface . . . . .	9		



---

## About this book

This document describes how to set up and use the webSecurity webApp.secure component in the context of Linux<sup>®</sup> Utilities for IBM<sup>®</sup> System z<sup>™</sup> (Linux Utilities).

Linux Utilities are a suite of Linux solutions configured and tested on System z in a z/OS and Linux workload scenario. Linux Utilities provide specific infrastructure functions that are complementary to functions on z/OS. With Linux Utilities you have an additional option to optimize your z/OS environment. Linux Utilities help to provide quick deployment, easy installation, and reduced time-to-market of infrastructure functions with minimal impact on z/OS skills and resources.

For more information on Linux Utilities visit [www.ibm.com/zseries/os/linux/utilities](http://www.ibm.com/zseries/os/linux/utilities). On this site you might also find updates to this document.

For information on running Linux on System z mainframes see:

- *z/VM and Linux on IBM System z: The Virtualization Cookbook for SLES9*, SG24-6695
- *z/VM and Linux on IBM System z: The Virtualization Cookbook for Red Hat Enterprise Linux 4*, SG24-7272



---

## Chapter 1. Overview

The webScurity<sup>®</sup> webApp.secure<sup>®</sup> client for Linux on System z protects web application servers running on IBM systems under z/OS<sup>®</sup> from web application attacks which take advantage of the stateless nature of the Web protocol (HTTP). The client stops indiscriminate HTTP worm or virus attacks, and also discriminates targeted Internet attacks directed at the application source code.

Even when protected by a general firewall, web applications are still vulnerable to critical attacks such as SQL injection, cross-site scripting, cookie poisoning, hidden field manipulation, and others. The webScurity webApp.secure client operates invisibly and protects the application by examining the HTTP network traffic to ensure that it conforms to Intended Use Guidelines specified for the site.

The functions provided by the utility include:

- Provision of a trusted gateway that protects all web application code, z/OS, WebSphere<sup>®</sup> or other middleware and their vulnerabilities ,
- Checking of web content in the de-militarised zone (DMZ) with no risk to the application servers running on z/OS,
- Set & Forget controls that autonomically derive and update policy,
- An added layer of regulatory compliance that exceeds government guidelines for GLBA, HIPAA and SOX,
- Isolation of z/OS from Internet traffic and threats, using HiperSockets<sup>™</sup> for fast communications that are physically secure.

As shown in Figure 1, webApp.secure runs in the DMZ between the external firewall and the Linux web proxy. After the packaging of network traffic has been verified by the external firewall, and before the traffic is passed through the internal firewall to the z/OS application, the contents of the traffic are verified by webApp.secure.

