Tivoli® System Automation for Multiplatforms

IBM

Version 2.2

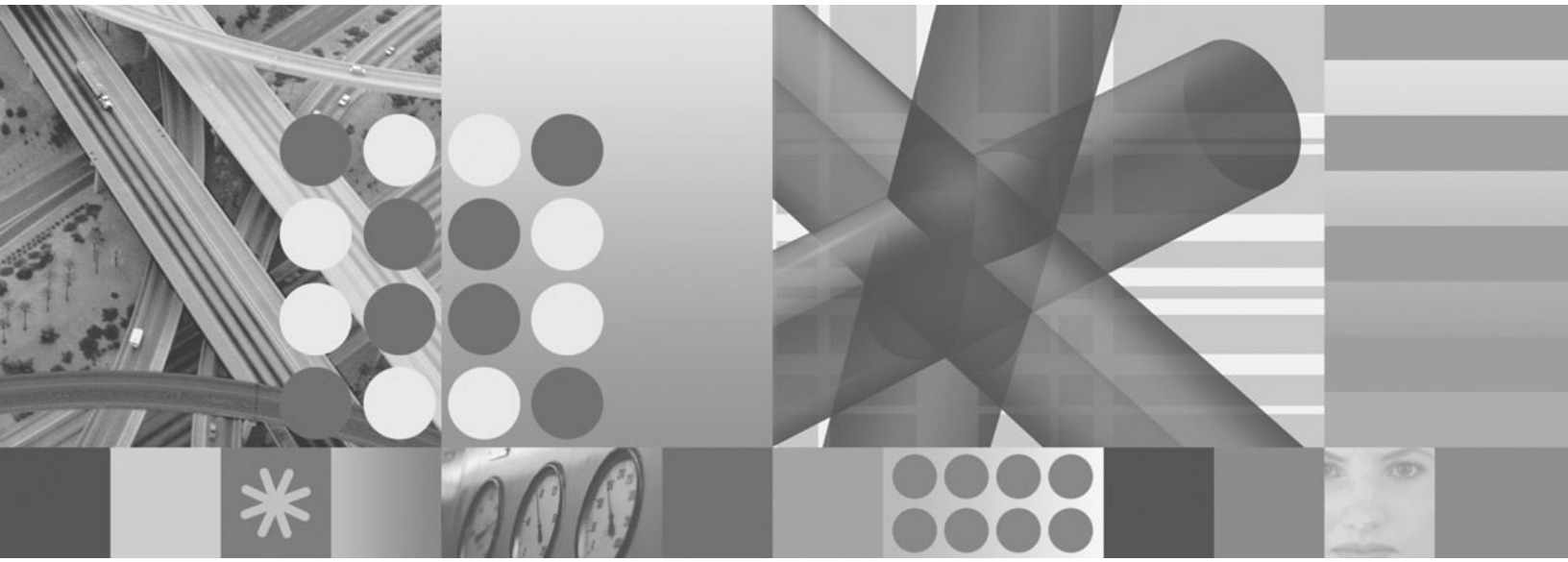
Installation and Configuration Guide

SC33-8273-01

Tivoli® System Automation for Multiplatforms

IBM

Version 2.2



Installation and Configuration Guide

SC33-8273-01

Note!
Before using this information and the product it supports, read the information in Appendix E, "Notices," on page 223.

Second Edition (December 2006)

This edition of the *Installation and Configuration Guide* applies to Version 2, Release 2, Modification 0, Fix 1 of IBM Tivoli System Automation for Multiplatforms, program number 5724–M00, and to all subsequent releases and modifications of this product until otherwise indicated in new editions.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

IBM Deutschland Entwicklung GmbH
Department 3248
Schoenaicher Str. 220
D-71032 Boeblingen
Federal Republic of Germany

FAX (Germany): 07031+16-3456
FAX (Other Countries): (+49)+7031-16-3456

Internet e-mail: eservdoc@de.ibm.com

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:
- Title and order number of this book
- Page number or topic related to your comment

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

Contents

Figures

Tables

About this guide

This guide provides information needed to plan, install, configure, and upgrade IBM Tivoli System Automation for Multiplatforms.

Who should read this guide

This guide is for planners, installers, and administrators who plan to install and configure IBM Tivoli System Automation for Multiplatforms.

How to use this guide

This guide is divided into the following parts:

- Part 1, "Base component and operations console," on page 1 describes the tasks that you must perform when you install the base component.
- Part 2, "End-to-end automation management component," on page 57 describes the tasks that you must perform when you install the end-to-end automation management component.
- Part 3, "Installing and configuring the end-to-end automation adapters," on page 139 describes the tasks that you must perform to install and configure the HACMP and the MSCS adapters and how you configure the end-to-end automation adapter of the base component of IBM Tivoli System Automation for Multiplatforms, which is installed automatically when you install the base component.
- The Appendixes provide troubleshooting information.

Where to find more information

In addition to this manual, the IBM Tivoli System Automation for Multiplatforms library contains the following books:

- *IBM Tivoli System Automation for Multiplatforms Base Component Administrator's and User's Guide*, SC33-8272
- *IBM Tivoli System Automation for Multiplatforms Base Component Reference*, SC33-8274
- *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, SC33-8275
- *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Reference*, SC33-8276

You can download the complete documentation at

`http://publib.boulder.ibm.com/tividd/td/IBMTivoliSystemAutomationforMultiplatforms2.2.html`

The IBM Tivoli System Automation for Multiplatforms home page contains useful up-to-date information, including support links and downloads for maintenance packages.

You find the IBM Tivoli System Automation for Multiplatforms home page at:

`www.ibm.com/software/tivoli/products/sys-auto-linux/`

Conventions used in this guide

This guide uses several conventions for special terms and actions and operating system commands and paths.

Typeface conventions

This guide uses the following conventions:

- Typically, file names, directories, and commands appear in a different font. For example:
  - File name: `setup.jar`
  - Directory: `/etc/hosts`
  - Command: `startServer server1`
- Variables are either italicized, enclosed in brackets, or both. For example:
  - http://<hostname.yourco.com>/index.html
- Frequently, variables are used to indicate a root installation directory:
  - Root installation directory of the end-to-end automation management component:

    <EEZ_INSTALL_ROOT> or EEZ_INSTALL_ROOT
  - WebSphere Application Server root installation directory: <was_root> or was_root
  - Runtime root directory of Integrated Solutions Console: <isc_runtime_root> or isc_runtime_root
- Directories are shown with forward slashes (/), unless operating-system specific information is provided. On Windows systems, you should use backward slashes (\) when typing at a command line, unless otherwise noted.
- Operating-system specific information is provided. For example:
  - **AIX, Linux:** `/opt/IBM/tsamp/eez`
  - **Windows:** `C:\Program Files\IBM\tsamp\eez`

Related information

This topic to provides information about publications and Web sites related to IBM Tivoli System Automation for Multiplatforms:

WebSphere Application Server publications:

The latest versions of all WebSphere Application Server publications can be found on the WebSphere Application Server library Web site at

`www.ibm.com/software/webservers/appserv/was/library/`

IBM Reliable Scalable Cluster Technology (RSCT) documentation:

- The following RSCT publications are available on the IBM Tivoli System Automation for Multiplatforms Base Component CD:
  - *RSCT Administration Guide*, SA22-7889
  - *RSCT for AIX 5L: Technical Reference*, SA22-7890
  - *RSCT for Linux: Technical Reference*, SA22-7893
  - *RSCT Messages*, GA22-7891
  - *RSCT Diagnosis Guide*, SA23-2202
- RSCT publications can also be found at the following Web site:

  `www.ibm.com/servers/eserver/clusters/library/`

- The following IBM Redpaper provides information to help readers plan for and install a high availability solution for Linux on System z running under z/VM:
  – *Linux on IBM zSeries® and S/390®: High Availability for z/VM® and Linux*

  It can be found at the following Web site:

  `http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp0220.html`

IBM DB2 publications:
DB2 publications can be found on the IBM DB2 UDB Web site at

`www.ibm.com/software/data/db2/udb/support/`

The link to the PDF manuals is available in the **Other resources** section on the Web page.

What's new in release 2.2

For release 2.2, the IBM Tivoli System Automation for Multiplatforms library was restructured. This *Installation and Configuration Guide* describes all of the tasks that you need to perform to install and configure the end-to-end automation component, the base component, including the automation adapter, and the operations console of the base component. In addition, it introduces the following topics:

Automation adapter for Microsoft Server Clustering (MSCS) clusters
The installation and configuration of this new feature of the end-to-end automation management component is described in Chapter 15, "Installing and configuring the MSCS adapter," on page 177.

Automation adapter for High Availability Cluster Multi-Processing (HACMP) clusters
The installation and configuration of this new feature of the end-to-end automation management component is described in Chapter 14, "Installing and configuring the HACMP adapter," on page 161.

Release upgrade
As release 2.2 is the second release of IBM Tivoli System Automation for Multiplatforms in which the end-to-end automation management component and the operations console are shipped, this guide describes for the first time how a release upgrade for these parts of the product are performed.

Part 1. Base component and operations console

Chapter 1. Installing the base component

This chapter describes how you install, configure, migrate, uninstall, and service the base component of IBM Tivoli System Automation, in these main sections:

Planning for the installation

Coexistence with other products:

IBM Tivoli System Automation can coexist with General Parallel File System (GPFS) or Cluster Systems Management (CSM). If these products are installed, IBM Tivoli System Automation shares packages with those products. You can check if any of these packages is installed with the commands:

```
rpm -q gpfs
```

or

```
rpm -q csm
```

respectively.

For AIX, use the lslpp -l product* command to check if any of these packages is installed, In order to see, if, for example, CSM is installed, issue the following command:

```
root@boepb06 ~# lslpp -l csm*
```

If you find that GPFS prior to version 2.2 is installed, IBM Tivoli System Automation **cannot** be used with this version of GPFS at the same time.

Contents of the CD:

The CD labeled "IBM Tivoli System Automation for Multiplatforms 2.2 Base component all Platforms" contains scripts and software packages for each platform and the corresponding architecture.

CDs / archives for the base component

When you order the base component of IBM Tivoli System Automation, you find it on the following CD/in the following archive:

Base component CD

To install the base component, you use the installation script listed in the right column of the table below.

Table 1. Product CD versions

Operating system	Product CD label	Installation script
Linux & AIX	IBM Tivoli System Automation Multiplatforms V2.2.0 Base component all platforms	`SAM2200Base/installSAM`

Electronic distribution of IBM Tivoli System Automation

If you prefer electronic distribution to delivery on the CD, we offer you the possibility to download the product from the Web. After you have purchased IBM Tivoli System Automation you get an URL where you can download a tar file for the Linux and AIX operating systems.

Archives

Linux:

Table 2. Archives for Linux platforms

Archive name	Description
C947PML.tar	This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the *tar xf* command to extract the archive. When you have extracted the files, you find the installation script `installSAM` in the following directory: `SAM2200Base`

AIX:

Table 3. Archives for AIX platforms

Archive name	Description
C947QML.tar	This is the archive you use to install the product. Use the *tar xf* command to extract the archive. When you have extracted the files, you find the installation script `installSAM` in the following directory: `SAM2200Base`

Supported platforms

Version 2.2 of IBM Tivoli System Automation supports Linux on System z, System x, System i, and System p, as well as AIX 5.2 and AIX 5.3.

IBM Tivoli System Automation runs on all IBM eServer machines running Linux, and on IBM eServer pSeries machines running AIX.

Detailed information about support of specific Linux distributions and AIX versions can be found in the following table. For the latest information, refer to the IBM Tivoli System Automation for Multiplatforms Release Notes. To obtain a copy of the release notes, go to the IBM Tivoli System Automation for Multiplatforms home page and click **Technical Documentation**. The IBM Tivoli System Automation home page is located at:

`www.ibm.com/software/tivoli/products/sys-auto-linux`

Table 4. Supported platforms for the base component of IBM Tivoli System Automation for Multiplatforms

	System x[1]	System z	System p	System i
SUSE SLES 9 (32 bit)	x	x[2]		
SUSE SLES 10 (32 bit)	x			
SUSE SLES 9 (64 bit)	x	x[2]	x	x
SUSE SLES 10 (64 bit)	x	x	x	x
RedHat RHEL 4.0 (32 bit)	x			
RedHat RHEL 4.0 (64 bit)	x	x	x	x
AIX 5.2			x[3]	
AIX 5.3			x [3]	

Notes:

1. xSeries (except Intel IA64 based servers) and any other 32-bit Intel based server, or AMD Opteron based server (64-bit), or Intel EM64T based server (64 bit).
2. Requires SUSE SLES9 SP1
3. Requires C++ Runtime Library for AIX version 7.0.0.1, which is included in PTFs U800738 and U800739

Supported network interfaces

All platforms support 10 Megabit Ethernet, Fast Ethernet, and Gigabit Ethernet. In addition, the zSeries platform also supports Hipersockets, CTC, and VM Guest LAN.

Preparing for installation

IBM Tivoli System Automation is contained in several packages which must be installed on every node in the cluster to be automated. The type of packages and content depends on the operation system:

Operating system	Type of package	Content
Linux	'rpm' stands for RedHat Packaging Manager. It manages installation and uninstallation of software packages in RPM format.	System Automation rpms and RSCT rpms. RSCT is the underlying infrastructure.
AIX	'installp' filesets	Only System Automation installp filesets. RSCT is part of AIX. However, a more recent level of RSCT may be required. The installation of IBM Tivoli System Automation requires the following RSCT APARs to be installed: • IY87838 (AIX 5.2) • IY87839 (AIX 5.3) Check the Release Notes document for RSCT APARs required for IBM Tivoli System Automation fix packs. Make sure that Java 1.4 32bit, an optional package on the AIX CD, is installed.

Note that the scripts *installSAM* and *uninstallSAM* are supplied to ensure that packages are installed or uninstalled in the correct order. The packages must be made available on nodes where IBM Tivoli System Automation is to be installed. For example, you may use FTP to transfer the files from a PC (with the CDRom mounted) to the node. Also you may install the packages over a shared Network File System.

Prerequisites

Before starting the installation you must fulfill these requirements:

- Install the Public Domain Korn Shell (pdksh) package (if not already done).
- If you are using both the AIX 5.2 platform and the System Automation for Multiplatforms end-to-end automation adapter (see Chapter 13, "Configuring the end-to-end automation adapter of the base component of IBM Tivoli System Automation for Multiplatforms," on page 143) make sure to have a `pam.conf` file in the */etc* directory. You can find a sample `pam.conf` file in the `SAM2200Base/AIX` directory.
- Perl is required to use the command line interface of IBM Tivoli System Automation for Multiplatforms including native RSCT commands. It is by default installed on your Linux or AIX systems as part of the operating system, but if you are using IBM Tivoli System Automation in a language other than English, a special version of Perl may be required. Due to known problems with Perl 5.8.0 and how it handles UTF-8 encoded locales, some characters may not

be properly displayed. This can occur on systems with Perl 5.8.0 installed, while using a UTF-8 encoded locale. When previous or subsequent versions of Perl are used, or non-UTF-8 encoded locales are used, this problem does not occur.
AIX 5.2 uses Perl 5.8.0 and there is currently no opportunity to order a different version of Perl for that AIX release.
If you decide to upgrade your Perl 5.8.0 version on a Linux distribution, perform the following steps:

1. Download Perl 5.8.1 source, referring `http://dev.perl.org/perl5/news/2003/perl-5.8.1.html`.
2. Unzip and tar -xvf on any directory.
3. Compile and install on the UTF-8 machine, referring the instruction provided with the downloaded files.
4. Change the symbolic link pointing to the directory of the Perl version that is used by IBM Tivoli System Automation from: `/usr/sbin/rsct/perl5/bin/perl->/usr/bin/perl` to the directory where the new version of Perl is per default installed:
   `/usr/sbin/rsct/perl5/bin/perl->/usr/local/bin/perl`.

- Also make sure that the directories ***/usr/sbin*** and ***/opt*** have at least 100 MB free space, and that the directory ***/var*** also provides at least 100 MB free space.
- On any node where the adapter can run at least 128 MB RAM must be available.
- During installation of IBM Tivoli System Automation on AIX the correct level of RSCT will be checked and a higher level of RSCT may be required. If this is required for your systems, download and install the appropriate RSCT filesets from the AIX service center.
- For other operating systems specific requirements, see the requirements Web page at `http://www-306.ibm.com/software/tivoli/products/sys-auto-linux/requirements.html`.
- For languages using the double-byte character set (DBCS), the Telnet dialog buffer must be large enough to ensure that long messages are properly displayed. If this is not the case, enlarge the Telnet dialog buffer.

Initial configurations

You must perform these initial configurations:

- Set the following environment variable for all users of IBM Tivoli System Automation on all nodes:
  CT_MANAGEMENT_SCOPE=2 (peer domain scope). You can set the variable permanently if you set it in the profile.
- Be aware that you have to carry out the following steps if you are both using a SUSE LINUX distribution and a language other than English:

  1. Start YaST2.
  2. Select ″System″ icon from a list.
  3. Select ″Editor for /etc/sysconfig″ from a pane.
  4. Select ″Base-Administration″ from a list. Click the ″+″ icon.
  5. Select ″Localization″ from a list. Click the ″+″ icon.
  6. Select “rc_lang” from the list and set a correct locale from the locale table to RC_LANG parameter.
  7. Select ″root_uses_lang″ from a list. Set ″yes″ to ROOT_USES_LANG parameter.
  8. Press the ″Save″ button. When the ″Save sysconfig variables″ dialog box appears, press the ″OK″ button.

9. Restart the system.

- In order to verify that your system is set to the locales supported by this product (reference our locale support tables), perform the following steps:
  1. Log in as root and issue the following command:
     ```
     locale
     ```
     Verify that the LANG value is listed on the language of your choice.
  2. If the returned values are not set to a locale that is supported (reference our locale support tables) or set to POSIX, continue with the following steps:
  3. Issue the following command:
     ```
     export LANG=xx_XX
     ```
     You have to choose a locale which can be displayed by your terminal.
  4. In order to verify the terminal has been set to the locale you wanted, issue this command:
     ```
     locale
     ```
     and make sure LANG is set to **xx_XX**.
  5. Proceed with regular product tasks.

