

AIX 5L Version 5.1



Web-based System Manager Administration Guide

AIX 5L Version 5.1



Web-based System Manager Administration Guide

Second Edition (April 2001)

Before using the information in this book, read the general information in "Appendix B. Notices" on page 53.

This edition applies to AIX 5L Version 5.1 and to all subsequent releases of this product until otherwise indicated in new editions.

A reader's comment form is provided at the back of this publication. If the form has been removed, address comments to Publications Department, Internal Zip 9561, 11400 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial Internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

© Copyright International Business Machines Corporation 2000, 2001. All rights reserved.

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

Contents

About This Book	v
Who Should Use This Book	v
Highlighting	v
ISO 9000	v
Related Publications	v
Trademarks	v
Chapter 1. Introduction to Web-based System Manager	1
Key Concepts of Web-based System Manager	1
Modes of Operation	3
Standalone Application Mode	3
Client-Server Mode	3
Applet Mode	4
PC Client Mode	4
Custom Applications	5
Chapter 2. Installation and System Requirements	7
Minimum Recommended System Requirements	7
Web-based System Manager Installation	7
Configuring Web-based System Manager in Client-Server Mode	8
Optional Filesets Available with Web-based System Manager	8
Installation Requirements to Support Applet Mode	9
Configuring the Client (Browser)	10
Installing Web-based System Manager PC Client	10
Minimum Recommended System Requirements for PC Client	10
Installation Requirements to Support PC Client Mode	10
Configuring an AIX Server for PC Client Installation	10
Installing Web-based System Manager PC Client on the Windows System	11
Uninstalling Web-based System Manager PC Client from a Windows System	11
Installation Requirements for Secure Socket Layer Support	11
Integrating Web-based System Manager into Tivoli Netview Management Console	12
Chapter 3. Using Web-based System Manager	13
Navigation Area	13
Contents Area	13
Containers	14
Overviews	15
Launchers	15
Menu and Toolbar Actions	16
Tips Area	17
Status Bar	17
Console Workspace	17
Preference Files	18
Error Handling for Loading or Saving Preference Files	19
Command Line Tools	20
User-Editable Files	22
Help	23
Filtering and Sorting Views	24
Working Dialog	24
Keyboard Control of Web-based System Manager	25
Using Mnemonics and Shortcuts	25
Navigating the Console with the Keyboard	26
Navigating Dialog Boxes with the Keyboard	26

Accessing Help with the Keyboard	27
Session Log	27
Chapter 4. Management Environment Configuration	29
Adding a Machine to Web-based System Manager	29
Examples	30
Removing a Machine	30
Chapter 5. Web-based System Manager Security	33
Installing Web-based System Manager Security	33
Configuring Web-based System Manager Security	33
Security Scenarios	34
Using Ready-to-Go Key Ring Files	34
Administering Multiple Sites.	36
Avoiding Transfer of Private Keys	39
Using Another Certificate Authority	40
Configuring for the SMGate Daemon	43
Viewing Configuration Properties	43
Public Key Ring Content	44
Enabling Web-based System Manager Security	44
Enabling the SMGate Daemon	44
Running Web-based System Manager Security	45
Application mode	45
Applet Mode	45
Chapter 6. Web-based System Manager Accessibility	47
Keyboard Accessibility.	47
Text-to-Speech Support	47
Using Web-based System Manager with the Self-Voicing Kit	47
Appendix A. Troubleshooting	49
Troubleshooting Remote Machines	49
Troubleshooting Web-based System Manager in Applet Mode	50
Troubleshooting Web-based System Manager in PC Client Mode	50
Troubleshooting Security.	51
Appendix B. Notices	53

About This Book

This book provides information on how to use Web-based System Manager to administer systems.

Who Should Use This Book

This book should be used by systems administrators who want to use Web-based System Manager to administer their systems.

Highlighting

The following highlighting conventions are used in this book:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
<i>Italics</i>	Identifies parameters whose actual names or values are to be supplied by the user.
Monospace	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Related Publications

The following books contain information related to Web-based System Manager:

- *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*

Trademarks

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

- AIX
- IBM

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

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

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

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

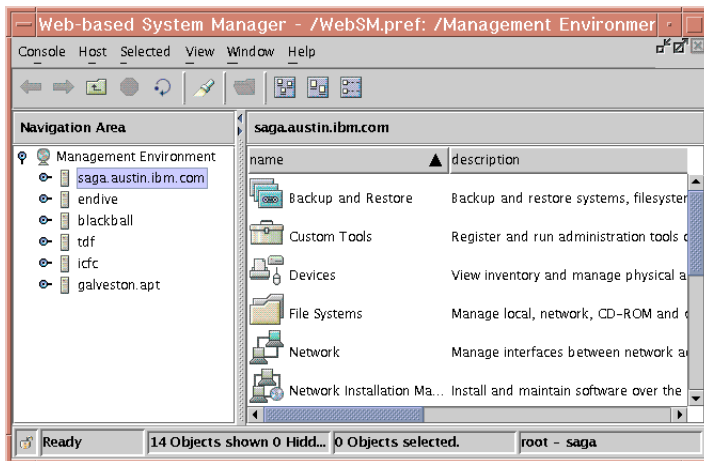
Chapter 1. Introduction to Web-based System Manager

Web-based System Manager is a system management application for administering computers. It is installed by default on graphical systems, and has been substantially revised for AIX 5.1.

Web-based System Manager features a system management console for administering multiple hosts. A plug-in architecture makes it easier to extend the suite. In addition, Web-based System Manager supports dynamic monitoring and administrator notification of system events.

Key Concepts of Web-based System Manager

Web-based System Manager is a client-server application that gives the user a powerful interface to manage UNIX systems. Web-based System Manager uses its graphical interface to enable the user to access and manage multiple remote machines. Following is an example of a Web-based System Manager console:

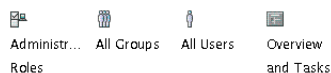


The figure shows a *Console Window* containing two primary panels. The panel on the left displays the machines that the user can manage from the Console Window. This panel is referred to as the *Navigation Area*. The panel on the right (the *Contents Area*) displays results based on the item selected in the *Navigation Area*. The user selects the machine to perform management operations from the *Navigation Area*. As the user navigates to the desired operation in the *Navigation Area*, the *Contents Area* is updated to show the allowable choices.

The following sequence of steps provides an example of how Web-based System Manager could be used to modify the properties of a user:

1. From the *Contents Area*, either double-click on the **Users** icon, or single-click on the **Users and Groups** icon in the *Navigation Area*.

The *Contents Area* will look similar to the following:



2. Double-click the **All Users** icon. The *Contents Area* will look similar to the following:

Name	Description	Type
sandy		Basic
servdir		Basic
sys		Administrator
uucp		Administrator
verena		Basic
xrx		Basic
yrx		Basic
zrx		Basic

3. Double-click the icon representing the user whose properties you want to modify. A property dialog displays similar to the following illustration:

The dialog box is titled "User guest Properties @ saga" and has three tabs: "General", "Groups", and "Environment". The "General" tab is active. It contains the following sections:

- Identification:** "User name:" is set to "guest" and "User ID:" is set to "100". There is an empty "Description:" field.
- Enable logon:** Two checkboxes are checked: "Locally from console" and "Remotely with rlogin and telnet commands".
- Status:** The checkbox "Account is locked by administrator" is unchecked. A "Schedule Expiration..." button is located at the bottom right of this section.

At the bottom of the dialog are four buttons: "OK", "Apply", "Cancel", and "Help".

Use this dialog to modify the properties of the selected user.

4. To save the changes, press the **OK** button. To cancel the changes, press the **Cancel** button.

The client portion of the Web-based System Manager application runs on the *managing machine*. In the above example, it was not stated if the user being modified was a user on the machine running Web-based System Manager (the client) or on a managed machine (a server). To modify a user on a managed machine, select a machine from the Navigation Area. If this machine has not already been accessed, a dialog similar to the following displays:

The dialog box is titled "Log On" and contains the following fields and options:

- Text: "Login to the management server" with a small icon.
- Fields: "Host name:" (set to "saga"), "User name:", and "Password:".
- Options:
 - Specify a console preferences file
 - Reuse this user name and password to access other hosts
 - Enable secure communication

At the bottom are three buttons: "Log On", "Clear", and "Cancel".

Use this dialog to log in to the managed machine. After you have logged in to a machine, you can perform operations from the Web-based System Manager console on another managed machine and return to the machine (by selecting it from the Navigation Area) without needing to log in again.

Each Web-based System Manager user will want to maintain a Web-based System Manager *home* machine. This *home* machine should be used as the managing machine even if the user starts Web-based System Manager from a machine other than the *home* machine. This is because the initial appearance of the console window is derived from a file on the managing machine. This enables a Web-based System Manager user to start Web-based System Manager at a colleague's desk, specify a personal *home* machine as the managing machine, and thus create a console window with the user's saved preferences.

The most important portion of the saved user preferences may be the machine Management Environment. The Management Environment is a powerful mechanism for defining and accessing the set of machines for which an administrator is responsible. When a machine in the Management Environment is selected by a user, it starts a *Web-based System Manager server* on the selected machine. This server provides the client (and indirectly the console window) with *remote managed objects*. The client portion of the application presents these remote managed objects through windows and other standard graphical user interface (GUI) elements. By working with these GUI elements, the client side of the application can display information about objects on the remote *managed machine*, as well as allow the user to update this information.

After a machine in the Management Environment is *active* (this occurs through selecting a machine in the Management Environment and logging in to the machine), the user can switch from managing one machine to managing another machine with a few mouse clicks.

The result is that the administrator can manage a large number of machines through a powerful interface.

Modes of Operation

Web-based System Manager can be configured to run in a variety of operating modes. The operating environments in which Web-based System Manager can be started as are *standalone application*, *client-server*, and *applet*. These modes of operation are described in the following sections.

The modes of operation are as follows:

- “Standalone Application Mode”
- “Client-Server Mode”
- “Applet Mode” on page 4
- “PC Client Mode” on page 4

Standalone Application Mode

No configuration is necessary to run Web-based System Manager in the standalone application mode. From the command line, type the following command:

```
/usr/websm/bin/wsm
```

To start the Web-based System Manager Console from the Common Desktop Environment (CDE), do the following:

1. Select the **Application Manager** icon in the CDE front panel.
2. Select the **System_Admin** icon.
3. Select the **Management Console** icon.

By default, you can perform system management tasks on the machine you started the console on.

Client-Server Mode

You can manage your local machine from the Web-based System Manager Console. You can also manage machines that have been configured for remote management (see “Configuring Web-based

System Manager in Client-Server Mode” on page 8). You specify the machines you want to manage by adding them to the Management Environment (see “Chapter 4. Management Environment Configuration” on page 29).

You can also select a different host than your local machine as the *managing machine*. To do this, use the following command:

```
/usr/websm/bin/wsm -host [managing machine host]
```

The host you specify as [*managing machine host*] displays under the Navigation Area as the first host name under the list of hosts that can be managed. This host is also used to load the Web-based System Manager user preference file (**\$HOME/WebSM.pref**). Using the **-host** argument displays the console to the machine you are using, but uses the preferences file of the remote host you specify (see “Preference Files” on page 18).

Note: Any target host to be managed by Web-based System Manager must have the Web-based System Manager server installed and configured. See “Configuring Web-based System Manager in Client-Server Mode” on page 8 for more information.

Applet Mode

Applet mode is similar to using Web-based System Manager in client-server mode when using the **-host** argument. In client-server mode, you use the following command:

```
/usr/websm/bin/wsm -host [managing machine]
```

while in applet mode, you point your browser to

```
http://managing machine/wsm.html
```

In both cases, *managing machine* is the machine that contains the Web-based System Manager application. The *managed machine* is the first machine to be listed in the Management Environment.

There is a significant difference between using applet mode and client-server mode. In applet mode, it is only possible to manage a set of machines that have the same version of Web-based System Manager installed. The reason for this is that applets in general are restricted for security reasons to loading Java classes only from the HTTP server running the applet. While the Java classes needed to operate the Web-based System Manager console come from the *managing machine*, another set of Java classes is used to operate tasks on the managed machines. These classes must be loaded from the machine being managed (this is different from the managing machine) in order for these classes to match the operating system being managed. In applet mode, this situation is not possible.

PC Client Mode

PC Client Mode allows the user to run the Web-based System Manager console on a Windows PC and manage remote AIX computers. This method is similar to using Web-based System Manager in client-server mode when using the *-host* argument. There are several ways to start PC Client on the Windows platform:

- Double-click the **Web-based System Manager PC Client** icon located on the Windows desktop to open the login panel where the host, username, and password are entered.
- Click the Start button in the Task bar, then select **Programs** —> **Web-based System Manager** —> **Web-based System Manager PC Client**.
- From an MS-DOS prompt, run the **wsm.bat** command in the PC Client bin directory.
- Using Windows Explorer or Netscape Communicator, double-click the **wsm.bat** icon in the PC Client bin folder.

