AIX 6.1

IBM Systems Director Console for AIX

SC23-5242-00

AIX 6.1

IBM Systems Director Console for AIX

SC23-5242-00

Note

Before using this information and the product it supports, read the information in “Notices” on page 17.

First Edition (November 2007)

This edition applies to AIX Version 6.1 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 Information Development, Department 04XA-905-6C006, 11501 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.

Contents

About this document v
Highlighting v
Case-sensitivity in AIX v
ISO 9000 v

IBM Systems Director Console for AIX 1
IBM Systems Director Console for AIX overview 1
Operational modes 1
System requirements 1
IBM Systems Director Console for AIX accessibility 1
IBM Systems Director Console for AIX installation and configuration 2
Installing IBM Systems Director Console for AIX 2
Enabling the runtime 2
Changing port values 3
Starting IBM Systems Director Console for AIX 3
IBM Systems Director Console for AIX user interface layout 3
Navigating the IBM Systems Director Console for AIX 4
Authorization 5
Logging in to IBM Systems Director Console for AIX 5
Authorizing console users 5
Console administrator role 7
User authority task 7
Main page 8
Add page 8
Modify page 8
Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client 9
Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client using CA-signed certificates 9
Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client using self-signed certificates 13
Troubleshooting IBM Systems Director Console for AIX 16

Notices 17
Trademarks 18

Index 19

About this document

The IBM Systems Director Console for AIX allows for the web-enabled administration of AIX management tasks. The console can be accessed from any supported web browser. A programmer, system administrator, or service representative should use this guide when installing, configuring, or performing problem determination.

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.

Italics 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.

Case-sensitivity in AIX

Everything in the AIX operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type `LS`, the system responds that the command is `not found`. Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

ISO 9000

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

IBM Systems Director Console for AIX

IBM® Systems Director Console for AIX® is a Web-based application that provides a graphical interface with which you can administer AIX servers remotely. IBM Systems Director Console for AIX is installed as part of the system management bundle.

You can access the IBM Systems Director Console for AIX from the following supported Web browsers: Internet Explorer 7 on Windows®, Mozilla Firefox 2.0 on Windows, and Mozilla Firefox 1.5.0.10 on AIX.

The IBM Systems Director Console for AIX console window contains two primary panels. The panel on the left displays the tasks you can perform from the console. This panel is called the navigation tree. The panel on the right, called the work area, displays results that are based on the item that is selected in the navigation tree. When you select a task in the navigation tree, the work area is updated to show the available choices.

IBM Systems Director Console for AIX overview

This section lists the IBM Systems Director Console for AIX system requirements and accessibility features.

Operational modes

IBM Systems Director Console for AIX runs in any supported Web browser. You are not required to install a console component on your client.

System requirements

IBM Systems Director Console for AIX has the following system requirements.

Server

- AIX 6.1
- 80 MB of disk space
- Java™ 5

Client

- Microsoft® Windows Internet Explorer 7.0 or later on Windows
- Mozilla Firefox, 2.0 on Windows
- Mozilla Firefox 1.5.0.10 on AIX

IBM Systems Director Console for AIX accessibility

The IBM Systems Director Console for AIX user interface runs in your browser. Consult the documentation for your browser for information about your browser's accessibility features.

The following features are provided for vision-impaired users:

- Supports interfaces commonly used by screen readers (Microsoft® Windows® systems only)
- Can be operated by using only the keyboard
- Communicates all information independent of color
- Supports interfaces commonly used by screen magnifiers (Microsoft Windows systems only)
- Supports the attachment of alternate output devices
- Provides help information in an accessible format

The following features are provided for users who have mobility impairments or limited use of their hands:

- Allows the user to request more time to complete timed responses
- Can be operated by using only the keyboard
- Supports the attachment of alternative input and output devices

The following features are provided for the deaf and hard-of-hearing users:

- Supports alternatives to audio information
- Supports adjustable volume control

The IBM Systems Director Console for AIX help system has the following accessibility features:

- Uses the accessibility support enabled by the browser that is used to display the help
- Enables navigation by using the keyboard

IBM Systems Director Console for AIX installation and configuration

IBM Systems Director Console for AIX installation and configuration includes installing the required and optional filesets, enabling the IBM Systems Director Console for AIX runtime, and changing port values if needed.

Installing IBM Systems Director Console for AIX

To use IBM Systems Director Console for AIX, it must installed on each managed server. IBM Systems Director Console for AIX is included in the System Management bundle (SystemMgmtClient.bnd) and is part of the default operating system installation.