  You need to repeat step 3 to step 5 each time you start a new terminal window in order to issue IBM Tivoli System Automation commands.

Installing and upgrading the base component

If this is a first time installation of the base component, go to "Installing the base component" below. If a previous version of the base component is already installed, you need to perform some steps before the new version of the base component can be installed. To perform a migration to a new version of the product, go to "Migrating the base component" on page 12.

Installing the base component

You use an installation script to install the base component. The installation script performs the following actions:

- A complete prerequisites check to verify that all prerequisites are available and at the required level. If your system does not pass the check, the installation does not start, and you need to provide the missing prerequisites and restart the installation.
- Installs the base component, including the end-to-end automation adapter.

To avoid having to restart the installation, you can invoke the prerequisites check separately, before starting the installation.

Performing the prerequisites check

Complete the following steps:

1. If you downloaded the tar file from the Internet, extract the file, using the following command:

   ```
   tar -xvf <tar file>
   ```

   If you got the product on a CD, mount the CD and change to the directory where the CD is mounted.
2. Enter:

   ```
   cd SAM2200Base
   ```
3. To start the prerequisites check, issue the following command:

   ```
   ./prereqSAM
   ```

   Typically, you do not need to specify any of the options that are available for the **prereqSAM** command. For a detailed description of the command, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.
4. When the check is complete, check the following log file for information about missing prerequisites:

   ```
   /tmp/prereqSAM.<#>.log
   ```

   where <#> is a number; the highest number identifies the most recent log file.
5. If your system did not pass the prerequisites check, correct any problems before starting the installation.

Installing the base component

Before you begin:

Ensure that the node on which you are invoking the installation script is offline. Otherwise, the installation is canceled.

To install the product, including the automation adapter, perform the following steps:

1. If you downloaded the tar file from the Internet and have not yet extracted the file, extract it using the following command:

```
tar -xvf <tar file>
```

If you got the product on a CD, mount the CD and change to the directory where the CD is mounted.

2. Enter:

   ```
   cd SAM2200Base
   ```

3. Invoke the installation script:

   ```
   ./installSAM
   ```

   Typically, you do not need to specify any of the options that are available for the **installSAM** command. For a detailed description of the command, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.

4. Read the information in the License Agreement and the License Information that is displayed. You can scroll forward line by line using the "Enter" key, and page by page using the "spacebar", which is basically the "more" functionality in UNIX®. Once you have scrolled to the bottom of the License information file and you want to accept the terms of the license agreement, type 'y'. Any other input will cancel the installation.

   The installation is also canceled when no license file is found.

5. After you accept the license agreement, the installation program performs a complete prerequisites check to verify that all prerequisites are available and at the required level.

   If your system does not pass the check, the installation does not start, and you need to provide the missing prerequisites and restart the installation.

   Information about the results of the prerequisites check is available in the log file `/tmp/installSAM.<#>.log` (for details, see step 6).

   If your system passed the check, the product, including the automation adapter, is installed.

6. Check the following log file for information about the installation:

   ```
   /tmp/installSAM.<#>.log
   ```

   where <#> is a number; the highest number identifies the most recent log file.

   The entries in the log file have the following prefixes:

   prereqSAM
   Entries that were written during the prerequisites check.

   installSAM
   Entries that were written during the installation of the product.

7. To find out which packages were installed, issue the following command:

   - **AIX:**

     ```
     lslpp -l sam*
     ```

   - **Linux:**

     ```
     rpm -qa | grep -E "^src|^rsct|^sam"
     ```

     See the rpm man page for details about the rpm command.

Installing the product license

IBM Tivoli System Automation requires that a valid product license is installed on each system it is running on. The license is contained on the installation medium in the 'license' sub directory. The installation of the license is usually performed during the product installation process. In case this did not succeed, issue the following command to install the license:

```
samlicm –i license_file
```

In order to display the license, issue:

```
samlicm -s
```

See the *IBM Tivoli System Automation for Multiplatforms Base Component Reference* for a detailed description of the **samlicm** command.

Upgrading from a Try & Buy license to a full product license

If you have installed the Try & Buy version of the IBM Tivoli System Automation for Multiplatforms base component and then purchase the full product version, you will receive another copy of the installation media, which contains the license file for the full license.

The license file is located on the installation medium in the `license` subdirectory. It is recommended to perform the license upgrade by issuing the following command:

```
samlicm -i <license_file_name>
```

In order to display the license, issue:

```
samlicm -s
```

(See “Installing the product license” on page 10.)

If there is service available for IBM Tivoli System Automation for Multiplatforms already, it is also recommended to install the latest service level after upgrading the license.

Languages supported by IBM Tivoli System Automation

This section is only of interest for you if you want to use IBM Tivoli System Automation for Multiplatforms in a language other than English as shown in the following tables.

Table 5 shows which encodings are supported for the Linux distribution. If you are using the end-to-end automation adapter for the IBM Tivoli System Automation base component, note that new versions of Linux operating systems may not support all encodings, but UTF-8 encoding is always supported.

Table 5. Supported languages

Language	UTF-8	ISO-8859-1	EUC/GBK	Euro	GB18030/BIG5
German	de_DE.UTF-8	de_DE, de_DE.ISO-8859-1		de_DE@euro	
Spanish	es_ES.UTF-8	es_ES, es_ES.ISO-8859-1		es_ES@euro	
French	fr_FR.UTF-8	fr_FR, fr_FR.ISO-8859-1		fr_FR@euro	
Italian	it_IT.UTF-8	it_IT, it_IT.ISO-8859-1		it_IT@euro	
Japanese	ja_JP.UTF-8		ja_JP.eucJP		
Korean	ko_KR.UTF-8		ko_KR.eucKR		
Portugese/ Brazilian	pt_BR.UTF-8	pt_BR			

Table 5. Supported languages (continued)

Language	UTF-8	ISO-8859-1	EUC/GBK	Euro	GB18030/BIG5
Simplified Chinese	zh_CN.UTF-8		zh_CN.GBK, zh_CN.GB2312		zh_CN.GB18030
Traditional Chinese	zh_TW.UTF-8				zh_TW.Big5, zh_TW

The following encoding is supported on the AIX distribution:

Language	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/BIG5
German	DE_DE	de_DE		
Spanish	ES_ES	es_ES		
French	FR_FR	fr_FR		
Italian	IT_IT	it_IT		
Japanese	JA_JP		ja_JP	Ja_JP
Korean	KO_KR		ko_KR	
Portugese/Brazilian	PT_BR	pt_BR		
Simplified Chinese	ZH_CN		zh_CN	Zh_CN
Traditional Chinese	ZH_TW		zh_TW	Zh_TW

Migrating the base component

If the IBM Tivoli System Automation 2.1 base component is already installed, it can be migrated to the new version IBM Tivoli System Automation 2.2.

Before migrating consider the following:

- The migration process starts when any node within the active cluster is upgraded to the higher version code.
- You can always upgrade from a lower code level to a higher code level, but a downward migration is not possible.
- The migration process is only complete when the active version number is equal to the highest installed code version number. Until then, different code levels can coexist. See "Verifying the active and installed version number" on page 14 and "Completing the migration" on page 14 how to complete the migration process.

You can use one of the following procedures to migrate the IBM Tivoli System Automation base component:

- It is recommended to use the procedure described in "Migrating an entire domain"
- "Migrating a node step by step" on page 13

Migrating an entire domain

Note: To minimize the downtime, you can perform a prerequisites check before starting the actual migration (for more information, see "Performing the prerequisites check" on page 9).

Keep the following in mind when migrating an entire domain:

1. The domain will not be available for automation during the upgrade, which means that the resource must be offline.
2. Check if the System Automation for Multiplatforms end-to-end automation adapter is running:

   ```
   samadapter status
   ```

   If it is running, stop the automation adapter:

   ```
   samadapter stop
   ```
3. Stop all online resource groups by setting their NominalState to Offline:

   ```
   chrg -o Offline <resource-group-name>
   ```
4. If the domain is online, stop the domain:

   ```
   stoprpdomain <domain-name>
   ```
5. Run **./installSAM** from the installation directory on all nodes. For more information on the **installSAM** script, see "Installing the base component" on page 9.
6. Start the domain:

   ```
   startrpdomain <domain-name>
   ```
7. Check the code levels with the **lssrc –ls IBM.RecoveryRM** command (see the sample in "Verifying the active and installed version number" on page 14). All the nodes should have the newly installed code level, but the active code level should still be the previous one.
8. In order to activate the new version continue with "Completing the migration" on page 14.

Migrating a node step by step

Note: You can perform a prerequisites check before starting the actual migration (for more information, see "Performing the prerequisites check" on page 9).

Migrating a node step by step has the advantage that IBM Tivoli System Automation is still available during migration. Keep the following in mind when migrating a node step by step:

1. Make sure that the node to be migrated is excluded from automation, so that resources are activated on other nodes.

   ```
   samctrl -u a <node>
   ```

   Note that if a resource group was running on the node to be excluded, automation will try to move it to another node. This may take a little while.
2. Stop the node from another node in the domain, and verify that it is stopped:

   ```
   stoprpnode <node>; lsrpnode
   ```
3. Run **./installSAM** from the installation directory to upgrade the node. For more information on the **installSAM** script, see "Installing the base component" on page 9.
4. Start the node:

   ```
   startrpnode <node>
   ```
5. Take the newly upgraded node back to automation:

   ```
   samctrl -u d <node>
   ```
6. The newly upgraded node can now join the existing domain. Use the **lssrc –ls IBM.RecoveryRM** command (see the sample in "Verifying the active and installed version number" on page 14) to display the installed version and the active version of the product. The new code features will not be activated until

the active IBM Tivoli System Automation version number is equal to the highest IBM Tivoli System Automation version number installed within the cluster, and you cannot fully utilize these new code features until all the nodes are upgraded.

7. Repeat the steps 1-6 for other nodes within the cluster.
8. In order to activate the new version continue with "Completing the migration."

Verifying the active and installed version number

After the upgrade the new features of the new code are not yet activated. The previous and new code levels can coexist until the migration is completed. The **lssrc –ls IBM.RecoveryRM** command shows you the active version number **AVN** (2.1.0.0 in the sample below) and the installed version number **IVN** (2.2.0.0. in the sample below) of the product. When IVN and AVN are the same, migration is complete.
The output looks like:

```
Subsystem         : IBM.RecoveryRM
PID               : 27973
Cluster Name      : ws
Node Number       : 1
Daemon start time : Wed Nov 15 08:09:10 2006

Daemon State:
   My Node Name         : lnxcm3x
   Master Node Name     : lnxcm3x (node number = 1)
   Our IVN              : 2.2.0.0
   Our AVN              : 2.1.0.0
   Our CVN              : 11082527751 {0x140861007}
   Total Node Count     : 1
   Joined Member Count  : 1
   Config Quorum Count  : 1
   Startup Quorum Count : 1
   Operational Quorum State: HAS_QUORUM
   In Config Quorum     : TRUE
   In Config State      : TRUE
   Replace Config State : FALSE
```

Figure 1. Verifying the active and installed version number

In order to activate the new version, continue with "Completing the migration."

Completing the migration

In order to check and complete the migration, perform the following steps:

1. Make sure that the domain is started and all nodes in the domain are online.
2. Issue the **lsrpdomain** command to see the current RSCT active version number and the mixed version status:

   ```
   Name       OpState  RSCTActiveVersion  MixedVersions  TSPort  GSPort
   SA_Domain  Online   2.4.4.1            Yes            12347   12348
   ```

3. Issue the **lsrpnode** command to see the current RSCT install version number for all nodes. Keep in mind that all nodes must be online:

   ```
   Name   OpState RSCTVersion
   node01 Online  2.4.5.4
   node02 Online  2.4.5.4
   node03 Online  2.4.5.4
   ```

4. If the RSCT peer domain is running in mixed version mode (MixedVersions = Yes) and all nodes have been upgraded to the new release of IBM Tivoli System Automation, you must update the RSCTActiveVersion by running the RSCT

CompleteMigration action on one of the nodes. Before running the action, review the RSCT migration preparation procedures described in Chapter 3 of the *IBM RSCT Administration Guide*.

To update the RSCTActiveVersion, make sure that all nodes are online, and issue the following command on one of the nodes:

```
runact -c IBM.PeerDomain CompleteMigration Options=0
```

To verify the that the active RSCT version has been updated, issue the **lsrpdomain** command again:

```
Name        OpState  RSCTActiveVersion  MixedVersions  TSPort GSPort
SA_Domain   Online   2.4.5.4            No             12347  12348
```

5. Run the **samctrl -m** command to activate the new features of the new code and to finish the migration. For more information about the command, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.

The code version of the ActiveVersion and the InstalledVersion of IBM Tivoli System Automation should now be the same for all nodes. Until this is true, the new code features have not been activated and cannot be used.

Chapter 2. Installing the operations console

Planning for the installation

Packaging

When you order the base component of IBM Tivoli System Automation, you find the operations console on the following CD and in the following archive, respectively:

Operations console CD

The following table lists the versions of the operations console CDs that are available for the base component. To install the operations console, you use the installation wizard file listed in the right column of the table.

Table 6. Product CD versions

Operating system	Product CD label	Installation wizard file
Windows	IBM Tivoli System Automation Multiplatforms V2.2.0 Base component, Operations Console for Windows	`EEZ2200E2EWindows\Windows\setup.exe`
AIX	IBM Tivoli System Automation Multiplatforms V2.2.0 Base component, Operations Console for AIX	`EEZ2200E2EAIX/AIX/setup`
Linux on System x	IBM Tivoli System Automation Multiplatforms V2.2.0 Base component, Operations Console for Linux on System x	`EEZ2200E2EI386/i386/setup`
Linux on POWER	IBM Tivoli System Automation Multiplatforms V2.2.0 Base component, Operations Console for Linux on POWER	`EEZ2200E2EPPC/ppc/setup`
Linux on System z	IBM Tivoli System Automation Multiplatforms V2.2.0 Base component, Operations Console for Linux on System z	`EEZ2200E2ES390/s390/setup`

Electronic distribution

You can also obtain the base component through electronic distribution. In this case, you can download the deliverables from a URL you receive after purchasing the product.

For each platform, one archive is available for installing the operations console. The archives are listed in the following tables.

Windows:

Table 7. Archives for Windows platforms

Archive name	Description

C947IML.exe	This is the archive you use to install the operations console. The archive is self-extracting.
	Note: Windows only!
	Due to path length restrictions you must extract the files to the root directory of a Windows drive. The installation of the operations console fails if the archive is extracted to a directory other than the root directory.
	
	When you have extracted the files, you find the installation wizard in the following directory:
	`<drive>:\EEZ2200E2EWindows\Windows\setup.exe`
	
	For example:
	`C:\EEZ2200E2EWindows\Windows\setup.exe`

AIX:

Table 8. Archives for AIX platforms

Archive name	Description
C947JML.bin	This is the archive you use to install the operations console. The archive is self-extracting. When you have extracted the files, you find the installation wizard in the following directory: `EEZ2200E2EAIX/AIX/setup`

Linux on System x:

Table 9. Archives for Linux on System x

Archive name	Description
C947KML.tar	This is the archive you use to install the product. Use the *tar -xf* command to extract the archive. When you have extracted the files, you find the installation wizard in the following directory: `EEZ2200E2EI386/i386/setup`

Linux on POWER:

Table 10. Archives for Linux on POWER

Archive name	Description
C947LML.tar	This is the archive you use to install the product. Use the *tar -xf* command to extract the archive. When you have extracted the files, you find the installation wizard in the following directory: `EEZ2200E2EPPC/ppc/setup`

Linux on System z:

Table 11. Archives for Linux on System z

Archive name	Description
C947MML.tar	This is the archive you use to install the product. Use the *tar -xf* command to extract the archive. When you have extracted the files, you find the installation wizard in the following directory: `EEZ2200E2ES390/s390/setup`

Product requirements

The following sections list the software and hardware requirements for the operations console. For the latest information, refer to the IBM Tivoli System Automation for Multiplatforms Release Notes. To obtain a copy of the release notes, go to the IBM Tivoli System Automation for Multiplatforms home page and click **Technical Documentation**. The IBM Tivoli System Automation home page is located at:

`www.ibm.com/software/tivoli/products/sys-auto-linux`

Supported operating systems

The following table lists the operating systems that are supported for the base component operations console:

Table 12. Supported operating systems

Operating system	System x[1]	System i	System p	System z
Windows Server 2003 Standard Edition (32 bit)	X			
Windows Server 2003 Enterprise Edition (32 bit)	X			
AIX 5.2 (AIX 5L Version 5.2) ML 5			X	
AIX 5.3 (AIX 5L Version 5.3) ML 2[4]			X	
SUSE SLES 9 (32 bit[2])	X			
SUSE SLES 9 (64 bit[3])		X	X	X
SUSE SLES 10 (32 bit[2])	X			
SUSE SLES 10 (64 bit[3])		X	X	X

Table 12. Supported operating systems (continued)

Operating system	System x[1]	System i	System p	System z
Red Hat RHEL 4.0 AS (32 bit[2])	X			
Red Hat RHEL 4.0 AS (64 bit[3])		X	X	X

Notes:
1. IBM x/Series systems with IA32, EM64T, or AMD64 architecture.
   Any other systems with IA32, EM64T, or AMD64 architecture are also supported.
   Systems with IA64 architecture are not supported.
2. The following Linux kernel architectures are supported for running with 32 bit:
   - x86 on IBM System x
3. The following Linux kernel architectures are supported for running with 64 bit:
   - ppc64 on IBM System i and IBM System p
   - s390x on IBM System z is supported for some distributions
4. APAR IY65979 must be installed

Browser requirements

The operations console is displayed in a Web browser that connects to the WebSphere Application Server on which the operations console is running. The Web browser may run on an arbitrary system.

The following Web browsers are supported:
- Microsoft Internet Explorer 6.x
- Mozilla 1.7
- Netscape 7

For information on how the Web browser must be configured, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Administrator's and User's Guide*, section "Configuring your Web browser".