As with client-server mode, the systems listed in the Management Environment area are managed machines. However, PC Client differs from client-server mode in that the Windows system running PC Client is the managing machine and does not show up in the Management Environment area.

Security issues are identical to those found in client-server mode with regard to loading classes, as opposed to the limitations found in Applet mode, where it is only possible to manage a set of machines that have the same version of Web-based System Manager installed. For more information on security issues, see “Chapter 5. Web-based System Manager Security” on page 33.

For more information, see “Client-Server Mode” on page 3 and “Applet Mode” on page 4.

Custom Applications

You can use the Custom Tools application to add existing commands and applications available on your AIX system to the Web-based System Manager environment, which can then be executed directly from directly from the Console Window.

If you would like more integration that the Custom Tools application provides, you can extend the power of Web-based System Manager by writing custom applications. Writing custom applications requires knowledge of the Java programming language. If this is of interest to your organization, contact your sales representative.

Chapter 2. Installation and System Requirements

The following topics provide information on installing Web-based System Manager:

- “Minimum Recommended System Requirements”
- “Configuring Web-based System Manager in Client-Server Mode” on page 8
- “Optional Filesets Available with Web-based System Manager” on page 8
- “Installation Requirements to Support Applet Mode” on page 9
- “Installing Web-based System Manager PC Client” on page 10
- “Installation Requirements for Secure Socket Layer Support” on page 11
- “Integrating Web-based System Manager into Tivoli Netview Management Console” on page 12

Minimum Recommended System Requirements

Using Web-based System Manager effectively requires that the client computer have at least the following characteristics:

- Base Operating System AIX 5.1 (including Java 1.3.0.0)
- Attached graphics display
- 50 MB free disk space
- 256 MB of memory
- 300 MHz CPU

If you are using a PC to run Web-based System Manager in applet mode, it should have a processor speed of at least 500 MHz.

If you are using a PC to run Web-based System Manager in PC Client mode, see “Minimum Recommended System Requirements for PC Client” on page 10 for additional requirements.

While it is not absolutely necessary to have a computer that meets these requirements for memory and processor speed, the performance might be diminished on lesser machines. But the minimum system requirements listed above apply primarily to the client computer. If the client computer does not meet the minimum recommended system requirements, the performance might be diminished.

Because the server machines do not involve displaying graphics to the user, it is not critical that they meet the minimum recommended system requirements. For details, read “Modes of Operation” on page 3.

In applet and client-server modes, the client machine is not necessarily the machine on which you see the Web-based System Manager console.

Use of Web-based System Manager with X-emulators (such as those used on a PC) is not recommended. The performance with these emulators is not satisfactory.

Web-based System Manager Installation

To use Web-based System Manager, it must be installed on the client used to run it and on any managed machines. If you have AIX 5.1 or later installed on your machine, you might already have Web-based System Manager installed.

To verify this, enter the following:

```
lsipp -h sysmgt.websm.framework
```

If Web-based System Manager is not installed, you will see a message similar to the following:

ls1pp: Fileset sysmgt.websm.framework not installed.

If Web-based System Manager is installed, you will see something similar to the following:

Fileset	Level	Action	Status	Date	Time

Path: /usr/lib/objrepos					
sysmgt.websm.framework	5.1.0.0	COMMIT	COMPLETE	03/09/01	17:30:14
Path: /etc/objrepos					
sysmgt.websm.framework	5.1.0.0	COMMIT	COMPLETE	03/09/01	17:35:31

If you do not have the **sysmgt.websm.framework** fileset installed, use the operating system installation tools. To access the installation tools, use the following command (assuming the version AIX 5.1 CD is loaded to your CD drive):

```
/usr/lib/instl/sm_inst installp_cmd -a \  
-d /dev/cd0 -f sysmgt.websm.framework -c -N -g -X
```

This action installs the required set of images needed to run Web-based System Manager.

Configuring Web-based System Manager in Client-Server Mode

In client-server mode (see “Modes of Operation” on page 3), the Web-based System Manager client requests server services from a managed machine through inetd port 9090. Client-server mode needs to be enabled on the servers that are to be managed as remote machines. Enabling and disabling a machine to act as a Web-based System Manager Server can be done through the **wsmserver** command (see “Command Line Tools” on page 20) as follows:

```
/usr/websm/bin/wsmserver -enable
```

Note: Client-Server mode is *not* enabled by default.

To disable a machine so that it cannot be managed from a Web-based System Manager client, run the following command:

```
/usr/websm/bin/wsmserver -disable
```

If you need to use a port number other than 9090, you can set an alternative port number in the **/etc/services** file. If this is done, the **-port** argument would be used with the **wsm** command (see “Command Line Tools” on page 20).

Optional Filesets Available with Web-based System Manager

The following optional filesets can be installed to add additional function to Web-based System Manager:

sysmgt.websm.accessibility

Adds support for sight-impaired users using simulated speech technology. The Self Voicing Kit (SVK) is needed to use the simulated speech technology with Web-based System Manager. If the SVK is installed on the machine, this fileset allows the SVK to work with Web-based System Manager. For more information on how to obtain, install, and configure the SVK, go to: <http://www.alphaworks.ibm.com/tech/svk>

sysmgt.msg.Locale Language.websm.apps

Enables the locale language to be used if the **LANG** environment variable is set or if the **-lang** argument is used with the **wsm** command.

sysmgt.websm.security

Adds support for Secure Socket Layer communication between client and server. Supports 40-bit encryption. Available on Expansion Pack.

sysmgt.websm.security-us

Adds support for Secure Socket Layer communication between client and server. Supports 128-bit encryption. Available on the Expansion Pack. Export and import laws could make this fileset unavailable in some countries.

The filesets in the preceding table are not installed by default as part of the base operating system (AIX 5.1). However, they can be installed in a manner similar to the one described above for installing the core Web-based System Manager images. The **sysmgt.websm.security** and **sysmgt.websm.security-us** filesets are available on the Expansion Pack CD. From the media containing the fileset, use the following command:

```
/usr/lib/inst1/sm_inst installp_cmd -a -d /dev/cd0 \  
-f desired_fileset_to_install -c -N -g -X
```

Installation Requirements to Support Applet Mode

In addition to the standard Web-based System Manager application mode, you need the **sysmgt.websm.webaccess** fileset to support applet mode. This fileset is automatically installed with the base operating system.

The machine to be used as the **managing machine** must be setup as an HTTP Server. This can be done by installing and configuring the HTTP Server of your choice. The IBM HTTP Server is available on AIX 5.1 Expansion Pack. Use the **/usr/websm/bin/configassist** command to automatically configure the HTTP Server.

The following table identifies the requirements for using Web-based System Manager in applet mode with various browsers:

Platform	Browser	Requirements
PC	Netscape Communicator	<ul style="list-style-type: none">• Netscape Communicator must be Version 4.7 or 4.7x. (Netscape Communicator 6.0 is not supported.)• The 1.3 Java plug-in must be installed.
PC	Internet Explorer	<ul style="list-style-type: none">• Operating System must be Windows 98 (or later), or Windows NT 4.0 (or later).• Internet Explorer must be Version 5.0 (or later).• The 1.3 Java plug-in must be installed

Note: Applet mode is not supported on the POWER-based platform. See “Modes of Operation” on page 3 to see how to manage POWER-based machines.

To configure a server for applet mode, complete the following steps:

1. Install an HTTP Server on the machine that Web-based System Manager resides. The recommended Web server is IBM HTTP Server. Refer to the documentation for each product on how to install and configure the HTTP Server.
2. After the HTTP Server is running, you can configure Web-based System Manager to run from it with the following command:

```
/usr/websm/bin/configassist
```

3. In Configuration Assistant, proceed until you reach the main panel.

4. Select **Configure a web server to run Web-based System Manager in a browser**.
5. Select **Next**.
6. Follow the instructions on the subsequent panels to finish the configurations.

Configuring the Client (Browser)

The following are requirements for the client:

- Netscape Communicator 4.7 or 4.7x (Netscape Communicator 6.0 is not supported), or Internet Explorer 5.0.
- The Java 1.3 plug-in

If you are using Internet Explorer as your browser, you will be prompted to download the plug-in automatically. If you click **yes**, the plug-in is downloaded and its installation script runs. If you click **no**, Web-based System Manager exits.

If you are using Netscape Communicator as your browser, it occasionally cannot locate the correct Java plug-in. If this happens, you can manually download and install it.

Installing Web-based System Manager PC Client

The following topics provide information on installing Web-based System Manager PC Client:

- “Minimum Recommended System Requirements for PC Client”
- “Installation Requirements to Support PC Client Mode”

Minimum Recommended System Requirements for PC Client

If you are going to use a PC to run Web-based System Manager in PC Client mode,

- 60 MB of free disk space on the default drive for temporary use during the install procedure
- 50 MB of free disk space on the drive you plan to use to install Web-based System Manager PC Client
- PC processor speed of at least 500 MHz
- 256 MB of memory

Installation Requirements to Support PC Client Mode

To install Web-based System Manager PC Client over a network, you must have the **sysmgt.websm.webaccess** fileset installed on at least one AIX systems. This fileset is installed automatically with the base operating system.

The machine used to install Web-based System Manager PC Client must be set-up as an HTTP Server. This is done by installing and configuring the HTTP Server of your choice. The IBM HTTP Server is available on AIX 5.1 Expansion Pack. Use the **/usr/websm/bin/configassist** command to automatically configure the HTTP Server.

The following table identifies the requirements for installing Web-based System Manager PC Client on a PC platform:

Netscape Communicator	<ul style="list-style-type: none"> • Netscape Communicator must be Version 4.7 or 4.7x. • Netscape Communicator 6.0 is not supported.
Internet Explorer	<ul style="list-style-type: none"> • Internet Explorer must be version 5.0 or later.

Configuring an AIX Server for PC Client Installation

Complete the following steps to configure an AIX server for Web-based System Manager PC Client installation:

1. Install an HTTP Server on the server where Web-based System Manager resides. The recommended Web server is IBM HTTP Server. Refer to the documentation for each product on how to install and configure the HTTP Server.
2. After the HTTP Server is running, run the following command to configure Web-based System Manager:
`/usr/websm/bin/configassist`
3. In Configuration Assistant, proceed until you reach the main panel.
4. Select **Configure a web server to run Web-based System Manager in a browser**.
5. Select **Next**.
6. Follow the instructions on the subsequent panels to finish the configurations.

Installing Web-based System Manager PC Client on the Windows System

1. Uninstall any previous version of Web-based System Manager PC Client. For more information, see “Uninstalling Web-based System Manager PC Client from a Windows System”.
2. Enter the following Web address in the PC Web browser:
`hostname/pc_client/pc_client.html`, where *hostname* is the name of the AIX server configured for Web-based System Manager PC Client installation.
3. Click **Proceed** at the warning screen to install.
4. On Internet Explorer, a Security Warning will be displayed requesting permission to temporarily install and run a Java JVM file. Select **YES** to complete the installation. On Netscape Communicator, two Java Security messages will be displayed, you must select **Grant** for both to complete the installation.
5. When the **PC Client Installer** panel is displayed, press **Next** to continue.
6. To install using the default location, press **Next**, otherwise enter the desired location, then press **Next**.
7. A confirmation panel will be displayed showing the install location, the package being installed, and the approximate size of the install package. Press **Next** to start the installation.
8. A status panel is displayed showing either that the installation completed successfully, or any messages if errors occurred during the installation. Press **Finish** to close the panel.

Uninstalling Web-based System Manager PC Client from a Windows System

1. From the taskbar, select **Start** —> **Settings** —> **Control Panel**.
2. In the **Control Panel**, double-click the **Add/Remove Programs** icon.
3. Select **Web-based System Manager PC Client** from the list of programs on the **Install/Uninstall** tab, then press the **Add/Remove** button to start the Uninstall wizard.
4. Press **Next** in the initial panel.
5. Press **Next** in the Confirmation panel to uninstall PC Client.
6. A status panel is displayed showing either that the installation completed successfully, or any messages if errors occurred during the installation. Press **Finish** to close the panel.

Installation Requirements for Secure Socket Layer Support

To have Web-based System Manager operate in a secure mode (using SSL Sockets that encrypts data transmitted over the network), the **sysmgt.websm.security** fileset must be installed and configured on both client and server machines.

For 128-bit encryption of data sent over the network, the **sysmgt.websm.security-us** fileset must be installed in addition to the **sysmgt.websm.security** fileset. Configuration is discussed in detail in “Chapter 5. Web-based System Manager Security” on page 33.