To verify that IBM Systems Director Console for AIX is installed, you can use the SMIT List Installed Software menus or the operating system command line tools. For example, you can run the following command:

```
lslpp –h sysmgt.pconsole.rte
```

If IBM Systems Director Console for AIX is not installed, you can install it using the SMIT Software Installation menus or the operating system command line tools. For example, you can run the following command:

```
/usr/lib/instl/sm_inst installp_cmd –a –d /dev/cd0 –f sysmgt.pconsole –c –N –g -X
```

This installs the required filesets for IBM Systems Director Console for AIX. The required filesets are:

- lwi.runtime
- sysmgt.pconsole.rte
- sysmgt.pconsole.apps.wsmit
- sysmgt.pconsole.apps.wdcem
- sysmgt.pconsole.apps.wrbac
- sysmgt.pconsole.aps.websm

Enabling the runtime

The IBM Systems Director Console for AIX runtime is registered as a subsystem under the control of the system resource controller (SRC). It is started by default at system start up.

You can check, stop, and start the runtime using the SMIT -> Processes & Subsystems -> Subsystems menus or the command line tools for SRC. For example, run the following command to check the runtime:

```
lssrc –s pconsole
```

To stop the runtime, run the following command:

```
stopsrc –s pconsole
```

To start the runtime, run the following command:

```
startsrc –s pconsole
```

Changing port values

IBM Systems Director Console for AIX uses the http: 5335 and https: 5336 ports.

Modify the following properties in the **/pconsole/lwi/conf/overrides/config.properties** file and then restart **pconsole** to change these ports:

- com.ibm.pvc.webcontainer.port=5335
- com.ibm.pvc.webcontainer.port.secure=5336

Also modify **/pconsole/lwi/conf/webcontainer.properties**. Change all occurrences of 5336 to the secure port you wish to use.

Starting IBM Systems Director Console for AIX

You can access the IBM Systems Director Console for AIX from a Web browser.

Start IBM Systems Director Console for AIX in your browser by launching the following URL:

http://*HostName*:5335/ibm/console

Where *HostName* is the name of the server you want to manage.

IBM Systems Director Console for AIX user interface layout

The IBM Systems Director Console for AIX user interface layout has three major elements, the banner and tool bar, the navigation tree, and the work area.

Banner and tool bar

The banner and tool bar display a common image across IBM Systems Director Console for AIX installations. The banner and toolbar includes a greeting to the user who is logged in and links to log out of the console and to open console help.

Navigation tree

The navigation tree lists the tasks that are available in the console. Tasks are grouped into organizational nodes that represent categories of tasks (for example, **OS Management** or **Settings**). The organizational nodes can be nested in multiple levels.

The navigation tree only displays tasks to which you have access, according to the authorizations you have been given. When you select a task in the navigation tree, a page containing one or more modules for completing the task is displayed in the work area.

Work area

When you initially log in to the console, the work area displays a welcome page. After you launch a task from the navigation tree, the contents of the task are displayed in a page in the work area. A page contains one or more console modules that are used to perform operations. Each console module has its own navigation controls. Some pages include a control to close the page and return to the welcome page.

Navigating the IBM Systems Director Console for AIX

This topic describes how to navigate pages and modules in IBM Systems Director Console for AIX.

IBM Systems Director Console for AIX navigation includes the following tasks:

- Launching pages from the navigation tree
- Using the title bar controls
- Accessing help
- Using the console help controls

Launching pages from the navigation tree

The console navigation tree provides a hierarchical view of all of the applications or tasks available in the console. A task is a page in the work area. All of the modules to start and complete the task are provided on the page. To open a task, press the task name in the navigation tree. The task is opened in a new page in the work area.

The following table describes the controls for the console navigation tree and entries in the tree:

Icon	**Function**
+	Represents an organizational node in the navigation tree that contains pages or other navigation nodes. Click the icon to expand the node.
-	Closes an organizational node.
None	This is an elementary administrative task. When you click on this type of node, the work area will display all of the necessary selectors and dialogs to perform the action, as well as suggestions for contents.

Using the title bar controls

Each page contains one or more Web applications or console modules. A console module enables you to perform an operation, such as displaying a list or stopping a managed system. The title and the controls for the module are displayed on the title bar. The functions supported by the module determine which icons are displayed.

In addition to the controls on the title bar, a module can include controls for other actions, such as a button to submit input. Some modules have controls that launch other modules. If a module launches another module, the newly launched module is displayed on the same page in an area near the bottom of the page.

Accessing help

Help is available for the entire console or for a specific module in the console. To access console help, perform the following steps:

1. Press Help on the console toolbar. The help is displayed in a separate browser window.
2. In the help navigation tree, select the help set you want to view. For example, press **Console help** to view topics that provide helpful information for new console users. Use the console help controls as needed.

To access help for a module on a page, perform the following steps:

1. On the title bar for the module, click the ? icon. This icon is displayed only if help is available for the module. The help is displayed in a separate browser window.