Hardware requirements

Memory: 1.5 GB is required on the server on which the operations console is installed.

Disk space requirements: The following table lists the disk space requirements on Windows systems.

Table 13. Disk space requirements for the installation on Windows systems

Description	Default directory	Disk space
Base component installation directory	C:\Program Files\IBM\tsamp\eez	60 MB
Operations console installation directory	C:\Program Files\IBM\ISC	700 MB
Installation log and response files	The value of the system variable %TEMP%. Typically this is: `C:\Documents and Settings\Administrator\Local Settings\Temp`	75 MB
Temporary disk space needed for installation	The value of the system variable %TEMP%. Typically this is: `C:\Documents and Settings\Administrator\Local Settings\Temp`	100 MB

Table 13. Disk space requirements for the installation on Windows systems (continued)

Description	Default directory	Disk space
Tivoli Common Directory	C:\Program Files\IBM\tivoli\common\eez	250 MB
Installer registry	C:\Windows\vpd.properties	10 KB

The following table lists the disk space requirements on AIX and Linux systems:

Table 14. Disk space requirements on AIX and Linux systems

Description	Default directory	Disk space
Base component installation directory	/opt/IBM/tsamp/eez	60 MB
Operations console installation directory	/opt/IBM/ISC	700 MB
Temporary disk space required for the installation	/tmp	300 MB
Tivoli Common Directory	/var/ibm/tivoli/common/eez	250 MB
Installer registry	~root/vpd.properties	10 KB

Preparing for the installation of the operations console

Collecting the information you need to provide during installation

The installation of the operations console is wizard-driven. The wizard guides you through the installation and prompts you for installation and configuration parameters. The following tables list the parameters you need to specify on the installation wizard panels in the order in which they must be specified.

Installation directory and Tivoli Common Directory

The parameters listed in the following table must always be specified.

Table 15. Installation directory and Tivoli Common Directory

Parameter	Description	Default

Installation directory name	The directory to which the installable features are installed.
	
	In this guide, this directory is referred to as `EEZ_INSTALL_ROOT`.
	
	When specifying a directory other than the default, observe the following restrictions:
	
	Windows:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The colon character is allowed only once, immediately following the drive letter. For example, `C:\<directory_name>` is allowed, but `C:\<directory_name>:<directory_name>` is not allowed.
	• The space character and the underscore character (_) are allowed.
	
	AIX, Linux:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The underscore character (_) is allowed.
	• The space and colon characters are not allowed.
		Windows:
		
		`C:\Program Files\IBM\tsamp\eez`
		
		AIX, Linux:
		
		`/opt/IBM/tsamp/eez`

Table 15. Installation directory and Tivoli Common Directory (continued)

Parameter	Description	Default

Tivoli Common Directory	The Tivoli directory for storing serviceability information.
	
	During installation, you are only prompted for input when no Tivoli Common Directory is found on the system.
	
	In the Tivoli Common Directory, the subdirectory `eez` is created for storing product-specific data.
	
	When specifying a directory other than the default, observe the following restrictions:
	
	Windows:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The colon character is allowed only once, immediately following the drive letter. For example, `C:\<directory_name>` is allowed, but `C:\<directory_name>:<directory_name>` is not allowed.
	• The space character and the underscore character (_) are allowed.
	
	AIX, Linux:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The underscore character (_) is allowed.
	• The space and colon characters are not allowed.
		Windows:
		
		`C:\Program Files\IBM\tivoli\common`
		
		AIX, Linux:
		
		`/var/ibm/tivoli/common`

Table 15. Installation directory and Tivoli Common Directory (continued)

Parameter	Description	Default
Operations console installation directory	The directory into which the operations console is installed. In this guide, this directory is referred to as <isc_home>. The directory also contains the product registry for Integrated Solutions Console (product.reg) and the properties file (isc.properties). Do not modify these files. They are used by the operations console at runtime. If you use an existing directory, the directory cannot contain any of the following files and directories: • The files product.reg and isc.properties • The directory _uninst or a file named _uninst • The directory \AppServer or a file named AppServer When specifying a directory other than the default, observe the following restrictions: • The length of the installation path must be 32 characters or less. • The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9). Additional restrictions: **Windows:** • The colon character is allowed only once, immediately following the drive letter. For example, C:\<directory_name> is allowed, but C:\<directory_name>:<directory_name> is not allowed. • The space character is allowed. **AIX, Linux:** • The space and colon characters are not allowed.	**Windows:** C:\Program Files\IBM\ISC\ **AIX, Linux:** /opt/IBM/ISC

Installation parameters for the operations console

The parameters listed in the following table must always be specified.

Table 16. Installation parameters for Integrated Solutions Console

Parameter	Description	Default
ISC administrator user	The user ID of the operations console administrator. During installation, the administrator is given access to all console modules. The user ID is added to the operations console administrator group. After the installation, the administrator can change the password and add other user IDs to the operations console administrator group. The user ID must comply with the following conditions: • The user ID must be unique. • The length is 3 to 60 characters. • A valid user ID may contain only the characters a-z, A-Z, period (.), hyphen (-), underscore (_), and double-byte character set (DBCS) characters. No other characters are permitted in this field. For example, diacritics, such as the umlaut, are not permitted.	iscadmin
Password	The password of the operations console administrator. The password must comply with the following conditions: • The length is 5 to 60 characters. • A valid password may contain only the characters a-z, A-Z, period (.), hyphen (-), and underscore (_). No other characters are permitted in this field. For example, DBCS characters and diacritics, such as the umlaut, are not permitted.	No default value is provided
Fully qualified host name	The fully qualified host name of the system where the operations console will be installed	The fully qualified host name is detected on your system and displayed as default value.
Console Help Port	The port that the help system (based on Eclipse technology) will use to receive requests for help files. This value must not conflict with existing port assignments on the system.	8423
Register ISC server and ISC Help server as system service	To automatically restart the operations console and the console help server each time the system is restarted, these services can be registered as system services	Enabled

Table 16. Installation parameters for Integrated Solutions Console (continued)

Parameter	Description	Default
Console Service ID	To automatically restart the console server each time the operating system is restarted, specify this parameter. For Linux, the string must be 1 to 4 characters. The installation program checks the length of the value you specify. For AIX, the length must be 1 or more characters. For Linux and AIX, the operating system file `/etc/inittab` is edited directly to include the value you specify. The line that is added to the file has the following format: `service_ID:23:boot:isc_home/PortalServer/ bin/startISC.sh ISC_Portal ISCUSER ISCPASS` For Windows systems only: Set the value to a unique string. Valid characters are a-z, A-Z, and 0-9. The string must be 1 or more characters and the value is used to add a service to the operating system. If this parameter is specified, you must also specify the Console Help Service ID parameter.	CS01
Console Help Service ID	For Windows systems only: Set the value to a unique string. Valid characters are a-z, A-Z, and 0-9. The string must be 1 or more characters. The value is used to add a service to the operating system. If this parameter is specified, you also must specify the Console Service ID parameter. For AIX and Linux: The Console Help Service is started as part of the service defined by the Console Service ID parameter. The Console Help Service ID parameter is not shown.	HS01

Port assignment for the operations console server

The parameters listed in the following table must always be specified.

Table 17. Port assignment for the operations console server

Parameter	Description	Default
HTTP Port	The number of the HTTP port that the operations console will use. Select a port that is not being used by another process on the system. After the operations console is installed, you must include this port number in the URL for opening the console. The URL is composed of the protocol name, plus the fully-qualified host name, plus the port, plus ibm/console. This is an example of a full URL as it is needed for connecting to the operations console: `http://myhost.com:8421/ibm/console`	8421

Table 17. Port assignment for the operations console server (continued)

Parameter	Description	Default
HTTPS Port	The port that the operations console will use for secure HTTP transport (HTTPS). This value must not conflict with existing port assignments on the system.	8422
Bootstrap/RMI Port	The address for the bootstrap function and the port number for the Java Remote Method Invocation (RMI) connector on the operations console server. This value must not conflict with existing port assignments on the system.	8424
SOAP Port	The address for the Simple Object Access Protocol (SOAP) connector on the operations console server. This value must not conflict with existing port assignments on the system.	8425
Admin HTTP Port	The HTTP Administrative Console port on the operations console server. This value must not conflict with existing port assignments on the system.	8431
Admin HTTPS Port	The HTTPS Administrative Console secure port on the operations console server. This value must not conflict with existing port assignments on the system.	8432
SAS SSL ServerAuth Listener Address Port	The SAS SSL ServerAuth Listener Address port on the operations console server. This value must not conflict with existing port assignments on the system.	8439
CSIV2 SSL ServerAuth Listener Address Port	The CSIV2 SSL ServerAuth Listener Address port on the operations console server. This value must not conflict with existing port assignments on the system.	8440
CSIV2 SSL MutualAuth Listener Address Port	The CSIV2 SSL MutualAuth Listener Address port on the operations console server. This value must not conflict with existing port assignments on the system.	8441

Port assignment for the embedded application server

The parameters listed in the following table must always be specified.

Table 18. Port assignment for the embedded application server

Parameter	Description	Default
HTTP Port	The number of the HTTP port for the embedded application server. Select a port that is not being used by another process on the system.	8426

Table 18. Port assignment for the embedded application server (continued)

Parameter	Description	Default
HTTPS Port	The port that the embedded application server will use for secure HTTP transport (HTTPS). This value must not conflict with existing port assignments on the system.	8427
Bootstrap/RMI Port	The address for the bootstrap function and the port number for the Java Remote Method Invocation (RMI) connector on the embedded application server. This value must not conflict with existing port assignments on the system.	8428
SOAP Port	The address for the Simple Object Access Protocol (SOAP) connector on the embedded application server. This value must not conflict with existing port assignments on the system.	8429
Admin HTTP Port	The HTTP Administrative Console port on the embedded application server. This value must not conflict with existing port assignments on the system.	8433
Admin HTTPS Port	The HTTPS Administrative Console secure port on the embedded application server. This value must not conflict with existing port assignments on the system.	8434
ORB Listener Port	The ORB Listener port on the embedded application server. This value must not conflict with existing port assignments on the system.	8435
SAS SSL ServerAuth Listener Address Port	The SAS SSL ServerAuth Listener Address port on the embedded application server. This value must not conflict with existing port assignments on the system.	8436
CSIV2 SSL ServerAuth Listener Address Port	The CSIV2 SSL ServerAuth Listener Address port on the embedded application server. This value must not conflict with existing port assignments on the system.	8437
CSIV2 SSL MutualAuth Listener Address Port	The CSIV2 SSL MutualAuth Listener Address port on the embedded application server. This value must not conflict with existing port assignments on the system.	8438

Installation prerequisites

The following prerequisites must be satisfied before you can start the installation wizard for the operations console:

- WebSphere Application Server must **not** on be installed on the system on which you are installing the operations console.
- The user ID that is used to run the installer for the operations console must have administrator authority.

  On Linux and AIX, this user ID is typically ″root″.

- When installing the operations console to an AIX or Linux system, you must ensure that an XWindows session is available for displaying the graphical installation wizard panels.

Installing the operations console

This section describes how to install the operations console. The installation uses a graphical installation program, the so-called installation wizard. The required steps are described below.

Notes:

1. Although the screens in this section show a Linux installation, the screens that are displayed for other operating systems have a similar appearance. Make sure to conform to the conventions of your platform when specifying directory locations, files names and so on.
2. **Attention:** Do not cancel the installation after clicking **Install**. If you cancel an ongoing installation, the installation process may fail and you may need to clean up your system manually (see "Cleaning up from a failed installation" on page 199).

To install the operations console, perform these steps:

1. Insert the following CD in the CD drive:

   IBM Tivoli System Automation Multiplatforms V2.2.0 Base component, Operations Console for <operating_system_name>

   There are multiple CDs. Be sure to use the one for your platform.

   ---

2. Change to the directory that contains the installation program using the `cd` command. For the location of the directory, refer to "Packaging" on page 17.

   ---

3. Launch the installation wizard by starting the following program from the current working directory:
   - **Windows**: `setup.exe`
   - **AIX, Linux**: `setup`

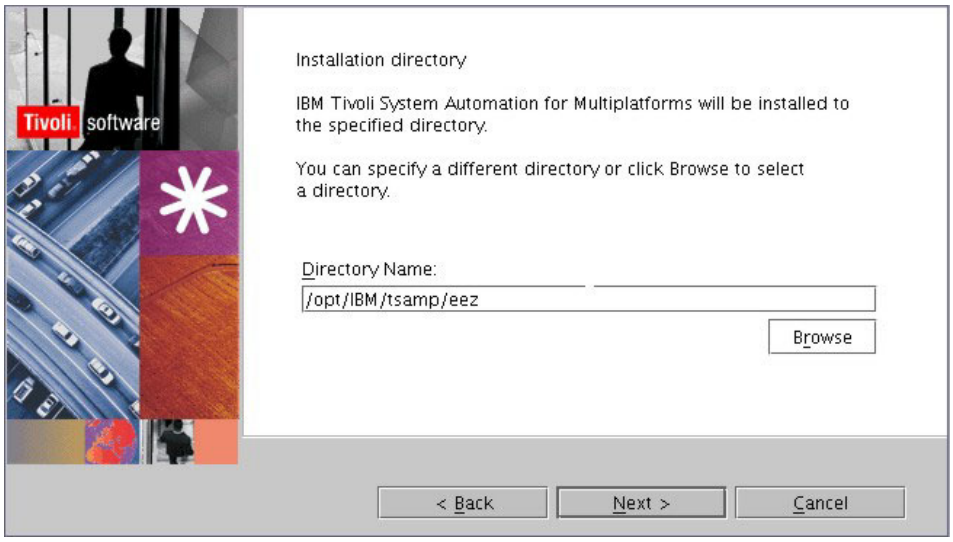
   When the wizard was launched successfully, the Welcome panel appears.

   ---

4. On the Welcome panel, click **Next** to display the License agreement panel.

5. Select **I accept the terms of the license agreement** and click **Next**

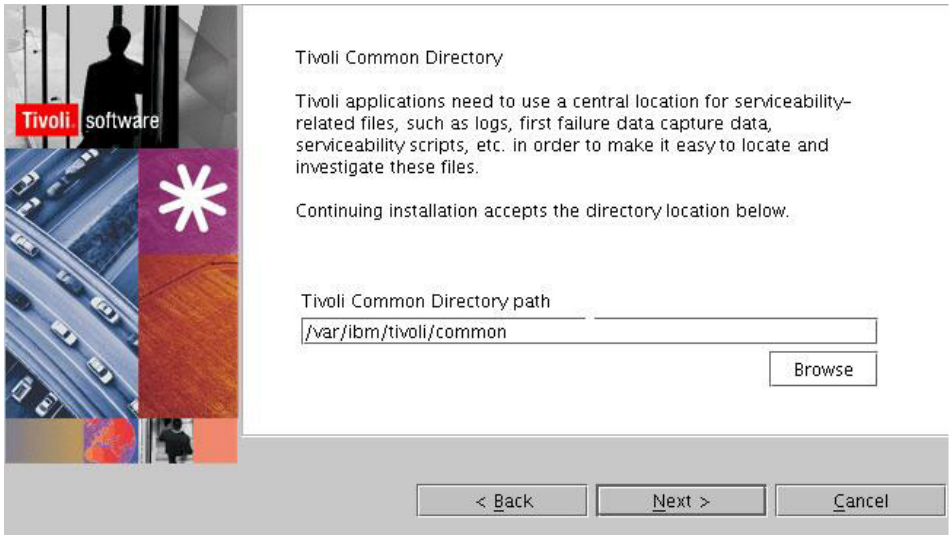
6. Specify the installation directory or accept the default location. Click **Next**.



7. If the installation program detected a Tivoli Common Directory on your system, for example, because a Tivoli product is already installed, the directory must also be used for IBM Tivoli System Automation for Multiplatforms. In this case, the entry field that is displayed on this panel is write-protected.

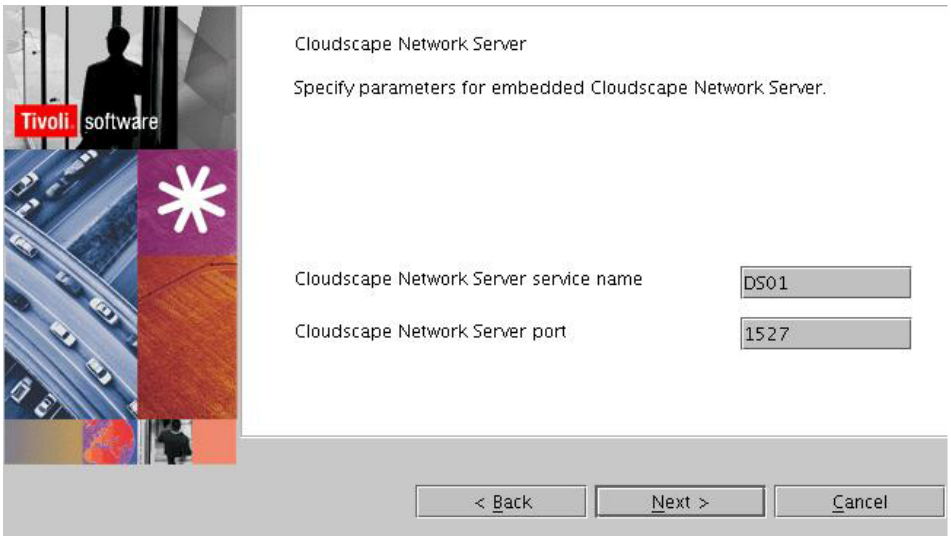
   If the installation program did not detect a Tivoli Common Directory on your system, accept the default location or specify the directory to which the Tivoli log files are to be written.

   Click **Next**.