Integrating Web-based System Manager into Tivoli Netview Management Console

If you are using Tivoli NetView for AIX, you can integrate Web-based System Manager into the console. This integration allows the AIX server systems appearing on the NetView console to be managed using Web-based System Manager.

To integrate Web-based System Manager into Tivoli NetView run the following command by typing:

```
/usr/websm/bin/install_nv6k
```

Note: You must have Tivoli NetView installed and working correctly before running this command.

To remove the Web-based System Manager from Tivoli NetView, run the following command by typing:

```
/usr/websm/bin/remove_nv6k
```

Chapter 3. Using Web-based System Manager

You can access the Web-based System Manager console from any system that is locally attached to the console and is running a graphical desktop. Use one of the following methods to start the Web-based System Manager console:

- Double-click on the **Management Console** icon in the Common Desktop Environment (CDE). Select the **Application Manager** icon in the CDE front panel, then open the **System_Admin** folder. The **Management Console** icon is located in this folder.
- Type `wsm` from a terminal window.
- If a host has been set up with an HTTP Server, it can be accessed remotely from any computer capable of running Microsoft Internet Explorer or Netscape Communicator with the Java plug-in. To access the console from a browser, enter the system Web address: (*hostname*/wsm.html).

The console has five distinct elements, consisting of the following:

- “Navigation Area”
- “Contents Area”
- “Menu and Toolbar Actions” on page 16
- “Tips Area” on page 17
- “Status Bar” on page 17

Navigation Area

The *Navigation Area* displays a hierarchy of icons that represent collections of computers, individual computers, managed resources, and tasks. Each Navigation Area icon identifies a *plug-in*. At the highest point, or root of the tree, is the *Management Environment*. The Management Environment plug-in contains one or more host computer plug-ins that are managed by the console. Each computer plug-in contains multiple application plug-ins that contain managed objects, tasks, and actions for a related set of system entities or resources.

When you click on a plug-in icon in the Navigation Area, it opens to display its contents in the Contents Area. Navigation Area icons that are preceded by an expansion symbol (plus sign or '+') represent plug-ins that contain other plug-ins. When the expansion symbol is in the closed state (minus sign or '-'), a single-click on the icon causes the plug-in to display its lower-level plug-ins in the Contents Area, but does not expand the Navigation Area branch represented by the expansion symbol. A single click on the expansion symbol causes the Navigation Area branch to expand, revealing lower-level plug-ins, but does not update the Contents Area. By double-clicking on a Navigation Area icon, the navigation branch expands and the contents area updates to display the lower-level plug-ins.

You can adjust the width of the Navigation Area with respect to the Contents Area by clicking and dragging the Navigation Area sash to the right or left. If you need to maximize the space available for the Contents Area within the console, you can completely close off the navigation area by dragging the sash all the way to the left. A single click on the sash also causes the Navigation Area to close, and a subsequent click causes it to reopen to the previous position.

Contents Area

The contents area displays the contents of a plug-in. Three primary types of plug-ins are defined by what is presented in the contents area:

- “Containers” on page 14
- “Overviews” on page 15
- “Launchers” on page 15

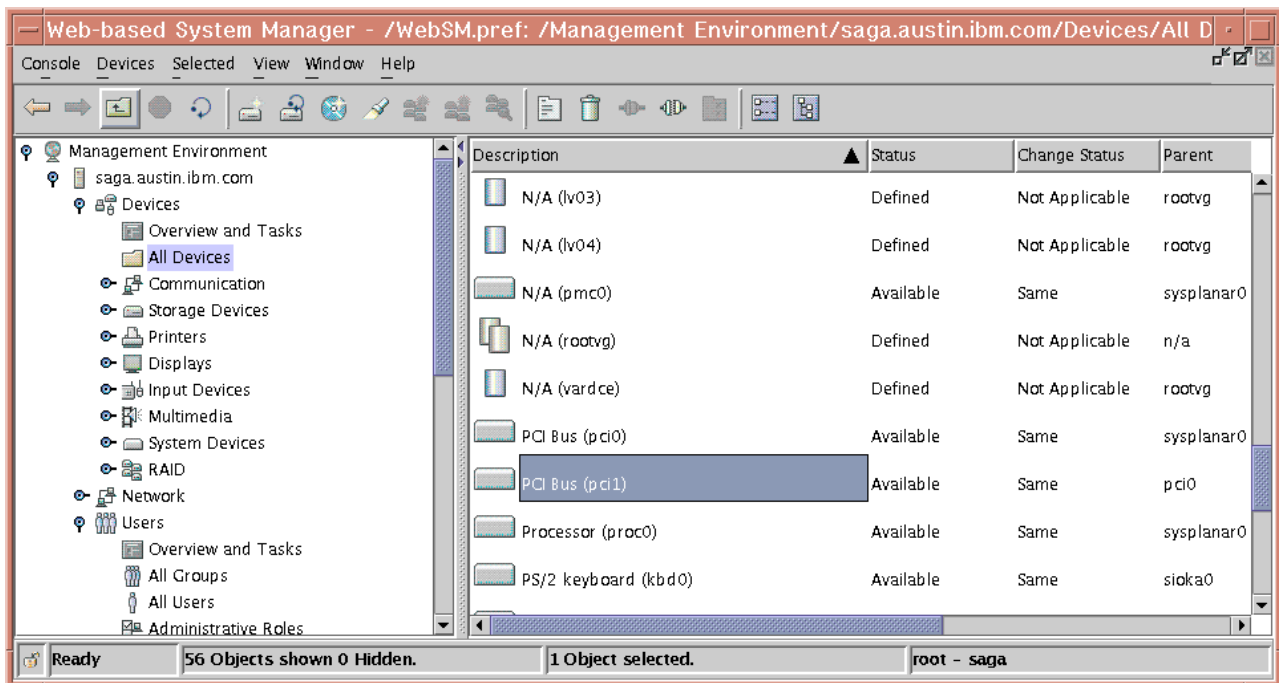
Containers

Containers or *container plug-ins* hold other plug-ins, icons that represent system resources (*managed objects*), or a mixture of managed objects and plug-ins. Containers are the most common type of plug-in in the Web-based System Manager user interface. You can think of them as folders that hold other folders or information objects.

Containers allow you to view properties as well as create, delete, or perform other actions on system resources. They present resource objects in one or more *views*. Web-based System Manager supports the following views:

- Large Icon
- Small Icon
- Details
- Tree
- Tree-Details

The following illustration is an example of the console Details view:



The Large Icon, Small Icon, and Details views allow you to decide which objects you want to see in the view by *filtering* the view. Filtering the view can be helpful if a container has a large number of objects and you only want to see certain objects or object types. For example, if you are managing users, you may want to view only administrative users.

The Large Icon, Small Icon, and Details views also allow you to change the order in which objects are listed in the view by sorting them. You can sort objects according to many different attributes (or *properties*) of the object.

You can sort in two ways:

- **Icon View**











You can sort the objects by selecting the **View** menu, then **Arrange Icons**. You then see a list of menu options for properties on which you can sort the view.

- **Details View**

You can sort objects by clicking on the column heading that defines an attribute on which you want to sort. The column heading toggles between ascending and descending sorts with each subsequent click.

Details view also allows you to change the order of columns and the width of individual columns. To change the position of a column, drag the column heading to the desired position (the leftmost column heading, typically the name of the objects, cannot be moved). To change the width of a column, drag the line dividing two column headings to the right or left.

In Web-based System Manager, icons are often used to indicate the state of a managed object. The following table shows some conventions that are used to indicate common conditions or states:

Condition or State	Appearance	Example Icons	Meaning
Normal, Active Object	Filled icon	  	Active user account Logical volume (online) Active process
Inactive, unconfigured, incomplete object	Unfilled outline of object	  	Expired user account Logical volume (offline) Inactive process
Missing object	Dotted outline of object		Defunct (zombie) process
Processing - object is updating	Clock indicator		Updating
Problem with object	Alert indicator		Warning
Critical problem with object - immediate attention is required	Critical indicator		Critical problem

Overviews

Overview plug-ins, Web page-like interfaces that display in the contents area, do the following:

- Explain the function provided by one or more plug-ins that constitutes an application.
- Provide easy access to routine or *getting started* tasks
- Summarize the status of key resources managed by the application

Because overviews do not display objects, they can provide quicker and easier access to frequently performed tasks. Overviews are also used when a management function is purely task-based and does not need icons to represent system resources (for example, back up and restore).

Launchers

Launch plug-ins resemble overviews. They are Web page-like panels that describe and provide a launch point for applications that run in their own window outside the Web-based System Manager console.

Menu and Toolbar Actions

The console menu bar provides all of the operations performed on the console and managed objects. The menus are organized as follows:

Console Menu

The Console Menu contains choices that control the console. It allows you to add and remove computers from the management environment, save console preferences, specify whether to automatically attempt to log in to a host with a stored password, view the console session log, and exit the console (see “Preference Files” on page 18).

Object Menu

The title of the *Object Menu* changes to indicate the type of resource managed by the current plug-in. For example, when the plug-in that manages hardware devices is selected, the Object Menu title becomes *Devices*. The Object Menu contains general choices and actions for a plug-in that do not require the selection of specific objects to act on. Typically, actions for creating new resource objects are located in the Object Menu. The **find** function is also located in the Object Menu. The contents of the Object Menu are updated when a new plug-in is selected.

Selected Menu

The Selected Menu contains those actions for a plug-in that require the user to select which managed objects an action is to apply to, such as *Open*, *Properties*, *Copy*, *Delete*, or *Start*. The contents of the Selected Menu are updated when a new plug-in is selected. It is disabled when Overview and Launch plug-ins are loaded.

View Menu

The View Menu contains choices for navigating, such as *Back*, *Forward*, and *Up One Level*. It also includes choices for customizing the console in the *Show* submenu. For example, you can select to show or hide the tool bar and status bar. When container plug-ins are loaded, the View Menu includes options that control how objects are presented. For example, if the plug-in provides a choice of views, such as *Large Icon*, *Small Icon*, *Details*, and *Tree*, these choices are listed here. If the plug-in only supports a single view, no view choices are listed. When a plug-in is displaying an icon or *Details* view, the View Menu includes choices for sorting and filtering the container.

Window Menu

The Window Menu contains actions for managing sub-windows in the console workspace. *New Window* creates a new console sub-window in the workspace. Other choices control how all console sub-windows are presented. For example, you can choose to have the windows completely cover the workspace like tiles, or have them stacked in a cascade fashion.

Help Menu

The Help Menu lists user assistance choices. When the computer that is acting as the system management server is properly configured with a HTTP Server to act as the *Documentation Server*, extensive online information is accessible through a Web browser. Different choices allow you to view help contents, search for help on a particular topic, and view help information on shortcut keys.

Pop-up Menus

Pop-up menus (sometimes called *context menus*) provide a quick way of accessing menu choices. To use pop-up menus with a mouse, point to an object, then click the right mouse button on a two- or three-button mouse. The pop-up menu lists the actions found in the Selected and Object menus for the current object or objects.

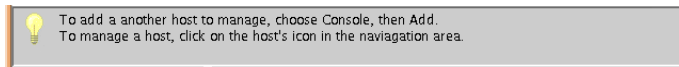
Tool Bar

The tool bar lists commonly used actions that are available when the current plug-in is loaded. It includes navigation controls, Find, and View choices (if available). The tool bar also provides tool tip help when the mouse pointer remains over a tool bar icon for a few seconds.

Tips Area

The Tips Area provides quick answers to frequent questions. A *tip* can be a simple one-line instruction, such as "To add another host to manage, choose Console, then Add." More frequently, however, tips are in the form of hypertext links. If browser-based help is correctly configured, clicking on a hypertext tip will open your default Web browser on the topic described in the link. You can choose to display or hide the Tips Bar by checking or unchecking the Tips Area option in the Show submenu under *View*.

The following illustration is an example of a tip.



Status Bar

The *status bar* displays at the lower edge of a console window. It has five fields for displaying status information, as follows:

- A **padlock** icon indicates whether the console is running in *secure* mode. In secure mode, communications between the client platform that is running the console, and the managed computer, is encrypted using SSL. The **padlock** icon is closed in secure mode and open when secure communications is not active.
- Plug-in loading status. When a plug-in is loaded, the text Ready is present. When a plug-in is in the process of loading, a graphic bounce bar displays.
- Number of objects that are visible in the contents area. Objects can be present on the managed host but hidden from the view by the view filter.
- Number of objects selected in the contents area.
- Security context (user name and host name) that the administrator is in for the currently active plug-in.