2. Close the help window when you are finished viewing the help.

Console settings

The **Console Settings** category in the navigation tree contains tasks for setting and modifying console properties such as user-to-role assignments and enabling logging.

Authorization

IBM Systems Director Console for AIX security considerations include logging in, authorizing console users, use of the console administrator role, the user authority task, user authorization, and configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client.

Logging in to IBM Systems Director Console for AIX

To access IBM Systems Director Console for AIX, enter your user ID and password for the server and press **Log in**. IBM Systems Director Console for AIX relies on your AIX user account for user-logon security.

If the user ID that you provide is already logged into the console, the console prompts you to choose between logging out from the other session or returning to the login page. If you choose to log out from the other session, the console will not recover any unsaved changes that were made by that user.

Be sure to use the **Logout** link in the console toolbar when you are finished using the console to prevent unauthorized access. If there is no activity during the login session for an extended period of time, the session expires and you must log in again to access the console. The default session timeout period is 30 minutes.

The following steps provide an example of how IBM Systems Director Console for AIX can be used to modify the properties of a user name:

1. Start the console in a browser from the URL http://*HostName*:5335/ibm/console, where *HostName* is your server name.
2. On the login page, enter your user name and password for this server.
3. In the navigation tree, expand **OS Management** and select **Security & Users**. The work area shows the choices for **Security & Users**.
4. Select **Users**. The work area shows the choices for **Users**.
5. Select **Change / Show Characteristics of a User**.
6. Select the user name you want to modify the properties for and click **OK**. The work area displays the properties for this user.
7. Modify the properties of the selected user. Press **OK** to save the changes.

Authorizing console users

You can log into the console as root, which gives you the authority to perform all tasks, or you can delegate certain tasks to non-root users. If the only user that you want to authorize as a console user is root, no further set up is required.

The root id has console administrator authorization, which authorizes them to launch any console task. By default, console tasks are visible only to root. If you want to authorize non-root users to perform console tasks, some additional setup is required. You must authorize each user to access one or more tasks that appear in the console navigation area and you must assign to each user the AIX authorizations for the actions performed by these tasks.

The following table lists the tasks that appear in the console navigation area, the corresponding AIX authorizations, and the console role for each task. For your convenience, the table includes space for you to record user ids and AIX role names for future reference. (Note: Review the Readme file in /pconsole for updates to the information in this table.) The AIX authorizations shown in this table are supported when AIX enhanced role based access control (RBAC) is enabled. With these authorizations, it is possible for non-root users to perform tasks that previously could only be performed by root. You can authorize users to perform tasks in the console with the following steps:

1. Identify your console users and their responsibilities.
2. Identify the tasks in the console navigation area that each user may perform. Record this information in the User ID column of this table for future reference.
3. Create AIX roles containing the AIX authorizations required for each of the tasks. Decide on the role names and record them in the AIX Role column of this table for future reference. To create the roles, log into the console as root, expand OS Management and select the Roles Based Access Control task in the console navigation area. Refer to the table for the authorizations required for each task.
4. Assign the AIX roles to users according to their responsibilities. Log in to the console as root, expand **OS Management**, and select the **Security & Users** task in the console navigation area. Refer to the role name and user ID information that you recorded in this table.
5. Authorize the users to access tasks in the console by assigning their user ids to console roles. Log in to the console as root, expand **Settings**, and select the **User Authority** task in the console navigation area. Refer to the table for the console role associated with each task. When a user logs in to the console, only the tasks for which he has the console role will be visible to him.

Table 1.

Task	Console Role	AIX authorizations	User ID	AIX role name
Software Installation and Maintenance	aixSoftware	aix.system.install aix.system.stat		
Software License Management	aixLicenses	aix (This authorization is equivalent to root authority.)		
Devices	aixDevices	aix.device		
System Storage Management	aixStorage	aix.fs		
Security & Users	aixUsers	aix.security.user aix.security.role		
Communication Applications and Services	aixNetwork	aix.network		
Workload Partition Administration	aixWorkloadPartitions	aix.wpar		
Print Spooling	aixPrinters	aix.device.config.printer aix.device.stat.printer		
Advanced Accounting	aixAdvancedAccounting	aix (This authorization is equivalent to root authority.)		
Problem Determination	aixProblemDetermination	aix.ras		
Performance & Scheduling	aixPerformanceAndScheduling	aix.system.stat aix.system.config.perf aix.system.config.cron aix.system.config.wlm		
System Environments	aixSystemEnvironments	aix.system aix.ras.dump aix.ras.error		
Processes & Subsystems	aixProcessesAndSubsystems	aix.proc		

Table 1. (continued)

Task	Console Role	AIX authorizations	User ID	AIX role name
Cluster Systems Management	aixCSM	aix (This authorization is equivalent to root authority.)		
SMIT – Classic View	aixSMITclassic	aix (This authorization is equivalent to root authority.)		
DCEM	aixDCEM	aix (This authorization is equivalent to root authority.)		
Role Based Access Control	aixRBAC	aix (This authorization is equivalent to root authority.)		
Web-based System Manager	aixWebSysMgr	aix (This authorization is equivalent to root authority.)		

