WebSEAL Installation Guide

Version 4.1
Contents

Preface ..................................................... v
Who should read this book .................................. v
What this book contains .................................. v
Publications .................................................. vi
   Release information .................................. vi
   Base information ...................................... vi
   WebSEAL information ................................ vii
   Web security information ............................. vii
   Developer references ................................ vii
   Technical supplements ................................ vii
   Related publications ................................. viii
   Accessing publications online ....................... x
Accessibility .............................................. x
Contacting software support ............................... x
Conventions used in this book ............................. x
Typeface conventions ..................................... x
Operating system differences ............................. xi

Chapter 1. Installation overview ............................ 1
Supported platforms ....................................... 1
Disk and memory requirements ............................. 1
Installation packages ..................................... 2
Software prerequisites ................................... 2
   WebSEAL server prerequisites ........................ 2
   WebSEAL ADK prerequisites ............................ 3
Installation options ........................................ 3

Chapter 2. Using easy installation .......................... 5
WebSEAL easy installation programs ......................... 5
   Using the WebSEAL easy installation program ...... 6
   Using the WebSEAL ADK easy installation program . 7
Configuring WebSEAL using the easy installation programs . 8
   Obtaining configuration settings interactively ...... 8
   Obtaining configuration settings from response files . 10
Easy installation limitations ............................... 10

Chapter 3. Using native installation ......................... 13
Installing and configuring WebSEAL server on UNIX .... 13
   Installing WebSEAL server on AIX ................. 14
   Installing WebSEAL server on HP-UX ............ 15
   Installing WebSEAL server on Linux on zSeries 16
   Installing WebSEAL server on Solaris ............ 16
Configuring WebSEAL server on UNIX .................... 17
Installing the WebSEAL ADK on UNIX ..................... 19
   Installing the WebSEAL ADK on AIX ............... 19
   Installing the WebSEAL ADK on HP-UX .......... 20
   Installing the WebSEAL ADK on Linux on zSeries . 21
   Installing the WebSEAL ADK on Solaris .......... 21
Installing WebSEAL server and the WebSEAL ADK on Windows . 22
   Configuring WebSEAL server on Windows ......... 23

Chapter 4. Upgrading WebSEAL from version 3.8 to 4.1 .................. 25
Upgrading WebSEAL on AIX ................................ 25
Upgrading WebSEAL on HP-UX ............................ 26
Upgrading WebSEAL on Solaris ........................................... 28
Upgrading WebSEAL on Windows ........................................ 29

Chapter 5. Upgrading WebSEAL from version 3.9 to 4.1 ............... 31
Upgrading WebSEAL on AIX ................................................. 31
Upgrading WebSEAL on HP-UX .......................................... 32
Upgrading WebSEAL on Linux on zSeries ............................ 34
Upgrading WebSEAL on Solaris .......................................... 35
Upgrading WebSEAL on Windows ........................................ 36

Chapter 6. Unconfiguring and removing WebSEAL .................... 39
Unconfiguring WebSEAL on UNIX ........................................ 39
Unconfiguring WebSEAL on Windows ................................... 40
Removing WebSEAL from AIX ............................................ 41
Removing WebSEAL from HP-UX ........................................ 41
Removing WebSEAL from Linux on zSeries .......................... 42
Removing WebSEAL from Solaris ........................................ 42
Removing WebSEAL from Windows ..................................... 43
  Removing WebSEAL and WebSEAL ADK ......................... 43
  Removing WebSEAL ADK only ....................................... 43

Appendix. Notices ............................................................ 45
Trademarks ................................................................... 47
Preface

IBM® Tivoli® Access Manager WebSEAL is a security manager for Web-based resources. WebSEAL is a high performance, multi-threaded Web server that applies fine-grained security policy to the protected Web object space. WebSEAL can provide single sign-on solutions and incorporate back-end Web application server resources into its security policy.

Note: IBM 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.

The IBM Tivoli Access Manager WebSEAL Installation Guide explains how to install, configure, and upgrade Tivoli Access Manager WebSEAL software.

Who should read this book

The target audience for this installation guide includes:

- Security administrators
- Network system administrators
- IT architects
- Application developers

Readers should be familiar with:

- Internet protocols, including HTTP, TCP/IP, file transfer protocol (FTP), and telnet
- Deployment and management of Web servers
- Security management, including authentication and authorization

If you are enabling Secure Sockets Layer (SSL) communication, you also should be familiar with SSL protocol, key exchange (public and private), digital signatures, cryptographic algorithms, and certificate authorities.

What this book contains

This document contains the following chapters:

- **Chapter 1, “Installation overview”, on page 1**
  Lists the supported platforms and describes the software dependencies on the IBM Tivoli Access Manager Base.
- **Chapter 2, “Using easy installation”, on page 5**
  Describes how to use easy installation programs to expedite the installation and configuration of a WebSEAL server or WebSEAL ADK system.
- **Chapter 3, “Using native installation”, on page 13**
  Describes how to install and configure WebSEAL and prerequisite software using native operating system utilities.
- **Chapter 4, “Upgrading WebSEAL from version 3.8 to 4.1”, on page 25**
  Describes how to upgrade a Version 3.8 WebSEAL server to Version 4.1.
- **Chapter 5, “Upgrading WebSEAL from version 3.9 to 4.1”, on page 31**
Describes how to upgrade a Version 3.9 WebSEAL server to Version 4.1.

- **Chapter 6, “Unconfiguring and removing WebSEAL”, on page 39**
  Describes how to unconfigure and remove WebSEAL from each of the supported operating system platforms.

### Publications

The Tivoli Access Manager library is organized into the following categories:

- “Release information”
- “Base information”
- “WebSEAL information”
- “Web security information” on page vii
- “Developer references” on page vii
- “Technical supplements” on page vii

#### Release information

- **IBM Tivoli Access Manager Read Me First Card**
  GI11-4198-00 (am41_readme.pdf)
  Provides information for installing and getting started using Tivoli Access Manager.

- **IBM Tivoli Access Manager Release Notes**
  SC32-1130-00 (am41_relnotes.pdf)
  Provides late-breaking information, such as software limitations, workarounds, and documentation updates.

#### Base information

- **IBM Tivoli Access Manager Base Installation Guide**
  SC32-1131-01 (am41_install.pdf)
  Explains how to install, configure, and upgrade Tivoli Access Manager software, including the Web Portal Manager interface.

- **IBM Tivoli Access Manager Base Administrator’s Guide**
  SC32-1132-01 (am41_admin.pdf)
  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.

#### WebSEAL information

- **IBM Tivoli Access Manager WebSEAL Installation Guide**
  SC32-1133-01 (amweb41_install.pdf)
  Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application developer kit.

- **IBM Tivoli Access Manager WebSEAL Administrator’s Guide**
  SC32-1134-01 (amweb41_admin.pdf)
  Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.
Web security information

- **IBM Tivoli Access Manager for WebSphere Application Server User’s Guide**
  SC32-T136-01 (amwas41_user.pdf)
  Provides installation, removal, and administration instructions for Tivoli Access Manager for IBM WebSphere® Application Server.

- **IBM Tivoli Access Manager for WebLogic Server User’s Guide**
  SC32-T137-01 (amwls41_user.pdf)
  Provides installation, removal, and administration instructions for Tivoli Access Manager for BEA WebLogic Server.

- **IBM Tivoli Access Manager Plug-in for Edge Server User’s Guide**
  SC32-T138-01 (amedge41_user.pdf)
  Describes how to install, configure, and administer the plug-in for IBM WebSphere Edge Server application.

- **IBM Tivoli Access Manager Plug-in for Web Servers User’s Guide**
  SC32-T139-01 (amws41_user.pdf)
  Provides installation instructions, administration procedures, and technical reference information for securing your Web domain using the plug-in for Web servers.

Developer references

- **IBM Tivoli Access Manager Authorization C API Developer’s Reference**
  SC32-T140-01 (am41_authC_devref.pdf)
  Provides reference material that describes how to use the Tivoli Access Manager authorization C API and the Access Manager service plug-in interface to add Tivoli Access Manager security to applications.

- **IBM Tivoli Access Manager Authorization Java Classes Developer’s Reference**
  SC32-T141-01 (am41_authJ_devref.pdf)
  Provides reference information for using the Java™ language implementation of the authorization API to enable an application to use Tivoli Access Manager security.

- **IBM Tivoli Access Manager Administration C API Developer’s Reference**
  SC32-T142-01 (am41_adminC_devref.pdf)
  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 Administration Java Classes Developer’s Reference**
  SC32-T143-01 (am41_adminJ_devref.pdf)
  Provides reference information for using the Java language implementation of the administration API to enable an application to perform Tivoli Access Manager administration tasks.

- **IBM Tivoli Access Manager WebSEAL Developer’s Reference**
  SC32-T135-01 (amweb41_devref.pdf)
  Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Technical supplements

- **IBM Tivoli Access Manager Command Reference**
  GC32-T1107-01 (am41_cmdref.pdf)
Provides information about the command line utilities and scripts provided with Tivoli Access Manager.

- **IBM Tivoli Access Manager Error Message Reference**
  SC32-1144-01 (am41_error_ref.pdf)
  Provides explanations and recommended actions for the messages produced by Tivoli Access Manager.

- **IBM Tivoli Access Manager Problem Determination Guide**
  GC32-1106-01 (am41_pdg.pdf)
  Provides problem determination information for Tivoli Access Manager.

- **IBM Tivoli Access Manager Performance Tuning Guide**
  SC32-1145-01 (am41_perftune.pdf)
  Provides performance tuning information for an environment consisting of Tivoli Access Manager with the IBM Directory server defined as the user registry.

**Related publications**

This section lists publications related to the Tivoli Access Manager library.

The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at: [http://www.ibm.com/software/tivoli/library/](http://www.ibm.com/software/tivoli/library/)

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available, in English only, from the *Glossary* link on the left side of the Tivoli Software Library Web page [http://www.ibm.com/software/tivoli/library/](http://www.ibm.com/software/tivoli/library/)

**IBM Global Security Kit**

Tivoli Access Manager provides data encryption through the use of the IBM Global Security Kit (GSKit). GSKit is included on the IBM Tivoli Access Manager Base CD for your particular platform.

The GSKit package installs the iKeyman key management utility, gsk5ikm, which enables you to create key databases, public-private key pairs, and certificate requests. The following document is available on the Tivoli Information Center Web site in the same section as the IBM Tivoli Access Manager product documentation:

- **Secure Sockets Layer Introduction and iKeyman User’s Guide**
  (gsk1km5c.pdf)
  Provides information for network or system security administrators who plan to enable SSL communication in their Tivoli Access Manager environment.

**IBM DB2 Universal Database**

IBM DB2® Universal Database™ is required when installing IBM Directory Server, z/OS™, and OS/390® LDAP servers. DB2 is provided on the product CDs for the following operating system platforms:

- IBM AIX®
- Microsoft® Windows™
- Sun Solaris Operating Environment

DB2 information is available at: [http://www.ibm.com/software/data/db2/](http://www.ibm.com/software/data/db2/)
IBM Directory Server
IBM Directory Server, Version 4.1, is included on the IBM Tivoli Access Manager Base CD for all platforms except Linux for zSeries™. You can obtain the IBM Directory Server software for Linux for S/390 at:


If you plan to use IBM Directory Server as your user registry, see the information provided at:


IBM WebSphere Application Server
IBM WebSphere Application Server, Advanced Single Server Edition 4.0.3, is included on the Web Portal Manager CDs and installed with the Web Portal Manager interface. For information about IBM WebSphere Application Server, see:


IBM Tivoli Access Manager for Business Integration
IBM Tivoli Access Manager for Business Integration, available as a separately orderable product, provides a security solution for IBM MQSeries®, Version 5.2, and IBM WebSphere® MQ for Version 5.3 messages. IBM Tivoli Access Manager for Business Integration allows WebSphere MQSeries applications to send data with privacy and integrity by using keys associated with sending and receiving applications. Like WebSEAL and IBM Tivoli Access Manager for Operating Systems, IBM Tivoli Access Manager for Business Integration, is one of the resource managers that use the authorization services of IBM Tivoli Access Manager for e-business.