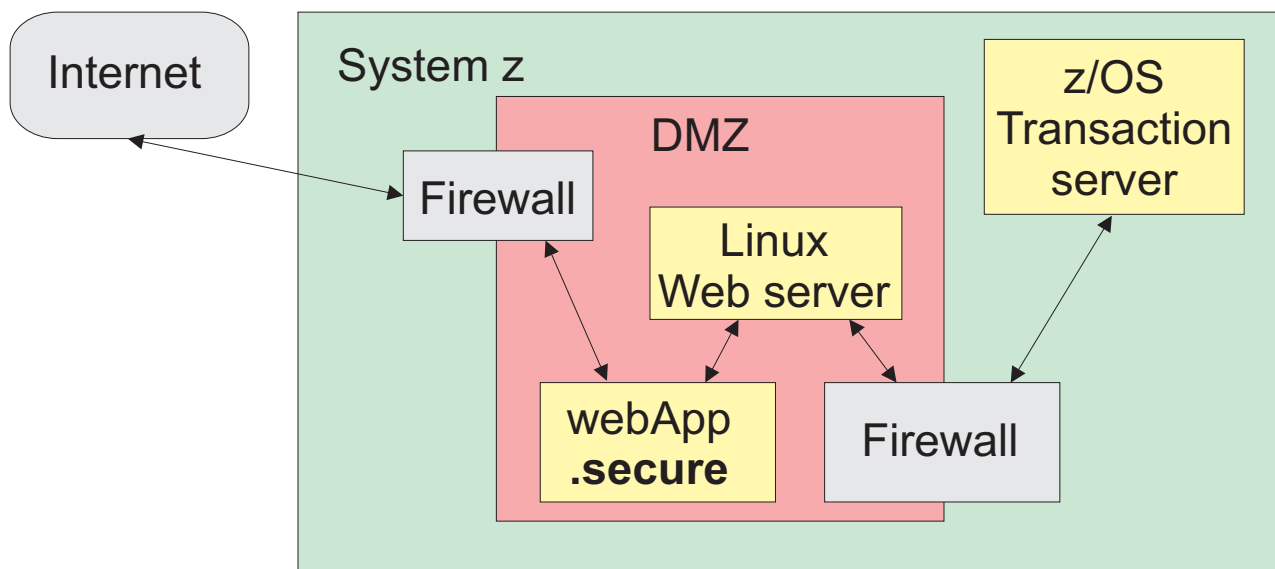


Figure 1. Base scenario

This can be used as a starting point in the transition from the distributed environment, but the maximum benefits from webApp.secure can be gained in an environment such as that illustrated in Figure 2. Here the necessary firewall functions are performed by IPSec and IPS in the z/OS TCP/IP stack. In this way the complexity and expense of the "choke" or private firewall can be eliminated and increased performance will result.

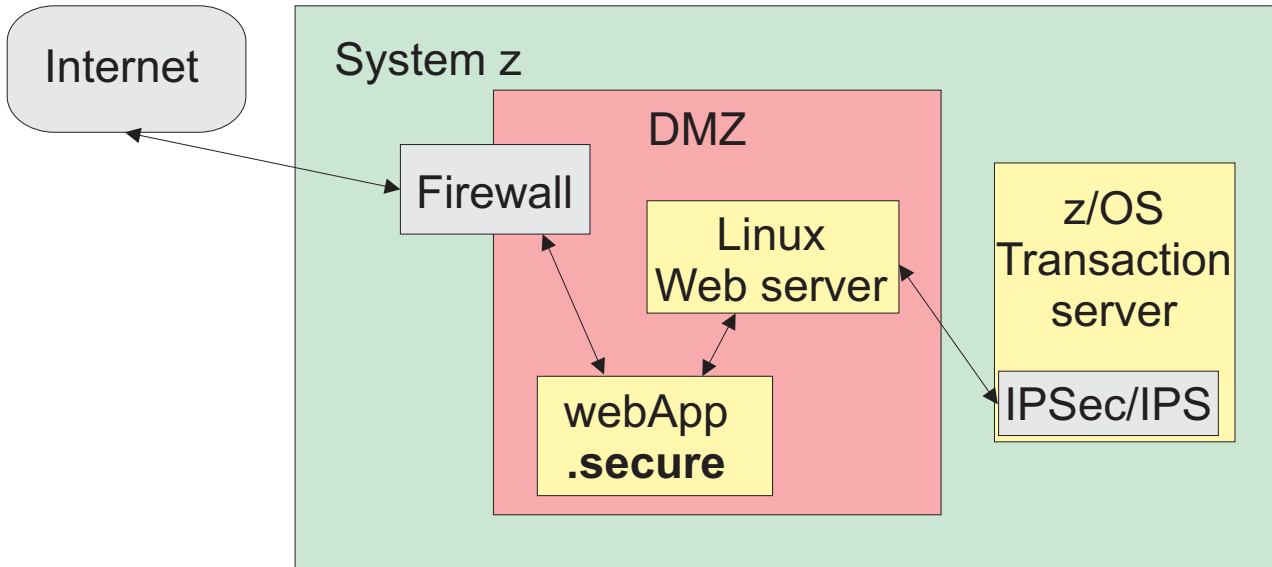


Figure 2. Advanced scenario

---

## Chapter 2. Pre-requisites

This section identifies pre-requisites for the webScurity webApp.secure client for Linux on System z.