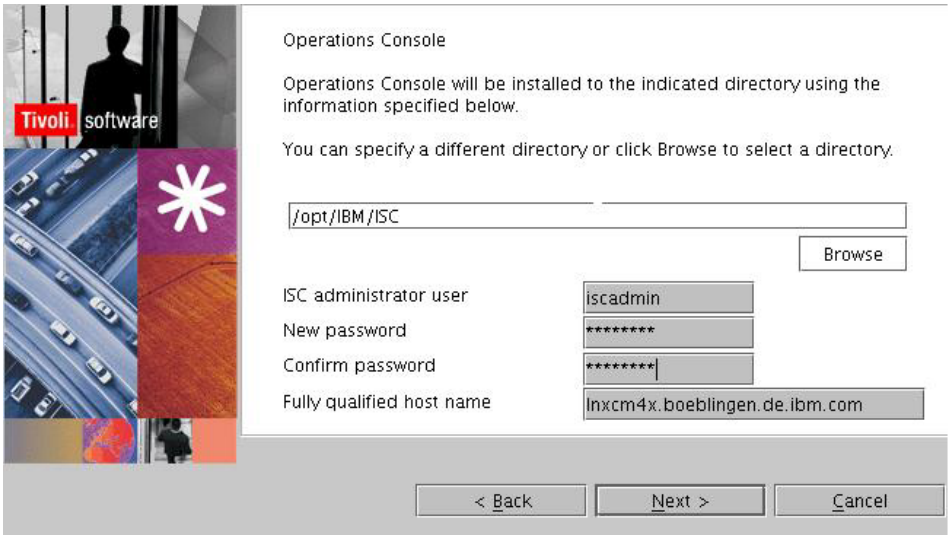


8. Specify the parameters for the embedded Cloudscape Network Server or accept the default parameters.

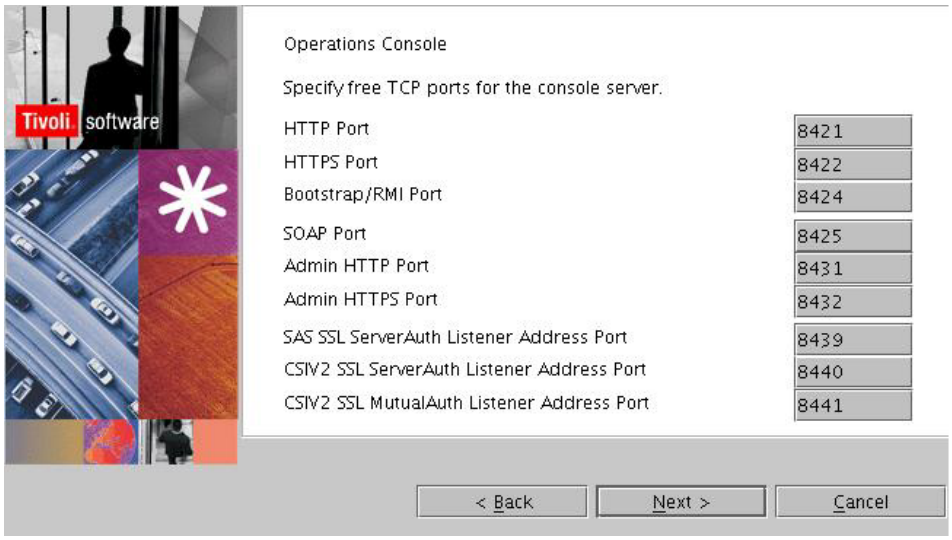
   Click **Next**.



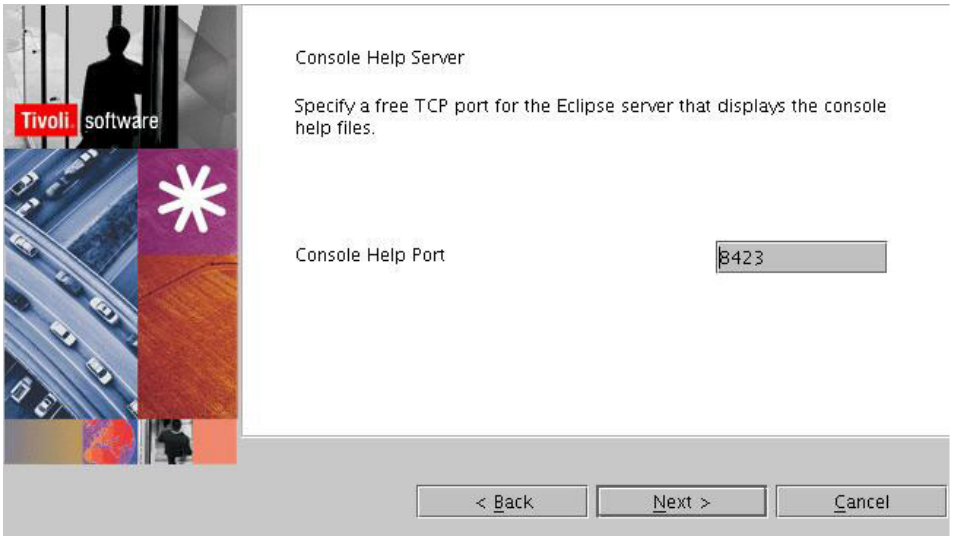
9. Choose a user ID and password for the operations console administrator. If you specify an operations console installation directory other than the default, note that the length of the installation path must be 32 characters or less (for further restrictions, refer to Table 15 on page 24). Click **Next**.



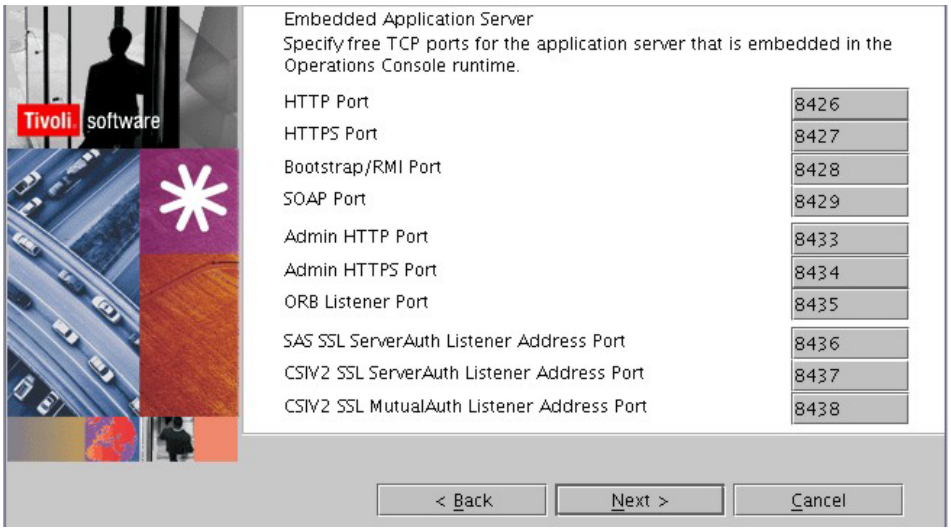
10. Specify the ports you want to use for the operations console or accept the default values. Click **Next**.



11. Specify the port number for the Eclipse Help System server or accept the default value, and click **Next**.

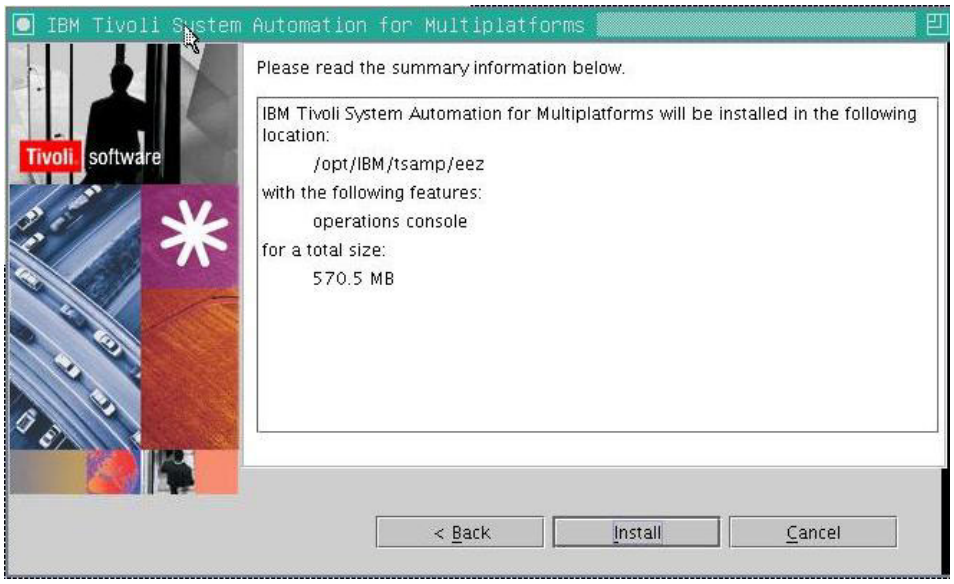


12. Specify the ports you want to use for the embedded application server or accept the default values. Click **Next**.



13. If you want to register the operations console server and the Eclipse Help System server as system services, specify service IDs or accept the default service IDs and click **Next**.

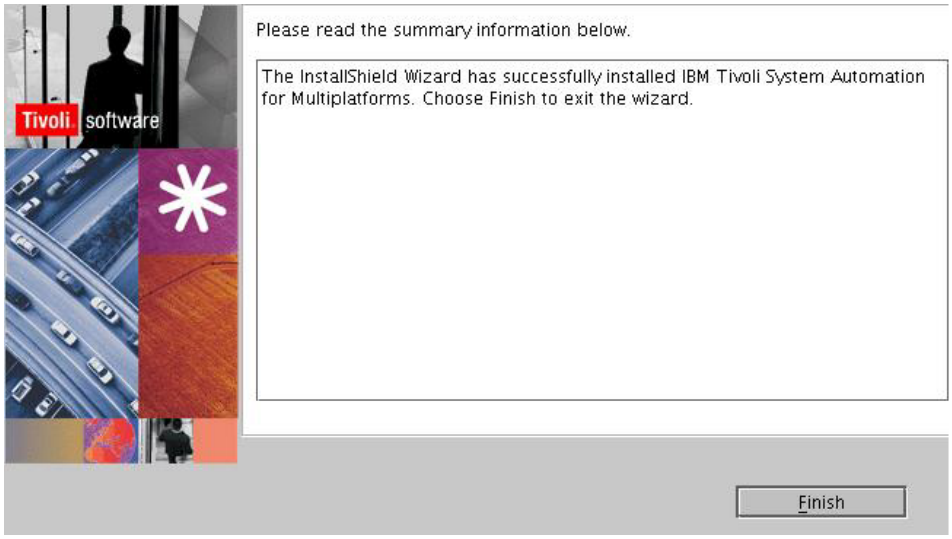
14. When you have specified all required information on the wizard panels, a summary panel appears.



Click **Install**. The installation wizard begins installing the operations console. The installation may take up to two hours to complete. While installation tasks are performed, the progress bar may appear to stall.

Attention: Do not cancel the installation after clicking **Install**. If you cancel an ongoing installation, the installation process may fail and you may need to clean up your system manually (see "Cleaning up from a failed installation" on page 199).

15. When the operations console was installed successfully, a summary panel appears. Click **Finish** to close the installation wizard.



Verifying the installation

Perform the following steps to verify that the operations console was installed successfully:

1. In a Web browser window, specify the address `http://<your_host_name>:<your_isc_port>/ibm/console` to display the Login panel of Integrated Solutions Console. The default ISC port is 8421.

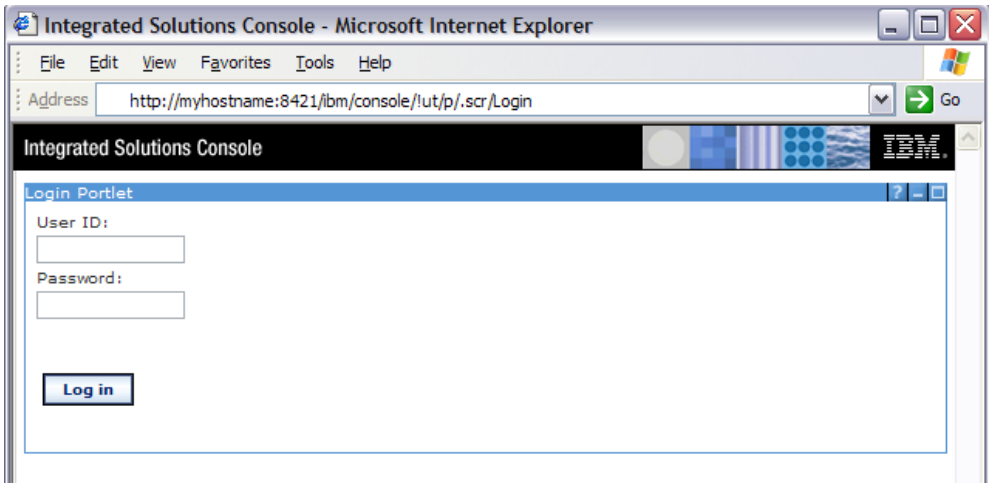


Figure 2. Log in panel of Integrated Solutions Console

2. Type the Integrated Solutions Console user ID and password that you specified during the installation and click **Log in**. The Welcome panel is displayed. On the Work Items page, you should see these entries:
   - Integrated Solutions Console
   - Tivoli System Automation for Multiplatforms

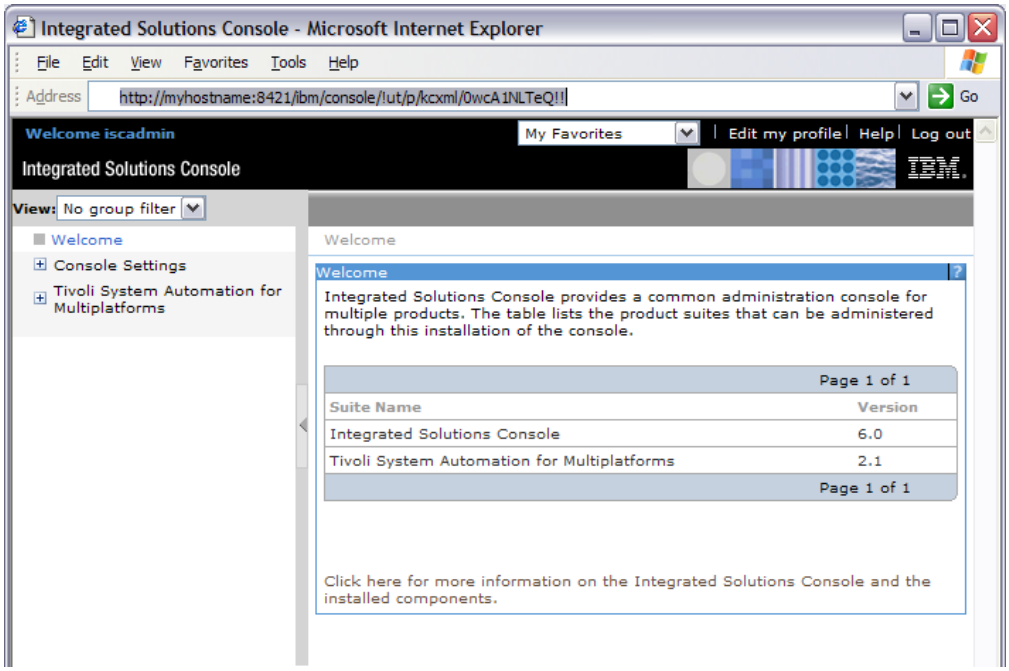


Figure 3. Welcome panel of Integrated Solutions Console

3. Expand the folder Tivoli System Automation for Multiplatforms.
4. Click **SA operations console**. When the main panel of the operations console is displayed, the installation was successful.

Chapter 3. Upgrading the operations console from release 2.1

If the operations console of the base component 2.1 is already installed, you can upgrade to release 2.2. The minimum release level required for upgrading is 2.1.1.0. If a lower release level is installed, you must first upgrade to level 2.1.1.0 by installing service.

To perform the upgrade to release 2.2, you use the following files:

- **AIX/Linux:** `update`
- **Windows:** `update.exe`

To find the `update` file on the product CD or in the product archive, refer to the description of the `setup` file in "Packaging" on page 17. The location of the `update` and `setup` files is identical.

To launch the update wizard, invoke the `update` file. Follow the instructions on the wizard panels to upgrade the operations console to release 2.2. No further migration actions are required.

Chapter 4. Configuring the operations console

Configuring the end-to-end automation adapter to use the operations console

The System Automation for Multiplatforms end-to-end automation adapter must be configured in order to be able to directly access the operations console. "**Host using adapter** tab" on page 149 describes how to do this.

See Chapter 13, "Configuring the end-to-end automation adapter of the base component of IBM Tivoli System Automation for Multiplatforms," on page 143 to learn more about the System Automation for Multiplatforms end-to-end automation adapter.

Configuring the operations console for direct access mode

This is necessary if your operations console cannot use port 2002 to receive events from adapters, or if you want to use the SSL (Secure Socket Layer) protocol for the transmission of requests from the operations console to the adapter.

Planning the configuration

If you want to change the port number, obtain a valid port number from your network administrator. Note that all adapters that are connected to the operations console must send events to the same "Event port".

The operations console supports the Secure Socket Layer (SSL) protocol but it does not enforce it on adapters. Whether SSL is used for transport must be specified for the adapter, for example, on the Security tab of the adapter configuration dialog (see "**Security** tab" on page 153). All adapters that require SSL must have the same truststore file, keystore file, alias name and password for the keystore specified. The operations console uses the same information. Therefore, the truststore file and the keystore file must be placed on the host of the operations console.

If no truststore and keystore keys have been generated yet, you can use **ikeyman.bat** to generate them. **ikeyman.bat** is available in the directory `<isc_home>/AppServer/bin`. The resulting information should be the location of truststore and keystore, and alias name and password to access the keystore. Note that actual keys would be obtained from a certification authority.