The following documents associated with IBM Tivoli Access Manager for Business Integration Version 4.1 are available on the Tivoli Information Center Web site:

• IBM Tivoli Access Manager for Business Integration Administrator’s Guide (SC23-4831-00)
• IBM Tivoli Access Manager for Business Integration Release Notes (GI11-0957-00)
• IBM Tivoli Access Manager for Business Integration Read Me First (GI11-0958-00)

IBM Tivoli Access Manager for Operating Systems
IBM Tivoli Access Manager for Operating Systems, available as a separately orderable product, provides a layer of authorization policy enforcement on UNIX systems in addition to that provided by the native operating system. IBM Tivoli Access Manager for Operating Systems, like WebSEAL and IBM Tivoli Access Manager for Business Integration, is one of the resource managers that use the authorization services of IBM Tivoli Access Manager for e-business.

The following documents associated with IBM Tivoli Access Manager for Operating Systems Version 4.1 are available on the Tivoli Information Center Web site:

• IBM Tivoli Access Manager for Operating Systems Installation Guide (SC23-4829-00)
• IBM Tivoli Access Manager for Operating Systems Administration Guide (SC23-4827-00)
• IBM Tivoli Access Manager for Operating Systems Problem Determination Guide (SC23-4828-00)
• IBM Tivoli Access Manager for Operating Systems Release Notes (GI11-0951-00)
• IBM Tivoli Access Manager for Operating Systems Read Me First (GI11-0949-00)
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](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**).

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.

Contacting 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 site: [http://techsupport.services.ibm.com/guides/handbook.html](http://techsupport.services.ibm.com/guides/handbook.html)

The guide provides the following information:
- Registration and eligibility requirements for receiving support
- Telephone numbers and e-mail addresses, 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 backslash (\) in directory paths. If you are using the bash shell on a Windows system, you can use the UNIX conventions.
Chapter 1. Installation overview

Before you begin installing Tivoli Access Manager WebSEAL or the WebSEAL application developer kit (ADK), you must become familiar with its components and installation options. This chapter includes the following sections:

- “Supported platforms”
- “Disk and memory requirements”
- “Installation packages” on page 2
- “Software prerequisites” on page 2
- “Installation options” on page 3

Attention

See the IBM Tivoli Access Manager Release Notes for last-minute information, including required fix packs and patches for each supported operating system platform.

Supported platforms

Tivoli Access Manager WebSEAL and the Tivoli Access Manager WebSEAL ADK are supported on the following platforms:

- Sun Solaris Operating System 2.7 and 2.8
- AIX 4.3.3 and 5.1.0
- Red Hat Linux 7.1 and 7.2
- SuSE Linux Enterprise Server 7 for S/390 and zSeries (Kernel 2.4.7, 31-bit, glibc 2.2.4-31, gcc 2.95.3-119) (with Maintenance Patch-CD 1)
- SuSE Linux Enterprise Server 7 for IBM zSeries (Kernel 2.4.17, 64-bit with 31-bit compatibility mode, glibc 2.2.4-12, gcc 2.95.3-61)
- HP-UX 11.0 and 11i
- Windows NT 4.0 (with Service Pack 6a)
- Windows 2000 Advanced Server (with Service Pack 2)

Disk and memory requirements

WebSEAL has the following hardware requirements:

- Disk space: 10 MB
  When combined with the prerequisite Tivoli Access Manager runtime (65 MB), the minimum required disk space is 75 MB.
  It is recommended that you reserve an additional 100 MB of disk space for WebSEAL log files.
- Memory: 64 MB Minimum (256 MB Recommended)
  Note that the 64 MB minimum is in addition to the 64 MB minimum needed by the Tivoli Access Manager runtime. A total memory of 256 MB or greater will produce optimum performance results.
Installation packages

The IBM Tivoli Access Manager Web Security CD contains installation packages for the following WebSEAL software:

- **Tivoli Access Manager WebSEAL**
  This package includes the WebSEAL server and configuration files.
- **Tivoli Access Manager WebSEAL ADK**
  This package contains development APIs for the Tivoli Access Manager Cross-domain Authentication Service (CDAS), the Tivoli Access Manager Cross-domain Mapping Framework (CDMF), and the Tivoli Access Manager Password Strength Module.

The Web Security CD also contains the following software prerequisite packages. (These packages are provided to allow you to complete the WebSEAL installation without requiring access to the IBM Tivoli Access Manager Base CDs.)

- **Tivoli Access Manager runtime**
- **IBM Directory client**
- **IBM Global Security Kit (GSKit)**
- **Tivoli Access Manager ADK**

Software prerequisites

The following sections list the software prerequisites for each of the WebSEAL packages:

- "WebSEAL server prerequisites” on page 2
- "WebSEAL ADK prerequisites” on page 3

**Note:** Software prerequisites and any necessary product patches are installed automatically when using easy installation scripts (UNIX) and batch files (Windows). For more information about easy installation, see “Installation options” on page 3.

WebSEAL server prerequisites

The following prerequisite software must be installed and configured on each computer that hosts a WebSEAL server:

- **IBM Global Security Kit (GSKit)**
- **IBM Directory client**
- **Tivoli Access Manager runtime**

You must establish a Tivoli Access Manager secure domain before installing WebSEAL or the WebSEAL ADK. To establish a secure domain, the following software must be installed and configured either on the same computer that hosts the WebSEAL server or on a remote computer:

- **Tivoli Access Manager policy server**
- **A supported LDAP server, such as IBM Directory server**

Thus, there are two deployment scenarios for the WebSEAL server:

1. **On the same computer** as the Tivoli Access Manager policy server
2. **On a different computer** from the Tivoli Access Manager policy server
In the first scenario, all of the WebSEAL prerequisites are satisfied during the installation and configuration of the policy server. Installation of the policy server requires installation of the Tivoli Access Manager runtime, the IBM Directory client, and GSKit. When you deploy WebSEAL in this configuration, you can simply install WebSEAL without installing any further prerequisites.

In the second scenario, you must first configure the computer into an existing secure domain, and then install the WebSEAL server. To configure the computer into the secure domain, you must install and configure the following software:

- IBM Global Security Kit (GSKit)
- IBM Directory client
- Tivoli Access Manager runtime

After you have configured the Tivoli Access Manager runtime, you can install and configure the WebSEAL server.

**Note:** The WebSEAL server has no dependencies on the Tivoli Access Manager authorization server. The authorization server is distributed as part of the IBM Tivoli Access Manager Base for your particular operating system.

**WebSEAL ADK prerequisites**

The following software must be installed and configured on the same computer as the WebSEAL ADK:

- IBM Global Security Kit (GSKit)
- IBM Directory client
- Tivoli Access Manager runtime
- Tivoli Access Manager ADK
- Tivoli Access Manager WebSEAL server

To install and use the WebSEAL ADK, you must first install and configure a WebSEAL server. In addition, you must install the Tivoli Access Manager ADK.

**Installation options**

Table 1 provides a quick summary of available installation options. Choose an installation option and follow instructions in the chapter listed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy installation</td>
<td>Use to expedite the installation and configuration of one or more Tivoli Access Manager WebSEAL systems in a secure domain using an LDAP-based registry. You cannot use easy installation if you are using Active Directory or Domino as your registry or if you installed Tivoli Access Manager on the Linux for zSeries platform.</td>
<td>See Chapter 2, “Using easy installation”, on page 5</td>
</tr>
</tbody>
</table>
Table 1. Installation options  (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native installation</td>
<td>Use to step through the installation and configuration of Tivoli Access Manager WebSEAL components using native operating system utilities.</td>
<td>Unlike the automated scripts used in easy installation, you must manually install each component and any prerequisite software in the appropriate order. See Chapter 3, “Using native installation”, on page 13.</td>
</tr>
</tbody>
</table>
Chapter 2. Using easy installation

Before you begin

- Install all operating system patches and review system requirements listed in the IBM Tivoli Access Manager Release Notes.
- Become familiar with the configuration decisions that you need to make during easy installation. For descriptions of easy installation configuration options, see Table 3 on page 9.
- To view status and messages in a language other than English (default), you must install a language support package before running easy installation scripts (UNIX) or batch files (Windows). For instructions about installing language support packages, see the IBM Tivoli Access Manager Base Installation Guide.

Easy installation makes it easy for you to install a WebSEAL server or WebSEAL development system by automatically installing software prerequisites at the same time. You can use the easy installation programs as an alternative to using operating system utilities such as pkgadd, installp, swinstall or InstallShield. Easy installation also detects when required products are installed and does not attempt to reinstall them.

Easy installation programs prompt you to supply the information necessary for installation and configuration of WebSEAL, WebSEAL ADK, and the prerequisite software. The programs provide default values when appropriate. After you supply the necessary configuration values, the easy installation program installs and configures products and the software prerequisites without any further intervention.

The easy installation programs save the configuration information supplied by the user into a data file called a response file. The easy installation programs can read the configuration settings from this file during future installations instead of prompting the user to supply them. This feature enables the easy installation program to be run in a non-interactive or silent mode.

The WebSEAL easy installation programs are useful in a variety of deployment scenarios. You can combine them with the easy installation program for the policy server to quickly install and configure WebSEAL into a single system in the Tivoli Access Manager secure domain. This can be useful for prototyping, application development, testing, or demonstration purposes. You can also use easy installation when deploying multiple WebSEAL servers. In this case, you can use the response files to expedite the deployment. In addition, the WebSEAL ADK easy installation program is useful for quickly setting up a WebSEAL development environment.

WebSEAL easy installation programs

Table 2 on page 6 lists easy installation programs, which are included in the root directory on the IBM Tivoli Access Manager Web Security CD for your particular platform.
**Table 2. Easy Installation Files**

<table>
<thead>
<tr>
<th>Script Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ezinstall_pdweb | Sets up a WebSEAL server system with the following software packages:  
|                 | • IBM Global Security Kit  
|                 | • IBM Directory client  
|                 | • Tivoli Access Manager runtime  
|                 | • Tivoli Access Manager WebSEAL server |
| ezinstall_pdwebadk | Sets up a WebSEAL development system with the following software packages:  
|                 | • IBM Global Security Kit  
|                 | • IBM Directory client  
|                 | • Tivoli Access Manager runtime  
|                 | • Tivoli Access Manager Application Development Kit  
|                 | • Tivoli Access Manager WebSEAL  
|                 | • Tivoli Access Manager WebSEAL Application Development Kit |
| ezinstall_pdauthadk | Sets up a Tivoli Access Manager development system with the following software packages:  
|                 | • IBM Global Security Kit  
|                 | • IBM Directory client  
|                 | • Tivoli Access Manager runtime  
|                 | • Tivoli Access Manager Application Development Kit |
| install_pdrte    | Sets up a Tivoli Access Manager runtime system with the following software packages:  
|                 | • IBM Global Security Kit  
|                 | • IBM Directory client  
|                 | • Tivoli Access Manager runtime |

The WebSEAL easy installation scripts are described in the following sections:

- [“Using the WebSEAL easy installation program” on page 6](#)
- [“Using the WebSEAL ADK easy installation program” on page 7](#)

**Using the WebSEAL easy installation program**

The **ezinstall_pdweb** program is typically used in one of the following scenarios:

- Creating a new Tivoli Access Manager secure domain in order to use WebSEAL to protect Web-based resources.