- The utility must be installed into Linux on System z running in an LPAR or under z/VM<sup>®</sup>.
- System Requirements – Compatibility
  - All major web browsers
  - All HTTP web servers
  - All HTTP application servers
  - Fully compatible with HTTP 1.0 and 1.1
  - Fully compatible with HTML 3.2 and 4.0, including cascading style sheets
  - Fully compatible with client side scripting languages (JavaScript<sup>™</sup>, VBScript, etc.)
  - SSL 40/128 bit encryption and global ID
- System Requirements – Minimum
  - 128 Mbytes RAM recommended
  - 300 Mbytes free disk space recommended
- If you host multiple web sites on the same server using IP-based virtual hosting, then you will need to set up a separate instance for each IP. Set the <listen-ip> property (see Chapter 4, “Configuration,” on page 7) of each instance to the IP address of each web site.

Check “Obtaining updates” on page 17 for the latest version of the webApp.secure client.



---

## Chapter 3. Installation

Installation of the webScurity webApp.**secure** client on System z

As the webScurity webApp.**secure** client runs entirely on Linux there is nothing to install on z/OS.

The Linux software is supplied as a RPM package, for example `webApp.secure.pe-3.0-1.s390x.rpm`. This is installed in Linux on System z using the `rpm -i` command.

Full details are given in the *webApp.**secure** Installation and Setup Guide*, [http://www.webscurity.com/pdfs/wa\\_installation\\_setup\\_guide.pdf](http://www.webscurity.com/pdfs/wa_installation_setup_guide.pdf). More information about installation on Linux or UNIX<sup>®</sup> is contained in the document */usr/local/wa/doc/Welcome\_unix.pdf* which is installed as part of the RPM package.



---

## Chapter 4. Configuration

How to configure webApp.secure on z/OS and on Linux on System z.

Configuration on z/OS will generally be unnecessary. The only exception would be if webApp.secure is required to monitor web access originating in z/OS. In this case it is necessary to modify the routing table on z/OS to direct the net traffic through the webApp.secure client. The original routing table entries are used in the configuration of the utility on Linux.

The webScurity webApp.secure client is configured on Linux in a set of XML files which are maintained with the use of a text editor such as vi. The first of these files is the locations file, etc/wa.conf. This file holds a pointer to the main configuration settings in properties\_file, as well as pointers to log files and flags for log settings. Basic details are given in the section *To Install webApp.secure on Linux* in the *webApp.secure Installation and Setup Guide*, [http://www.webscurity.com/pdfs/wa\\_installation\\_setup\\_guide.pdf](http://www.webscurity.com/pdfs/wa_installation_setup_guide.pdf).

The default location for the properties file is */usr/local/wa/etc/WAProperties.xml*. The principle entries in this file are the web-server-name, web-server-port, listenport, and host-name which identify the web server to be protected. Other entries may be added to define policies and detection settings.

The formats of the principal entries are:

### Web Server Name

```
<web-server-name>server_ip_address</web-server-name>
```

for example:

```
<web-server-name>our.server</web-server-name>
```

or:

```
<web-server-name>192.168.0.2</web-server-name>
```

This is the internal reference of the web server webApp.secure is protecting. It is typically an IP address or an internal server name.

### Web Server Port

```
<web-server-port>server_port</web-server-port>
```

for example:

```
<web-server-port>8080</web-server-port>
```

If webApp.secure is running on the physical web server this should be a non-standard port number. However, if they are running on separate machines, this can be any valid TCP port number not accessible from the outside.

### Listen IP

```
<listen-ip>ip_to_monitor</listen-ip>
```

for example:

```
<listen-ip>192.168.0.2</listen-ip>
```

This is an optional IP address that webApp.secure should use. If no IP is specified, webApp.secure will use all available.