Using the configuration dialog

Perform the following steps to configure the operations console:

1. Invoke the configuration dialog:
   a. Change the directory to

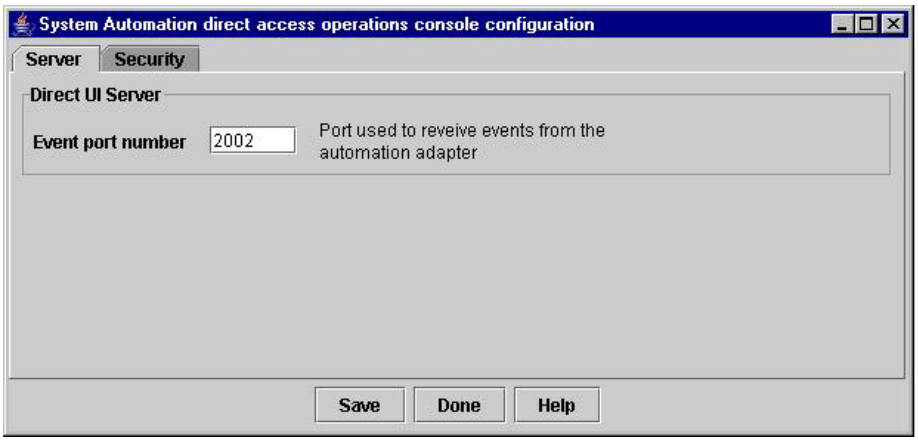
      Windows: `<drive>:<isc_home>\AppServer\profiles\default\Tivoli\EEZ` where `<drive>` is the letter of the drive and `<isc_home>` is the directory where the operation console is installed.

      AIX and Linux: `/opt/<isc_home>/AppServer/profiles/default/Tivoli/EEZ` where `<isc_home>` is the directory where the operation console is installed.

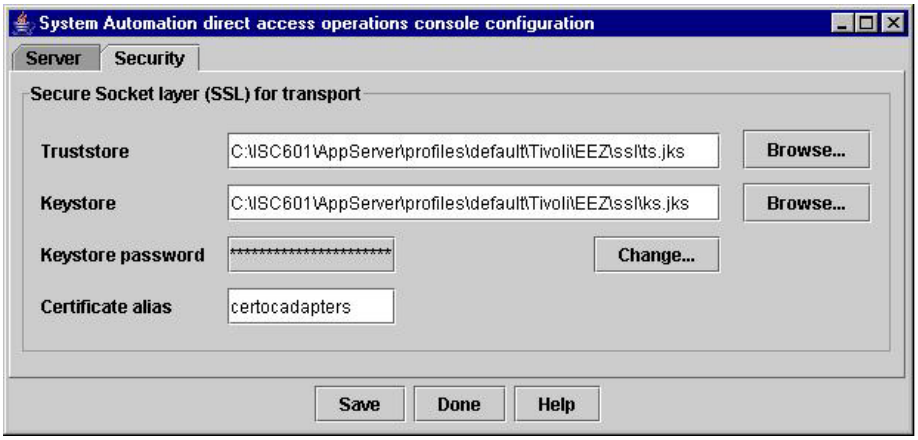
   b. Type `cfgdirect`.

The configuration dialog is displayed. The fields on the dialog pages show the current settings.

2. The event port number on the Server page specifies the port on which the operations console listens for events from the adapter.



3. In the fields on the Security page you can specify the information required for using the SSL protocol (see "Planning the configuration" on page 39).



4. To save your changes, click **Save**.

5. Click **Done** to close the dialog.

Setting up SSL for the operations console

This is an optional post-installation task to allow for secure HTTP transport (HTTPS) between client browsers and the operations console.

To set up SSL for Integrated Solutions Console, perform the following procedure:

1. Configure the Web server to support HTTPS. If you are doing this in a production environment, you need to obtain a certificate from a certificate authority. For testing purposes, you can use IKEYMAN to generate a

self-signed certificate. Refer to the WebSphere Application Server documentation for detailed instructions.

---

2. Add the virtual host defined in the Web server to the Web server virtual host alias list. Add a host alias for the SSL port that the Web server uses. To create the settings, perform the following steps:
   a. Use a text editor to open the following file:
      ```
      <isc_home>/profiles/default/config/cells/DefaultNode/virtualhosts.xml
      ```
      where <isc_home> is the operations console installation directory.

      ---

   b. Add the following element before the ending element </host:VirtualHost> for the virtual host named default_host. Add the element to the list of aliases:
      ```
      <aliases xmi:id="HostAlias_x" hostname="*" port="alias_port"/>
      ```
      where x is the next number in the HostAlias sequence and alias_port is the value specified for the HTTPS Port parameter.

      ---

   c. Save the file.

---

3. Edit the ConfigService.properties file in
   ```
   isc_home/PortalServer/shared/app/config/services
   ```
   where isc_home is the operations console installation directory.

   Change the following parameters:
   ```
   redirect.login.ssl = true
   redirect.logout.ssl = true
   host.port.https = alias_port
   ```
   where alias_port is the port number used for the virtual host alias that you specified in step 2.

---

4. Set the security constraints for the console URL. To do so, perform the following steps:
   a. Use an editor to open the file web.xml. It is located in the following directory:
      ```
      <isc_home>/profiles/default/config/cells/DefaultNode/applications/
                wps.ear/deployments/wps/wps.war/WEB-INF
      ```
      where <isc_home> is the operations console installation directory.

      ---

   b. In the web.xml file, change the <security-constraint> element for the console URL to use HTTPS as shown in the following example:
      ```
      <security-constraint id="SecurityConstraint_1">
           <web-resource-collection id="WebResourceCollection_1">
              <web-resource-name></web-resource-name>
              <url-pattern>/console/*</url-pattern>
              <http-method>DELETE</http-method>
              <http-method>GET</http-method>
              <http-method>POST</http-method>
              <http-method>PUT</http-method>
          </web-resource-collection>
      ```

```
        <auth-constraint id="AuthConstraint_1">
           <description></description>
           <role-name>All Role</role-name*gt;
        </auth-constraint>
        <user-data-constraint id="UserDataConstraint_4">
           <transport-guarantee>CONFIDENTIAL</transport-guarantee>
           <!-- replace NONE with CONFIDENTIAL  -->
        </user-data-constraint>
     </security-constraint>
```

5. From a command prompt, change to the following directory:
   `<isc_home>/PortalServer/config`

   where `<isc_home>` is the operations console installation directory.

6. Edit the file `wpconfig.properties` and set the PortalAdminPwd parameter to your console administrator user ID's password.

7. Run the following command from the command line:
   `WPSconfig.bat|sh init action-deploy-setupisc-ssl`

8. From a command prompt, change to the following directory:
   `<isc_home>/PortalServer/bin`

   where `<isc_home>` is the operations console installation directory.

9. Run the following command from the command line:
   Windows:
   `stopISC.bat ISC_Portal iscadmin iscpass`
   AIX, Linux:
   `./stopISC.sh ISC_Portal iscadmin iscpass`

   where `iscadmin` is the console administrator user ID and `iscpass` is the console administrator user ID's password.

10. Run the following command from the command line:
    Windows:
    `startISC.bat ISC_Portal`
    AIX, Linux:
    `./startISC.sh ISC_Portal`

11. Test your changes by launching the home page of the console in a Web browser. The login page that is displayed is not secure. However, when you click **Log in**, the credentials are encrypted and the session is directed to a secure connection.

Modifying the session timeout values

After the installation of the operations console, you should set the session timeout values for Lightweight Third Party Authentication (LTPA) and HTTP to values that are appropriate for your environment. LTPA and HTTP session timeouts should have the same value.

Modifying the HTTP session timeout value

The HTTP session timeout value defines after how many minutes of inactivity a user is automatically logged out from the operations console. During the installation of the operations console, the HTTP session timeout is set to 30 minutes.

Perform these steps to set the HTTP session timeout to an appropriate value:

1. Open the following configuration file:

   `<isc_home>\AppServer\profiles\default\config\cells\DefaultNode\nodes\DefaultNode\servers\ISC_Portal\server.xml`
2. In the file, search for `invalidationTimeout`. This is the parameter that sets the HTTP session timeout. By default `invalidationTimeout` is set to `30`, which means that a user is logged out automatically after 30 minutes of inactivity.
3. Set `invalidationTimeout` to an appropriate value. For example, if a session is to last for 24 hours, change the value to `1440` (24 hours × 60 minutes/hour = 1440 minutes)
4. Save the file.
5. Restart the operations console.

LTPA session timeout

The LTPA session timeout value defines after how many minutes after logging on a user will be logged out, regardless of whether the user performed any actions on the console or not. The default value is 120 minutes.

To modify the LTPA session timeout value, perform the following steps:

1. Open the following configuration file:

   `<isc_home>\AppServer\profiles\default\config\cells\DefaultNode\security.xml`
2. Set the timeout value in the following section of the file to an appropriate value, for example, to `1440` (the value should be identical to the HTTP session timeout value described above):

```
<authMechanisms xmi:type="security:LTPA"
  xmi:id="LTPA_1" OID="oid:1.3.18.0.2.30.2"
   authContextImplClass="com.ibm.ISecurityLocalObjectTokenBaseImpl.WSSecurityContextLTPAImpl"
     authConfig="system.LTPA" simpleAuthConfig="system.LTPA" authValidationConfig="system.LTPA"
    timeout="120" password="{xor}Niw8Lz4sLA==">
```

Chapter 5. Installing and uninstalling service

Installing service

Installing service means applying corrective service fix packs to release 2.2 of IBM Tivoli System Automation for Multiplatforms or upgrading the software release level from release 2.2. Such service fix packs are referred to as product fix packs in this guide. Product fix packs are available for the base component including the operations console.

Product fix packs are delivered in the following formats:

- For Linux: Archives in TAR-format
- For AIX: Archives in TAR-format or self-extracting archives (operations console only)
- For Windows: Self-extracting archives for Windows (operations console only)

Where to obtain fix packs

Read the release notes to find out which fix packs are required for a release update. To obtain a copy of the release notes, go to the IBM Tivoli System Automation for Multiplatforms home page and click **Technical Documentation**. The IBM Tivoli System Automation home page is located at:

`www.ibm.com/software/tivoli/products/sys-auto-linux`

Archives for product fix packs can be downloaded from the IBM Tivoli System Automation support site at:

`www.ibm.com/software/sysmgmt/products/support/IBMTivoliSystemAutomationforLinux.html`

Download the archive to a temporary directory. Typically, one archive is available for each platform. For information about the naming conventions that apply to product fix pack archives, refer to "Archive naming conventions."

Archive naming conventions

The archives for product fix packs for the base component of IBM Tivoli System Automation including the operations console have the following syntax:

`2.2.0-TIV-SABASE-<platform>-FP<fix_pack_number>.<archive_type>` containing the service for the base component, and

`2.2.0-TIV-SAE2E-<platform>-FP<fix_pack_number>.<archive_type>` containing the service for the operations console.

where

- `<platform>` represents the platform on which IBM Tivoli System Automation for Multiplatforms is installed
- `<fix_pack_number>` represents the fix pack number
- `<archive_type>` is either tar, bin, or exe

Example:

This is the tar archive that is used to install fix pack 1 for IBM Tivoli System Automation for Multiplatforms 2.2 on AIX platforms:

`2.2.0-TIV-SABASE-AIX-FP0001.tar`

Installing service for the base component

You can download these tar files for applying service for the Linux and AIX operating systems:

Archives

Linux:

Table 19. Archive for Linux platforms

Archive name	Description
2.2.0-TIV-SABASE-LIN-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the *tar -xf* command to extract the archive. Then there is the install script `SAM22<maintenance_level>/installSAM`

AIX:

Table 20. Archive for AIX platforms

Archive name	Description
2.2.0-TIV-SABASE-AIX-FP<fix_pack_number>.tar	Use the *tar -xf* command to extract the archive. Then there is the install script `SAM22<maintenance_level>/installSAM`

Steps for installing service for the base component

Before you begin:

- Installing service means upgrading IBM Tivoli System Automation from release 2.2. Therefore, release 2.2 must have been installed before any service can be applied.
- Product fix packs are always cumulative.
- You must have root authority to install a product fix pack.
- When you have downloaded the archives from the IBM Tivoli System Automation for Multiplatforms support site (see “Where to obtain fix packs” on page 45), unpack the product fix pack archive to a temporary directory. For information about how to unpack the archive for your platform, refer to “Archives.”
- Back up your system configuration before installing service. For information on how to do this, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Administrator's and User's Guide*, section "Automation Policy Management".
- To minimize the downtime, you can perform a prerequisites check before starting the installation (for more information, see “Performing the prerequisites check” on page 9).

Perform the following steps on each node in the peer domain:

1. Check if any resources are online on the node you want to service.
2. If the resources are online and must be kept available, exclude the node from automation using the command

   ```
   samctrl -u a Node
   ```

IBM Tivoli System Automation for Multiplatforms stops the resources on the node and, if possible, restarts them on another node in the peer domain.

3. If the resources need not be kept available during service, set the resource groups offline.
4. After receiving the archives, extract them. They create a directory structure with root directory SAM22*mf*Base, where *mf* stands for modification level and fix level.
5. Install the service fix pack with the *installSAM* script. For detailed information about the script, refer to "Installing the base component" on page 9.
6. If you had excluded the node in step 2, include the node into automation using the command

   ```
   samctrl -u d Node
   ```
7. If you require the resource groups to be online, set the resource groups online. Otherwise delay this step until after the last node in the peer domain has been serviced.
8. After all nodes have been serviced, perform the steps described in "Completing the migration" on page 14. This ensures that the changes become effective in the entire domain and the correct version is shown.

Installing service for the operations console

These are the archives for applying service for the operations console.

Usage instructions for the platform-specific archives

Windows:

Table 21. Windows platforms

Archive name	Description
2.2.0-TIV-SAE2E-WIN-FP<fix_pack_number>.exe	The archive is self-extracting. This is where you find the update installer program after unpacking the archive: EEZ22<maintenance_level>E2EWindows/Windows/update.exe

AIX:

Table 22. AIX platforms

Archive name	Description
2.2.0-TIV-SAE2E-AIX-FP<fix_pack_number>.bin	The archive is self-extracting. This is where you find the update installer program after unpacking the archive: EEZ22<maintenance_level>E2EAIX/AIX/update

Linux on IBM System x:

Table 23. Linux on IBM System x

Archive name	Description
2.2.0-TIV-SAE2E-I386-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. This is where you find the update installer program after unpacking the archive: EEZ22<maintenance_level>E2EI386/i386/update

Linux on POWER:

Table 24. Linux on POWER

Archive name	Description
2.2.0-TIV-SAE2E-PPC-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. This is where you find the update installer program after unpacking the archive: EEZ22<maintenance_level>E2EPPC/ppc/update

Linux on System z:

Table 25. Linux on System z

Archive name	Description
2.2.0-TIV-SAE2E-S390-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files to a temporary directory. This is where you find the update installer program after unpacking the archive: EEZ22<maintenance_level>E2ES390/s390/update

Installing product fix packs for the operations console

- When you have downloaded the archives from the IBM Tivoli System Automation for Multiplatforms support site (see "Where to obtain fix packs" on page 45), unpack the product fix pack archive to a temporary directory. For information about how to unpack the archive for your platform, refer to "Usage instructions for the platform-specific archives" on page 48.
- Before performing the subsequent steps, check the release notes for additional or deviating installation instructions.
- Change to the directory in which the update wizard program is located. For information on where to find the update wizard program, refer to "Usage instructions for the platform-specific archives" on page 48.
- Launch the update wizard.

  When the wizard is launched successfully, the Welcome panel appears.
- Follow the instructions on the wizard panels to install the product fix pack.

Uninstalling service

To uninstall a fix pack, you need to uninstall the complete product as described in the following sections:

- To uninstall the base component, follow the instructions in "Uninstalling the base component" on page 51
- To uninstall the operations console, follow the instructions in "Uninstalling the operations console" on page 52

After the uninstallation is complete, you can reinstall IBM Tivoli System Automation for Multiplatforms and the required service level (fix pack level).

Chapter 6. Uninstalling the base component and the operations console

Uninstalling the base component

Before you begin:

- Use the *uninstallSAM* script that is provided for your operating system to uninstall the base component. For example, run *./uninstallSAM* from the installation directory. This will ensure a proper deinstallation of the product.
- Before uninstalling you should save your configuration with the **sampolicy –S** command. For information on how to save IBM Tivoli System Automation, refer to the following documentation:
  - *IBM Tivoli System Automation for Multiplatforms Base Component Administrator's and User's Guide*, section "Automation Policy Management"
  - The description of the **sampolicy** command in the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*
- *uninstallSAM* will remove all configuration information that you defined for the domain. Never use *uninstallSAM* before upgrading to a new version.

To uninstall IBM Tivoli System Automation perform the following steps:

1. Ensure that the domain is offline:
   - Check if a domain is still online by entering the command:
     ```
     lsrpdomain
     ```
   - In order to stop a domain enter the command:
     ```
     stoprpdomain <domain>
     ```
2. Uninstall the product with the *uninstallSAM* script:
   ```
   ./uninstallSAM
   ```
   Typically, you do not need to specify any of the options that are available for the **uninstallSAM** command. For a detailed description of the command, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.

   If CSM or GPFS (which also use RSCT and System Resource Controller (SRC) packages) is installed on a Linux system from which you want to uninstall IBM Tivoli System Automation, RPM will ensure that RSCT and SRC will not be uninstalled with IBM Tivoli System Automation. RPM messages will indicate this.
3. Check the following log file for information about the uninstallation:
   ```
   /tmp/uninstallSAM.<#>.log
   ```
   where <#> is a number; the highest number identifies the most recent log file.
4. To verify which packages were uninstalled, issue the following command:
   - **AIX:**
     ```
     lslpp -l sam*
     ```
   - **Linux:**
     ```
     rpm -qa | grep -E "^src|^rsct|^sam"
     ```

   Any packages left installed will be listed. If no packages required by other products are left installed, no packages will be listed.

Uninstalling the operations console

This section describes how to uninstall the operations console. An uninstallation program is provided that removes the components that were installed by the installation wizard.