In the following example, you want to authorize a user to perform network and printer administration, but you prefer not to give them the root password:

1. Identify your administrative users and their responsibilities. Hank (user ID hank) is responsible for network and printer administration.
2. Identify the console tasks corresponding to administrative responsibilities. As network administrator, Hank will need to perform the Communication Applications and Services task. As printer administrator, Hank will need to perform the Print Spooling task.
3. Create AIX roles containing the AIX authorizations required for each of the tasks. Use the RBAC task to create an AIX role named XYZManageNetwork that contains the **aix.network** authorization and an AIX role named XYZManagePrinter that contains the **aix.device.config.printer** and **aix.device.stat.printer** authorizations.
4. Assign the AIX roles to users according to their responsibilities. Use the Security & Users task to assign the XYZManageNetwork and role XYZManagePrinter roles to Hank.
5. Authorize users to access tasks in the console by assigning their user IDs to console roles. Use the **User Authority** task to assign Hank to the **aixNetwork** and **aixPrinter** console roles.

When Hank logs into the console, only the **Communications Applications and Services** and **Print Spooling** tasks will be visible in the navigation tree. The console retrieves Hank's authorizations from the operating system and any actions that Hank performs are executed under Hank's user ID with his authorizations.

Console administrator role

The administrator role is a special console role that can access all console tasks. By default, the root user ID is assigned to the console administrator role. Since root is authorized to perform any task in AIX, as console administrator root can select and complete any of the console tasks.

If you want to authorize additional users to access all of the console tasks, you can use the User Authority task to add them to the console administrator role. This authorization allows them to select any task, but does not give them the AIX authorizations to complete the actions performed by the tasks. To authorize these users to complete these tasks, you can assign them a role that contains the **aix** authorization. This authorization is equivalent to being root.

User authority task

The **User Authority** task in the **Settings** category of the navigation tree allows a console administrator to add, modify, and remove the roles assigned to console users.

The IBM Systems Director Console for AIX user management feature allows a console administrator to modify the roles assigned to console users (any valid system users). With this feature, the administrator can add or remove roles from individual users as well as log users out.

Without creating or deleting users, this feature allows administrators to associate user names to role mappings. A user with no roles assigned will not be displayed in the **Console Users** portlet, even though the user may be able to log in to IBM Systems Director Console for AIX. Similarly, any user removed from IBM Systems Director Console for AIX by the **Console Users** portlet will not be prevented from logging in to IBM Systems Director Console for AIX. Their assigned roles will simply be removed.

The **Console Users** portlet is composed of three pages.

Main page

This page displays all current user role mappings and the current login status of each user.

The controls on this panel consist of the following:

Logout
Logs out all users whose checkbox is selected.

Add Changes the portlet view to the **Add** page.

Remove
Removes all roles from all selected users. Click a user's name to change the portlet view to the **Modify** page.

Add page

The **Add** page allows the administrator to add a user and specify the user's roles.

Because users are not actually added to the system through this portlet, they must already be valid system users. Because the portlet does not verify user names, it is possible for the administrator to map roles to a user name that may not be able to log in. Exercise caution to ensure that the spelling and capitalization of user names are correct. Controls on this panel consist of the following:

User Authority
Select this link to cancel the operation.

User Fill this text box with the name of the user being assigned roles.

Roles This multiple-selection list contains all available roles. Select one or more items to specify the user's initial role assignments.

Apply Press this button to create and store the user-to-role mappings, and then reset the page to allow you to create additional mappings.

OK Press this button to create and store the user-to-role mappings and then return to the **Main** page.

Reset Press this button to clear the **User** field and deselect all items in the **Roles** list.

Cancel
Press this button to abort the creation of a new user-to-role mapping and return to the **Main** page.

Modify page

When you click a user name on the **Main** page, the page displays the roles currently assigned to the user. Unlike the **Add** page, the user name is not an input field, but a display of the current user's information.

Controls on this panel consist of the following:

User Authority
Select this link to cancel the operation.

Roles This multiple-selection list contains all available roles. Select one or more items or deselect to specify the user's role assignments.

Apply Press this button to store the user-to-role mappings and then reset the page to allow additional modification.

OK Press this button to store the user-to-role mappings and then return to the **Main** page.

Reset Press this button to reset the Roles list to represent a user's current mappings.