#### Listen Port

```
<listen-port>normal_port</listen-port>
```

for example:

```
<listen-port>80</listen-port>
```

This is the TCP port number webApp.secure will use for unencrypted traffic. Normally this will be the standard HTTP port 80.

#### Host Names

```
<host-names>  
<host-name>host</host-name>  
<host-names>
```

for example:

```
<host-names>  
<host-name>www.maindomain.com</host-name>  
<host-name>www.subdomain.com</host-name>  
<host-names>
```

These are one or more fully-qualified external host names of the web sites webApp.secure is protecting. Add an entry for every name-based virtual web site hosted on the web server.

Full details of these fields and other configuration settings are given in the document *Welcome to webApp.secure*, `/usr/local/wa/doc/Welcome_unix.pdf`.

---

## Initialization

The webApp.secure process is started with the command `/usr/local/wa/bin/wa`. This will normally be added to a system boot procedure. No further initialization is required.

---

## Testing the configuration

Testing that the webScurity webApp.secure client has been successfully configured.

The configuration can be tested by following the examples given in the *Testing/Experimenting* section of the *webApp.secure Installation and Setup Guide*, [http://www.webscurity.com/pdfs/wa\\_installation\\_setup\\_guide.pdf](http://www.webscurity.com/pdfs/wa_installation_setup_guide.pdf), and the *Evaluation Installation Examples* section in the *Welcome to webApp.secure* document, `/usr/local/wa/doc/Welcome_unix.pdf`.

---

## Backing up the configuration

Backing up the configuration settings of the webScurity webApp.secure client

The configuration settings are held in text format in an XML file and a conf file (see Chapter 4, “Configuration,” on page 7 for details.) This file should be backed up by copying it to a secure location whenever it is modified. Restoration is simply a matter of copying it back again.

---

## Chapter 5. Operation

How to use the webScurity webApp.secure client

webApp.secure operates invisibly in the System z DMZ, by protecting each URL within a System z machine with "Set & Forget" controls that autonomically derive and update web site policy as content exits the web server. The webApp.secure Administration Console records and reports statistics for all HTTP daemon requests, showing total allowed and total blocked by attack attempt type.

---

### User interface

The webScurity webApp.secure client for Linux on System z is controlled using the browser-based Administration Option.

Example screens from the Administration Option can be found from the <http://www.webscurity.com/products.htm> page, by following the "Quick Start Guide" link.

The Remote Administration property group allows you to specify parameters for browser-based administration. There are safeguards to limit accessibility to the remote administration feature, and it does use SSL (<https://>), but it was designed to be used over an intranet. The parameters are:

```
<remote-admin>
  <enable>status</enable>
</remote-admin>
```

for example:

```
<remote-admin>
  <enable>>true</enable>
</remote-admin>
```

Set to "True" to enable browser-based administration.

```
<remote-admin>
  <listen-ip>ip_to_monitor</listen-ip>
</remote-admin>
```

for example:

```
<remote-admin>
  <listen-ip>192.168.0.2</listen-ip>
</remote-admin>
```

This is the specific IP address webApp.secure should use for browser-based administration.

If left blank all available IP addresses will be used.

```
<remote-admin>
  <listen-port>normal_port</listen-port>
</remote-admin>
```

for example:

```
<remote-admin>
  <listen-port>8020</listen-port>
</remote-admin>
```

This is the TCP port number webApp.secure should use for browser-based administration.

```
<remote-admin>
  <password>password</password>
</remote-admin>
```

for example:

```
<remote-admin>
  <password>admin</password>
</remote-admin>
```

This is a one-way hashed password to use for browser-based administration access.

**Note:** The default password is “admin” and can only be changed from the browser when this option is enabled.

```
<remote-admin>
  <client-ips>
    <client-ip>client_ip</client-ip>
  </client-ips>
</remote-admin>
```

for example:

```
<remote-admin>
  <client-ips>
    <client-ip>192.168.0.105</client-ip>
  </client-ips>
</remote-admin>
```

These are one or more client IP addresses that are allowed to connect to webApp.secure for browser-based administration.