  In this case one computer will host both the Tivoli Access Manager policy server and the WebSEAL server. The policy server has a corresponding easy installation program called **ezinstall_pdmgr**. You should first use **ezinstall_pdmgr** to install and configure the policy server.

  The **ezinstall_pdmgr** program is distributed on the IBM Tivoli Access Manager Base CD for your operating system. To use this program, see the instructions in the [IBM Tivoli Access Manager Base Installation Guide](#).

- Adding a WebSEAL server onto a computer that already has the policy server installed and configured.
In this case, the Tivoli Access Manager secure domain has already been established, and you are now extending the domain security to use WebSEAL to secure Web-based resources. You need only run ezinstall_pdweb. The easy installation program prompts the user for the WebSEAL installation and configuration information.

• Adding a WebSEAL server when adding a new computer into the Tivoli Access Manager secure domain.

In this case, the WebSEAL server will run on a computer that does not host the policy server, but instead will communicate with a remote policy server over the network. Computers in this role require that the IBM Tivoli Access Manager runtime be installed and configured to establish communication with the remote policy server. This is a prerequisite to installing WebSEAL.

The WebSEAL easy installation script ezinstall_pdweb will detect whether or not the runtime has been installed and configured.

Using the WebSEAL ADK easy installation program

The ezinstall_pdwebadk program is typically used in one of the following scenarios:

• Installing a WebSEAL development environment as part of creating a new Tivoli Access Manager secure domain in order to use WebSEAL to protect Web-based resources.

In this case one computer will host the Tivoli Access Manager policy server, the WebSEAL server, and the WebSEAL ADK. The policy server has a corresponding easy installation program called ezinstall_pdmgr. You should first use ezinstall_pdmgr to install and configure the policy server, and then use ezinstall_pdwebadk to install and configure WebSEAL and WebSEAL ADK.

Note: On Windows NT only, you must first run ezinstall_pdweb.bat to install the WebSEAL server and then run ezinstall_pdwebadk.bat to install the WebSEAL ADK. On Windows 2000 and on all UNIX platforms, you need only run ezinstall_pdwebadk.bat to install both WebSEAL and WebSEAL ADK.

The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK package. This package is distributed on the IBM Tivoli Access Manager Web Security CD and has its own easy installation program, ezinstall_pdauthadk. The ezinstall_pdwebadk program automatically calls ezinstall_pdauthadk if the ADK has not already been installed.

• Adding a WebSEAL server and development environment onto a computer that already has the policy server installed and configured.

In this case, the Tivoli Access Manager secure domain has already been established, and you are adding WebSEAL to secure Web-based resources, and adding a WebSEAL development environment. You need only run ezinstall_pdwebadk. The easy installation program calls ezinstall_pdauthadk if necessary to install the prerequisite ADK development environment, and then prompts the user for both the WebSEAL and WebSEAL ADK installation and configuration information.

Note: On Windows NT only, you must first run ezinstall_pdweb to install the WebSEAL server and then run ezinstall_pdwebadk to install the WebSEAL ADK. On Windows 2000 and on all UNIX platforms, you need only run ezinstall_pdwebadk to install both WebSEAL and WebSEAL ADK.
Adding a WebSEAL server and WebSEAL development environment when adding a new computer into the Tivoli Access Manager secure domain.

In this case, the WebSEAL server and WebSEAL ADK will run on a computer that does not host the policy server, but instead will communicate with a remote policy server over the network. Computers in this role require that the IBM Tivoli Access Manager runtime be installed and configured to establish communication with the remote policy server. This is a prerequisite to installing WebSEAL. These computers must also have the IBM Tivoli Access Manager ADK package installed as a prerequisite to using the WebSEAL ADK.

The `ezinstall_pdwebadk` program automatically checks for each software prerequisite. The easy installation program prompts the user for installation and configuration settings for each of the following packages, unless each is already configured:

- IBM Global Security Kit
- IBM Directory client
- Tivoli Access Manager runtime
- Tivoli Access Manager ADK
- Tivoli Access Manager WebSEAL

The easy installation program then installs and configures the WebSEAL ADK.

**Note:** On Windows NT only, you must first run `ezinstall_pdweb` to install the WebSEAL server and then run `ezinstall_pdwebadk` to install the WebSEAL ADK. On Windows 2000 and on all UNIX platforms, you need only run `ezinstall_pdwebadk` to install both WebSEAL and WebSEAL ADK.

---

**Configuring WebSEAL using the easy installation programs**

The easy installation programs can obtain the necessary configuration settings in two different ways. The first time a program is run, it prompts the user to supply all necessary configuration settings.

When the installation is complete, the easy installation programs save the settings in a data file called a `response` file. The next time, and all subsequent times that the easy installation program is called on the same computer, the program gives the user the option of using the saved data from the response file, instead of entering the configuration information at a command prompt.

These two methods of using the easy installation programs are described in the following sections:

- “Obtaining configuration settings interactively” on page 8
- “Obtaining configuration settings from response files” on page 10

---

**Obtaining configuration settings interactively**

The WebSEAL and WebSEAL ADK easy installation programs prompt for all necessary configuration information. When any software prerequisites have not been installed, the WebSEAL and WebSEAL ADK easy installation programs prompt for the necessary information.

The only exception is the prerequisite that WebSEAL has on the installation and configuration of a Tivoli Access Manager policy server on one system in the secure domain. If you are creating a new secure domain, you must satisfy this
dependence by running the policy server’s own easy installation program. This program is distributed on the IBM Tivoli Access Manager Base CDs.

Table 3 lists configuration information that you may need to provide when installing WebSEAL or WebSEAL ADK. Note that some of the information is needed to configure the prerequisite runtime. It is a good idea to identify these values before you are prompted during installation.

**Note:** The WebSEAL easy installation program uses default values for some of the WebSEAL configuration settings. You cannot change these settings. See “Easy installation limitations” on page 10.

**Table 3. Easy Installation Configuration Options**

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IBM Global Security Kit</strong></td>
<td>No configuration parameters are required.</td>
</tr>
<tr>
<td><strong>IBM Directory Client</strong></td>
<td>No configuration parameters are required. Communication with the LDAP server is configured during the runtime configuration.</td>
</tr>
<tr>
<td><strong>Tivoli Access Manager runtime</strong></td>
<td></td>
</tr>
<tr>
<td>Registry Type</td>
<td>Default: Ldap</td>
</tr>
<tr>
<td>LDAP Server Hostname</td>
<td>No default. Use a fully qualified domain name.</td>
</tr>
<tr>
<td>LDAP Server Port</td>
<td>Default: 389</td>
</tr>
<tr>
<td>Tivoli Access Manager policy server Hostname</td>
<td>No default. Use a fully qualified domain name.</td>
</tr>
<tr>
<td>LDAP DN for GSO Database</td>
<td>No default.</td>
</tr>
<tr>
<td>Enable SSL with LDAP server</td>
<td>Default is No.</td>
</tr>
<tr>
<td>LDAP SSL Keyfile</td>
<td>Full path to key database location.</td>
</tr>
<tr>
<td>LDAP SSL Keyfile DN</td>
<td>Key database file label.</td>
</tr>
<tr>
<td>LDAP SSL Keyfile Password</td>
<td>Key database file password.</td>
</tr>
<tr>
<td>LDAP Server SSL Port</td>
<td>Default: 636</td>
</tr>
<tr>
<td>Installation Directory</td>
<td>UNIX: /opt/pdweb</td>
</tr>
<tr>
<td></td>
<td>Windows: C:\Program Files\Tivoli\Policy Director</td>
</tr>
<tr>
<td>Access Manager Policy Server Hostname</td>
<td>No default. Use a fully qualified domain name.</td>
</tr>
<tr>
<td>SSL Server Port</td>
<td>Default: 7135</td>
</tr>
<tr>
<td>Policy Server CA Certificate Filename</td>
<td>No default.</td>
</tr>
<tr>
<td><strong>Tivoli Access Manager ADK</strong></td>
<td>No configuration parameters are required.</td>
</tr>
<tr>
<td><strong>Tivoli Access Manager WebSEAL</strong></td>
<td></td>
</tr>
<tr>
<td>Security Master Password</td>
<td>No default.</td>
</tr>
<tr>
<td>Enable SSL communication with LDAP Server</td>
<td>Default is No.</td>
</tr>
</tbody>
</table>
Table 3. Easy Installation Configuration Options (continued)

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP SSL Client Key File</td>
<td>Key database file location. No default. Example pathname: /var/ldap/keytabs/pd_ldapkey.kdb</td>
</tr>
<tr>
<td>SSL Client Certificate Label</td>
<td>No default</td>
</tr>
<tr>
<td>SSL Client Key File Password</td>
<td>No default</td>
</tr>
<tr>
<td>LDAP Server SSL port number</td>
<td>Default: 636</td>
</tr>
<tr>
<td>Tivoli Access Manager WebSEAL ADK</td>
<td>No configuration settings are required.</td>
</tr>
</tbody>
</table>

Obtaining configuration settings from response files

When you run the easy installation programs in interactive mode, your responses to prompts are saved into a data file called a response file. The name and location of the UNIX response files include:
/var/tmp/ezinstall_pdweb.rsp
/var/tmp/ezinstall_pdwebadk.rsp

The Windows platform uses only one response file:
%TEMP%\ezinstall.rsp

You can use the saved response file as automated input when you run the easy installation program later. This feature enables a non-interactive or silent installation. This feature is useful when deploying a series of WebSEAL servers within one secure domain. You can edit the response file to set values specific to a particular server, and then execute the script to complete a non-interactive installation.

Each time an easy installation program runs, it checks to see if a response file already exists. If a response file is found, the easy installation program asks if you want to use it. If you choose to use the response file, the easy installation program prompts you for the necessary passwords, and then completes the installation by reading the configuration settings from the response file.

The easy installation program does not save passwords because of the security risk of storing a password in clear text. You can use a text editor to add this information to the file.

You must edit the response file for the following values:
- Administrator password
- SSL Keyfile Password (optional)

This password is used only when you choose to configure SSL communication between the WebSEAL server and the LDAP server.

Easy installation limitations

When using the easy installation programs be aware of the following limitations:
- You cannot use the easy installation programs when upgrading WebSEAL from Version 3.8 or Version 3.9 to Version 4.1.
- You cannot use the `ezinstall_pdweb` program when you want to configure WebSEAL to use non-default values for the following WebSEAL configuration settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TCP HTTP</td>
<td>Yes</td>
</tr>
<tr>
<td>TCP Port Number</td>
<td>80</td>
</tr>
<tr>
<td>Enable HTTPS</td>
<td>yes</td>
</tr>
<tr>
<td>HTTPS Port Number</td>
<td>443</td>
</tr>
<tr>
<td>Web document root hierarchy</td>
<td>UNIX: <code>/opt/pdweb/www/docs</code></td>
</tr>
<tr>
<td></td>
<td>Windows: <code>C:\Program Files\Tivoli\PolicyDirector\PDWeb\www\docs</code></td>
</tr>
</tbody>
</table>
Chapter 3. Using native installation

This chapter provides instructions for installing and configuring the Tivoli Access Manager WebSEAL packages using native installation utilities. This chapter also provides instructions for installing the software prerequisites for each WebSEAL package.

Note: If you are upgrading WebSEAL from a previous version of Tivoli Access Manager, do not use this chapter. See either Chapter 5, “Upgrading WebSEAL from version 3.9 to 4.1”, on page 31 or Chapter 4, “Upgrading WebSEAL from version 3.8 to 4.1”, on page 25.

The WebSEAL product consists of two packages:

• WebSEAL server
• WebSEAL ADK

You can install the WebSEAL server without installing the WebSEAL ADK. If you want to install the WebSEAL ADK, you must install the WebSEAL server as a prerequisite.