Launching the graphical uninstallation program on Windows

To launch the uninstallation program on Windows, you can either issue the command `<EEZ_INSTALL_ROOT>/_uninst/uninstaller.exe` at a command prompt or perform the following steps:

1. Open the Control Panel (**Start —> Settings —> Control Panel**).

   ---

2. On the Control Panel, open **Add/Remove Programs**.

   ---

3. On the Add/Remove Programs panel, select **IBM Tivoli System Automation for Multiplatforms** and click **Change/Remove**. This brings up the Welcome panel of the uninstallation program.

Launching the graphical uninstallation program on AIX and Linux

To launch the uninstallation program on AIX and Linux, enter the following command in a shell:

```
<EEZ_INSTALL_ROOT>/_uninst/uninstaller.bin
```

This brings up the Welcome panel of the uninstallation program.

Using the uninstallation program

Before you begin:

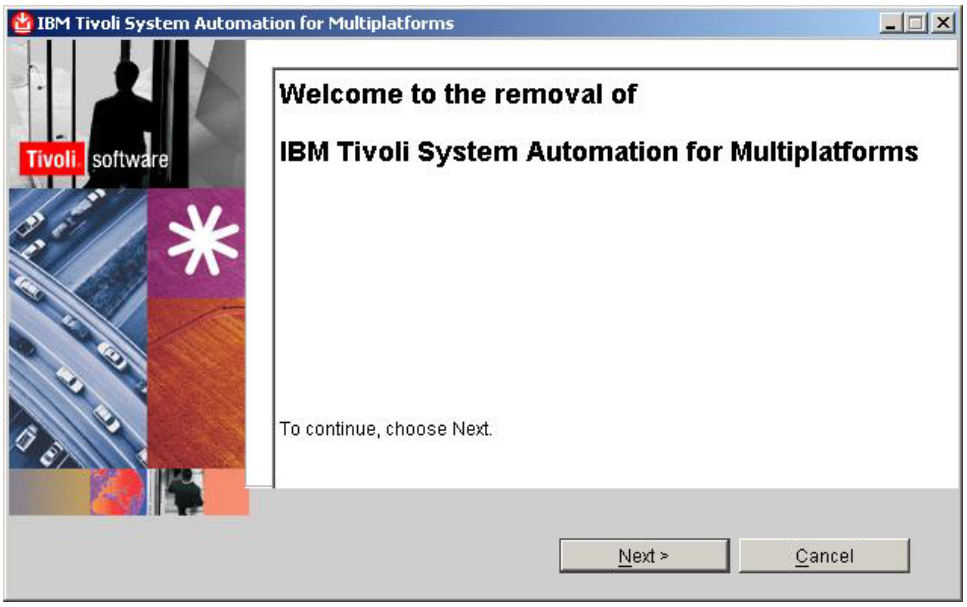
- Make backup copies of the following files in the directory `<isc_home>/AppServer/profiles/default/Tivoli/EEZ` to prepare for reusing them after reinstallation:
  - `directui-joined-domains-xml`
    Contains the domains that you saw most recently in the topology tree.
  - `directui-prefs.xml`
    Contains user preferences, such as hidden domains and resource filters.
  - `directui.properties`
    Contains the port on which the operations console listens for events from domains, and SSL information. If you never changed the port from the default and never specified SSL key information, you need not back up the file.
- Before starting the uninstallation of the operations console, make sure that the Integrated Solutions Console server is stopped. For information on how to stop the server, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Starting and stopping the operations console". .

During uninstallation, a number of panels may appear prompting you to confirm that specific files are to be deleted. Make sure that the files should be deleted before confirming the deletion.

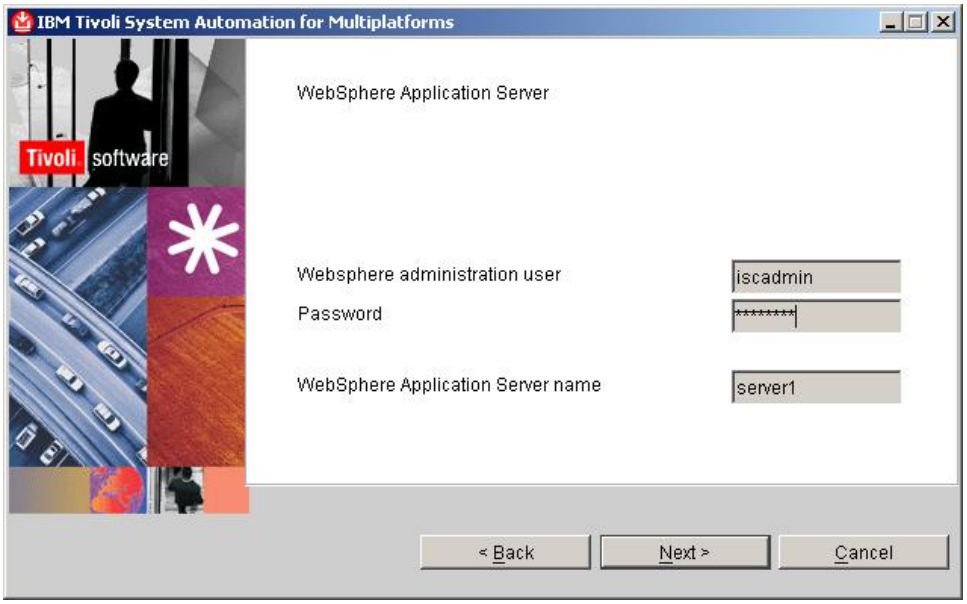
Perform the following steps to uninstall the operations console:

1. Launch the uninstallation program as described in the sections above.

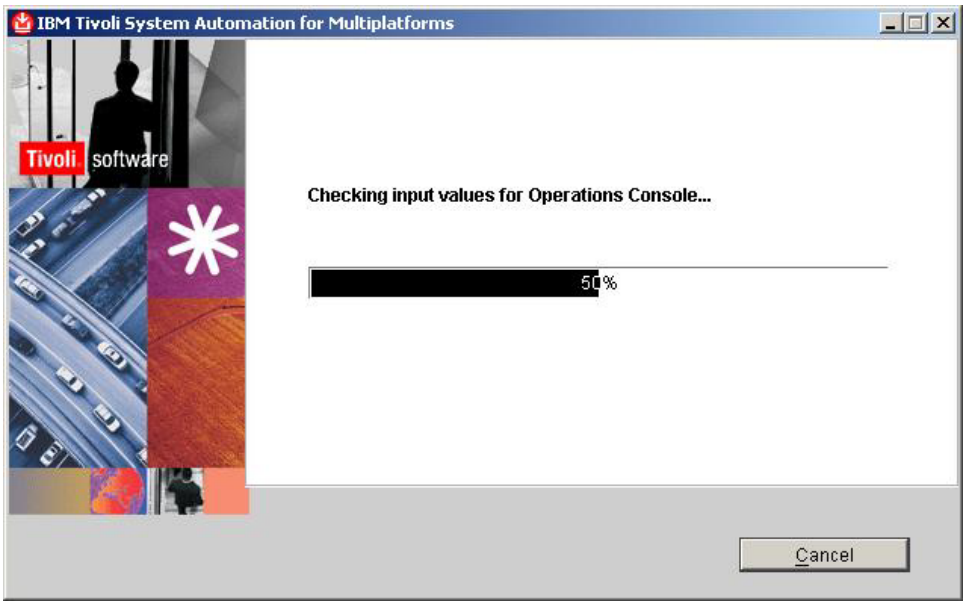
2. On the Welcome panel of the uninstallation program, click **Next**.



3. In the fields **WebSphere administration user** and **Password**, type the user ID and password of the Integrated Solutions Console administrator user. Click **Next**.

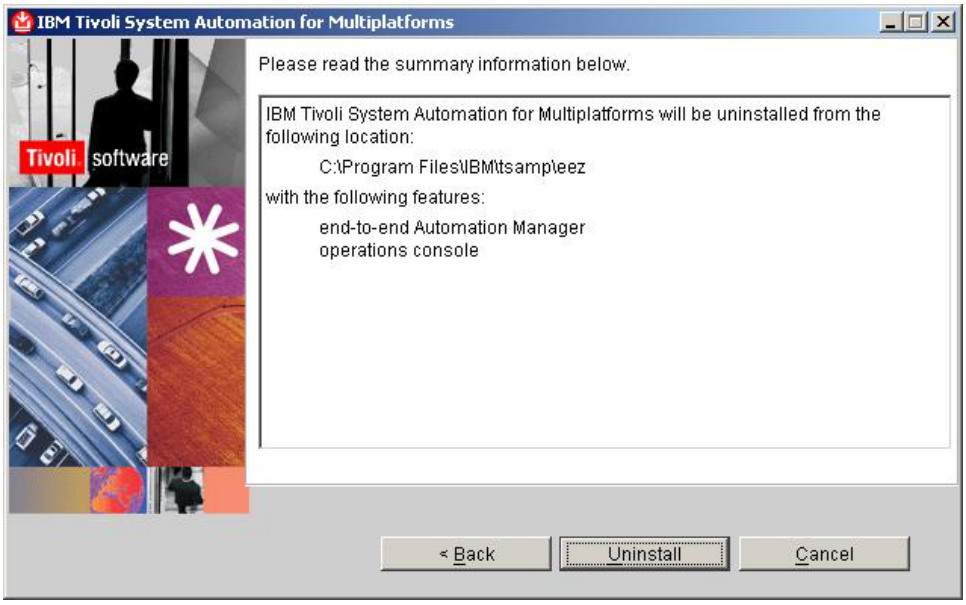


4. Some information panels are displayed while the uninstallation program checks your system for the information it needs for the uninstall. The following figure shows an example.

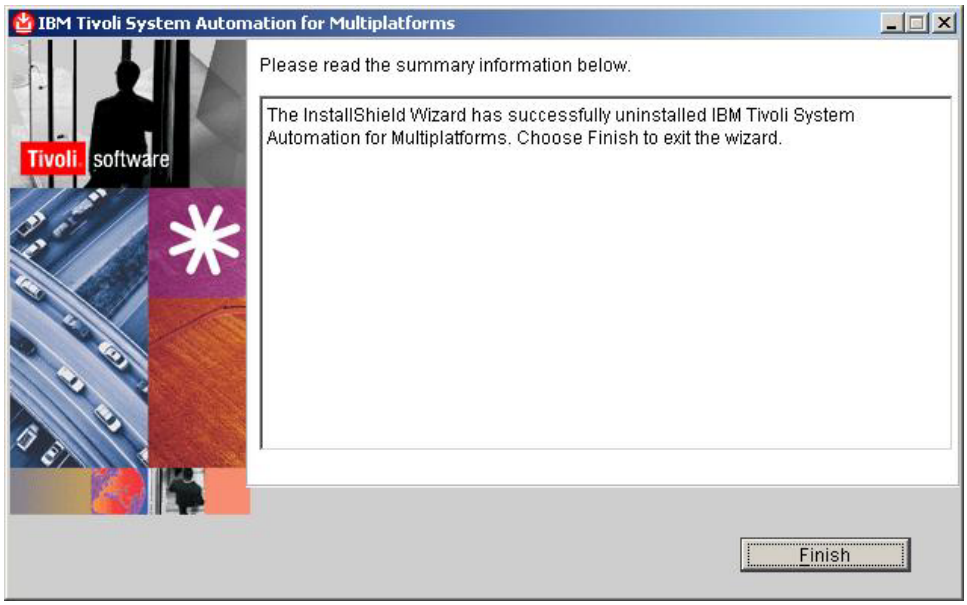


5. When all required information has been detected, a confirmation panel appears. To start the uninstallation, click **Uninstall**.

   Note that the uninstallation can take considerable time to complete. Use the progress indicators that are displayed throughout the uninstallation to monitor the progress.



6. When the uninstallation is complete, a summary panel is displayed. On the panel, click **Finish**.



Note: If problems were encountered during the uninstallation, an error panel appears before the summary panel is displayed. In such a case, do this:

- On the error panel, click **Next**.
- On the summary panel that appears, click **Finish**.
- Use the log files that were created by the uninstallation program to analyze and resolve the problems. For more information on the log files, refer to Appendix A, "Troubleshooting the installation of the base component operations console," on page 199.

Part 2. End-to-end automation management component

Chapter 7. Installing the end-to-end automation management component

Planning for installation

This chapter contains the information you need for preparing the installation of the end-to-end automation management component.

Packaging

The end-to-end automation management component can be ordered from IBM as media pack or downloaded from an IBM software distribution download site.

Product CD and WebSphere Application Server Upgrade CD

When you order the end-to-end automation management component on CD, you receive the following CDs:

- One product CD for each operating system on which the product can be installed. You use the product CD to install the end-to-end automation management component.
- One WebSphere Application Server Upgrade CD for each operating system on which the product can be installed. You use the upgrade CD to bring WebSphere Application Server to the version level required for the end-to-end automation management component.

For information about the middleware software CDs that are shipped with the end-to-end automation management component, refer to "What the middleware software CDs contain" on page 69.

Product CD: The following table lists the versions of the product CDs that are available for the end-to-end automation management component. To install the product, you use the installation wizard file listed in the right column of the table.

Table 26. Product CD versions

Operating system	Product CD label	Installation wizard file
Windows	IBM Tivoli System Automation Multiplatforms V2.2.0 End-to-End component for Windows	`EEZ2200E2EWindows/Windows/setup.exe`
AIX	IBM Tivoli System Automation Multiplatforms V2.2.0 End-to-End component for AIX	`EEZ2200E2EAIX/AIX/setup`
Linux on System x	IBM Tivoli System Automation Multiplatforms V2.2.0 End-to-End component for Linux on System x	`EEZ2200E2EI386/i386/setup`
Linux on POWER	IBM Tivoli System Automation Multiplatforms V2.2.0 End-to-End component for Linux on POWER	`EEZ2200E2EPPC/ppc/setup`

Table 26. Product CD versions (continued)

Operating system	Product CD label	Installation wizard file
Linux on System z	IBM Tivoli System Automation Multiplatforms V2.2.0 End-to-End component for Linux on System z	`EEZ2200E2ES390/s390/setup`

WebSphere Application Server upgrade CD: The following table lists the available versions of the WebSphere Application Server upgrade CDs.

Table 27. WebSphere Application Server upgrade CD versions

Operating system	CD label
Windows	IBM Tivoli System Automation Multiplatforms V2.2.0 WAS 6.0 upgrade for Windows
AIX	IBM Tivoli System Automation Multiplatforms V2.2.0 WAS 6.0 upgrade for AIX
Linux on System x	IBM Tivoli System Automation Multiplatforms V2.2.0 WAS 6.0 upgrade for Linux on System x
Linux on POWER	IBM Tivoli System Automation Multiplatforms V2.2.0 WAS 6.0 upgrade for Linux on POWER
Linux on System z	IBM Tivoli System Automation Multiplatforms V2.2.0 WAS 6.0 upgrade for Linux on System z

Electronic distribution

You can also obtain the end-to-end automation management component through electronic distribution. In this case, you can download the deliverables from a URL you receive after purchasing the product.

The following tables lists the archives that you need to download for each platform to install the WebSphere Application Server upgrade, which is required for running the end-to-end automation management component, and the product itself.

Archives: The following tables list the archives that you need for installing the WebSphere Application Server upgrade and the product itself.

Windows:

Table 28. Archives for Windows platforms

Archive name	Description
C947YML.exe	This is the archive you use to install the product. The archive is self-extracting. After extraction, the directory structure is identical to that on the corresponding CD.
C94IXML.exe	The self-extracting archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.

AIX:

Table 29. Archives for AIX platforms

Archive name	Description
C947ZML.bin	This is the archive you use to install the product. The archive is self-extracting. After extraction, the directory structure is identical to that on the corresponding CD.
C94IYML.bin	The self-extracting archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.

Linux on System x:

Table 30. Archives for Linux on System x

Archive name	Description
C9480ML.tar	This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files to a temporary directory. After extraction, the directory structure is identical to that on the corresponding CD.
C94IZML.tar	The archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.

Linux on POWER:

Table 31. Archives for Linux on POWER

Archive name	Description
C9481ML.tar	This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files to a temporary directory. After extraction, the directory structure is identical to that on the corresponding CD.
C94J1ML.tar	The archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.

Linux on System z:

Table 32. Archives for Linux on System z

Archive name	Description
C9482ML.tar	This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files to a temporary directory. After extraction, the directory structure is identical to that on the corresponding CD.
C94J0ML.tar	The archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.

Product features, DB2 setup options, and user registry options

The two major subcomponents of the end-to-end automation management component, namely, the end-to-end automation manager and the operations console are installed on the same node and run in the same WebSphere Application Server environment:

- During installation, the automation J2EE framework and the resource adapters are installed to an existing server in WebSphere Application Server. Typically, the name of this server is server1.
- The installation of the operations console creates a new server in WebSphere Application Server. The name of this server is ISC_Portal.

The following figure depicts the setup of the end-to-end automation management component.

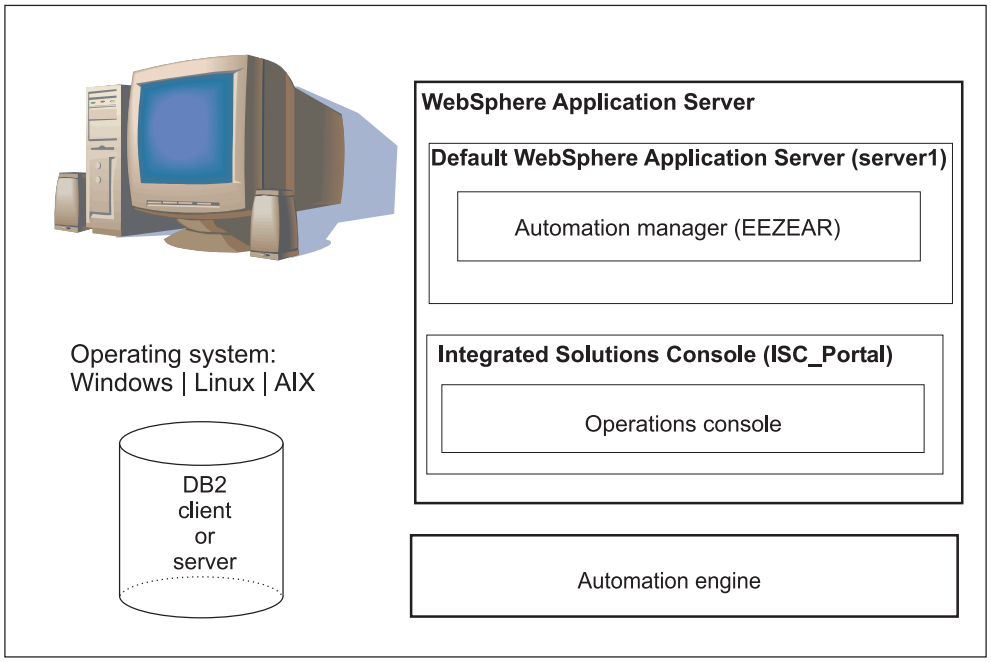


Figure 4. Setup of the end-to-end automation management component

For more information about the components of the end-to-end automation management component, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Components of end-to-end automation management".