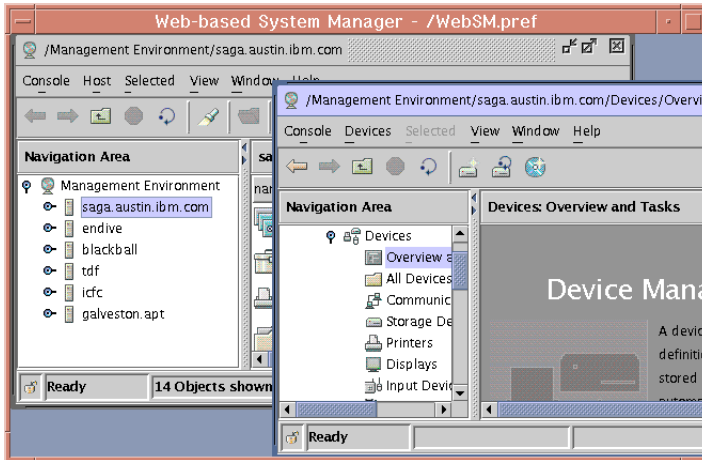
The status bar can be hidden or shown by unchecking or checking the **Status Bar** option in the Show submenu under *View*.

Console Workspace

The Web-based System Manager console has a Multiple Document Interface (MDI), allowing you to present different perspectives into the Management Environment. An MDI can be set to display multiple sub-windows, called *documents*, inside the outer window frame, called the *workspace*. By default, when the console opens, a single document window displays in a maximized state. To create multiple views of the Management Environment, first reduce the size of document window by using the window management controls on the right side of the toolbar.

The middle symbol reduces the size of the document window. The leftmost symbol minimizes the window inside the outer console. You can create a second document window by selecting the **New Window** choice in the Window Menu.

You can independently navigate to different locations within each document window. In this way, you can easily compare configuration settings of different resources on different hosts. The following diagram illustrates this process.



The Window Menu in each internal window provides menu choices for managing multiple windows in the workspace. The following table summarizes these choices.

Menu Choice	Function
New Window	Create a new instance of the workspace internal window.
Cascade	Organize the internal windows into a stack.
Tile Horizontally	Arrange the internal windows to completely fill the workspace from left to right.
Tile Vertically	Arrange the internal windows to completely fill the workspace from top to bottom.
Minimize other Windows	Minimize all internal windows except for the window that currently has focus (the window that this menu choice was made from).
Restore All	Restore all minimized windows to their previous size and position.
1. /Management Environment/	List of current internal windows. Selecting a window from this list opens it (if minimized), brings it to the front, and gives it focus.

Preference Files

The **preference** file is used to control the following functions in Web-based System Manager:

- Format a child window in the console window so that only user-specified components are displayed
- Set up user-specified view, filter, and sort preferences
- Provide a mechanism for managing different domains of machines

When Web-based System Manager is started, the preference file that is chosen displays the session using the preferences stored when it was last saved. This includes such preferences as the console window format and the machines being managed. By default the preference file is saved to:

```
$HOME/WebSM.pref
```

where \$HOME is the user's home directory on the managing machine.

To save the state of the console, use the menu option **Console -> Save**.

The state of the console can also be saved to other preference files. To save the state of the console to a file other than the default, use the menu option **Console -> Save As...** to display a dialog where you can specify an alternative pathname.

To use a preference file other than the default, see “Modes of Operation” on page 3.

A child window within the console window for Web-based System Manager has multiple components that can be displayed or hidden, based on a user’s preference. These child window format preferences are saved in the preference file, and are used whenever a session is started with the the specified preference file. The components of the child window can be displayed or hidden by using the cascade menu option **View -> Show**. The actual components of the child window that can be displayed or hidden, and whether they are saved in the preference file, are as follows:

Component	Status saved in preference file?
Navigation Area	No
Tool Bar	Yes
Tips Bar	Yes
Description Bar	Yes
Status Bar	Yes

During a Web-based System Manager session, a user can open multiple child windows. The child window format preferences that are saved when a session ends (assuming the user indicates that preferences are to be saved during exit) are those of the child window that had focus when the user ends the session. When this preference file is used to start another session, the child window in the console window (only one child window is created when a session is started) uses the saved child window format preferences.

For each application that is loaded, a user can define the objects that are displayed and how they are displayed through view, sort, and filter options that are defined by the application. The options that a user selects for each application are stored in the preference file. These options are then used whenever a session is started with the preference file where they were saved. A user can set these options in the following ways:

- Choose an application view by selecting the menu option **View -> View Option** checkbox.
- Choose a sort order for objects by selecting the cascade menu option **View -> Arrange Icons**
- Choose to filter displayed objects by selecting the menu option **View -> Filter Icons**

The host computers that are managed during a Web-based System Manager session are saved in the preference file. This allows a user to manage different domains of machines by starting sessions with different preference files. Thus a user can have a preference file that represents a group of machines that are HTTP Servers, and a preference file that represents a group of machines that are transaction servers.

For a group of machines to be saved to a preference file, they must be added to the Web-based System Manager Management Environment during a session. To add machines to the Management Environment during a session, select the menu option **Console -> Add -> Hosts...** This menu option displays a dialog where a user can enter individual host computers, a list of host computers from a file, or the host machines from a specified domain.

Error Handling for Loading or Saving Preference Files

The following situations can cause errors to occur:

- If the user does not specify any preference file, the default **\$HOME/WebSM.pref** file is used. This user does not have read access to this file or this file contains bad data. A warning dialog displays and default settings are used. The user can select another file with menu option **Console -> Save As...**, or

select the **Save the state of the console for the next session** option in the Exit Confirmation dialog when exiting a Web-based System Manager session.

- A user specifies a preference file, but does not have read access to this file, or this file contains bad data. The same procedures as above apply to these situations. The user does not have write access to the saving file. A warning dialog displays and the user can select another file with menu option **Console -> Save As...**, or exit without saving the preference file.
- If the preference-loading process fails, default settings will be used. During a Web-based System Manager exit session, the **Save the state...** option will be unselected to prevent a user from overwriting unintended data. The user can select **Save the state...** to overwrite the selected file.

Command Line Tools

The following table identifies commonly used command-line commands that are used to maintain Web-based System Manager:

Command	Used to:
/usr/websm/bin/configassist	The Configuration Assistant wizard displays automatically after the operating system is installed and is used to assist with configuration tasks. It can also be run at any time to complete additional configuration. Use the Configuration Assistant to configure a system that has an HTTP Server installed to run Web-based System Manager in a browser. See "Applet Mode" on page 4 for more informatoin. Arguments: None.

Command	Used to:
<p>/usr/websm/bin/wsm</p>	<p>Start a Web-based System Manager client session.</p> <p>Arguments:</p> <ul style="list-style-type: none"> • -host <i>managing host</i> Forces Web-based System Manager to initially connect to the specified host. Even though you can easily manage other hosts while running Web-based System Manager, this option allows you to start Web-based System Manager with the preferences you set up on the specified host machine. • -lang <i>Language</i> Specifies in which language messages are displayed. If the sysmgt.msg.Language.websm.apps fileset is not installed, messages will be displayed in English. • -port <i>port number</i> Causes Web-based System Manager to connect to any other hosts using the specified port. This port number used must match the port number on the managed machines for the wsmserver service specified in the /etc/services file. • -profile <i>pathname of preference file</i> Specifies an <i>alternate</i> preference file. The default preference file will be a file named WebSM.pref found in the user's home directory. Using this option enables the user to use a different preference file. This can be useful if the user manages different sets of machines for different clients. <p style="text-align: right;">Note: The preference file is read from either the local machine, or from the machine specified in the -host argument.</p>
	<ul style="list-style-type: none"> • -user <i>username</i> Causes Web-based System Manager to run as the given user name. You will be prompted for the user's password. • DdefaultTurners=<i>value</i> When the <i>value</i> is true, Java Look and Feel turners are used instead of Windows turners for parent tree nodes in the Navigation Area and the Contents Area. No angled lines are drawn between tree objects. • -DdrawTreeLine=<i>value</i> When <i>value</i> is true and -DdefaultTurners=true, causes angled lines to be drawn between tree objects in the Navigation Area and the Contents Area. • -Ddatadir=<i>path</i> Specifies an alternate directory to look for configuration files normally found in /var/websm/config/user_settings.
<p>/usr/websm/bin/wsmaccess</p>	<p>Wrapper around wsm command to enable Accessibility features.</p> <p>Arguments: Same as /usr/websm/bin/wsm.</p>

Command	Used to:
<p>/usr/websm/bin/wsmserver</p>	<p>Enables or disables a machine as a Web-based System Manager server, that is, a machine that can be managed through a Web-based System Manager client.</p> <p>Arguments:</p> <ul style="list-style-type: none"> • -enable Updates the TCP/IP services so that inetd daemon will listen for Web-based System Manager-client requests on port 9090 . By default, Web-based System Manager is configured during installation not to accept client requests. • -disable Removes port 9090 from those ports that are responded to by the inetd daemon. This disables the machine from responding to new Web-based System Manager client requests. It does not terminate existing Web-based System Manager server processes. • -start Starts a Web-based System Manager server. This server waits for a request from a Web-based System Manager client. This option is not needed in normal operations. • -ssloptional Allows, at the discretion of the user, the server to be managed either in SSL or with a standard socket. • -sslalways Allows only the server to be managed by a client if an SSL connection can be created between the client and server.

User-Editable Files

A few Web-based System Manager files might need modification by the user or administrator. In general, the state of a session is saved for each user in the preference file (see “Preference Files” on page 18). The only files that might be modified to change some global behavior of Web-based System Manager are as follows:

- **/var/websm/config/user_settings/websm.cfg**

This file contains settings that control global behavior of the Web-based System Manager application.

The following table identifies the file contents:

Variable Name	Description	Possible Values
<i>forcssl</i>	<p>If set to true, indicates that the machine on which the websm.cfg file exists can only be managed if the client attempting to manage it can do so by establishing an SSL connection to the managing machine. See “Chapter 5. Web-based System Manager Security” on page 33.</p> <p>Note: Web-based System Manager on systems prior to AIX 5.1 used a different interpretation for the <i>forcssl</i> flag. At that time, the interpretation was that SSL communication would be required if the <i>forcssl</i> flag was set to true <i>and</i> SSL was configured on the server. In AIX 5.1, if the <i>forcssl</i> flag is set to true and the server does not have SSL configured, then the server cannot be managed by a remote client.</p>	true or false
<i>remote_timeout</i>	The amount of time (in milliseconds) that a client will wait for a connection to a managed machine. If the connection cannot be made in this amount of time, the client abandons the server. If the client did not abandon the server, then it would continue to wait indefinitely if an attempt was made to manage a non-existent machine.	<p>Integer values</p> <p>An appropriate value can depend on network performance. The default value is 30000 (30 seconds). If network performance is slow (it is often the case that a remote machine cannot be accessed even though it is known that the remote machine exists and is available) this value should be increased.</p>

The only option that Web-based System Manager currently uses in this file is the *forcssl* flag. This flag is used when a client connects to a managed machine. If the value of the *forcssl* flag is **true**, then the server will only connect to a client through secure connections (SSL sockets). If this flag is set to **false**, the server will attempt to communicate to a client through secure socket connections if SSL is configured on both the client and the server. But if there is a problem connecting through SSL sockets, the server will allow the client to connect through non-secure sockets (see “Chapter 5. Web-based System Manager Security” on page 33).

Help

Web-based System Manager provides a variety of ways of obtaining assistance and additional information.

Hover Help

Provides assistance for icons in the tool bar. Position the mouse pointer over a tool bar icon and wait for a couple of seconds. A text label displays, identifying the meaning of the icon.

Tips Provides assistance on common tasks performed with the currently active plug-in. Tips are displayed between the menu and tool bars. Tips are provided in the form of simple text instructions or hypertext links to browser-based help. The user can hide or show the tips area according to preference by using the Show submenu in the View menu. (See “Tips Area” on page 17 for additional information).

Context Help

Provides assistance on the use of dialog windows. Access context help by clicking the **Help** button in the lower-right corner of the dialog. A small context help window displays. When you click on individual controls in the dialog, assistance on the use of that control displays in the context help window. When context help is running, you can only access the controls in the dialog to view help.

To use the controls, you must first close the context help window either by clicking the **Close** button on the context help window or clicking the **Help** button in the dialog that you sought help on.

Browser-based Help

Provides extensive information for tasks in the browser-based help system. To use the browser-based help system, you must first have a document server configured. After the help server has been identified to the managed host, you can access browser-based help by making a selection from the Help menu in the menu bar or by clicking on a link in a Tips area.