Both the WebSEAL server and the WebSEAL ADK require that the Tivoli Access Manager runtime is installed and configured. In addition, the WebSEAL ADK requires that the Tivoli Access Manager ADK is installed.

Note: For complete installation instructions and configuration options for the Tivoli Access Manager runtime and the Tivoli Access Manager ADK, see the IBM Tivoli Access Manager Base Installation Guide.

This chapter contains separate sections for installing and configuring WebSEAL server and WebSEAL ADK on each supported UNIX system. You must complete the UNIX section for installing WebSEAL server before you use the UNIX section for installing the WebSEAL ADK.

Instructions for installing and configuring WebSEAL server and the WebSEAL ADK on Windows are included in one section.

Note: As an alternative to the instructions in this chapter, you may be able to use easy installation programs. For more information, see Chapter 2, “Using easy installation”, on page 5.

To install WebSEAL, see the instructions in the appropriate section below:

• “Installing and configuring WebSEAL server on UNIX” on page 13
• “Installing the WebSEAL ADK on UNIX” on page 19
• “Installing WebSEAL server and the WebSEAL ADK on Windows” on page 22

Installing and configuring WebSEAL server on UNIX

To install a WebSEAL server on a UNIX system, complete the instructions in the appropriate section:

• “Installing WebSEAL server on AIX” on page 14
• “Installing WebSEAL server on HP-UX” on page 15
After you install the WebSEAL server package, you must configure the WebSEAL server by using the instructions in the following section:

**Installing WebSEAL server on AIX**

The WebSEAL installation separates file extraction from package configuration. Use the `installp` utility to install software packages on AIX. Then use the Tivoli Access Manager configuration utility `pdconfig` to configure WebSEAL.

**Note:** If you have already installed and configured WebSEAL and need to reinstall it, you must first unconfigure and remove the WebSEAL package. For instructions, see Chapter 6, "Unconfiguring and removing WebSEAL", on page 39.

To install a WebSEAL server on AIX, complete the following instructions:

1. Log in as **root**.
2. Verify that any required patches for your version of the AIX operating system are installed before continuing. Refer to the IBM Tivoli Access Manager Release Notes for complete software prerequisite information.
3. Determine if this computer has the Tivoli Access Manager runtime configured. The runtime will be configured if the Tivoli Access Manager policy server is installed on this computer, or if the computer has previously been added to the Tivoli Access Manager secure domain.
4. Do one of the following:
   - If this computer already has the runtime configured, skip to step 5.
   - If this computer does not have the Tivoli Access Manager runtime configured, install and configure the necessary software prerequisites by completing platform-specific instructions in the IBM Tivoli Access Manager Base Installation Guide.
5. Insert the IBM Tivoli Access Manager Web Security for AIX CD and then enter the following command to install the WebSEAL server package:

   ```bash
   installp -c -a -g -X -d /dev/cd0 PDWeb.Web
   ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c</code></td>
<td>Commits all specified updates that are currently applied but not committed.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Applies one or more software products or updates. This is the default action. This flag can be used with the <code>-c</code> flag to apply and commit a software product update when installed.</td>
</tr>
<tr>
<td><code>-g</code></td>
<td>When used to install or commit, this flag automatically installs or commits, respectively, any software products or updates that are prerequisites of the specified software product.</td>
</tr>
<tr>
<td><code>-X</code></td>
<td>Attempts to expand any file systems where there is insufficient space to do the installation.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Specifies where the installation media can be found. For example: <code>/dev/cd0</code></td>
</tr>
</tbody>
</table>

6. The WebSEAL files are installed. The Results section of the Installation Summary table indicates SUCCESS for each package successfully installed.
7. To configure the WebSEAL server, see "Configuring WebSEAL server on UNIX" on page 17.

Installing WebSEAL server on HP-UX

The WebSEAL installation separates file extraction from package configuration. Use swinstall to install software packages on HP-UX. Then use the Tivoli Access Manager configuration utility pdconfig to configure WebSEAL.

**Note:** If you have already installed and configured WebSEAL and need to reinstall it, you must first unconfigure and remove the WebSEAL package. For instructions, see Chapter 6, “Unconfiguring and removing WebSEAL”, on page 39.

To install a WebSEAL server on HP-UX, complete the following steps:

1. Log in as user **root**.
2. Verify that any required patches for your version of the HP-UX operating system are installed before continuing. Refer to the IBM Tivoli Access Manager Release Notes for complete software prerequisite information.
3. Insert the IBM Tivoli Access Manager Web Security for HP-UX CD in the drive.
4. Start **pfs_mountd** and then **pfsd** in the background, if they are not running. Mount the CD with the **pfs_mount** command. For example, enter the following:
   ```
   /usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cdrom
   ```
   where /dev/dsk/c0t0d0 is the CD device and /cdrom is the mount point.
5. Determine if this computer already has the Tivoli Access Manager runtime configured. The runtime will already be configured if the Tivoli Access Manager policy server is installed on this computer, or if the computer has previously been added to the secure domain.
6. Do one of the following:
   - If this computer already has the runtime configured, skip to step 7.
   - If this computer does not have the Tivoli Access Manager runtime configured, install and configure the necessary software prerequisites by completing platform-specific instructions in the IBM Tivoli Access Manager Base Installation Guide.
7. Enter the following command to install the WebSEAL server package:
   ```
   swinstall -s /cdrom/hp PDWeb
   ```
   where /cdrom/hp is the directory and PDWeb specifies the WebSEAL server package.
   A message appears indicating that the analysis phase has succeeded. Another message appears indicating that the execution phase is beginning.
   Files are extracted from the CD and installed on the hard disk. A message appears indicating that the execution phase has succeeded.
   The swinstall utility exits.
8. To configure the WebSEAL server, see "Configuring WebSEAL server on UNIX" on page 17.
Installing WebSEAL server on Linux on zSeries

The WebSEAL installation separates file extraction from package configuration. Use `rpm` to install software packages on Linux on zSeries. Then use the Access Manager configuration utility `pdconfig` to configure WebSEAL.

**Note:** If you have already installed and configured WebSEAL and need to reinstall it, you must first unconfigure and remove the WebSEAL package. For instructions, see Chapter 6, “Unconfiguring and removing WebSEAL”, on page 39.

To install a WebSEAL server on Linux on zSeries, complete the following instructions:

1. Log in as user `root`.
2. Verify that any required patches for your version of the Linux on zSeries operating system are installed before continuing. Refer to the [IBM Tivoli Access Manager Release Notes](#) for complete software prerequisite information.
3. Obtain access to the Access Manager WebSEAL for Linux on zSeries `rpm` files. Note that Linux on zSeries does not support attachment of a CD drive at this time. Use one of the following methods to obtain the necessary files:
   - Load the WebSEAL for Linux on zSeries files onto another workstation. Use `ftp` to transfer the files to a directory on the Linux for zSeries machine.
   - Mount the *IBM Tivoli Access Manager for Linux on zSeries* CD on another workstation. Then use NFS to access it from the Linux on zSeries machine. The WebSEAL files are located on the CD in the following directory: `/zSeries`
4. Determine if this computer already has the Tivoli Access Manager runtime configured. The runtime will already be configured if the Tivoli Access Manager policy server is installed on this computer, or if the computer has previously been added to the Tivoli Access Manager secure domain.
5. Do one of the following:
   - If this computer already has the runtime configured, skip to step 6.
   - If this computer does not have the runtime configured, install and configure the necessary software prerequisites by completing platform-specific instructions in the *IBM Tivoli Access Manager Base Installation Guide*.
6. Enter the following command to install the WebSEAL server package:
   ```
   rpm -i PDWeb-PD-4.1.0-0.s390.rpm
   ```
   Files are extracted from the CD and installed on the hard disk. The `rpm` utility exits.
7. To configure the WebSEAL server, see “Configuring WebSEAL server on UNIX” on page 17.

Installing WebSEAL server on Solaris

The WebSEAL installation separates file extraction from package configuration. Use `pkgadd` to install software packages on Solaris. Then use the Tivoli Access Manager configuration utility `pdconfig` to configure WebSEAL.

**Note:** If you have already installed and configured WebSEAL and need to reinstall it, you must first unconfigure and remove the WebSEAL package. For instructions, see Chapter 6, “Unconfiguring and removing WebSEAL”, on page 39.
To install a WebSEAL server on Solaris, complete the following instructions:

1. Log in as user root.

2. Verify that any required patches for your version of the Solaris operating system are installed before continuing. Refer to the IBM Tivoli Access Manager Release Notes for complete software prerequisite information.

3. Mount the IBM Tivoli Access Manager Web Security for Solaris CD on /cdrom/cdrom0.

4. Change directory to /cdrom/cdrom0/solaris.

5. Determine if this computer has the Tivoli Access Manager runtime configured. The runtime will be configured if the Tivoli Access Manager policy server is installed on this computer, or if the computer has previously been added to the secure domain.

6. Do one of the following:
   - If this computer already has the runtime configured, skip to step 7.
   - If this computer does not have the Tivoli Access Manager runtime configured, install and configure the necessary software prerequisites by completing platform-specific instructions in the IBM Tivoli Access Manager Base Installation Guide.

7. Enter the following command to install the WebSEAL server package:
   pkgadd -d . PDWeb

   A message asks, "Do you want to install these as setuid/setgid".

8. Type y and press Enter.
   When prompted to continue, type y and press Enter.
   Files are extracted from the CD and installed on the hard disk.
   A message appears indicating that installation of the WebSEAL package was successful. The pkgadd utility exits.

9. To configure the WebSEAL server, see on page 17 "Configuring WebSEAL server on UNIX"

**Configuring WebSEAL server on UNIX**

Use the Tivoli Access Manager configuration utility pdconfig to configure WebSEAL on a UNIX platform. The configuration steps for the WebSEAL server are identical on all UNIX platforms.

To configure a WebSEAL server on a UNIX system, complete the following instructions:

1. As root, enter the following command at a UNIX shell prompt:
   pdconfig

   The Access Manager for e-business Setup Menu appears.

   Access Manager for e-business Setup Menu

   1. Configure Package
   2. Unconfigure Package
   3. Display Configuration Status
   x. Exit

   Please select the menu item [x]:

2. Type 1 for Configure Package.
   The Access Manager for e-business Configuration Menu appears.
Access Manager for e-business Configuration Menu

1. Access Manager WebSEAL Configuration
   x. Return to Access Manager for e-business Setup Menu

Please select the menu item [x]:

3. Type the menu number for **Access Manager WebSEAL Configuration**.

The Access Manager WebSEAL for e-business Setup Menu appears.

Access Manager WebSEAL for e-business Setup Menu

1. Configure
   2. Display Configuration Status
   x. Exit

Please select the menu item [x]:

4. Type 1 for **Configure** and press Enter.

   A prompt appears requesting you to enter the password of the Tivoli Access
   Manager Administrator.

5. Enter the password for **sec_master**.

   **Troubleshooting Note:** If you repeatedly enter an incorrect password, you
   may see the error message: Error: This account has been temporarily
   locked out due to too many failed login attempts. If this occurs, obtain the
   correct password, wait five minutes for the lock to clear, and then restart
   *pdconfig*.

   You are prompted to enable SSL communication between the WebSEAL server
   and the LDAP server.

6. Type *y* (yes) or *n* (no) to enable SSL communication between the Access
   Manager server and the LDAP server.

   Do you want to enable SSL communication between the
   Access Manager server and the LDAP server (y/n) [Yes]?

   Go to step 7 if you want secure SSL communication between the WebSEAL
   instance and the LDAP server.

   Go to step 8 if you do not want secure SSL communication between the
   WebSEAL instance and the LDAP server.

7. Type *y* (yes) only if you want secure SSL communication between the
   WebSEAL instance and the LDAP server. Type the following information
   (press Enter for each entry):

   - Enter the location of the LDAP SSL Client Key File:
   - Enter the SSL Client Certificate Label (if required):
   - Enter the LDAP SSL Client Key File Password:
   - Enter the LDAP Server SSL Port Number:

   The client certificate label is usually not required. This label is needed only
   when the LDAP server is configured to ask for client-side certificates.
   Typically, LDAP servers require only server-side certificates. If your LDAP
   server does not require client-side certificates, you can just press Enter at this
   prompt.

   The default LDAP server SSL port is 636.

8. Type *n* (no) if you do not want secure SSL communication between the
   WebSEAL instance and the LDAP server. Press Enter.
9. Check the Web server configuration values. Modify any that need to be changed. In most cases, you can accept the default values. The following screen dialog appears:

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

Note: If you are running any other Web servers on this computer (such as IBM HTTP Server), verify that the TCP HTTP port for the other servers does not conflict with the WebSEAL TCP HTTP port. In general, if there is any conflict with the port number, the pdconfig utility detects the conflict and increments the port number choice.

10. When you are satisfied that the configuration is correct, type the letter a to accept the configuration and continue the installation. Press Enter.

Several status messages appear as the WebSEAL server is configured.
When the configuration is complete, a status message indicates that the WebSEAL server is starting.

11. Press Enter to continue.

The Access Manager WebSEAL for e-business Setup Menu appears.

12. Press Enter to select the default choice of x to exit the utility.

Note: Tivoli Access Manager WebSEAL supports multiple instances of WebSEAL servers on each host computer. See the IBM Tivoli Access Manager WebSEAL Administrator’s Guide for information on configuring multiple instances of WebSEAL servers.

Installing the WebSEAL ADK on UNIX

This section contains instructions for installing the WebSEAL ADK on each of the supported UNIX platforms. The WebSEAL ADK requires that the Tivoli Access Manager ADK is installed.

Note: The WebSEAL ADK has a prerequisite on the WebSEAL server. If you have not yet installed a WebSEAL server on this computer, go to “Installing and configuring WebSEAL server on UNIX” on page 13

To install the WebSEAL ADK, follow the instructions in the appropriate section:
• “Installing the WebSEAL ADK on AIX” on page 19
• “Installing the WebSEAL ADK on HP-UX” on page 20
• “Installing the WebSEAL ADK on Linux on zSeries” on page 21
• “Installing the WebSEAL ADK on Solaris” on page 21

Installing the WebSEAL ADK on AIX

To install the WebSEAL ADK on AIX, complete the following instructions:

1. Verify that the WebSEAL server package has been installed and configured. If the WebSEAL server has not been installed, complete the instructions in “Installing WebSEAL server on AIX” on page 14
2. Verify that you are logged in as root and that the IBM Tivoli Access Manager Web Security for AIX CD is in the CD drive.

3. The WebSEAL ADK requires that the Tivoli Access Manager ADK is installed first. If the Tivoli Access Manager ADK is already installed, skip this step. If this ADK is not currently installed, enter the following command:

   `installp -c -a -g -X -d /dev/cd0 PD.AuthADK`

   The ADK files are installed. The Results section of the Installation Summary table indicates SUCCESS for each package successfully installed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c</code></td>
<td>Commits all specified updates that are currently applied but not committed.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Applies one or more software products or updates. This is the default action. This flag can be used with the <code>-c</code> flag to apply and commit a software product update when installed.</td>
</tr>
<tr>
<td><code>-g</code></td>
<td>When used to install or commit, this flag automatically installs or commits, respectively, any software products or updates that are prerequisites of the specified software product.</td>
</tr>
<tr>
<td><code>-X</code></td>
<td>Attempts to expand any file systems where there is insufficient space to do the installation.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Specifies where the installation media can be found. For example: <code>/dev/cd0</code></td>
</tr>
</tbody>
</table>

4. Enter the following command to install the WebSEAL ADK:

   `installp -c -a -g -X -d . PDWeb.ADK`

   The WebSEAL ADK files are installed. The Results section of the Installation Summary table indicates SUCCESS for each package successfully installed.

   The WebSEAL ADK does not require any configuration. Installation of the WebSEAL ADK is now complete.

**Installing the WebSEAL ADK on HP-UX**

To install the WebSEAL ADK on HP-UX, complete the following instructions:

1. Verify that the WebSEAL server package has been installed and configured. If a WebSEAL server has not been installed, complete the instructions in “Installing WebSEAL server on HP-UX” on page 15.

2. Verify that you are logged in as root

3. Insert the IBM Tivoli Access Manager Web Security for HP-UX CD in the drive.

4. Start `pfs_mountd` and then `pfsd` in the background, if they are not running. Mount the CD with the `pfs_mount` command. For example, enter the following:

   `/usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cdrom`

   where `/dev/dsk/c0t0d0` is the CD device and `/cdrom` is the mount point.

5. The WebSEAL ADK requires that the Tivoli Access Manager ADK is installed first. If the Tivoli Access Manager ADK is already installed, skip this step. If this ADK is not currently installed, enter the following command:

   `swinstall -s /cdrom/hp PDAuthADK`
When prompted to continue, type y and press Enter. Files are extracted from the CD and installed on the hard disk. A status message appears indicating that installation of the Tivoli Access Manager ADK package was successful. The swinstall utility exits.

6. Enter the following command to install the WebSEAL ADK:

```bash
swinstall -s /cdrom/hp PDWebADK
```

When prompted to continue, type y and press Enter. Files are extracted from the CD and installed on the hard disk. A status message appears indicating that installation of the WebSEAL ADK package was successful. The swinstall utility exits.

The WebSEAL ADK does not require any configuration. Installation of the WebSEAL ADK is now complete.

### Installing the WebSEAL ADK on Linux on zSeries

To install the WebSEAL ADK, complete the following instructions:

1. Verify that the WebSEAL server package has been installed and configured.
   - If the WebSEAL server has not been installed, complete the instructions in “Installing WebSEAL server on Linux on zSeries” on page 16

2. Verify the following information:
   - You are logged in as root.
   - You can access the rpm packages from the IBM Tivoli Access Manager Web Security for Linux on zSeries CD. Note that this CD cannot be mounted on the Linux for zSeries machine. For access instructions, see “Installing and configuring WebSEAL server on UNIX” on page 13

   The installation packages are located in the /zSeries directory on the CD.

3. The WebSEAL ADK requires that the Tivoli Access Manager ADK is installed first. If the Tivoli Access Manager ADK is already installed, skip this step. If this ADK is not currently installed, enter the following command:

   ```bash
   rpm -i PDAuthADK*.rpm
   ```

   Files are extracted from the CD and installed on the hard disk. The rpm utility exits.

4. Enter the following command to install the WebSEAL ADK:

   ```bash
   rpm -i PDWebADK-PD-4.1.0-0.s390.rpm
   ```

   Files are extracted from the CD and installed on the hard disk. The rpm utility exits.

The WebSEAL ADK does not require any configuration. Installation of the WebSEAL ADK is now complete.

### Installing the WebSEAL ADK on Solaris

To install the WebSEAL ADK on Solaris, complete the following instructions:

1. Verify that the WebSEAL server package has been installed and configured.
   - If the WebSEAL server has not been installed, complete the instructions in “Installing WebSEAL server on Solaris” on page 16

2. Verify the following information:
   - You are logged in as root.
The IBM Tivoli Access Manager Web Security for Solaris CD is mounted on /cdrom/cdrom0.

The current directory is: /cdrom/cdrom0/solaris

3. The WebSEAL ADK requires that the Tivoli Access Manager ADK is installed first. If the Tivoli Access Manager ADK is already installed, skip this step. If this ADK is not currently installed, enter the following command:

```bash
pkgadd -d . PDAuthADK
```

When prompted to continue, type y and press Enter. Files are extracted from the CD and installed on the hard disk. A status message appears indicating that installation of the Tivoli Access Manager ADK package was successful. The pkgadd utility exits.

4. Enter the following command to install the WebSEAL ADK:

```bash
pkgadd -d . PDWebADK
```

When prompted to continue, type y and press Enter. Files are extracted from the CD and installed on the hard disk. A status message appears indicating that installation of the WebSEAL ADK package was successful. The pkgadd utility exits.

The WebSEAL ADK does not require any configuration. Installation of the WebSEAL ADK is now complete.

## Installing WebSEAL server and the WebSEAL ADK on Windows

The WebSEAL installation separates file extraction from package configuration. Use an InstallShield program to install the WebSEAL files. Next, use the pdconfig configuration utility to configure the WebSEAL server.

**Note:** If you have already installed and configured WebSEAL and need to reinstall it, you must first unconfigure and remove the WebSEAL package. For instructions, see [Chapter 6, “Unconfiguring and removing WebSEAL”](#), on page 39.

To install and configure WebSEAL on Windows, complete the following instructions:

1. Log in to the Windows domain as a user with Windows administrator privileges.
2. Verify that any required patches for your version of the Windows operating system are installed before continuing. Refer to the [IBM Tivoli Access Manager Release Notes](#) for complete software prerequisite information.
3. Insert the IBM Tivoli Access Manager Web Security for Windows CD into the CD drive.
4. Determine if this computer has the runtime configured. The runtime will be configured if the policy server is installed on this computer, or if the computer has previously been added to the secure domain.
5. Do one of the following:
   - If this computer already has the runtime configured, skip to step 6 on page 23.
   - If this computer does not have the runtime configured, install and configure the necessary software prerequisites by completing platform-specific instructions in the [IBM Tivoli Access Manager Base Installation Guide](#).
Additionally, if you want to install the WebSEAL ADK, you must install the prerequisite Tivoli Access Manager ADK. Refer to the [IBM Tivoli Access Manager Base Installation Guide](#) for complete instructions.

6. Run the WebSEAL InstallShield setup program by double-clicking on the following file (where the letter E: in the following command represents the CD drive):