DB2 setup options and user registry options

When planning for the installation of the end-to-end automation management component, you must decide:

- whether you want to use a local or remote DB2 setup for the two DB2 databases that are required for the end-to-end automation management component.
- whether you want to use DB2 or LDAP as the user registry.

Using a local or remote DB2 setup

In a local DB2 setup, the DB2 server is installed and runs on the same node on which the end-to-end automation management component is installed.

In a remote DB2 setup, the DB2 server is installed and runs on a node other than that on which the end-to-end automation management component is installed. In this case, you need to install a DB2 client on the end-to-end automation management node.

Using LDAP or DB2 as the user registry

When using LDAP, the user and group information needed by the operations console for authentication is stored in an LDAP directory.

When using DB2 as the user registry, the user and group information needed by the operations console for authentication is stored in a DB2 database.

For more information, refer to"Security concepts" on page 68.

Product requirements

The following sections list the software and hardware requirements for the end-to-end management component.

Supported operating systems

The following table lists the operating systems that are supported for the end-to-end automation management component:

Table 33. Supported operating systems

Operating system	System x[1]	System i	System p	System z
Windows Server 2003 Standard Edition (32 bit)	X			
Windows Server 2003 Enterprise Edition (32 bit)	X			
AIX 5.2 (AIX 5L Version 5.2) ML 5			X	
AIX 5.3 (AIX 5L Version 5.3) ML 2[5]			X	
SUSE SLES 9 (32 bit[2])	X			
SUSE SLES 9 (64 bit[3])		X	X	X[4]
SUSE SLES 10 (32 bit[2])	X			
SUSE SLES 10 (64 bit[3])		X	X	X[4]
Red Hat RHEL 4.0 AS (32 bit[2])	X			
Red Hat RHEL 4.0 AS (64 bit[3])		X	X	X[4]

Notes:

1. IBM System x with IA32, EM64T, or AMD64 architecture.
   Any other systems with IA32, EM64T, or AMD64 architecture are also supported.
   Systems with IA64 architecture are not supported.
2. The following Linux kernel architectures are supported for running with 32 bit:
   - x86 on IBM System x
3. The following Linux kernel architectures are supported for running with 64 bit:
   - ppc64 on IBM System i and IBM System p
   - s390x on IBM System z is supported for some distributions
4. SUSE SLES 9, SUSE SLES 10, and RHEL 4.0 AS on s390x kernel require IBM DB2 UDB Version 8.2 Run-Time Client with Fix Pack 10 running as

31 bit application. This precludes IBM DB2 UDB Version 8.2 server from running on the same system, that is, remote DB2 setup is required.

5. APAR IY65979 must be installed.

Middleware software requirements

Before you can install the end-to-end automation management component, the following two software prerequisites must be manually installed on the system on which the end-to-end automation management component will run:

- A DB2 server for a local DB2 setup or a DB2 client for a remote DB2 setup
- IBM WebSphere Application Server 6.0.2 (with particular Interim Fixes)

  The automation manager and the operations console share the same WebSphere Application Server environment (see Figure 4 on page 63).

Software prerequisites for a local DB2 setup: Before you can install the automation manager and the operations console, the following software prerequisite must be manually installed on the system on which the end-to-end automation management component will run:

- IBM DB2 UDB Version 8.2.3 (equivalent to Version 8.1.10) Enterprise Server Edition

Software prerequisites for a remote DB2 setup: Before you can install the automation manager and the operations console, the following software prerequisites must be manually installed:

- An IBM DB2 UDB server Version 8.2.3 (equivalent to Version 8.1.10) must be installed on a system other than that on which the end-to-end automation management component will run.
- Additionally, a DB2 client must be installed on the system on which the end-to-end automation management component will run. The following DB2 clients are supported:
  - IBM UDB DB2 Run-Time Client Version 8.2.3 (equivalent to Version 8.1.10; available for all operating systems)
  - IBM UDB DB2 Run-Time Client Lite Version 8.2.3 (equivalent to Version 8.1.10; only available for Windows)

Software prerequisites: LDAP is used as the user registry: When using LDAP as the user registry, one of the following LDAP servers must be running on an arbitrary system and must be reachable from the system on which the end-to-end automation management component will run:

- IBM Tivoli Directory Server Version 5.2
- IBM Directory Server Version 5.1

More information on IBM Tivoli Directory Server can be found at

```
www.ibm.com/software/tivoli/products/directory-server/
```

Note: IBM Tivoli Directory Server is not contained on the CDs that are shipped with the end-to-end automation management component. If you want to use LDAP, you must provide one of the LDAP servers listed above.

Software prerequisites: DB2 is used as the user registry: When using DB2 as the user registry, you do not need to install additional software manually.

Browser requirements

The operations console is the user interface of the end-to-end automation management component. It is displayed in a Web browser that connects to the WebSphere Application Server on which the operations console is running. The Web browser may run on an arbitrary system.

The following Web browsers are supported:

- Microsoft Internet Explorer 6.x
- Mozilla 1.7
- Netscape 7

For information on how the Web browser must be configured, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Configuring your Web browser".

Hardware requirements

The following sections describe the hardware requirements for the end-to-end automation management component. The description does not cover the hardware requirements that need to be satisfied for installing and running the required middleware software. For more information on hardware requirements for the required middleware software, refer to "Installing the middleware software" on page 69.

Memory: **Memory: 1.5 GB** is required on the server on which the end-to-end automation management component is installed (for WebSphere Application Server, Integrated Solutions Console, and the end-to-end automation management component).

TCP/IP connectivity: The end-to-end automation management component consists of various components that may run on one or several systems. For example:

- When you use a local DB2 setup, the automation manager, the operations console, and the DB2 server run on the same system (single-node setup).
- When you use a remote DB2 setup, the end-to-end automation management component and the DB2 server run on separate systems (multi-node setup).

Be sure that TCP/IP connections can be established between the following components:

- the WebSphere Application Server that is running the automation J2EE framework, the resource adapters, and the operations console
- the DB2 server
- the LDAP server (if LDAP security setup is used)

Disk space requirements:

Disk space requirements on Windows systems: The following table lists the disk space requirements for the end-to-end automation management component on Windows systems. Note that the table does not include the space required for the installation of the middleware software.

Table 34. Disk space requirements on Windows systems

Description	Default directory	Disk space
End-to-end automation management component installation directory	`C:\Program Files\IBM\tsamp\eez`	70 MB
Automation manager and operations console deployed in WebSphere Application Server	`C:\Program Files\IBM\WebSphere\AppServer`	60 MB
Operations console installation directory	`C:\Program Files\IBM\ISC`	600 MB
DB2 database	`C:\DB2`	120 MB
Installation log and response files	The value of the system variable %TEMP% Typically, this is: `C:\Documents and Settings\Administrator\Local Settings\Temp`	75 MB
Temporary disk space needed for installation	The value of the system variable %TEMP% Typically, this is: `C:\Documents and Settings\Administrator\Local Settings\Temp`	100 MB
Configuration file directory and policy pool directory of the end-to-end automation management component	`C:\Program Files\IBM\tsamp\eez\cfg` `C:\Program Files\IBM\tsamp\eez\policyPool`	1 MB
Tivoli Common Directory	`C:\Program Files\IBM\tivoli\common\eez`	250 MB
Installer registry	`C:\Windows\vpd.properties`	10 KB

Disk space requirements on AIX and Linux systems: The following table lists the disk space requirements for the end-to-end automation management component on AIX and Linux systems. Note that the table does not include the space required for the installation of the middleware software.

Table 35. Disk space requirements on AIX and Linux systems

Description	Default directory	Disk space
Installation directory of the end-to-end automation management component	`/opt/IBM/tsamp/eez`	70 MB
Automation manager and operations console deployed in WebSphere Application Server	AIX: `/usr/IBM/WebSphere/AppServer` Linux: `/opt/IBM/WebSphere/AppServer`	60 MB
Operations console installation directory	`/opt/IBM/ISC`	500 MB
DB2 database	`~db2inst1`	120 MB
Installation log and response files	`/tmp`	75 MB
Temporary disk space needed for the installation	`/tmp`	100 MB

Table 35. Disk space requirements on AIX and Linux systems (continued)

Description	Default directory	Disk space
Configuration file directory and policy pool directory of the end-to-end automation management component	`/etc/opt/IBM/tsamp/eez/cfg` `/etc/opt/IBM/tsamp/eez/policyPool`	1 MB
Tivoli Common Directory	`/var/ibm/tivoli/common/eez`	250 MB
Installer registry	`~root/vpd.properties`	10 KB

Security concepts

The following sections describe the security concepts for end-to-end automation management.

Security considerations

If you are using a local DB2 setup, the end-to-end automation management component and the external components needed for running it, namely, WebSphere Application Server, Integrated Solutions Console, and DB2, are installed on the same system and you do not have to secure the connections between these components over SSL.

However, external connections will be established between the components listed below. If possible, these connections should be secured with SSL. This is recommended when the external components are running in different security domains, separated by firewalls.

External connections will be established between the following components (the port numbers given in brackets are default values):

- The connection between the automation engine and the automation adapters (port 2001).
- The connection between the automation adapters and the automation engine (port 2002). Note that SSL is not supported for this connection.
- When LDAP security is used: The connection between WebSphere Application Server and the LDAP server (port 389; for connections secured over SSL, port 636 is used)
- The connection between the Web browser in which the operations console is displayed and Integrated Solutions Console (HTTP port 8421, HTTPS port 8422)

Considerations for choosing between LDAP and DB2 as the user registry

WebSphere Application Server can be configured to use either an LDAP directory or a DB2 database for storing user information and for authenticating the users of the end-to-end automation management component. Regardless of which type of configuration you choose, you can use the user management function of Integrated Solutions Console to manage the user IDs and passwords for end-to-end automation management.

The following considerations may help you to decide which type of user registry to choose:

- If you are already using an LDAP server for authentication or are planning to set up an LDAP server anyway, you should consider using this LDAP server for end-to-end automation management as well. Note that only LDAP servers with write support can be used for end-to-end automation management. Read-only LDAP servers are not supported.

- If you are currently not using an LDAP server, you can use DB2 for storing user information and for authenticating users.

User management

For information on how user IDs and passwords for end-to-end automation management are managed, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, chapter "Managing users".

Installing the middleware software

Depending on the setup type you choose, middleware software has to be installed on one or more systems before the end-to-end automation management component can be installed.

- For information on possible setup types, refer to "DB2 setup options and user registry options" on page 63
- For information on the required middleware software for each system, refer to "Middleware software requirements" on page 65

What the middleware software CDs contain

The middleware software CDs that are shipped with the end-to-end automation management product CDs contain the following software products:

- IBM DB2 UDB Version 8.2 Enterprise Server Edition (DB2 server)
- IBM UDB DB2 Run-Time Client Version 8.2 (DB2 client)
- IBM UDB DB2 Run-Time Client Lite Version 8.2 (DB2 client)
- IBM WebSphere Application Server Base Version 6.0 (WAS)

Notes:

1. In addition to a WebSphere Application Server 6.0 CD for every supported platform, a WAS 6.0.0 upgrade CD is available for every supported platform. The upgrade CD is needed for bringing WebSphere Application Server to the required product level.
2. Please note that the IBM Tivoli Directory Server is not contained on the middleware software CDs.

Installing a DB2 server

DB2 server requirements

Check which requirements need to be met for installing and running a DB2 server. The information can be found in the following publications:

- IBM DB2 Universal Database - Quick Beginnings for DB2 Servers - Version 8.2 (GC09-4836)
- IBM DB2 Universal Database - Release Notes - Version 8

The latest versions of these publications can be found on the IBM DB2 UDB Web site at

`www.ibm.com/software/data/db2/udb/support/`

You find the link to the PDF manuals in the **Other resources** section on the Web page.

In addition, check for the latest system requirements at

www.ibm.com/software/data/db2/udb/sysreqs.html

The DB2 release notes can also be found on the CD labeled *IBM DB2 Universal Database Enterprise Server Edition Version 8.2* for your platform. Make sure that all requirements for installing and running a DB2 server are met. Otherwise, the end-to-end automation management component may not install or work properly.

DB2 server installation

You can use the DB2 Setup wizard to install the DB2 server. You find the DB2 Setup wizard on the CD labeled *IBM DB2 Universal Database Enterprise Server Edition Version 8.2* for your platform.

The typical installation of a single-partition database environment is recommended.

On a Windows system, the DB2 administration server user, the fenced user, and the instance owner user must be local users.

You need to create a DB2 instance as a prerequisite for installing the end-to-end automation management component. If you are asked whether the DB2 instance is to be installed with 32-bit or 64-bit instance word size, choose 32-bit.

Make sure that the DB2 server has the required version level (refer to "Middleware software requirements" on page 65).

When you install the end-to-end automation management component, you will need the following information:

- The host name of the system where the DB2 server is installed.
- The port number of the DB2 instance

  The port number is displayed on the summary panel of the DB2 Setup wizard. The summary panel appears immediately before the wizard copies the program files.
- The directory to which the DB2 server is installed if a local DB2 setup is used
- The name and password of the instance owner user or of a different user who is authorized to drop and create databases and database tables, and to select, insert, delete, and update rows in tables.

Note: Chapter 7. "Controlling database access" in *IBM DB2 Universal Database Administration Guide: Implementation*, Version 8.2 (SC09-4820) explains the security concepts of the DB2 server and describes how a user ID can be authorized to perform certain tasks.

Post-installation tasks for remote DB2 setup

The following tasks must be completed on the DB2 server system:

- Identify the DB2 instance that will hold the databases. Identify the instance owner user ID and password. Identify the host name of the DB2 server system. Identify the TCP/IP port of the DB2 instance.
- Create the automation manager database (for information on how to do this, see below).
- Create the automation manager tables in the database (for information on how to do this, see below).

  Note: If the database has already been created and tables already exist, you must drop the existing tables before creating the tables.

- Create the operations console database (for information on how to do this, see below).

The CD *IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component* for your platform contains scripts for creating the required databases and tables.

Creating the automation manager database and the database tables:

On Windows: Perform the following steps if your DB2 server runs under Windows:

1. Log in with a user ID that has SYSADM privileges on the DB2 instance.
2. On the CD labeled *IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component for Windows*, change the directory to `DDL\Script`
3. Run the following batch file from this directory:

   ```
   db2_create_automgr_db.bat <db_name> <instance_owner> <instance_pw>
   ```

   where
   - `<db_name>` is the desired name of the automation manager database (Example: EAUTODB)
   - `<instance_owner>` is the instance owner user ID of the DB2 instance (Example: db2admin)
   - `<instance_pw>` is the password of the instance owner user ID

On AIX and Linux: Perform the following steps if your DB2 server runs under Linux or AIX:

1. Log in as root.
2. On the CD labeled *IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component* for your operating system, change the directory to `DDL/Script`.
3. Run the following shell script from this directory:

   ```
   db2_create_automgr_db.sh <db_name> <instance_owner> <instance_pwd>
   ```

   where
   - <db_name> is the desired name of the automation manager database (Example: EAUTODB)
   - <instance_owner> is the instance owner user ID of the DB2 instance (Example: db2inst1)
   - <instance_pwd> is the password of the instance owner user ID

Creating the operations console database:

On Windows: Perform the following steps if your DB2 server runs under Windows:

1. Log in with a user ID that has SYSADM privileges on the DB2 instance.
2. On the CD labeled *IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component for Windows*, change the directory to `DDL\Script`
3. Run the following batch file from this directory:

   ```
   db2_create_opcons_db.bat <db_name>
   ```

   where `<db_name>` is the desired name of the operations console database (Example: OPCONDB)

On AIX and Linux: Perform the following steps if your DB2 server runs under Linux or AIX:

1. Log in as root.
2. On the CD labeled *IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component* for your operating system, change the directory to `DDL/Script`.
3. Run the following shell script from this directory:

   ```
   db2_create_opcons_db.sh <instance_owner> <db_name>
   ```

   where

   - <instance_owner> is the instance owner user ID of the DB2 instance (Example: db2inst1)
   - <db_name> is the desired name of the operations console database (Example: OPCONDB)

Installing a DB2 client

The following sections only apply when you are using a remote DB2 setup.

DB2 client requirements

Check which requirements need to be met for installing and running a DB2 client. The information can be found in the following publications:

- IBM DB2 Universal Database - Quick Beginnings for DB2 Clients - Version 8.2 (GC09-4832)
- IBM DB2 Universal Database - Release Notes - Version 8

The latest versions of these publications can be found on the IBM DB2 UDB Web site at

```
www.ibm.com/software/data/db2/udb/support/
```

You find the link to the PDF manuals in the **Other resources** section on the Web page.

In addition, check for the latest system requirements at

```
www.ibm.com/software/data/db2/udb/sysreqs.html
```

The DB2 release notes can also be found on the CD labeled *IBM DB2 Run-time Client Version 8.2* for your platform. Make sure that all requirements for installing and running a DB2 client are met. Otherwise, the DB2 client or the end-to-end automation management component may not work properly.

DB2 client installation

You can use the DB2 Setup wizard to install the DB2 client. You find the DB2 Setup wizard on the CD labeled *IBM DB2 Run-Time Client Version 8.2* for your platform.