Filtering and Sorting Views

When a plug-in supports Large Icons, Small Icons, or Details view, you can make it easier to locate objects by filtering or sorting the view. Filtering reduces the number of objects displayed in the contents area. You can filter a view either by specifying the names of objects or by defining one or more rules for excluding objects from the view:

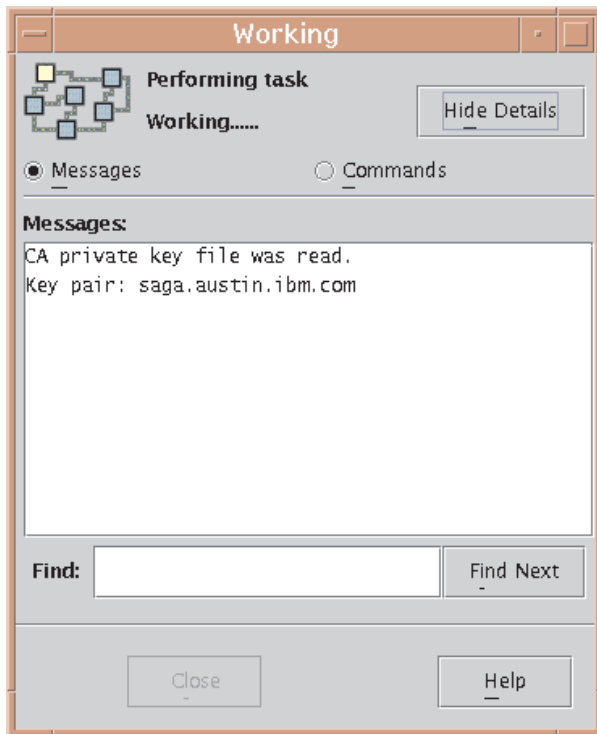
- To filter objects, select the View menu, then the **Filter** icon. The **Filter** tab lets you define a list of objects to exclude from the view. To specify an object to hide, type its name in the field to the right of the **Add** button. Then press the **Add** button. Repeat this task for each object that you want to hide. Alternatively, you can click the **Browse** button to display a list of objects that can be hidden. Select those objects that you want to hide and click **OK**. They display in the **Hidden Objects** list. To remove the listed objects from the contents area, press either **OK** or **Apply**.
- The **Advanced** tab lets you define one to three rules for hiding objects based on specific attributes of those objects. For example, to hide all of the administrative users from the All Users plug-in, open the filter dialog and select the **Advanced** tab. Make sure the **Hide the objects** check-box is checked. Then select the **Type** property, and the = relationship. Enter the matching value **Administrator**, and click **OK** or **Apply**. All of the administrative users are removed from the view. You can supply additional rules by clicking the **Add Rule** button. An additional rule definition row displays. Multiple rules are combined by an AND operation. To remove rules, click on the **Remove** button to the right of the rule. To remove the last rule, clear the matching value from the rule.

Both the **Filter** tab and the **Advanced** tab can be used together if the **Hide** check-box is checked on both tabs.

Working Dialog

The working dialog displays when long-running actions are being performed on a managed computer. Depending upon the application, it can display as a simple dialog with an animation to indicate that the action is progressing.

The following illustration is an example of the Working dialog:



When running in simple mode, the dialog can be expanded to display details of the action that is executing. To view details, click the **Details** button at the bottom of the dialog. You can view two types of details:

Commands

The shell script that is currently executing.

Messages

Information being displayed to standard output (stdout).

Conversely, when details are displayed, you can shrink the size of the dialog by clicking the same button to hide details.

Depending on the nature of the application, the working dialog may automatically dismiss when the action completes successfully. If the action fails, the dialog remains open and expands to reveal message details to assist in diagnosing the problem. For tasks in which it is important that the user review the results of a successfully completing action, the working dialog may remain open upon completion so that the user can review messages before dismissing the dialog.

Keyboard Control of Web-based System Manager

Web-based System Manager can be used with or without a pointing device, such as a mouse. If you choose not to use a pointing device, you can move among controls and menus using only the keyboard.

Using Mnemonics and Shortcuts

You can access menu functions using the following keyboard methods:

- **Mnemonics:** Mnemonics are underscored letters in menu choices and control text. To access a visible menu choice or control, press the Alt key followed by the mnemonic. When using mnemonics, it is not necessary to use the space bar or Enter key to select an item.

- **Shortcuts:** Shortcuts (also known as *accelerators*) are keyboard combinations that directly access frequently used controls. Shortcuts also use a combination of keys to access functions, in this case, the Ctrl key followed by a character. Unlike mnemonics, menu shortcuts do not require that a menu choice be visible to be directly accessed.

Navigating the Console with the Keyboard

Use the following keystrokes to navigate the Web-based System Manager console:

Key Stroke	Actions
Arrow Keys	Moves focus between: <ul style="list-style-type: none"> • Objects in the Navigation Area. Right and left arrows expand and contract nodes; up and down arrows move vertically through items. • Objects in the Contents Area • Icons in tool bar • Items in menus
Ctrl + Arrow Key	Move location focus to another object in the contents area without selecting it. By using Ctrl+Arrow keys and the space bar, you can select multiple objects that are not contiguous.
Escape	Closes an open menu without activating a choice
F1	Opens browser-based help to contents section
F8	Moves focus to the splitter bar between the Navigation Area and Contents Area of the console. Moves the splitter bar using Home, End, and the arrow keys.
F10	Moves focus to and from the Menu bar
Shift + Arrow Key	Extends a contiguous selection
Spacebar, Enter	Selects the object that has focus
Tab, Shift + Tab	Moves focus between areas of the console

Navigating Dialog Boxes with the Keyboard

Use the following keystrokes to navigate Web-based System Manager dialog boxes:

Key Strokes	Actions
Alt+F6	Moves focus into or out of a dialog box
Arrow keys	<ul style="list-style-type: none"> • Opens drop down lists • Moves between options in lists • Moves between tabs in tabbed dialogs when a tab has focus
Ctrl + Tab, Ctrl + Shift + Tab	Moves focus between controls
Enter	Activates the command button that has focus
Escape	Cancel the dialog box
F1	Opens the context help window
Space Bar	<ul style="list-style-type: none"> • Selects the option that has focus • Activates the command button which has the location cursor on it.

Accessing Help with the Keyboard

Use the following keystrokes to navigate the Web-based System Manager help system:

Note: The help system must first be configured before these keyboard functions will operate.

F1	<ul style="list-style-type: none">• Opens browser-based help to the Contents Area• In dialog boxes, opens context help window
F9	Shows keys help.
Alt + F6	In context help mode, moves focus between context help window and parent dialog.

Session Log

The Session Log is a console facility that tracks changes made on managed hosts during a Web-based System Manager session. Each time an administrator uses Web-based System Manager to make a change on a host, an entry in the log is created. Entries may also be generated by applications to report intermediate results, warnings, or error conditions. Each entry includes the time and date of the change, the user who made the change, the host where the change was made, and a short message. The user can double-click on a message to see the complete message text. Click on the columns displayed in the log window to change the sort order of entries, for example, the entries can be sorted by time and date (default order), host name, user name, and message. The log window includes a *Find* capability for searching for entries that include a particular text string. The administrator can also manage the log by erasing its contents using the **Clear** button, and by saving it to a file.

To view the session log, select **Console -> Session Log**.

Chapter 4. Management Environment Configuration

The Management Environment is a set of machines that a user can manage from within the Web-based System Manager application. The user can add or delete members from this set. The Navigation Area and Contents Area in the Web-based System Manager application window provide an interface to access these machines. The user performs system administration tasks on this set of machines. The Web-based System Manager application provides the user with two approaches to adding or deleting a machine. The first approach is through the Console menu. The second approach is through the Web-based System Manager Management Environment plug-in. Either approach guides the user in adding or deleting a machine from the Management Environment.

In addition, the Web-based System Manager application provides the user with a means to save a set of machines to a particular session. When Web-based System Manager is initially launched, the only machine that is present in the Navigation Area and Contents Area is the managing machine. After a machine is added, that machine can be preserved for future use if the user selects to save preferences either through the Console menu or upon exiting the Web-based System Manager application.

Adding a Machine to Web-based System Manager

Web-based System Manager identifies machines in the Management Environment by the exact name that the user provides when the machine is added to the environment. This means that a machine that is added with both a fully qualified host name, as well as an abbreviation for the fully qualified host name, will be listed twice in the Management Environment, as if they are two different computers.

For example, if your domain name is *mycorp.com*, you will be able to create a managed machine in the Management Environment called *machine_name*, as well as *machine_name.mycorp.com*. To Web-based System Manager, these are two different machines. A warning dialog that informs you that another machine has the same first element hostname, thus alerting you that both *machine_name* and *machine_name.mycorp.com* will be added. If you do not intend to have both machine names in the Management Environment, you can take preventive action.

You can use either of two methods to add a machine to Web-based System Manager:

Console menu:

1. Select **Console** in Web-based System Manager application menu.
2. Select **Add**.
3. Select **Hosts**.

Web-based System Manager Management Environment plug-in:

1. Select **Management Environment** in the Navigation Area.
2. Select **Management Environment** in Web-based System Manager application menu.
3. Select **New**.
4. Select **Hosts**.

After the user has launched the add dialog, you can add the machine in one of three ways:

- Add single host computer with option to verify existence on network.
- Add a list of computers from a file.
- Add computers in a domain.

Examples

To add a single machine called `chocolate.austin.ibm.com`:

1. Select **Add the host computer with this name**:
2. Enter `chocolate.austin.ibm.com` in text field.
3. Press the **Add** button.

The assigned computer name appears in the Navigation Area and Navigation Pane. A message below the progress bar states `Successfully added... chocolate.austin.ibm.com`.

To add a single machine and verify existence on the network:

1. Select **Add the host computer with this name**:
2. Enter `coconut.austin.ibm.com` in text field.
3. Select **Verify that the host is on the network**.
4. Press the **Add** button.

The assigned computer name appears in Navigation Area and Navigation Pane. If the host does not exist on the network, a Web-based System Manager error dialog displays, stating that the following host cannot be contacted.

To add a list of machines from a file:

1. Select **Add the host computers listed in this file**.
2. Enter the complete file path in the text field, or select **Browse** and then select **file**.
3. Select **yes** from the confirmation dialog to add list of machines.

A message below the progress bar indicates which machine is currently being added. After it is complete, a message displays stating `Successfully completed`. The added computers appear in Navigation Area and Navigation Pane.

To add machines from domain:

1. Select **Add the computers in this domain**.
2. Enter domain name.
3. Select **yes** from the confirmation dialog to add list of machines.

A message below the progress bar indicates which machine is currently being added. After it is complete, a message displays stating `Successfully completed`. The added computers appear in Navigation Area and Navigation Pane.

Removing a Machine

The Web-based System Manager application has two approaches to removing or deleting machines from the Navigation Area:

Console menu:

1. Select **Console** in Web-based System Manager application menu.
2. Select **Remove**.
3. Select **Hosts**.
4. Select the machines to remove.
5. Press the **Remove** button.
6. Select **yes** in the confirmation dialog to remove the selected machines.

Management Environment plug-in:

1. Select **Management Environment** in the Navigation Area.
2. Select machines to delete from the Navigation Pane.
3. Select **Selected** in Web-based System Manager application menu.
4. Select **yes** in the confirmation dialog to remove the selected machines.

Chapter 5. Web-based System Manager Security

Web-based System Manager Security provides for the secure operation of the Web-based System Manager in client-server mode. In the Web-based System Manager secure operation, the managed machines are servers, and the managing users are the clients. The communication between the servers and clients is over the SSL protocol that provides server authentication, data encryption, and data integrity. The user manages the machine on Web-based System Manager using an account on that machine and authenticates to the Web-based System Manager server by sending the user ID and password over the secured SSL protocol.

Each Web-based System Manager server has its private key and a certificate of its public key signed by a Certificate Authority (CA) that is trusted by the Web-based System Manager clients. The private key and the server certificate are stored in the server's private key ring file. The Web-based System Manager client has a public key ring file that contains the certificates of the CAs that it trusts.

In applet mode (working from the browser), the client must be assured that the applet (**.class** files) arriving at the browser is coming from the intended server. Moreover, in this mode, the public key ring file resides on the server and is transferred to the client with the rest of the applet **.class** files, because the browser does not allow applets to read local files. For sender authentication and integrity of these files, the client must use the SSL capabilities of the browser and contact the server only with the **HTTPS** protocol (**HTTPS://...**). For this, you can use the SSL capability of the HTTP Server on each managed machine, or you can use the **SMGate** daemon installed with Web-based System Manager Security. The **SMGate** daemon serves as an SSL gateway between the client browser and the web server.

This section discusses the following procedures and processes related to Security:

- “Installing Web-based System Manager Security”
- “Configuring Web-based System Manager Security”
- “Enabling Web-based System Manager Security” on page 44
- “Enabling the SMGate Daemon” on page 44
- “Running Web-based System Manager Security” on page 45.