```
E:\Windows\PolicyDirector\Disk Images\Disk1\WebSEAL\Disk Images\Disk 1\setup.exe
```

The Choose Setup Language dialog box appears.

7. Select the appropriate language and click **OK**.

The InstallShield program starts and the Welcome dialog box appears.

8. Click **Next**.

The License Agreement dialog box appears.

9. Click **Yes** to accept the License Agreement.

The Choose Destination Location dialog box appears.

10. Accept the default or click **Browse** to specify an alternative location. Click **Next**.

The Select Components dialog box appears.

11. Select the check box for each package that you want to install:

   - **PDWeb**
     This package contains the WebSEAL server and utilities. By default, this package is pre-checked.
   - **PDWebADK**
     This package contains WebSEAL ADKs. You must select this check box if you want to install this package. You must first install **PDAuthADK** before you can install the **PDWebADK** package. Installation of **PDWebADK** will fail if **PDAuthADK** has not been previously installed.

12. Click **Next**.

The files for the selected packages are extracted to the disk. A message appears indicating that the packages have been installed.

13. Click **Finish** to exit the InstallShield program.

14. To configure the WebSEAL server, see "Configuring WebSEAL server on Windows" on page 23.

### Configuring WebSEAL server on Windows

To configure a WebSEAL server, complete the following instructions. The WebSEAL ADK does not require any configuration.

1. Log in to the Windows domain as a user with Windows administrator privileges.
2. Select **Start → Programs → Access Manager for e-business → Configuration**.

   The Access Manager for e-business Configuration dialog box appears.
3. Select **Access Manager WebSEAL** and click **Configure**.

   The Access Manager WebSEAL for e-business Configuration dialog box appears.
4. Select Default WebSEAL and click **Configure**.

   The Access Manager Administrator Password dialogue box appears.
5. Enter the password for **sec_master** and click **OK**.

   **Troubleshooting Note:** If you repeatedly enter an incorrect password, you may see the error message: Error: This account has been temporarily
locked out due to too many failed login attempts. If this occurs, obtain the correct password, wait five minutes for the lock to clear, and then restart the configuration program.

6. The SSL Communication with the LDAP Server dialogue box appears.
   Go to step 7 if you want secure SSL communication between WebSEAL and the LDAP server.
   Go to step 8 if you do not want secure SSL communication between WebSEAL and the LDAP server.

7. Check "yes" only if you want secure SSL communication between WebSEAL and the LDAP server.
   a. Enter LDAP client SSL information:
      • Port number for SSL listening
      • Key database file full path location
      • Certificate label
      • Password for the key database file
   b. Click OK.
   c. The HTTP Properties dialogue box appears. Go to Step 9.

8. Check "no" if you do not want secure SSL communication between WebSEAL and the LDAP server. Click OK.
   The HTTP Properties dialogue box appears. Continue with Step 9.

9. Select or deselect the Allow unsecure TCP HTTP access check box. If you allowed unsecure TCP HTTP access, specify the port number. In most cases, you can accept the default port number of 80. If there is any conflict with the port number, the pdconfig utility detects the conflict and increments the port number choice.

10. Select or deselect the Allow HTTPS access check box. If you allowed HTTPS access, specify the port number. In most cases, you can accept the default port number of 443. If there is any conflict with the port number, the pdconfig utility detects the conflict and increments the port number choice. Click OK.
   The status message Configuring Tivoli Access Manager WebSEAL appears.
   When configuration completes, a status message states that the configuration was successful. The Access Manager WebSEAL for e-business Configuration dialog box appears.

11. Click Close.
   The Access Manager for e-business Configuration dialog box appears.

12. Click Close.
   Configuration of WebSEAL on Windows is now complete.

Note: Tivoli Access Manager WebSEAL supports multiple instances of WebSEAL servers on each host computer. See the IBM Tivoli Access Manager WebSEAL Administrator’s Guide for information on configuring multiple instances of WebSEAL servers.
Chapter 4. Upgrading WebSEAL from version 3.8 to 4.1

Tivoli Access Manager supports an upgrade of Tivoli Access Manager WebSEAL from Version 3.8 or Version 3.9 to Version 4.1. This chapter describes how to upgrade a Version 3.8 WebSEAL server to Version 4.1.

**Note:** Please check the [IBM Tivoli Access Manager Release Notes](https://www.ibm.com/support) on the Tivoli support Web site for possible limitations to the WebSEAL upgrade process.

Before you can use the following upgrade procedures for WebSEAL, you must ensure that the following Tivoli Access Manager components have been upgraded to Version 4.1:

- IBM Global Security Kit (GSKit)
- IBM Directory client
- Tivoli Access Manager runtime

Refer to the [IBM Tivoli Access Manager Base Installation Guide](https://www.ibm.com/support) for instructions on upgrading these components to Version 4.1.

**Upgrading WebSEAL on AIX**

To upgrade a WebSEAL server on AIX, complete the following instructions:

1. Log in as user **root**.

2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1. For policy server upgrade instructions, see the [IBM Tivoli Access Manager Base Installation Guide](https://www.ibm.com/support). Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:

   ```
   pdadmin login -a sec_master -p password
   pdadmin> acl list
   ```

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Stop the WebSEAL server. Enter the following command:
   ```
   /usr/bin/pdweb stop
   ```

4. Mount the **IBM Tivoli Access Manager Web Security for AIX** CD.

5. Change directory to:
   ```
   mount_point/usr/sys/inst.images
   ```

6. Obtain the Tivoli Access Manager `migrate.conf` file. This file is located on the CD in:
   ```
   mount_point/usr/sys/inst.images/migrate/migrate.conf
   ```
   a. Copy `migrate.conf` to:
      ```
      /tmp/migrate.conf
      ```
   b. Edit `migrate.conf` and add the **sec_master** password for your secure domain.
pdadmin-login = sec_master
pdadmin-pwd = sec_master_password

Use the default values for the other entries in migrate.conf.

7. Ensure you are located in the inst.images directory.
cd mount_point/usr/sys/inst.images

8. Enter the following command to install the WebSEAL server package:
installp -c -a -X -F -d . PDWeb.Web

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

The Results section of the Installation Summary indicates SUCCESS for packages successfully installed.

The installp utility exits.

The WebSEAL server is restarted automatically.

9. If you want to upgrade the WebSEAL ADK on this computer, install it now.
   The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the Web Security CD. If you have not already installed the Version 4.1 Tivoli Access Manager ADK, install it now. Use installp to install each package:
   installp -c -a -X -F -d . PDAuthADK
   installp -c -a -X -F -d . PDWebADK

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

   The Results section of the Installation Summary indicates SUCCESS for packages successfully installed.

   The installp utility exits.

   Neither the IBM Tivoli Access Manager ADK package nor the WebSEAL ADK package require any configuration steps.

The upgrade of WebSEAL on AIX is now complete.

You do not need to run pdconfig to configure WebSEAL. WebSEAL automatically uses the Version 3.8 configuration information. The original webseald.conf configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.

---

**Upgrading WebSEAL on HP-UX**

To upgrade WebSEAL on HP-UX, complete the following instructions:

1. Log in as user root.

2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.
   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample pdadmin command. For example:
pdadmin login -a sec_master -p password
pdadmin> acl list

If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Copy the WebSEAL certificate key file database and password stash file to a temporary directory:
   cp /var/pdweb/www/certs/pdsrv.kdb /temporary_directory
   cp /var/pdweb/www/certs/pdsrv.sth /temporary_directory

4. Enter the following commands:
   cd /opt/pdweb/.configure
   touch upgrade38

5. Stop the WebSEAL server. Enter the following command:
   /usr/bin/pdweb stop

6. Mount the IBM Tivoli Access Manager Web Security for HP-UX CD:
   /usr/sbin/pfs_mount mount_device mount_point

   For example:
   /usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cdrom

7. Obtain the Tivoli Access Manager migrate.conf file. This file is located on the CD in
   mount_point/hp/migrate/migrate.conf
   a. Copy migrate.conf to:
      /tmp/migrate.conf
   b. Edit migrate.conf and add the sec_master password for your secure domain.
      pdadmin-login = sec_master
      pdadmin-pwd = sec_master_password

      Use the default values for the other entries in migrate.conf.

8. Ensure you are located in the hp directory.
   cd mount_point/hp

9. Use the swinstall utility to install the WebSEAL server package:
   swinstall -s mount_point/hp PDWeb

   A message appears indicating that the analysis phase has succeeded. Files are extracted from the CD and installed on the hard disk.

   A message appears indicating that the execution phase has succeeded. The swinstall utility exits.

10. If you want to use the WebSEAL ADK on this computer, install it now. If you do not want to use it, skip this step and go to the next step.
    The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the Web Security CD.
    a. Use swinstall to install the Tivoli Access Manager ADK:
       swinstall -s /mount_point/hp PDAuthADK

       A status message appears when the analysis phase has succeeded. Files are extracted onto the hard disk. A status message appears when the execution phase has succeeded. The swinstall utility exits.
The Tivoli Access Manager ADK package does not require any configuration.

b. Use `swinstall` to install the WebSEAL ADK:

```
swinstall -s /mount_point/hp PDWebADK
```

A status message appears when the analysis phase has succeeded. Files are extracted onto the hard disk. A status message appears when the execution phase has succeeded. The `swinstall` utility exits.

The WebSEAL ADK package does not require any configuration.

11. Restore the Version 3.8 WebSEAL certificate files that you preserved before starting the WebSEAL upgrade:

```
cp /temporary_directory/pdsrv.kdb /opt/pdweb/www/certs/pdsrv.kdb
cp /temporary_directory/pdsrv.sth /opt/pdweb/www/certs/pdsrv.sth
```

12. Run the WebSEAL upgrade script:

```
cd /opt/pdweb/sbin
PDWeb_upgrade
```

**Note:** After upgrading, the `swlist` command may still display a listing for Policy Director WebSEAL 3.8.0. You can ignore this entry. The WebSEAL 3.8 binaries have been upgraded to Version 4.1.

Neither the Tivoli Access Manager ADK package nor the WebSEAL ADK package require any configuration steps.

The upgrade of WebSEAL on HP-UX is now complete.

You do not need to run `pdconfig` to configure WebSEAL. WebSEAL automatically uses the Version 3.8 configuration information. The original `webseald.conf` configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.

---

**Upgrading WebSEAL on Solaris**

To upgrade a WebSEAL server on Solaris, complete the following instructions:

1. Log in as user `root`.

2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   
a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.

   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:

```
pdadmin login -a sec_master -p password
pdadmin> acl list
```

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Stop the WebSEAL server. Enter the following command:

```
/usr/bin/pdweb stop
```

4. Mount the IBM Tivoli Access Manager Web Security for Solaris CD on:

```
/cdrom/cdrom0
```

5. Change directory to:
6. Obtain the Tivoli Access Manager migrate.conf file. This file is located on the CD in

\texttt{mount\_point/solaris/migrate/migrate.conf}

a. Copy migrate.conf to:

\texttt{/tmp/migrate.conf}

b. Edit \texttt{migrate.conf} and add the \texttt{sec\_master} password for your secure domain.

\begin{verbatim}
pdadmin-login = sec_master
pdadmin-pwd = sec_master_password
\end{verbatim}

Use the default values for the other entries in \texttt{migrate.conf}.

7. Ensure you are located in the \texttt{solaris} directory.

\texttt{cd mount\_point/solaris}

8. Enter the following command to install the WebSEAL server package:

\texttt{pkgadd -a /mount\_point/solaris/pddefault -d . PDWeb}

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

A message appears indicating that an upgrade is taking place.

A message appears indicating that installation of the WebSEAL package was successful. The \texttt{pkgadd} utility exits.

The WebSEAL server is restarted automatically.

9. If you want to upgrade the WebSEAL ADK on this computer, install it now.

The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the Web Security CD. If you have not already installed the Version 4.1 Tivoli Access Manager ADK, install it now. Use \texttt{pkgadd} to install each package:

\begin{verbatim}
pkgadd -a mount\_point/solaris/pddefault -d . PDAuthADK
pkgadd -a mount\_point/solaris/pddefault -d . PDWebADK
\end{verbatim}

Files are extracted from the CD and installed on the hard disk. A message appears indicating that installation of the WebSEAL ADK package was successful. The \texttt{pkgadd} utility exits.

Neither the IBM Tivoli Access Manager ADK package nor the WebSEAL ADK package require any configuration steps.

The upgrade of WebSEAL on Solaris from Version 3.8 to Version 4.1 is complete.

You do not need to run \texttt{pdconfig} to configure WebSEAL. WebSEAL automatically uses the Version 3.8 configuration information. The original \texttt{webseald.conf} configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.

**Upgrading WebSEAL on Windows**

To upgrade WebSEAL on Windows, complete the following instructions:

1. Log in to the Windows domain as a user with Windows administrator privileges.
2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.
   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:
      
      ```
      MSDOS> pdadmin login -a sec_master -p password
      pdadmin> acl list
      ```
      
      If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Ensure that the WebSEAL server is not running. Use the Services icon to stop the WebSEAL server.

4. Insert the IBM Tivoli Access Manager Web Security for Windows CD into the CD drive.

5. Obtain the Tivoli Access Manager `migrate.conf` file from the Web Security CD. This file is located on the CD in:
   
   ```
   E:\Windows\migrate\migrate.conf
   ```
   
   a. Copy `migrate.conf` to:
      
      ```
      %TEMP%\migrate.conf
      ```
      
      If `%TEMP%` is not set, place `migrate.conf` in `%TMP%`.
   b. Edit `migrate.conf` and add the `sec_master` password for your secure domain.
      
      ```
      pdadmin-login = sec_master
      pdadmin-pwd = sec_master_password
      ```
      
      Use the default values for the other entries in `migrate.conf`.

6. Run the WebSEAL setup program: (where the letter `E:` in the following command represents the CD drive):

   ```
   MSDOS> E:\Windows\PolicyDirector\Disk Images\Disk1\WebSEAL\Disk Images\Disk1\setup.exe
   ```

   The Choose Setup Language dialog box appears.

7. Select the appropriate language and click OK.

   The InstallShield program starts.

8. Click Finish to exit the setup program.

   WebSEAL is automatically started.

   The upgrade of WebSEAL on Windows is now complete.

   You do not need to run `pdconfig` to configure WebSEAL. WebSEAL automatically uses the Version 3.8 configuration information. The original `webseald.conf` configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.
Chapter 5. Upgrading WebSEAL from version 3.9 to 4.1

Tivoli Access Manager supports an upgrade of Tivoli Access Manager WebSEAL from Version 3.8 or Version 3.9 to Version 4.1. This chapter describes how to upgrade a Version 3.9 WebSEAL server to Version 4.1.

Note: Please check the IBM Tivoli Access Manager Release Notes on the Tivoli support Web site for possible limitations to the WebSEAL upgrade process.

Before you can use the following upgrade procedures for WebSEAL, you must ensure that the following Tivoli Access Manager components have been upgraded to Version 4.1:
- IBM Global Security Kit (GSKit)
- IBM Directory client
- Tivoli Access Manager runtime

Refer to the IBM Tivoli Access Manager Base Installation Guide for instructions on upgrading these components to Version 4.1.

Upgrading WebSEAL on AIX

To upgrade a WebSEAL server on AIX, complete the following instructions:

1. Log in as user root.

2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.
   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample pdadmin command. For example:
      pdadmin login -a sec_master -p password
      pdadmin> acl list
   
      For policy server upgrade instructions, see the IBM Tivoli Access Manager Base Installation Guide

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Stop the WebSEAL server. Enter the following command:
   /usr/bin/pdweb stop

4. Mount the IBM Tivoli Access Manager Web Security for AIX CD.

5. Ensure you are located in the inst.images directory.
   cd mount_point/usr/sys/inst.images

6. Enter the following command to install the WebSEAL server package:
   installp -c -a -X -F -d . PDWeb.Web

   Files are extracted from the CD and installed on the hard disk.
The Results section of the Installation Summary indicates SUCCESS for packages successfully installed.

The `installp` utility exits.

The WebSEAL server is restarted automatically.

7. If you want to upgrade the WebSEAL ADK on this computer, install it now. The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the Web Security CD. If you have not already installed the Version 4.1 Tivoli Access Manager ADK, install it now. Use `installp` to install each package:

   ```sh
   installp -c -a -X -F -d . PDAuthADK
   installp -c -a -X -F -d . P0WebADK
   ```

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

The Results section of the Installation Summary indicates SUCCESS for packages successfully installed.

The `installp` utility exits.

Neither the Tivoli Access Manager ADK package nor the WebSEAL ADK package require any configuration steps.

The upgrade of WebSEAL on AIX is now complete.

You do not need to run `pdconfig` to configure WebSEAL. WebSEAL automatically uses the Version 3.9 configuration information. The original `webseald.conf` configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.

**Upgrading WebSEAL on HP-UX**

To upgrade WebSEAL on HP-UX, complete the following instructions:

1. Log in as user `root`.

2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.
   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:
      ```sh
      # pdadmin login -a sec_master -p password
      pdadmin> acl list
      ```
      If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Copy the WebSEAL certificate key file database and password stash file to a temporary directory:

   ```sh
   cp /var/pdweb/www/certs/pdsrv.kdb /temporary_directory
   cp /var/pdweb/www/certs/pdsrv.sth /temporary_directory
   ```

4. Enter the following commands:

   ```sh
   cd /opt/pdweb/.configure
   touch upgrade39
   ```
5. Stop the WebSEAL server. Enter the following command:

   /usr/bin/pdweb stop

6. Mount the IBM Tivoli Access Manager Web Security for HP-UX CD:

   /usr/sbin/pfs_mount mount_device mount_point

   For example:

   /usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cdrom

7. Ensure you are located in the hp directory.

   cd mount_point/hp

8. Use the `swinstall` utility to install the WebSEAL server package:

   swinstall -s mount_point/hp PDWeb

   A message appears indicating that the analysis phase has succeeded. Files are extracted from the CD and installed on the hard disk.

   A message appears indicating that the execution phase has succeeded. The `swinstall` utility exits.

9. If you want to use the WebSEAL application developer kit (ADK) on this computer, install it now. If you do not want to use it, skip this step and go to the next step.

   The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the WebSEAL CD.

   a. Use `swinstall` to install the Tivoli Access Manager ADK:

      swinstall -s /mount_point/hp PDAuthADK

      A status message appears when the analysis phase has succeeded. Files are extracted onto the hard disk. A status message appears when the execution phase has succeeded. The `swinstall` utility exits.

      The Tivoli Access Manager ADK package does not require any configuration.

   b. Use `swinstall` to install the WebSEAL ADK:

      swinstall -s /mount_point/hp PDWebADK

      A status message appears when the analysis phase has succeeded. Files are extracted onto the hard disk. A status message appears when the execution phase has succeeded. The `swinstall` utility exits.

      The WebSEAL ADK package does not require any configuration.

10. Restore the Version 3.9 WebSEAL certificate files that you preserved before starting the WebSEAL upgrade:

    cp /temporary_directory/pdsrv.kdb /opt/pdweb/www/certs/pdsrv.kdb
    cp /temporary_directory/pdsrv.sth /opt/pdweb/www/certs/pdsrv.sth

11. Run the WebSEAL upgrade script:

    cd /opt/pdweb/sbin
    PDWeb_upgrade

   **Note:** After upgrading, the `swlist` command may still display a listing for Policy Director WebSEAL 3.9.0. You can ignore this entry. The WebSEAL 3.9 binaries have been upgraded to Version 4.1.

   Neither the Tivoli Access Manager ADK package nor the WebSEAL ADK package require any configuration steps.
The upgrade of WebSEAL on HP-UX is now complete.

You do not need to run `pdconfig` to configure WebSEAL. WebSEAL automatically uses the Version 3.9 configuration information. The original `webseald.conf` configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.

### Upgrading WebSEAL on Linux on zSeries

To upgrade a WebSEAL server on Linux on zSeries, complete the following instructions:

1. Log in as user `root`.
2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.
   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:
      ```
pdadmin login -a sec_master -p password
pdadmin> acl list
      ```
      If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.
3. Copy the WebSEAL certificate key file database and password stash file to a temporary directory:
   ```
cp /var/pdweb/www/certs/pdsrv.kdb /tmp
   cp /var/pdweb/www/certs/pdsrv.sth /tmp
   ```
4. Enter the following commands:
   ```
   cd /opt/pdweb/.configure
   touch upgrade39
   ```
5. Stop the WebSEAL server. Enter the following command:
   ```
   /usr/bin/pdweb stop
   ```
6. Obtain access to the Access Manager WebSEAL for Linux on zSeries `rpm` files. Note that Linux on zSeries does not support attachment of a CD drive at this time. Use one of the following methods to obtain the necessary files:
   - Load the WebSEAL for Linux on zSeries files onto another workstation. Use `ftp` to transfer the files to a directory on the Linux for zSeries machine.
   - Mount the *IBM Tivoli Access Manager for Linux on zSeries* CD on another workstation. Use NFS to access it from the Linux on zSeries machine. The WebSEAL files are located on the CD in the following directory:
     ```
     /zSeries
     ```
7. Use the `rpm` utility to install the WebSEAL server package:
   ```
   rpm -U PDWeb-PD-4.1.0-0.s390.rpm
   ```
   Files are extracted from the CD and installed on the hard disk.

The `rpm` utility exits.
8. If you want to use the WebSEAL application developer kit (ADK) on this computer, install it now. If you do not want to use it, skip this step and go to the next step.
The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the WebSEAL CD.

a. Use `rpm` to install the Tivoli Access Manager ADK:
   ```
   rpm -U PDAuthADK-PD-4.1.0-0.s390.rpm
   ```

   Files are extracted onto the hard disk. The `rpm` utility exits.

   The Tivoli Access Manager ADK package does not require any configuration.

b. Use `rpm` to install the WebSEAL ADK:
   ```
   rpm -U PDWebADK-PD-4.1.0-0.s390.rpm
   ```

   Files are extracted onto the hard disk. The `rpm` utility exits.

   The WebSEAL ADK package does not require any configuration.

9. Restore the Version 3.9 WebSEAL certificate files that you preserved before starting the WebSEAL upgrade:
   ```
   cp /temporary_directory/pdsrv.kdb /opt/pdweb/www/certs/pdsrv.kdb
   cp /temporary_directory/pdsrv.sth /opt/pdweb/www/certs/pdsrv.sth
   ```

10. Run the WebSEAL upgrade script:
    ```
    cd /opt/pdweb/sbin
    ./PDWeb_upgrade
    ```

    Messages appear indicating the package has been successfully upgraded and that the server has started.

11. Verify that WebSEAL is running:
    ```
    ./pd_start status
    Access Manager Servers
    Server   Enabled   Running
    _______________________________________
    webseald yes yes
    ```

### Upgrading WebSEAL on Solaris

To upgrade a WebSEAL server on Solaris, complete the following instructions:

1. Log in as user `root`.
2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.
   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:
      ```
      pdadmin login -a sec_master -p password
      pdadmin> acl list
      ```
      If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.

3. Stop the WebSEAL server. Enter the following command:
   ```
   /usr/bin/pdweb stop
   ```

4. Mount the IBM Tivoli Access Manager Web Security for Solaris CD on:
   ```
   /cdrom/cdrom0
   ```
5. Ensure you are located in the solaris directory.
   
   `cd mount_point/solaris`
   
6. Enter the following command to install the WebSEAL server package:
   
   `pkgadd -a /mount_point/solaris/pddefault -d . PDWeb`
   
   Files are extracted from the CD and installed on the hard disk.
   
   A message appears indicating that an upgrade is taking place.
   