If no IPs are specified connections will be accepted from any IP address.

Example addressing from a browser:

```
https://192.168.0.2:8020/
```

(Please note the use of https in this example.)

---

## Chapter 6. Security

Data security is achieved when using the webSecurity webApp.**secure** client for Linux on System z.

webApp.**secure** protects all elements of the web environment including operating system, HTTP daemon, development and deployment framework, and DBMS. It also ensures that web sites, their applications, and their associated databases are accessed and used exactly as intended, with a positive model, by enforcing web site guidelines, rules and policy.

Web site policy is automatically secured after webApp.**secure** maps the web application business logic, including vulnerabilities (for example legacy and new application software), upon installation and autonomically derives and updates policy as content exits the server.

webApp.**secure** is a web application firewall, residing in the DMZ between the standard firewall and the Linux web server, and protects against attacks seeking to exploit software vulnerabilities through:

- SQL injection,
- Cross-site scripting,
- Hidden field manipulation,
- Cookie poisoning,
- Stealth commanding,
- Forceful browsing,
- Buffer overruns, and
- URL parameter tampering.



---

## Chapter 7. Data integrity considerations

Ensuring data integrity between the webSecurity webApp.**secure** client for Linux on System z and z/OS.

Data integrity is automatically assured by validation with web site policy when the HTTP stream passes through a standard firewall, and autonomically upon exit from the web server.



---

## Chapter 8. Tuning

Tuning the webSecurity webApp.secure client for Linux on System z.

Tuning on z/OS is not applicable; all tuning is performed on Linux.

The parameters which can be modified to adjust the performance of webApp.secure for Linux on System z are:

**<max-connections></max-connections>**

The maximum number of simultaneous client connections that will be served. Once the threshold is reached the operating system's listen queue will be used.

**<max-listen-queue></max-listen-queue>**

The maximum number of pending connections that will be served from the operating system's listen queue.



---

## Chapter 9. Service and upgrade

Migrating to the latest version of the webScurity webApp.**secure** client for Linux on System z.

This will normally be performed by downloading and installing the latest RPM from webScurity as described in Chapter 3, "Installation," on page 5. Installation will replace the executable `/usr/local/wa/bin/wa` executable with the latest webApp.**secure** version (currently version 4.0).

The tasks to perform are:

1. Shut down webApp.**secure**,
2. Copy the executable,
3. Start webApp.**secure**.

---

### Obtaining updates

Obtaining fixes to the current release of the webScurity webApp.**secure** client, and acquiring a new release

The latest version of the webScurity webApp.**secure** client can be downloaded from <http://www.webscurity.com/download.htm>



---

## Appendix. Notices

This information was developed for products and services offered in the U.S.A.

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant 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 106-0032, 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 has been exchanged, should contact:

IBM Corporation  
Software Interoperability Coordinator, Department 49XA  
3605 Highway 52 N  
Rochester, MN 55901  
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 information 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 measurements 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.

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Trademarks

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

HiperSockets  
IBM  
System z

WebSphere  
z/OS  
z/VM

All Java-based trademarks are 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.

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

webScurity inc. and webApp.**secure** are trademarks of webScurity Inc. in the United States, other countries, or both.

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



---

## Readers' Comments — We'd Like to Hear from You

Linux Utilities for IBM System z  
Installing and using the webScurity webApp.secure client

Publication No. SC33-8322-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Complete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to find	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to understand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Well organized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicable to your tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please tell us how we can improve this book:

Thank you for your responses. May we contact you?  Yes  No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

---

Name

---

Address

---

Company or Organization

---

Phone No.



Fold and Tape

**Please do not staple**

Fold and Tape

PLACE  
POSTAGE  
STAMP  
HERE

IBM Deutschland Entwicklung GmbH  
Information Development  
Department 3248  
Schoenaicher Strasse 220  
71032 Boeblingen  
Germany

Fold and Tape

**Please do not staple**

Fold and Tape





SC33-8322-00