Cancel
Press this button to abort any pending changes to the user-to-role mappings and return to the **Main** page.

Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client

By default, the IBM Systems Director Console for AIX provides a Secure Sockets Layer (SSL) certificate that enables HTTPS connections between the IBM Systems Director Console for AIX and the Web browser client. However, to ensure server authentication, data privacy, and data integrity, you need to replace the default certificate with either a self-signed certificate or a certificate that is signed by a certificate authority (CA) and change the keystore password.

Configuring SSL ensures data integrity and data confidentiality between the server and the Web browser client. This is especially important if you access the IBM Systems Director Console for AIX from outside your network.

Note: Ensure that the host name you specify in the Common Name (**CN**) field of the Secure Sockets Layer (SSL) certificate matches the host name that you specify in the URL you use to access the Web interface. For example, if you specify a long name for the host name in the **CN** field of the certificate, you need to specify a long name in the URL. If these host names do not match, you may receive errors when you try to open the Web interface or start Launch-in-Context tasks. Follow the instructions in the following tasks to ensure that you specify the correct host name in the **CN** field of the certificate.

To replace the default certificate with a new certificate and change the keystore password for Secure Sockets Layer (SSL), perform one of the following tasks.

Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client using CA-signed certificates

You can replace the default certificate with a certificate signed by a certificate authority (CA). Use this method if you are working with the IBM Systems Director Console for AIX in a production environment.

By default, the IBM Systems Director Console for AIX provides a Secure Sockets Layer (SSL) certificate that enables HTTPS connections between the console and the Web browser client. However, to ensure server authentication, data privacy, and data integrity, you need to replace the default certificate with either a self-signed certificate or a CA-signed certificate and change the keystore password.

You can request a digital certificate from a certificate authority (CA). Since certificate authorities are public entities that issue certificates to identify other entities, CA-signed certificates provide a level of public trust. Therefore, this type of certificate is best suited for a production environment.

The process of replacing your default certificate and password involves the following tasks:

- Stopping the IBM Systems Director Console for AIX server.
- Using the key management utility (iKeyman) to perform the following tasks:
  - Open the default keystore file.
  - Delete the default certificate.

  – Create a certificate signing request (CSR).
  – Send the CSR to a CA.
  – Receive the CA-signed certificate.
  – Add the public version of the CA-signed certificate to the Web browser's truststore file.
  – Change the default password for the keystore file.
- Updating the web container properties.
- Restarting the IBM Systems Director Console for AIX server.
- Updating the browser with the new certificate.

Perform the following steps:

Note: Back up any files before you edit the files.

1. Enter the following commands on the AIX command line to stop the IBM Systems Director Console for AIX server:
   a. stopsrc -s pconsole
   b. lssrc -s pconsole
2. Perform the following steps to start the key management utility (iKeyman):

   Install_Location/**jre/bin/ikeyman.exe**

   Where *Install_Location* is the location of the Java 5 installation directory. The default installation directory is **/usr/java5**.
3. In iKeyman, perform the following steps:
   a. Open the default keystore file:
      1) From the menu bar, select **Key Database File > Open** and select or specify the following information:
         - For **Key Database Type**, select **JKS**.
         - For the **File Name** and **Location** fields, click **Browse...** and select the default keystore file as follows:

           Install_Location/**lwi/security/keystore/ibmjss2.jks**

           Where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.
         - Click **Open** and click **OK**.
         - In the **Password Prompt** window, specify the default password for the default keystore file and click **OK**. The default keystore file password for IBM Systems Director Console for AIX is **ibmpassw0rd**.
      2) Perform the following step to delete the default certificate:

         In the **Key Database Content** window, select the default personal certificate named **lwiks** and click **Delete**.
      3) Create a certificate signing request (CSR). You need to create a certificate signing request (CSR) so you can request a digital certificate from a CA.
         - From the menu bar, click **Create > New Certificate Request...**.
         - In the **Create New Key and Certificate Request** window, specify the following required information and click **OK**:

           Key Label
              Specify a label for the new certificate (for example, AIXConsole)

           Key Size
              Accept the default value

Common Name
Specify the fully qualified host name of the server for which you are creating the CA-signed certificate.

Note: This host name must match the host name that appears in the URL you specify in your browser to reach the IBM Systems Director Console for AIX. In most cases, you need to specify the fully qualified host name. However, if you use a short name in your URL, you must specify a short name for the Common Name.

Organization
Specify the name of your organization.

Country or region
Accept the default value.

– Specify or click **Browse...** to select the name of a file in which to store the certificate request (for example, **AIXConsoleSecPubCertreq.arm**)

4) Send the CSR to a CA. You need to submit the certificate signing request (CSR) to a CA. You can request either a test certificate or a production certificate from the CA. However, in a production environment, you need to request a production certificate. Send the file that you created earlier to the CA by following the instructions provided for requesting a new certificate provided by the CA. You can refer to the CA website for specific instructions.