   A message appears indicating that installation of the WebSEAL package was successful. The `pkgadd` utility exits.
   
   The WebSEAL server is restarted automatically.
   
7. If you want to upgrade the WebSEAL ADK on this computer, install it now.
   
   The WebSEAL ADK has a dependency on the Tivoli Access Manager ADK. Both ADK packages are included on the Web Security CD. If you have not already installed the Version 4.1 Tivoli Access Manager ADK, install it now. Use `pkgadd` to install each package:
   
   `pkgadd -a mount_point/solaris/pddefault -d . PDAuthADK`
   `pkgadd -a mount_point/solaris/pddefault -d . PDWebADK`
   
   Files are extracted from the CD and installed on the hard disk. A message appears indicating that installation of the WebSEAL ADK package was successful. The `pkgadd` utility exits.
   
   Neither the Tivoli Access Manager ADK package nor the WebSEAL ADK package require any configuration steps.
   
   The upgrade of WebSEAL on Solaris from Version 3.9 to Version 4.1 is complete.
   
   You do not need to run `pdconfig` to configure WebSEAL. WebSEAL automatically uses the Version 3.9 configuration information. The original `webseald.conf` configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.

---

**Upgrading WebSEAL on Windows**

To upgrade WebSEAL on Windows, complete the following instructions:

1. Log in to the Windows domain as a user with Windows administrator privileges.

2. Verify that the Tivoli Access Manager secure domain is able to upgrade WebSEAL:
   
   a. Verify that the Tivoli Access Manager policy server for the secure domain has already been upgraded to Version 4.1.

   b. Verify that the Tivoli Access Manager policy server is running, and that you can contact it. You can do this by executing a sample `pdadmin` command. For example:

      ```
      MSDOS> pdadmin login -a sec_master -p password
      pdadmin> acl list
      ```

      If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before continuing.
3. Ensure that the WebSEAL server is not running. Use the **Services** icon to stop the WebSEAL server.

4. Insert the *IBM Tivoli Access Manager Web Security for Windows* CD into the CD drive.

5. Run the WebSEAL setup program: (where the letter E: in the following command represents the CD drive):

   `MSDOS> E:\Windows\PolicyDirector\Disk Images\Disk1\WebSEAL\Disk Images\Disk1\setup.exe`

   The Choose Setup Language dialog box appears.

6. Select the appropriate language and click **OK**.
   The **InstallShield** program starts.

7. Click **Finish** to exit the setup program.
   WebSEAL is automatically started.

The upgrade of WebSEAL on Windows is now complete.

You do not need to run **pdconfig** to configure WebSEAL. WebSEAL automatically uses the Version 3.9 configuration information. The original `webseald.conf` configuration file, with your custom configuration settings, is preserved and updated with Version 4.1 stanzas and parameters.
Chapter 6. Unconfiguring and removing WebSEAL

This chapter describes how to unconfigure and remove WebSEAL and the WebSEAL ADK.

Note: Unconfiguring of WebSEAL removes all information from the WebSEAL junctions database. Ensure that this information is no longer needed before removing it.

WebSEAL depends on the Tivoli Access Manager runtime. This chapter does not describe how to remove the runtime. To remove the runtime, follow the instructions in the IBM Tivoli Access Manager Base Installation Guide.

WebSEAL unconfiguration and removal is a two step process. First you must use the pdconfig utility to unconfigure WebSEAL from the secure domain. Then you can use a platform-specific utility to remove the WebSEAL files from the hard disk.

To unconfigure WebSEAL, complete the instructions in one of the following sections:
- “Unconfiguring WebSEAL on UNIX”
- “Unconfiguring WebSEAL on Windows” on page 40

To remove WebSEAL files, complete the instructions in one of the following sections:
- “Removing WebSEAL from AIX” on page 41
- “Removing WebSEAL from HP-UX” on page 41
- “Removing WebSEAL from Linux on zSeries” on page 42
- “Removing WebSEAL from Solaris” on page 42
- “Removing WebSEAL from Windows” on page 43

Unconfiguring WebSEAL on UNIX

Use the pdconfig configuration utility to unconfigure WebSEAL.

1. Log in as root.
2. Start the pdconfig configuration utility:
   
   pdconfig

   The Access Manager for e-business Setup Menu appears.

   Access Manager for e-business Setup Menu
   
   1. Configure Package
   2. Unconfigure Package
   3. Display Configuration Status
   x. Exit

   Please select the menu item [x]:

3. Type 2 for Unconfigure Package.

   The Access Manager for e-business Unconfiguration Menu appears.

4. Type the menu number for Access Manager WebSEAL Unconfiguration.

   The Access Manager WebSEAL for e-business Setup Menu appears.
5. Type 2 to **Unconfigure**.
   The Access Manager WebSEAL for e-business Unconfiguration Menu appears.
6. Type 1 to select the default WebSEAL server.

   **Note:** If your system configuration contains multiple WebSEAL instances, you must remove all instances before you can unconfigure the default WebSEAL server. An error message warns you when this order of operation is not followed.

   A prompt appears requesting the password for the Tivoli Access Manager Administrator.
7. Enter the password for **sec_master**.
   A series of status messages appear. These messages indicate that the server is being unconfigured, that log files are being cleaned up, and that outgoing endpoints are being reclaimed. The WebSEAL server is stopped, and a final status message indicates that the unconfiguration was successful.
8. Press Enter.
   The unconfiguration is complete.
   The Access Manager WebSEAL for e-business Setup Menu appears.
9. Type x to exit the **pdconfig** utility.
10. Continue to the appropriate section for removing the WebSEAL files from the UNIX system.

---

### Unconfiguring WebSEAL on Windows

Use the **pdconfig** configuration utility to unconfigure WebSEAL.

To unconfigure WebSEAL and WebSEAL ADK on Windows, complete the following instructions:

1. Log in as a Windows user with administrator privilege.
2. Click **Start** → **Programs** → **Access Manager for e-business** → **Configuration**
   The Access Manager for e-business Configuration dialog box appears.
3. Select **Access Manager WebSEAL** and click **Unconfigure**.
   The Access Manager WebSEAL for e-business Configuration dialog box appears.
4. Select **Default WebSEAL** and click **Unconfigure**.
   The Access Manager Administrator Password dialog box appears.
5. Enter the password for **sec_master**. Click **OK**.
   A message appears indicating that WebSEAL is being unconfigured. The Access Manager WebSEAL for e-business Configuration dialog box appears.
6. Verify that you have unconfigured WebSEAL. The configuration status for Default WebSEAL is listed as "no".
7. Click **Close**.
   The Access Manager for e-business Configuration dialog box appears.
8. Click **Close**.
9. Continue to the appropriate section for removing the WebSEAL files from the Windows system.
Removing WebSEAL from AIX

Use **installp** to remove the WebSEAL files from AIX.

**Note:** You do not have to unconfigure the WebSEAL ADK before removing its files.

1. Log in as **root**.
2. Choose one of the following commands:
   - To remove the WebSEAL ADK, enter the following command:
     ```
     installp -u PDWeb.ADK
     ```
   - To remove WebSEAL, enter the following command:
     ```
     installp -u PDWeb.Web
     ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>–u</td>
<td>Removes the specified software product and any of its installed updates from the system.</td>
</tr>
</tbody>
</table>

**Note:** You must remove PDWebADK before removing PDWeb.

3. The WebSEAL files are removed. The Results section of the Installation Summary table indicates SUCCESS for each package successfully removed.

Removal of WebSEAL is complete.

If you want to remove the Tivoli Access Manager runtime, follow the instructions in the [IBM Tivoli Access Manager Base Installation Guide](#).

Removing WebSEAL from HP-UX

Use **swremove** to remove the WebSEAL files from HP-UX.

**Note:** You do not have to unconfigure the WebSEAL ADK before removing its files.

1. Log in as **root**.
2. Choose one of the following commands:
   - To remove the WebSEAL ADK, enter the following command:
     ```
     swremove PDWebADK
     ```
   - To remove WebSEAL, enter the following command:
     ```
     swremove PDWeb
     ```

   **Note:** WebSEAL ADK has a dependency on WebSEAL. Do not try to remove WebSEAL when WebSEAL ADK is still on the system. Remove WebSEAL ADK first.

   A series of status messages appear for each removal selection. A status message appears indicating that the analysis phase has succeeded. The **swremove** utility removes the WebSEAL files from the hard disk.

   When the removal is complete, the **swremove** utility exits.

Removal of WebSEAL on HP-UX is now complete.
If you want to remove the Tivoli Access Manager runtime, follow the instructions in the IBM Tivoli Access Manager Base Installation Guide.

Removing WebSEAL from Linux on zSeries

Use rpm to remove the WebSEAL files from Linux on zSeries.

Note: You do not have to unconfigure the WebSEAL ADK before removing its files.

1. Log in as root.
2. Choose one of the following commands:
   - To remove the WebSEAL ADK, enter the following command:
     ```
rpm -e PDWebADK-PD-4.1.0-0
     ```
   
   Note: You must first remove the WebSEAL ADK before you can successfully remove WebSEAL.
   - To remove WebSEAL, enter the following command:
     ```
rpm -e PDWeb-PD-4.1.0-0
     ```
   - To remove both the WebSEAL ADK and WebSEAL, enter the following command (the order in which the package arguments are listed makes no difference):
     ```
rpm -e PDWebADK-PD-4.1.0-0 PDWeb-PD-4.1.0-0
     ```

   No message or status appears to confirm the removal of the selected package. The rpm utility exits.

Removal of the selected packages is complete. If you want to remove the Tivoli Access Manager runtime, follow the instructions in the IBM Tivoli Access Manager Base Installation Guide.

Removing WebSEAL from Solaris

Use pkgrm to remove the WebSEAL files from Solaris.

Note: You do not have to unconfigure the WebSEAL ADK before removing its files.

1. Log in as root.
2. Choose one of the following commands:
   - To remove the WebSEAL ADK, enter the following command:
     ```
pkgrm PDWebADK
     ```
   - To remove WebSEAL, enter the following command:
     ```
pkgrm PDWeb
     ```
   
   Note: You must remove PDWebADK before removing PDWeb.
   - To remove both WebSEAL and the WebSEAL ADK, enter the following command:
     ```
pkgrm PDWeb PDWebADK
     ```

   A prompt appears asking you to confirm the removal of the selected package.
3. Type y.
   A message asks, "Do you want to continue with removal of this package".
4. Type y.
A status message lists each file as it is removed.

After the postremove script runs, a status message indicates that the removal of the software package was successful.

The pkgrm utility exits. Removal of the selected packages is complete.

If you want to remove the Tivoli Access Manager runtime, follow the instructions in the IBM Tivoli Access Manager Base Installation Guide.

---

**Removing WebSEAL from Windows**

WebSEAL on the Windows platform consists of two components: WebSEAL and WebSEAL ADK. You can either remove both components, or can choose to remove only the WebSEAL ADK component.

If you choose to remove the WebSEAL server, the WebSEAL ADK is automatically removed.

Follow the instructions in the appropriate section:

- “Removing WebSEAL and WebSEAL ADK” on page 43
- “Removing WebSEAL ADK only” on page 43

**Removing WebSEAL and WebSEAL ADK**

Use the Windows Add/Remove Programs icon interface to remove the files for each package.

To remove WebSEAL and WebSEAL ADK on Windows, complete the following instructions:

1. Click the Add/Remove Programs icon.
2. Select Access Manager WebSEAL.
3. Click Change/Remove.
   The Choose Setup Language dialog box appears.
4. Select a language and click OK.
5. Select the Remove radio button. Click Next.
   The Confirm Uninstall dialog box appears.
6. Click OK.
   The WebSEAL files are removed. The WebSEAL ADK files are also removed.
   The Maintenance Complete dialog box appears.
7. Click Finish.
   Removal of WebSEAL is complete.

If you want to remove the Tivoli Access Manager runtime, follow the appropriate instructions in the IBM Tivoli Access Manager Base Installation Guide.

**Removing WebSEAL ADK only**

You can remove the WebSEAL ADK files without removing the WebSEAL server files.

**Note:** You do not have to unconfigure the WebSEAL ADK before removing its files.
To remove only the WebSEAL ADK on Windows, complete the following instructions:

1. Click the **Add/Remove Programs** icon.
2. Select **Tivoli Access Manager WebSEAL**.
3. Click **Change/Remove**.
   The Choose Setup Language dialog box appears.
4. Select a language and click **OK**.
5. Select the **Modify** radio button. Click **Next**.
   The Select Components dialog box appears.
6. Clear the check box for **PDWebADKs**.

   **Note:** InstallShield designates this component for removal when you *clear* the check box.
7. Click **Next**.
   The WebSEAL ADK files are removed.
8. Click **Finish** to exit the program.

Removal of the WebSEAL ADK on Windows is now complete.
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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
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 has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
USA

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 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.

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 illustrates 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 softcopy, the photographs and color illustrations may not appear.

### Trademarks

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

AIX
DB2
IBM
IBM logo
Tivoli
Tivoli logo

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft 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.

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.