Installing Web-based System Manager Security

The Web-based System Manager Security fileset, **sysmgt.websm.security**, where available, can be found on the AIX 5.1 Expansion Pack.

An additional fileset, **sysmgt.websm.security-us**, with stronger encryption capabilities, is available on the AIX 5.1 Expansion Pack that ships in some countries. This fileset requires that you have **sysmgt.websm.security** installed.

Configuring Web-based System Manager Security

Web-based System Manager Security provides both a graphical interface and a command line interface to configure for secure administration. To access the graphical interface, select **Management Environment** → *hostname* → **System Manager Security** → **Overview and Status**. These tasks are visible only in local mode. In different scenarios discussed below, they are referred as the Certificate Authority Overview and Server Security Overview. In these scenarios, the graphical interface is used. The corresponding command is listed for each step.

Security Scenarios

The following scenarios or configuration possibilities are outlined:

- “Using Ready-to-Go Key Ring Files”
- “Administering Multiple Sites” on page 36
- “Avoiding Transfer of Private Keys” on page 39
- “Using Another Certificate Authority” on page 40.

Using Ready-to-Go Key Ring Files

Using the Ready-to-Go Key Ring Files is usually the fastest way to get into security operational state. In this scenario, use a single machine to define an internal CA (Certificate Authority) and generate ready-to-go key ring files for all of your Web-based System Manager servers and clients. This generates a public key ring file that you must copy to all of the servers and clients as well as a unique private key ring file for each server.

The following steps describe how to use Ready-to-Go Key Ring Files:

1. Define an Internal Web-based System Manager Certificate Authority.

You should use a safe system for the CA because its private key is the most sensitive data in the Web-based System Manager security configuration.

Note: Do not use diskless or dataless workstations as Certificate Authorities, because the private key would be transferred over the network.

After the CA machine is chosen, log in locally as the root user and start Web-based System Manager. The security configuration applications of Web-based System Manager are not accessible if you are not logged in as the root user or if you are running Web-based System Manager in remote application or applet mode.

Select **Management Environment** → *hostname* → **System Manager Security** → **Certificate Authority**.

On the task list for **Certificate Authority**, select **Configure this system as a Web-based System Manager Certificate Authority**. When the wizard opens, fill in the following information:

- **Certificate Authority distinguished name**
Enter a descriptive name that helps you identify the CA machine and the instance of the CA; for example, the machine’s host name plus a sequence number. Blanks are permitted in the name. If you redefine the CA, use a different sequence number so you will be able to determine which instance of the CA a certificate is signed by. The name should not be exactly the same as the full TCP/IP name, as this will not work with the **SMGate** daemon.
- **Organization name**
Enter a descriptive name that identifies your company or your organization.
- **ISO country code**
Enter your two-character ISO country code or select it from the list.
- **Expiration date**
After the certificate expires, reconfigure Web-based System Manager security by redefining the CA and generating new private key ring files for all of your servers. You can change this date or accept the default value.
- **Public key ring directory**
The public key ring containing the CA’s certificate is written to this directory. Copy this file to the **/usr/webasm/codebase** directory on all of the Web-based System Manager servers and clients.

- **Password**

The CA's private key ring file is encrypted with this password. You need to enter this password each time you perform a task on this CA.

You can also define an internal CA from the command line with the `/usr/websm/bin/smdefca` command.

2. **Generate Private Key Ring Files for Your Web-based System Manager Servers.**

Provide the full TCP/IP names of all of your Web-based System Manager servers.

On the task list for **Certificate Authority**, select **Generate Servers' Private Key Ring Files**. In the CA password dialog, enter the password that you specified when you defined the CA. Then fill in the following information:

- **List of servers**

Add the names of your Web-based System Manager servers to the list. You can enter them in the dialog one at a time, or you can provide a file containing a list of your servers, one per line. To get the server names from the file, enter the file name in the **File containing list of servers** entry field and click the **Browse file** button. Use the **Browse Server List File dialog** to select some or all of the servers in the list.

- **Organization name**

Enter a descriptive name that identifies your company or your organization.

- **ISO country code**

Enter your two-character ISO country code or select it from the list.

- **Location for private key ring files**

Enter the directory where you want the server private key ring files written. Later, you need to distribute them to the servers and install them.

- **Length in bits of server keys**

Select a key **length** (this field displays only if you have the `sysmgt.websm.security-us` fileset installed).

- **Expiration date**

After the certificate expires, you need to generate new private key ring files for your servers. You can change this date or accept the default.

- **Encrypt the server private key ring files**

This dialog creates a private key ring file for each server that you specified. Each private key ring file contains the private key of a server and therefore, must always be kept protected. You can protect the private key ring files by encrypting them. If you select this option, you are prompted for a password, which you need when you install the private key rings on the servers.

When you click **OK**, a private key ring file is created for each server that you specified.

You can also generate public key ring files from the command line with the `/usr/websm/bin/smgenprivkr` command.

3. **Distribute the Public Key Ring File (SM.pubkr) to All Servers and Clients.**

A copy of the CA public key ring file from the directory you specified in step 1 must be placed in the `/usr/websm/codebase` directory of your Web-based System Manager servers and clients.

Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus, access to this file on the client machine should be limited. In applet mode, the client can trust the server to send over this file along with the applet itself, provided the **HTTPS** protocol is used.

4. **Distribute the Private Key Ring Files to All Servers.**

Each server's private key ring file must be installed on the server.

You can move the files to their targets in any secure way. Shared directory and diskette TAR methods are described here:

- **Shared directory:** Place all of the key ring files on a shared directory (for example, NFS or DFS) accessible to each server.

Note: For this method, you should have chosen to encrypt the server private key ring files on the **Generate Servers Private Key Ring Files** dialog, because the files are transferred in the clear, that is, the files are transferred without encryption. It is also recommended that you restrict the access rights to the shared directory to the administrator.

- **Diskette TAR:** Generate a diskette TAR containing all of the server private key ring files. The TAR archive should contain only the file names without the paths. To do this, change directories to the directory containing the server private key ring files and run the command `tar -cvf /dev/fd0 *.privkr`.

Next, install the server private key rings on each server. Log on to each server as root user, start Web-based System Manager and select **Management Environment** → *hostname* → **System Manager Security** → **Server Security**. From the task list, select **Install the private key ring file for this server**. Select the source for the server private key ring files. If using a diskette, select `tar diskette`, insert the diskette, and then click **OK**. If the key ring files are encrypted, you are asked for the password. The server's private key is installed in `/var/websm/security/SM.privkr`. Repeat this procedure on each server.

You can also distribute private key ring files to all servers from the command line with the `/usr/websm/bin/sminstkey` command.

Administering Multiple Sites

Use this scenario if you have multiple sites and do not want to distribute private key ring files between sites. Suppose you have site A and site B, and you define your internal Web-based System Manager Certificate Authority (CA) on a machine in site A. See step 1 of "Ready-to-Go Key Ring Files" for directions on configuring a CA.

Note: For all clients and for site A servers, you can follow the instructions in using "Using Ready-to-Go Key Ring Files" on page 34.

For servers in site B, follow these steps:

1. Generate Private Keys and Certificate Requests for Your Web-based System Manager Servers.

Provide the full TCP/IP names of all Web-based System Manager servers in site B. You can enter them in the dialog one at a time, or you can provide a file containing a list of your servers, one per line.

On a server in site B, log in locally as root user and start Web-based System Manager. The security configuration applications of Web-based System Manager are not accessible if you are not logged in as root user or if you are running the Web-based System Manager in remote application or applet mode.

Select **Management Environment** → *hostname* → **System Manager Security** → **Server Security**.

On the task list for **Server Security**, select **Generate Servers' Private Keys and Certificate Requests**. Fill in the following information:

- **List of servers**
Add the names of your Web-based System Manager servers in site B to the list. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line. To get the server names from the file, enter the file name in the **File containing list of servers** entry field and click the **Browse file** button. Use the **Browse Server List File dialog** to select some or all of the servers in the list.
- **Organization name**
Enter a descriptive name that identifies your company or your organization.

- **ISO country code**
Enter your two-character ISO country code or select it from the list.
- **Location for private key ring files**
Enter the directory where you want the server private key ring files and certificate requests written. In step 2, transfer the certificate request files to the CA in site A for signing. In step 3, transfer the signed certificates from the CA in Site A back to this directory.
- **Length in bits of server keys**
Select a **key length** (this field displays only if you have the **sysmgt.websm.security-us** fileset installed).
- **Encrypt the server private key ring files**
This dialog creates a private key ring file for each server that you specified. Each private key ring file contains the private key of the server, and therefore, must always be kept protected. You can protect the private key ring files by encrypting them. If you select this option, you are prompted for a password, which you need when you import the signed certificates and when you install the private key rings on the servers.

When you click **OK**, a private key ring file and a certificate request is created for each server that you specified.

You can also generate private keys and certificate requests from the command line with the **/usr/websm/bin/smgenkeycr** command.

2. Get the Certificates Signed by the CA in Site A.

Transfer the certificate request files to the CA in site A. The certificate requests do not contain secret data. However, the integrity and authenticity during transfer must be ensured.

Transfer a copy of the certificate request files from the server in site B to a directory on the CA machine in site A.

Log in to the CA machine in site A locally as root user and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root user or if you are running the Web-based System Manager in remote application or applet mode.

Select **Management Environment** → *hostname* → **System Manager Security** → **Certificate Authority**.

On the task list for **Certificate Authority**, select **Sign Certificate Requests**. Fill in the following information:

- **Directory for certificate requests**
Enter the directory containing the certificate requests. Then click the **Update List** button. The certificate request list displays.
- **Select certificate requests to sign**
To select individual certificate requests, click on them in the list box. To select all of the listed certificate requests, click the **Select All** button.
- **Certificate expiration date**
After the certificate expires, you need to repeat this process to generate new private key ring files for your servers. You can change this date or accept the default date.

When you click **OK**, a certificate file is created for each server that you selected. The certificates are written to the directory containing the certificate requests.

You can also get the certificates signed by the CA by running the following command from the command line: **/usr/websm/bin/smsigncert**.

3. Import the Signed Certificates to the Servers Private Key Ring Files.

In this step, transfer the certificates from the CA in site A back to the server in site B. Copy them to the directory containing the certificate requests and server private key files that you created in step 1.

Then, on the server in site B from the **Server Security** task list, select **Import Signed Certificates**. Fill in the following information:

- **Directory for certificates and private keys**

Enter the directory containing the signed certificates and server private key files. Then, click the **Update List** button. The list of servers for which there is a signed certificate and a private key file displays.

- **Select one or more servers from the list**

To select individual servers, click on them in the list box. To select all of the listed servers, click the **Select All** button.

When you click **OK**, if the server private key files were encrypted in step 1, you are prompted for the password. Then, for each server that you selected, the certificate is imported into the private key file and the private key ring file is created.

You can import signed certificates from the command line with the `/usr/websm/bin/smimpservercert` command.

4. **Distribute the Private Key Ring Files to All Servers.**

Each server's private key ring file must be installed on the server.

You can move the files to their targets in any secure way. Shared directory and diskette TAR methods are described here:

- **Shared directory:** Place all of the key ring files on a shared directory (for example, NFS or DFS) that is accessible to each server.

Note: For this method, you should have chosen to encrypt the server private key ring files on the **Generate private keys and certificate requests for this server or other servers** dialog, because the files are transferred in the clear, that is, the files are transferred without encryption. It is also recommended that you restrict the access rights to the shared directory to the administrator.

- **Diskette TAR:** Generate a diskette TAR containing all of the server private key ring files. The TAR archive should contain only the file names without the paths. To do this, change directories to the directory containing the server private key ring files and run the command `tar -cvf /dev/fd0 *.privkr`.

Next, install the server private key rings on each server. Log in to each server as root user and start Web-based System Manager. Select **Management Environment** → *hostname* → **System Manager Security** → **Server Security**. Then select **Install the private key ring files for this server**. Select the source for the server private key ring files. If using a diskette TAR, insert the diskette before clicking **OK**. If the key ring files are encrypted, you are asked for the password. The server's private key is installed in `/var/websm/security/SM.privkr`. Repeat this procedure on each server.

You can also distribute the private key ring files from the command line with the `/usr/websm/bin/sminstkey` command.

5. **Distributing the CA Public Key Ring File to All Servers and Clients in Site B.**

A copy of CA public key ring file from the directory you specified in step 1 must be placed in the `/usr/websm/codebase` directory of your Web-based System Manager servers and clients.

Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus, make sure that you limit access to this file on the client machine. In applet mode, the client can trust the server to send over this file along with the applet itself, provided the **HTTPS** protocol is used.