5) Receive the CA-signed certificate. After the CA accepts the certificate signing request, the CA processes the request and verifies your identity. The CA sends the signed certificate back to you via e-mail. Receive and save the new certificate in the default keystore file.

- If the CA sends the new certificate to you as part of an e-mail message, cut and paste the certificate from the e-mail message and save it in a certificate file (for example, AIXConsoleSecPubCert.cert).

  Note: The e-mail message from the CA might include supplemental text in front of the certificate and after the certificate. For example you might see the text BEGIN CERTIFICATE in front of the certificate and END CERTIFICATE after the certificate. In this case, ensure that you cut and paste the supplemental text along with the certificate text.

  Save the certificate file in the *Install_Location***/lwi/security/keystore**, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.

- Open the default keystore file if it is not already open.

  Note: Start the key management utility (iKeyman) if you have not done so already.

  a) From the menu bar, select **Key Database File > Open**, and select or specify the following information:
     – For **Key Database Type**, select **JKS**.
     – For the **File Name** and **Location** fields, click **Browse...** and select the *Install_Location***/lwi/security/keystore/ibmjss2.jks** default keystore file, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.

  b) Click **Open** and click **OK**.

  c) In the **Password Prompt** window, specify the default password for the default keystore file and click **OK**. The default keystore file password for IBM Systems Director Console for AIX is **ibmpassw0rd**.

- In the **Key Database Content** section of the **iKeyman** window, select **Personal Certificates**.
- Click **Receive...**.
- In the **Receive Certificate from a File** window, select or specify the following information:

  Data type
  Select **Base64-encoded ASCII data**.

  Certificate file name
  Specify the name of the certificate file that you created when you received the certificate from the CA (for example, **AIXConsoleSecPubCert.cert**).

  Location
  Specify the directory path to the certificate file (*Install_Location***/lwi/security/keystore**, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.
- Click **OK**.
- In the **Enter a Label** window, specify a label for the certificate (for example, **AIXConsoleSec**).
- Click **OK**.

6) (Optional) Add the public version of the CA-signed certificate to the Web browser's truststore file. The public version of the certificate contains all identifying information as well as the public key associated with the certificate.

   This optional step can provide additional security within your SSL configuration. The Web browser can determine whether the server presents a certificate that is signed by a trusted signer. If the browser determines that the certificate is not signed by a trusted signer, the browser displays a warning that alerts you to a possible security breach. Configuring SSL for the browser is browser-specific. Consult your browser documentation for instructions.

7) Change the default keystore file password.
   a) From the menu bar, click **Key Database File > Change Password**.
   b) In the **Change Password** window, specify and confirm a new password and click **OK**.

8) Exit iKeyman.

b. Update the web container properties. Since you changed the password, you need to update the web container properties with the new password.

   To update the web container properties, do not edit properties directly within the **webcontainer.properties** file. Instead, create a file named **sslconfig** in the same directory, edit the properties in the **sslconfig** file, and restart the IBM Systems Director Console for AIX. The process of restarting the IBM Systems Director Console for AIX encrypts the new password in the web container properties.

   To update the web container properties, perform the following steps:

   1) Change to the *Install_Location***/lwi/conf** directory, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.
   2) Change the name of the **webcontainer.properties** file to **webcontainer.properties.bak**.
   3) In the same directory, create a file named **sslconfig** and copy the contents of the **webcontainer.properties.bak** file to the **sslconfig** file.
   4) Open the **sslconfig** file with a text editor and change the properties as follows:
      - **com.ibm.ssl.keyStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
      - **com.ibm.ssl.trustStore.5336=/../../security/keystore/ibmjsse2.jks**
      - **com.ibm.ssl.trustStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.

        - Remove the line **sslEnabled=true** from the **sslconfig** file.

    5) Save the **sslconfig** file.

       When you restart IBM Systems Director Console for AIX, the **sslconfig** file is used to automatically create a new **webcontainer.properties** file and encrypt the new password in this file. After the new **webcontainer.properties** file has been created, IBM Systems Director Console for AIX deletes the **sslconfig** file since it is no longer needed.

       Note: After you start and connect to the IBM Systems Director Console for AIX, you can delete the **webcontainer.properties.bak** file manually.

c. Restart the IBM Systems Director Console for AIX server by performing the following steps:

    1) startsrc -s pconsole
    2) lssrc -s pconsole

d. Update the Web browser with the new certificate.

    Note: Skip the next step if the public version of the CA-signed certificate is already stored in the browser truststore file. Some browsers contain the public version of well-known CA-signed certificates.

    1) In a Web browser, enter the following to point to the IBM Systems Director Console for AIX:

       http://*Your_Server_Name***:***Port_Number***/ibm/console**

       Where Your_Server_Name is the host name of the IBM Systems Director Console for AIX server and Port_Number is the port for the IBM Systems Director Console for AIX server. The default port is 5335.

       A security alert is displayed. For example, you might see the following message:

       ```
       The security certificate was issued by a company you have not chosen to trust.
       View the certificate to determine whether you want to trust the certifying
       authority.
       ```

    2) In the **Security Alert** window, click **View Certificate**.
    3) In the **Certificate** window, click **Install Certificate**.
    4) Complete the **Certificate Import Wizard**. In the **Security Warning** window, click **Yes**. In the **Certificate Import Wizard** window, click **OK**. In the **Certificate** window, click **OK**. In the **Security Alert** window, click **Yes**.

Note: Messages and settings might differ depending on your browser and the version of Java Web Start that you are running.

Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client using self-signed certificates

You can replace the default certificate with a self-signed certificate. Use this method if you are working with the IBM Systems Director Console for AIX in a test environment.

By default, the IBM Systems Director Console for AIX provides a Secure Sockets Layer (SSL) certificate that enables HTTPS connections between the IBM Systems Director Console for AIX and the Web browser client. However, to ensure server authentication, data privacy, and data integrity, you need to replace the default certificate with either a self-signed certificate or a CA-signed certificate and you need to change the keystore password.

Self-signed certificates are certificates that you create yourself for private use. After you create them, you can use them immediately. Because anyone can create self-signed certificates, they are not considered publicly trusted certificates. Therefore, use self-signed certificates only on a temporary basis while testing your environment.

The process of replacing your default certificate and password involves the following tasks:

- Stopping the IBM Systems Director Console for AIX server.

- Using the key management utility (iKeyman) to perform the following tasks:
  - Open the default keystore file.
  - Delete the default certificate.
  - Create a self-signed certificate for a test environment.
  - Change the default password for the keystore file.
- Updating the web container properties.
- Restarting the IBM Systems Director Console for AIX server.
- Updating the browser with the new certificate.

Complete the following steps:

Note: Back up any files before you edit the files.

1. Stop the IBM Systems Director Console for AIX server by completing the entering the following commands on the AIX command line:
   a. stopsrc -s pconsole
   b. lssrc -s pconsole
2. Run the following command to start the key management utility (iKeyman):

   *Install_Location***/jre/bin/ikeyman.exe**

   Where *Install_Location* is the location of your Java 5 installation directory. The default installation directory is **/usr/java5**.
3. In iKeyman, perform the following steps:
   a. Open the default keystore file:
      1) From the menu bar, select **Key Database File > Open**, and select or specify the following information:
         - For **Key Database Type**, select **JKS**.
         - For the **File Name** and **Location** fields, click **Browse...** and select the *Install_Location***/lwi/security/keystore/ibmjss2.jks** default keystore file, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.
      2) Click **Open** and click **OK**.
      3) In the **Password Prompt** window, specify the default password for the default keystore file and click **OK**. The default keystore file password for IBM Systems Director Console for AIX is **ibmpassw0rd**.
   b. Delete the default certificate. In the **Key Database Content** window, select the default personal certificate named **lwiks** and click **Delete**.
   c. Create a new self-signed certificate:

      From the menu bar, select **Create > New Self-Signed Certificate.....** In the **Create New Self-Signed Certificate** window, specify the following required information, and click **OK**:

      Key Label
      Specify a label for the new certificate (for example, AIXConsole).

      Version
      Select X509 V3

      Key Size
      Accept the default value

      Common Name
      Specify the fully qualified host name of the server for which you are creating the self-signed certificate

Note: The host name must match the host name that appears in the URL you specify in your browser to reach the IBM Systems Director Console for AIX. In most cases, you must specify the fully qualified host name. However, if you use a short name in your URL, you need to specify a short name for the **Common Name**.

Organization
Specify the name of your organization

Country or region
Accept the default value

Validity Period
Specify the lifetime of the certificate in days or accept the default value

d. Change the default keystore file password.

1) From the menu bar, select **Key Database File** > **Change Password**. In the **Change Password** window, specify and confirm a new password and click **OK**.

e. Exit iKeyman.

4. Update the web container properties. Since the password was changed in the previous step, you need to update the web container properties with the new password.

   To update the web container properties, do not edit properties directly within the **webcontainer.properties** file. Instead, create a file named **sslconfig** in the same directory, edit the properties in the **sslconfig** file, and restart the IBM Systems Director Console for AIX. The process of restarting the IBM Systems Director Console for AIX encrypts the new password in the web container properties.