Avoiding Transfer of Private Keys

Use this scenario if you want a private key to be generated on the server it belongs to, preventing it from being transferred (by network or diskette) to other systems. In this scenario, you configure each server separately. The process must be repeated on each server.

Before you follow this scenario, configure your CA, following the steps using “Using Ready-to-Go Key Ring Files” on page 34.

This scenario involves the following tasks:

1. Generate a Private Key and Certificate Request for Your Web-based System Manager Server.

On the server, log in locally as root user and start Web-based System Manager. The security configuration applications of Web-based System Manager are not accessible if you are not logged in as root user or if you are running Web-based System Manager in remote application or applet mode.

Select **Management Environment** → *hostname* → **System Manager Security** → **Server Security**.

On the task list for **Server Security**, select **Generate private keys and certificate requests for this server and other servers**. Fill in the following information:

- **List of servers**
Add the name of this Web-based System Manager server to the list. The server name is shown by default in the first text field. Click the **Add to List** button to add the server to the list.
- **Organization name**
Enter a descriptive name that identifies your company or your organization.
- **ISO country code**
Enter your two-character ISO country code or select it from the list.
- **Location for private key ring files**
Enter the directory where you want the server private key ring file and certificate request written. In step 2, transfer the certificate request file to your CA for signing. In step 3, transfer the signed certificate from the CA back to this directory.
- **Length in bits of server keys**
Select a **key length** (this field displays only if you have the **sysmgt.websm.security-us** fileset installed).
- **Encrypt the server private key ring files**
This dialog creates a private key ring file for the server that you specified. The private key ring file contains the private key of the server, and therefore, must always be kept protected. You can protect the private key file by encrypting it. If you select this option, you are prompted for a password, which you need when you import the signed certificate and when you install the private key ring in this server.

When you click **OK**, a private key ring file and a certificate request is created for this server.

You can perform this task from the command line with the **/usr/websm/bin/smgenkeycr** command.

2. Get the Certificates Signed by the CA.

Transfer the certificate request file to your CA. The certificate request does not contain secret data. However, the integrity and authenticity during transfer must be ensured.

Transfer a copy of the certificate request file from the server to a directory on the CA machine. To save time, you can transfer the certificate requests from all of your servers and have all of them signed by the CA in one step.

Log in to your CA machine locally as root user and start Web-based System Manager. The security configuration applications of Web-based System Manager are not accessible if you are not logged in as root user or if you are running Web-based System Manager in remote application or applet mode.

Select **Management Environment** → *hostname* → **System Manager Security** → **Certificate Authority**.

On the task list for **Certificate Authority**, select **Sign Certificate Requests**. Fill in the following information:

- **Directory for certificate requests**
Enter the directory containing the certificate requests. Then, click the **Update List** button. The certificate request displays.
- **Select certificate requests to sign**
Click on your server's certificate requests in the list box.
- **Certificate Expiration Date**
After the expiration date, you need to repeat this process to generate a new private key ring file for your server. You can change this date or accept the default date.

When you click **OK**, a certificate file is created for each server that you selected. The certificate is written to the directory containing the certificate request.

You can perform this task from the command line with the `/usr/websm/bin/smsigncert` command.

3. Import the Certificates to the Private Key Files.

Transfer the certificate from the CA back to the server. Copy it to the directory containing the certificate request and server private key file that you previously created in step 1.

Then, on the server, from the task list for **Server Security**, select **Import Signed Certificates**.

Fill in the following information:

- **Directory for certificates and private keys**
Enter the directory containing the signed certificate and server private key file. Then, click the **Update List** button. The server displays in the list box.
- **Select one or more servers from the list**
Click on your server's name in the list box.

When you click **OK**, if the server private key file was encrypted in step 1, you are prompted for the password. Your server's certificate is imported into the private key file, and the private key ring file is created in the directory containing the certificate request and private key file.

You can perform this task from the command line with the `/usr/websm/bin/smimpservercert` command.

4. Install the Private Key on the Server.

On the task list for **Server Security**, select **Install the private key ring file for this server**. Select the **Directory** button and enter the directory containing the server's private key ring file. If the key ring file was encrypted, you are asked for the password. The server's private key is installed in `/var/websm/security/SM.privkr`.

You can perform this task from the command line with the `/usr/websm/bin/sminstkey` command.

5. Distribute the Public Key Ring File (SM.pubkr) to All Servers and Clients.

A copy of **SM.pubkr** from the directory you specified in step 1 must be placed in the `/usr/websm/codebase` directory of your Web-based System Manager servers and clients.

Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus, make sure that you limit access to this file on the client machine. In applet mode, the client can trust the server to send over this file along with the applet itself, provided the **HTTPS** protocol is used.

Using Another Certificate Authority

Use this scenario if you do not want to use an internal Web-based System Manager CA, but instead you want to use another internal CA product that may already be functioning on your system. In this scenario, your certificate requests are signed by this other CA.

1. Generate Private Keys and Certificate Requests for Your Web-based System Manager Servers.

Provide full TCP/IP names of all your Web-based System Manager servers. You can enter them in the dialog one at a time, or you can provide a file containing a list of your servers, one per line.

On a server, log in locally as root user and start Web-based System Manager. The security configuration applications of Web-based System Manager are not accessible if you are not logged in as root user or if you are running Web-based System Manager in remote application or applet mode.

Select **Management Environment** → *hostname* → **System Manager Security** → **Server Security**.

On the task list for **Server Security**, select **Generate private keys and certificate requests for this server and other servers**. Fill in the following information:

- **List of servers**

Add the names of your Web-based System Manager servers to the list. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line. To get the server names from the file, enter the file name in the **File containing list of servers** entry field and click the **Browse file** button. Use the **Browse Server List File dialog** to select some or all of the servers in the list.

- **Organization name**

Enter a descriptive name that identifies your company or your organization.

- **ISO country code**

Enter your two-character ISO country code or select it from the list.

- **Location for private key ring files**

Enter the directory where you want the server private key ring files and certificate requests written. In step 2, transfer the certificate request files to the CA for signing. In step 3, transfer the signed certificates from the CA back to this directory.

- **Length in bits of server keys**

Select a **key length** (this field displays only if you have the **sysmgt.websm.security-us** fileset installed).

- **Encrypt the server private key ring files**

This dialog creates a private key ring file for each server that you specified. Each private key ring file contains the private key of a server, and therefore, must always be kept protected. You can protect the private key ring files by encrypting them. If you select this option, you are prompted for a password, which you need when you import the signed certificates and when you install the private key rings on the servers.

When you click **OK**, a private key file and a certificate request is created for each server that you specified.

You can perform this task from the command line with the **/usr/websm/bin/smgenkeycr** command.

2. **Get the Certificates Signed by the CA.**

Transfer the certificate request files to the CA. The certificate requests do not contain secret data. However, the integrity and authenticity during transfer must be ensured.

Transfer a copy of the certificate request files from the server to a directory on the CA machine.

Follow the instructions of your CA to generate the signed certificates out of the certificate requests.

3. **Import the Signed Certificates to the Server's Private Key Ring Files.**

Transfer the certificates from the CA back to the server. Copy them to the directory containing the certificate requests and server private key files that you created in step 1. This step requires that the certificate file of server *S* be named **S.cert**.

Then, on the server, from **Server Security**, select **Import Signed Certificates**.

Fill in the following information:

- **Directory for certificates and private keys**
Enter the directory containing the signed certificates and server private key files. Then click the **Update List** button. The list of servers for which there is a signed certificate and a private key file displays.
- **Select one or more servers from the list**
To select individual servers, click on them in the list box. To select all of the listed servers, click the **Select All** button.

When you click **OK**, if the server private key files were encrypted in step 1, you are prompted for the password. Then, for each server that you selected, the certificate is imported into the private key file and the private key ring file is created.

You can perform the above task from the command line with the `/usr/websm/bin/smimpservercert` command.

4. **Distribute the Private Key Ring Files to All Servers.**

Each server's private key ring file must be installed on the server.

You can move the files to their targets in any secure way. Shared directory and diskette TAR methods are described here:

- **Shared directory:** Place all of the key ring files on a shared directory (for example, NFS or DFS) accessible to each server.

Note: For this method, you should have chosen to encrypt the server private key ring files on the **Generate private keys and certificate requests for this server and other servers** dialog, because the files are transferred in the clear. It is also recommended that you restrict the access rights to the shared directory to the administrator.

- **Diskette TAR:** Generate a diskette TAR containing all of the server private key ring files. The TAR archive should contain only the file names without the paths. To do this, change directories to the directory containing the server private key ring files and run the command `tar -cvf /dev/fd0 *.privkr`.

Next, install the server private key rings on each server. Log in to each server as root user and start Web-based System Manager. Select **Management Environment** → *hostname* → **System Manager Security** → **Server Security**. Select **Install Private Key Ring**, then select the source for the server private key ring files. If using a diskette TAR, insert the diskette before clicking **OK**. If the key ring files are encrypted, you are asked for the password. The server's private key is installed in `/var/websm/security/SM.privkr`. Repeat this procedure on each server.

You can perform this task from the command line with the `/usr/websm/bin/sminstkey` command.

5. **Import the Certificate Authority's Certificate to the Public Key Ring File.**

Receive the self-signed CA certificate of your CA. Copy it to a directory on the server you are working on.

Then, on the server, from the task list for **Server Security**, select **Import CA Certificate**.

Fill in the following information:

- **Directory containing public key ring file**
Enter a directory for the CA public key ring file. This file needs to be distributed to all of your servers and clients.
- **Full path name of CA Certificate file**
Enter the directory containing the self-signed certificate of your CA.

When you click **OK**, the public key ring file **SM.pubkr** is written to the directory you specified.

You can perform the above task from the command line with the `/usr/websm/bin/smimpcacert` command.

6. **Distribute the Public Key Ring File to All Clients and Servers.**

A copy of the CA public key ring file must be placed in the `/usr/websm/codebase` directory of all Web-based System Manager servers and clients.

Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus, make sure that you limit access to this file on the client machine. In applet mode, the client can trust the server to send over this file along with the applet itself, provided the **HTTPS** protocol is used.

Configuring for the SMGate Daemon

The **SMGate** daemon installed with Web-based System Manager Security allows you to run in secure applet mode without having to configure security on each managed system. **SMGate** serves as an SSL gateway between the client browser and the local web server.

To use the **SMGate** daemon, install the certificate issued by the Certificate Authority (CA) onto each client browser, as follows:

1. If you are using the Web-based System Manager internal certificate authority, you can get the CA certificate using the following procedure:
 - a. Log in to the CA machine as root user.
 - b. Start Web-based System Manager.
 - c. Open the Management Environment and select your local host.
 - d. Select **Export Certificate Authority's Certificate** from the task list.
 - e. In the Export Certificate Authority's Certificate dialog, enter the full path name where the certificate is to be written.
 - f. Click **OK**.

Alternatively, from the command line, type:

```
/usr/websm/bin/smexpcacert
```

Note: If you are not using the Web-based System Manager internal certificate authority, then use your certificate authority's procedures for obtaining a copy of its certificate.

2. Copy the certificate to an HTTP Server directory so that you can access it from the client browser. The MIME type sent by the HTTP Server must be **application/x-x509-ca-cert**.
3. In each of your client browsers, point the browser to the CA certificate file and follow your browser's procedure to accept it as a signer certificate.

Your browsers are now set up to connect to your servers through the **SMGate** daemon. For information about enabling the **SMGate** daemon, see "Enabling the SMGate Daemon" on page 44. For information about running through SMGate, see "Applet Mode" on page 45.

Viewing Configuration Properties

After the security configuration has been completed, you can view the properties of the Certificate Authority (CA), any server, and any client's public key ring.

To view CA properties, do the following:

1. Open the Management Environment and select your local host.
2. Select the Web-based System Manager **Security** object.
3. Select the **Certificate Authority** object.
4. Select **Properties** from the task list.
5. Enter the password.

Note: The dialog provides read-only information for the CA.

Detailed information on all operations executed by the CA (for example, key ring generation or certificate signing) can be found in the `/var/websm/security/SMCa.log` CA log file.

You can perform this task from the command line using the `/usr/websm/bin/smcaprop` command.

To view a server's properties, do the following:

1. Open the Management Environment and select your local host.
2. Select the Web-based System Manager **Security** object.
3. Select **Server Security**.
4. Select **View properties for this server** from the task list.
5. Enter the password.

Note: The dialog provides read-only information for the server.

You can perform this task from the command line using the `/usr/websm/bin/smserverprop` command.

Public Key Ring Content

To view the CA certificate included in the CA public key ring, use the `/usr/websm/bin/smlistcerts` command.

Enabling Web-based System Manager Security

On each managed system, you can enable the security option that you want to enforce.