   To update the web container properties, perform the following steps:

   a. Change to the *Install_Location***/lwi/conf** directory, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is **/pconsole**.

   b. Change the name of the **webcontainer.properties** file to **webcontainer.properties.bak**.

   c. In the same directory, create a file named **sslconfig** and copy the contents of **webcontainer.properties.bak** file to the **sslconfig** file.

   d. Open the **sslconfig** file with a text editor and change the properties as follows:

   Note: Specify only plaintext values for the passwords in the **sslconfig** file.

   Note: In this example, the following properties indicate that IBM Systems Director Console for AIX is using secure port 5336. If you are using a secure port other than 5336, your properties will indicate a different port. Do not change the port indicated in the properties.

   - **com.ibm.ssl.keyStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
   - **com.ibm.ssl.trustStore.5336=/../../security/keystore/ibmjsse2.jks**
   - **com.ibm.ssl.trustStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
   - Remove the line **sslEnabled=true** from the **sslconfig** file.

   e. Save the **sslconfig** file.

   When you restart IBM Systems Director Console for AIX, the **sslconfig** file is used to automatically create a new **webcontainer.properties** file and encrypt the new password in this file. After the new **webcontainer.properties** file has been created, IBM Systems Director Console for AIX deletes the **sslconfig** file since it is no longer needed.

   Note: After you start and connect to the IBM Systems Director Console for AIX, you can manually delete the **webcontainer.properties.bak** file.

5. Restart the IBM Systems Director Console for AIX server by performing the following steps:

   a. startsrc -s pconsole
   b. lssrc -s pconsole
6. Update the Web browser with the new certificate.
   a. In a Web browser, type the following to point to the IBM Systems Director Console for AIX:

      http://*Your_Server_Name***:***Port_Number***/ibm/console**

      Where *Your_Server_Name* is the host name of the IBM Systems Director Console for AIX server and *Port_Number* is the port for the IBM Systems Director Console for AIX server. The default port is 5335.

      A Security Alert is displayed. For example, you might see the following message:

      ```
      The security certificate was issued by a company you have not chosen to trust.
      View the certificate to determine whether you want to trust the certifying
      authority.
      ```
   b. In the **Security Alert** window, click **View Certificate**.
   c. In the **Certificate** window, click **Install Certificate**.
   d. Complete the **Certificate Import Wizard**.
   e. In the **Security Warning** window, click **Yes**.
   f. In the **Certificate Import Wizard** window, click **OK**.
   g. In the **Certificate** window, click **OK**.
   h. In the **Security Alert** window, click **Yes**.

Note: Messages and settings might differ depending on your browser and the version of Java Web Start that you are running.

Troubleshooting IBM Systems Director Console for AIX

The following table lists some troubleshooting information for IBM Systems Director Console for AIX.

Symptom	**Possible cause**
You cannot log in	Verify that you have a user account on the server. Log in to the server on a directly attached terminal or with the **telnet** command.
You see only the **Welcome** page	There are no other tasks in the navigation tree. Your user ID is not authorized for tasks in the console. Contact the console administrator (usually the root user) to add your user ID to the desired console roles.

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.

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.

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.

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

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 are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

Index

A

accessibility 1
Add Page
  Apply 8
  Reset 8
  Roles 8
  User 8
  User Authority 8
AIX authorizations 5
authorization 5
authorizing console users 5

B

banner and tool bar 3

C

CA-signed certificates 9
configuration 2
console administrator role 7
console tasks 5

D

data confidentiality 9
data integrity 9

I

iKeyman 9, 13
installation 2
installing 2

L

Logging in 5

M

Main page
  Add 8
  Logout 8
  Remove 8
Modify page
  Apply 8
  Reset 8
  Roles 8
  User Authority 8

N

navigating 4
navigation tree 3, 4

O

operational modes 1

P

port values 3
products 17

R

runtime
  check 2
  start 2
  stop 2

S

Secure Sockets Layer 9, 13
self-signed certificates 13
starting 3
system requirements 1

T

terms 18
title bar 4
Troubleshooting 16

U

User authority task 8
user interface 3
user name 5

W

Web browser client 9
work area 3, 4

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

AIX 6.1
IBM Systems Director Console for AIX

Publication No. SC23-5242-00

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

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

Comments:

Thank you for your support.

Submit your comments using one of these channels:
- Send your comments to the address on the reverse side of this form.
- Send your comments via e-mail to: aix6koub@austin.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

E-mail address

Readers' Comments — We'd Like to Hear from You
SC23-5242-00

IBM

Cut or Fold
Along Line

Fold and Tape　　**Please do not staple**　　Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL　PERMIT NO. 40　ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department 04XA-905-6C006
11501 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.

SC23-5242-00