To enable security so that the managed system accepts secure or unsecure connections, run the `wsmserver -ssloptional` command. In this mode, the user at the client can select an option on the Web-based System Manager login dialog to specify a secure or unsecure connection.

To enable a managed system to only accept secure connections, run the `/usr/websm/bin/wsmserver -sslalways` command.

Enabling the SMGate Daemon

The SMGate daemon can only be enabled after the server's private key ring has been installed.

To enable SMGate, type the following command:

```
/usr/websm/bin/wsmserver -enablehttps
```

This command starts SMGate and adds an entry to the `/etc/inittab` file so that it is automatically activated when the system is restarted. The default port for SMGate is 9092. Examine the `/etc/services` file to make sure this port is not being used by another service. You can configure SMGate to use a different port by typing:

```
/usr/websm/bin/wsmserver -enablehttps port
```

where *port* is the port number you want it to use.

If you change the server's security configuration, you must disable SMGate. Disable SMGate by typing:

```
/usr/websm/bin/wsmserver -disablehttps
```

To configure the browser to work through SMGate, see "Configuring for the SMGate Daemon" on page 43.

Running Web-based System Manager Security

Web-based System Manager runs in application mode when you use a machine as a client to manage another machine.

Application mode

To activate application mode, on the client, type the following command:

```
wsm -host hostname
```

where *hostname* is the name of the remote machine that you want to manage.

If the machine to be managed is configured to allow secure connections only (see “Enabling Web-based System Manager Security” on page 44), then the client must have the **sysmgt.websm.security** fileset installed, and must have a copy of the CA public key ring file in the **/usr/websm/codebase** directory. In this mode, the Web-based System Manager login dialog indicates that security is required.

If the machine to be managed is configured to allow secure or unsecure connections (see “Enabling Web-based System Manager Security” on page 44) and the client has a copy of the CA public key ring file in the **/usr/websm/codebase** directory, the Web-based System Manager login dialog allows the client user to specify a secure or unsecure connection.

When running in application mode, security is indicated by a secure connection message on the status line at the bottom of the window.

Applet Mode

Web-based System Manager runs in applet mode when you use a browser to connect to the machine you want to manage. Applet mode adds another security consideration for the secure transfer of the CA public key ring file and the applet's **.class** files. For complete security in applet mode, the client must use the SSL capabilities of its browser and contact the server only with the **HTTPS** protocol. This requires that the HTTP Server is configured for security or that SMGate is configured through one of the following options:

- One option is to use the SSL capability of the Web server on the managed machine. For this option, the Web server must be configured for security. Follow the instructions provided with your Web server. Then you can access Web-based System Manager on the managed machine with the following Web address: **https://hostname/wsm.html**, where *hostname* is the name of the remote machine you want to manage. In this option, the applet and the **SM.pubkr** public key ring are transferred securely from the Web server on the managed machine to the client.
- Another option is to use the **SMGate** daemon. **SMGate** runs on managed machines and serves as an SSL gateway between the client browser and the local Web server. **SMGate** responds to the **HTTPS** request of the client browser, and creates an SSL connection with it by using the private key and certificate of the Web-based System Manager server. Inside the managed machine, **SMGate** creates an unsecure connection to the local Web server.

In this option, the applet and **SM.pubkr** public key ring are securely transferred from **SMGate** on the managed machine to the browser client. Communications between the managed machine and client are over SSL. When you are using **SMGate**, you can access Web-based System Manager on the managed machine with the following Web address: **https://hostname:9092/wsm.html**, where *hostname* is the name of the remote machine you want to manage.

Note: 9092 is the default port number for **SMGate**. If you enabled **SMGate** with a different port number, then specify that number.

When you are running in applet mode, make sure the following security indicators are present:

- The browser's **HTTPS** indication

- The secure connection message on the status line at the bottom of the Web-based System Manager windows.

If either indicator is missing, the connection is not completely secure.

Chapter 6. Web-based System Manager Accessibility

Web-based System Manager provides keyboard accessibility features and implementation of the Self Voicing Kit (SVK). Both are these features are described in detail in the following sections.

Keyboard Accessibility

The goal of keyboard accessibility is for the user to be able to use the Web-based System Manager without having to use a mouse. The following keyboard accessibility features are available:

- Menu mnemonics: All menu choices can be selected from the keyboard by typing the letter indicated in the menu title. For example, for a menu with **Properites** as a choice, open the menu and type **r** to select the Properites option.
- Menu accelerators or shortcut keys: Key combinations are available for common actions. For example, Ctrl + Q to quit and F9 for Key Help.
- Dialog Accessibility Features: Mnemonics and accelerators are available for dialog buttons. For example, pressing the Enter key activates the OK button and pressing Esc activates the Cancel button.

Keys Help (F9) provides a description of all keyboard shortcuts and accelerator keys. Other types of shortcuts include, special keys for moving between console areas and expanding tree branches.

Text-to-Speech Support

The Self Voicing Kit (SVK) provides a link between the Java code and a speech synthesizer which translates the Web-based System Manager GUI to speech output. This section describes how the SVK supports speech output for Java applications, such as Web-based System Manager, without requiring modification of the base code.

The following fileset is required to run the SVK within Web-based System Manager: **sysmgt.websm.accessibility**. This fileset is available on the base AIX installation CD.

The SVK is available from the IBM AlphaWorks web site at:

<http://www.alphaworks.ibm.com>

Using Web-based System Manager with the Self-Voicing Kit

The SVK, based on a new Access Engine technology from IBM, is launched as an assistive technology by Sun's Java Accessibility utility class, EventQueueMonitor. The engine communicates with Web-based System Manager's accessible components and manages the information from Web-based System Manager so that user interface presentation extensions can quickly access the information through the SVK Toolkit class library. The SVK class library contains many utility functions, which include, but are not limited to, speaking text, reading application text, and activating accessible components.

Once installed, the SVK loads automatically into the Java Virtual Machine (JVM) with the Web-based System Manager. Optionally, an external keypad can be connected to the other serial port to provide navigation functionality for a blind user. If the keypad is not installed, there is a key sequence to put the user into *review mode*. In *review mode*, keystrokes are directed to SVK to provide functionality similar to the external keypad.

For more information on the Self Voicing Kit, refer to the *IBM Self Voicing Kit User's Guide*.

Appendix A. Troubleshooting

The following troubleshooting topics are available:

- “Troubleshooting Remote Machines”
- “Troubleshooting Web-based System Manager in Applet Mode” on page 50
- “Troubleshooting Web-based System Manager in PC Client Mode” on page 50
- “Troubleshooting Security” on page 51

Troubleshooting Remote Machines

Problem	Action
Cannot manage a remote host as a Web-based System Manager managed machine.	<p>Verify the following:</p> <ul style="list-style-type: none"> • The host you are attempting to manage has operating system earlier than AIX 5.1. Systems at levels prior to AIX 5.1 can only be managed by systems at the same level. Therefore, to manage this system, a system at the same level must be used, the system must be updated to AIX 5.1 or later, or the system must be managed locally. • The host you are attempting to manage has a sysmgmt.websm.framework at a level prior to AIX 5.1 installed. Machines with sysmgmt.websm.framework levels prior to AIX 5.1 can only be managed by systems at the same level. Therefore, to manage this system, a system with sysmgmt.websm.framework at the same level must be used, the system must be updated to AIX 5.1 or later, or the system must be managed locally.
Cannot manage a remote host as a Web-based System Manager managed machine. (continued)	<ul style="list-style-type: none"> • The host you are attempting to manage is listening on inetd port 9090. If this is the case, there will be a line in the /etc/services file similar to: <pre>wmsserver 9090/tcp</pre> <p>In addition, there will be a line in the /etc/inetd.conf file similar to the following: <pre>wmsserver stream tcp nowait root \ /usr/websm/bin/wmsserver wmsserver -start</pre> <p>If this is not the case, use the following command: <pre>/usr/websm/bin/wmsserver -enable</pre> <p>This can be tested using the following command: <pre>tn hostname 9090</pre> <p>If the remote host is configured correctly, it will respond with a message similar to the following: <pre>Trying... Connected to saga.austin.ibm.com. Escape character is ' T'. Language received from client: Setlocale: en_US WServer.HANDSHAKING 41292 WServer.HANDSHAKING en_US</pre> <p>where <i>en_US</i> is replaced by the language fileset installed on your machine.</p> <p>If it does respond with the previous output, there is an idle server process running on the machine that is consuming system resources. Log in to the remote server and use the kill command on the idle WServer process.</p> </p></p></p></p>

Problem	Action
Plug-in installed on a remote host is not showing up when managing from a client.	<ul style="list-style-type: none"> The plug-in on the remote host may be at a level that cannot be managed by the sysmgt.websm.framework level that is installed on the client system. In this case, an error message is displayed when the connection is made to the remote host, which lists the plug-in and the plug-in's version and required sysmgt.websm.framework version needed to manage the plug-in. To manage this plug-in, you will need to find a system where the sysmgt.websm.framework version is at the correct level for the plug-in, or manage the plug-in locally on that host. The App*.db file on the remote host is not formatted correctly. An error message is displayed for the plug-in warning that the App*.db file is not in the correct format for that plug-in and that the plug-in could not be loaded. If this occurs, please contact your customer representative for corrective action.

Troubleshooting Web-based System Manager in Applet Mode

Problem	Action
When using Netscape Communicator on a PC, the browser prompts you to download the Java plug-in. Netscape Communicator opens the page, but cannot find the Java plug-in.	<ol style="list-style-type: none"> Verify you are using Netscape Communicator 4.7 or 4.7x. Netscape Communicator 6.0 is not supported. Netscape Communicator does not always find the correct plug-in. Manually download and install the plug-in.
The browser freezes after pressing the Refresh or Reload button bringing the Web-based System Manager back up.	<p>Browsers sometimes do not reload applets correctly. You can try either of the following:</p> <ul style="list-style-type: none"> Refresh or delete the browser's cache. Restart the browser. This forces the browser to reload the applets.
Attempting to connect to http://yourmachine/wsm.html shows only your Web server's home page.	<p>The html files did not get linked to the web server's pub directory. To correct the problem:</p> <ol style="list-style-type: none"> Run configassist. Configure a Web server to run Web-based System Manager. Verify that there are Web-based System Manager files in the web server's pub directory.

Troubleshooting Web-based System Manager in PC Client Mode

Problem	Action
Double-clicking on PC Client icon does not launch the application	System environmental variables are created or modified during installation. From the Environment tab in the Control Panel , check that the value of the WSMDIR variable only contains the value of the installation directory, for example C:\ProgramFiles\websm . This directory must also be contained within the PATH variable.

Installation fails	<p>The installation might have failed for any of the following reasons:</p> <ul style="list-style-type: none"> • There must be 60 MB free on the default drive. • There must 50 MB free on the destination drive. • The correct version of browser must be used. Netscape Communicator 6.0 is not supported. • The AIX server must be configured correctly to install PC Client. <p>For more information, see “Installing Web-based System Manager PC Client” on page 10.</p>
--------------------	---

Troubleshooting Security

Problem	Action
Security functions do not operate.	Make sure that you are logged in as the root user, and that you are operating Web-based System Manager on the local machine.
When trying to use the Certificate Authority (CA) for generating key rings or signing certificate requests, a message displays indicating that the Certificate Authority is in use.	If you are sure that no other administrator is currently using the CA, remove the CA lock file /var/websm/security/SMCa.lock .
In SMGate configuration, the browser does not recognize the CA certificate file as a CA certificate.	Check that the mime type being sent by the Web server for the certificate file is application/x-x509-ca-cert .
Secure remote activation of Web-based System Manager fails.	<ul style="list-style-type: none"> • Verify that Web-based System Manager works in non-secure remote mode. You might need to change the server's setting if it does not support non-secure connections. • Certificate matching and expiration: <ul style="list-style-type: none"> – Log in to the server as the root user and use the Server Properties dialog of the Server icon (or the smserverprop command) to verify the server's certificate expiration date. Record the CA name. – If the problem occurred in application mode, type: <code>/usr/websm/bin/smlistcerts /usr/websm/codebase</code> on the client and verify that the client includes a certificate of the CA that signed the server's certificate (above), and that this certificate has not expired. If the problem is in applet mode, run the following: <code>/usr/websm/bin/smlistcerts /usr/websm/codebase</code> on the server, because the public key ring resides on the server and is transferred to the client.

Appendix B. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement 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.

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
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and

cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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.

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

AIX 5L Version 5.1
Web-based System Manager Administration Guide

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

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

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

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

Please tell us how we can improve this book:

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

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

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



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

PLACE
POSTAGE
STAMP
HERE

IBM Corporation
Publications Department
Internal Zip 9561
11400 Burnet Road
Austin, TX
78758-3493

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line



Printed in U.S.A