If possible, use a 31-bit or 32-bit DB2 client.

Make sure that the DB2 client has the required version level.

When you install the end-to-end automation management component, you will need the following information:

- The directory into which the DB2 client is installed.

Post-installation tasks for remote DB2 setup

The following tasks must be performed on the DB2 client system:

- Catalog a TCP node for the DB2 server system. This is described in "Cataloging a TCP node."
- Catalog the operations console database. This is described in "Cataloging the operations console database."

  This step generates a database alias.
- Catalog the automation manager database. This is described in "Cataloging the automation manager database" on page 74.

  This step generates a database alias.

Cataloging a TCP node: Log in to the system as a user with sufficient database privileges:

- **Windows**: Log in as a user with SYSADM privileges on the DB2 client. Open a DB2 command line prompt.
- **AIX/ Linux**: Log in to DB2 using the name of the DB2 instance or your database user name. If you are logged in as root, enter the following command to change to the DB2 instance owner:

  ```
  su - <INSTANCE_OWNER>
  ```

Issue the following command:

```
db2 CATALOG TCPIP NODE <NODE_NAME> REMOTE <DB2_SERVER_HOST>
                  SERVER <DB2_SERVER_INSTANCE_PORT>
```

where

- <NODE_NAME> is an arbitrary name for the node
- <DB2_SERVER_HOST> is the (fully qualified) host name or the IP address of the DB2 server system
- <DB2_SERVER_INSTANCE_PORT> is the number of the port on which the selected DB2 server instance is listening

Cataloging the operations console database: Log in to the system as a user with sufficient database privileges:

- **Windows**: Log in as a user with SYSADM privileges on the DB2 client. Open a DB2 command line prompt.
- **AIX/ Linux**: Log in to DB2 using the name of the DB2 instance or your database user name. If you are logged in as root, enter the following command to change to the DB2 instance owner:

  ```
  su - <INSTANCE_OWNER>
  ```

Run the following command:

```
db2 CATALOG DB <DB_NAME> AS <DB_ALIAS> AT NODE <NODE_NAME>
```

where

- <DB_NAME> is the name of the operations console database on the DB2 server
- <DB_ALIAS> is an arbitrary alias for the operations console database, which is later specified in the installation wizard of the end-to-end management component
- <NODE_NAME> is the arbitrary name for the node that you specified when you cataloged the TCP node

Cataloging the automation manager database: Log in to the system as a user with sufficient database privileges:

- **Windows**: Log in as a user with SYSADM privileges on the DB2 client. Open a DB2 command line prompt.
- **AIX/ Linux**: Log in to DB2 using the name of the DB2 instance or your database user name. If you are logged in as root, enter the following command to change to the DB2 instance owner:

  ```
  su - <INSTANCE_OWNER>
  ```

Run the following command:

```
db2 CATALOG DB <DB_NAME> AS <DB_ALIAS> AT NODE <NODE_NAME>
```

where

- <DB_NAME> is the name of the automation manager database on the DB2 server
- <DB_ALIAS> is an arbitrary alias for the automation manager database, which is later on specified in the installation wizard of the end-to-end management component
- <NODE_NAME> is the arbitrary name for the node that you specified when you cataloged the TCP node

Installing WebSphere Application Server

Note that installing WebSphere Application Server from the IBM WebSphere Application Server Base Version 6.0 CD does not result in the required version level. To obtain the required version level, additional service from the WAS 6.0.0 upgrade CD must be applied in the following sequence:

1. WebSphere Application Server 6.0 Refresh Pack 2, to obtain WebSphere Application Server 6.0.2
2. Particular Interim Fixes

WebSphere Application Server 6.0.0.0 requirements

Check which requirements need to be met for installing and running WebSphere Application Server Base. The information can be found in the following publications:

- The ReadMe file on the product CD labeled *IBM WebSphere Application Server, Version 6*
- The "Getting started" topics in the Information center for IBM WebSphere Application Server, Version 6

The latest versions of all WebSphere Application Server publications can be found on the WebSphere Application Server library Web site at

```
www.ibm.com/software/webservers/appserv/was/library/
```

In addition, check for the latest system requirements at

```
www.ibm.com/software/webservers/appserv/was/requirements/
```

An IBM WebSphere Application Server, Version 6, *Getting started* document is available on the product CD for your platform, where it is also referred to as *Installation Guide*. Make sure that all requirements for installing and running

WebSphere Application Server are met. Otherwise, the end-to-end automation management component may not work properly.

Installing WebSphere Application Server 6.0.0.0

You can use the WebSphere Application Server installation wizard to install WebSphere Application Server. The WebSphere Application Server installation wizard can be started from the WebSphere Application Server LaunchPad. You find the LaunchPad on the CD labeled *IBM WebSphere Application Server Version 6.0* for your platform.

The typical installation is recommended.

Installing Refresh Pack 2 and the required Interim Fixes

The following table gives an overview of what you will find on the WebSphere Application Server 6.0.0 upgrade CD. For details, refer to the sections below.

Table 36. Contents of the WebSphere Application Server 6.0.0 upgrade CD

Directory	Contents
`Upgrade`	An archive containing Refresh Pack 2 and the UpdateInstaller for installing Refresh Pack 2
`Fixes`	The archive that contains the subdirectories with the required Interim Fixes

Installing Refresh Pack 2: In the directory `Upgrade` on the WebSphere Application Server 6.0.0 upgrade CD, you find an archive that contains Refresh Pack 2 and the UpdateInstaller for installing it.

The archive names have the following syntax:

```
6.0-WAS-<platform>-RP<refresh_pack_number>.<archive_type>
```

where

- `<platform>` represents the platform on which the end-to-end automation management component is installed
- `<refresh_pack_number>` represents the number of the refresh pack
- represents the platform-specific file extension of the archive

The documentation for the UpdateInstaller is available in the archive in directory `updateinstaller\docs`.

For more information about Refresh Pack 2, refer to `http://www.ibm.com/support/docview.wss?rs=180&uid=swg24009813`.
On the Web page, read the document *Readme for multiplatforms* to obtain information about how to install the Refresh Pack.

Installing the required Interim Fixes: In the directory `Fixes` on the WAS 6.0.0 upgrade CD, you find the required Interim Fixes.
The required Interim Fixes are located in directories that are prefixed with a number:

```
Fixes
 01_PKxxxxx
  <NAMExxxxx>.pak
 ...
 nn_PKyyyyy
  <NAMEyyyyy>.pak
```

The Interim Fixes are the files with the extension `.pak`.

When you install the Interim Fixes, be sure to observe the following rules:

- Install all Interim Fixes that are located in the directory `Fixes`.
- Install the Interim Fixes in exactly the sequence indicated by the number prefix of the directories in the directory `Fixes`.
- Install exactly these Interim Fixes, do not leave out any Interim Fixes and do not install any additional Interim Fixes unless you are explicitly advised to do so by Tivoli System Automation product support.

Post-installation tasks

Remove the default WebSphere Application Server profile using the `wasprofile` command and create a new default profile using the profile creation wizard.

When creating the new default profile, it is recommended that you accept the default port settings.

Refer to Chapter 10. "Configuring the product after installation" in the manual *WebSphereApplication Server, Version 6 - Installing your application serving environment* for more information on the `wasprofile` command and the profile creation wizard.

Under Windows, you can choose to run WebSphere Application Server as a service. When doing so, make sure that the user ID used to run the service has a valid DB2 environment setup.

For more information on setting up the DB2 environment, refer to Chapter 1. "Before creating a database" -> "Preparing to create a database" in *IBM DB2 Universal Database Administration Guide: Implementation*, Version 8.2 (SC09-4820).

Setting up an LDAP server

Note that the IBM Tivoli Directory Server is not contained on the middleware software CDs that are shipped with the end-to-end automation management component. If you want to use LDAP as the user registry for the end-to-end automation management component, you have to obtain a supported version of the product separately.

When LDAP is used as the user registry, user authentication and user membership in groups is performed using an LDAP server.

Before you can install the end-to-end automation management component, you need to create at least one group and one user for the end-to-end automation management component. The group that is required is iscadmins or an equivalent. Members of this group have administrative authority within the operations console. At least one operations console administrator user must be created within the group (refer to “Required user groups and users” on page 77 for more information).

Required LDAP directory tree structure

The LDAP directory tree that is used by the operations console must meet the following requirements:

- One distinguished name (DN) suffix needs to be defined. It must contain the users and groups mentioned above.

- The operations console must be able to add, delete, modify, and search entries under this suffix. In fact, new entries will be added below the suffix during the installation of the end-to-end automation management component.
- Directly below the suffix, one entry is needed for containing user entries. The relative distinguished name (RDN) of this entry is the LDAP user suffix.
- Directly below the suffix, one entry is needed for containing group entries. The relative distinguished name (RDN) of this entry is the LDAP group suffix.
- The object class of the user entries must allow for a password specification so that an LDAP bind request can be performed against user entries. An example of such an object class is inetOrgPerson, which is defined in IETF RFC 2798.
- The object class of the group entries must allow for specifying which user entries are members of a group. An example of such an object class is groupOfUniqueNames, which is defined in IETF RFC 2256.

The following figure shows the required structure. For an example of an LDAP configuration, refer to "Sample LDAP configuration" on page 78.

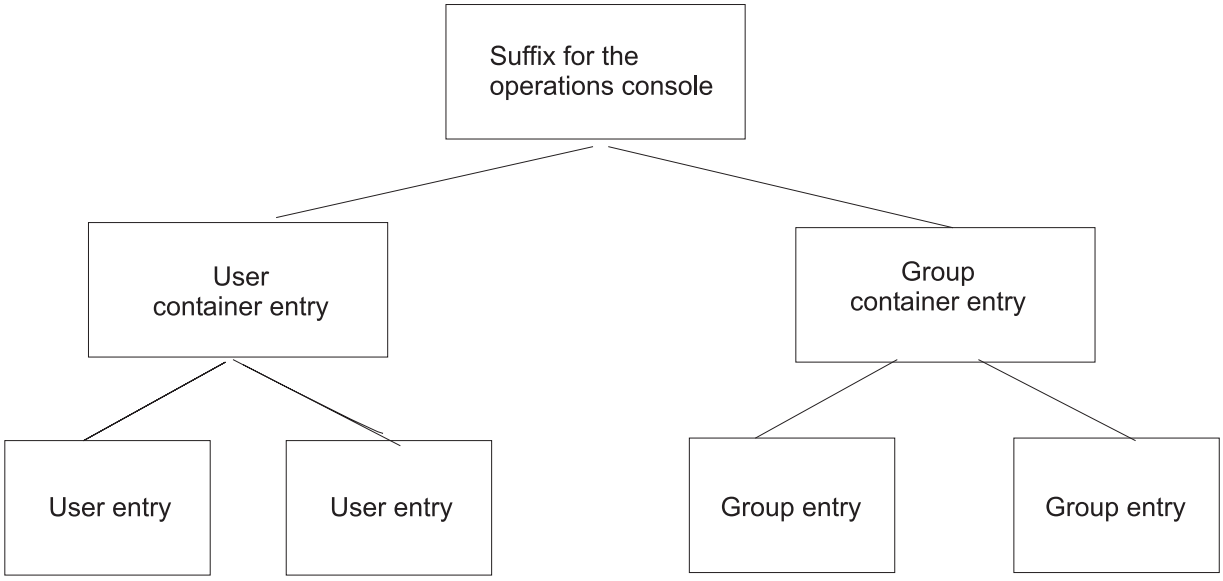


Figure 5. LDAP directory tree structure

Required user groups and users

When using LDAP as the user registry, the following rules apply:

- A system user is required for operating the automation engine. In this guide, this user is referred to as iscadmin.

  For this user, you need to create a group (iscadmins or an equivalent) and a user (iscadmin or equivalent) in the LDAP user registry before installing the end-to-end automation management component. You will need to enter this user ID on the LDAP configuration panels in the installation wizard during the installation of the end-to-end automation management component.
- A number of additional groups are required for the end-to-end automation management component. You can either create these groups in the LDAP user registry before installing the end-to-end automation management component or create them in Integrated Solutions Console after the installation is complete.

Regardless of which approach you use for creating the groups, you need to map the groups to the end-to-end automation management-specific access roles in WebSphere Application Server after installation.

For more information on the required user groups and the related access roles, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Post-installation tasks for administrators".

- You can create new users or authorize existing users for end-to-end automation management. You can create new users in the LDAP user registry or in Integrated Solutions Console. You authorize the user by assigning them to the end-to-end automation-specific user groups, either in the LDAP user registry or in Integrated Solutions Console.

For an example of an LDAP configuration, refer to "Sample LDAP configuration."

LDAP-related pre-installation tasks

Before you install the end-to-end automation management component, perform the following task on the LDAP server:

1. Install and configure the LDAP server as described in the installation instructions provided with the LDAP server.

---

2. You must create at least one group (`iscadmins` or an equivalent) and create at least one user (iscadmin or an equivalent) in that group.

   Observe the following guidelines when creating the user ID and password:

   - The user ID and password must be unique
   - The length must be 3 to 60 characters
   - Valid characters are a-z, A-Z, period (.), hyphen (-), and underscore (_)

     No other characters are permitted. For example, diacritics, such as the umlaut, and double-byte characters are not permitted.

Sample LDAP configuration

The following LDIF creates a user ID and a group in the LDAP server.

Before the LDIF can be loaded, the suffix must exist. You can create it using the following command:

```
ldapcfg -s o=<your_organization_suffix>
```

for example:

```
ldapcfg -s o=ibm.com
```

Use the following LDAP server command to load the LDIF file into the LDAP server:

```
ldapmodify -h <ldap_server_hostname> -p 389
           -D cn=<ldap_administrator> -w ldapadm -f e2e.ldif
```

for example:

```
ldapmodify -h <ldap_server_hostname> -p 389 -D cn=ldapdb2 -w ldapadm -f e2e.ldif
```

This is a sample LDIF file:

```
dn: o=ibm.com
objectclass: top
objectclass: organization
o: ibm
o: ibm.com

dn: ou=users,o=ibm.com
objectclass: top
objectclass: organizationalUnit
ou: users

dn: ou=groups,o=ibm.com
objectclass: top
objectclass: organizationalUnit
ou: groups

dn: uid=iscadmin,ou=users,o=ibm.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: iscadmin
userpassword: iscadmin
sn: iscadmin
cn: iscadmin

dn: cn=iscadmins,ou=groups,o=ibm.com
objectclass: top
objectclass: groupOfUniqueNames
ou: iscadmins
cn: iscadmins
uniqueMember: uid=iscadmin, ou=users, o=ibm.com
```

Preparing for the installation of the end-to-end automation management component

Collecting the information you need to provide during installation

The installation of the end-to-end automation management component is wizard-driven. The wizard guides you through the installation and prompts you for installation and configuration parameters. The following tables list the parameters you need to specify on the installation wizard panels in the order in which they must be specified.

Installation directory and Tivoli Common Directory

The parameters listed in the following table must always be specified.

Table 37. Installation directory and Tivoli Common Directory

Parameter	Description	Default

Installation directory name	The directory to which the installable features are installed.
	
	In this guide, this directory is referred to as `EEZ_INSTALL_ROOT`.
	
	When specifying a directory other than the default, observe the following restrictions:
	
	Windows:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The colon character is allowed only once, immediately following the drive letter. For example, `C:\<directory_name>` is allowed, but `C:\<directory_name>:<directory_name>` is not allowed.
	• The space character and the underscore character (_) are allowed.
	
	AIX, Linux:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The underscore character (_) is allowed.
	• The space and colon characters are not allowed.
		Windows:
		
		`C:\Program Files\IBM\tsamp\eez`
		
		AIX, Linux:
		
		`/opt/IBM/tsamp/eez`

Table 37. Installation directory and Tivoli Common Directory (continued)

Parameter	Description	Default

Tivoli Common Directory	The Tivoli directory for storing serviceability information.
	
	During installation, you are only prompted for input when no Tivoli Common Directory is found on the system.
	
	In the Tivoli Common Directory, the subdirectory `eez` is created for storing product-specific data.
	
	In this guide, this directory is referred to as `Tivoli_Common_Directory`.
	
	When specifying a directory other than the default, observe the following restrictions:
	
	Windows:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The colon character is allowed only once, immediately following the drive letter. For example, `C:\<directory_name>` is allowed, but `C:\<directory_name>:<directory_name>` is not allowed.
	• The space character and the underscore character (_) are allowed.
	
	AIX, Linux:
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	• The underscore character (_) is allowed.
	• The space and colon characters are not allowed.
		Windows:
		
		`C:\Program Files\IBM\tivoli\common`
		
		AIX, Linux:
		
		`/var/ibm/tivoli/common`

Table 37. Installation directory and Tivoli Common Directory (continued)

Parameter	Description	Default

Operations console installation directory	The directory into which the operations console is installed.
	
	In this guide, this directory is referred to as `isc_runtime_root`.
	
	The directory also contains the product registry for Integrated Solutions Console (product.reg) and the properties file (isc.properties). Do not modify these files. They are used by the operations console at runtime.
	
	If you use an existing directory, the directory cannot contain any of the following files and directories:
	• The files `product.reg` and `isc.properties`
	• The directory `\_uninst` or a file named `_uninst`
	• The directory `\AppServer` or a file named `AppServer`
	
	When specifying a directory other than the default, observe the following restrictions:
	• The length of the installation path must be 32 characters or less.
	• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
	
	Additional restrictions:
	
	Windows:
	• The colon character is allowed only once, immediately following the drive letter. For example, `C:\<directory_name>` is allowed, but `C:\<directory_name>:<directory_name>` is not allowed.
	• The space character is allowed.
	
	AIX, Linux:
	• The space and colon characters are not allowed.
		Windows:
		
		`C:\Program Files\IBM\ISC\`
		
		AIX, Linux:
		
		`/opt/IBM/ISC`

Installation parameters for DB2

The parameters listed in the following table must always be specified.

Table 38. DB2 data for local and remote DB2 setup

Parameter	Description	Default
DB2 UDB directory	The installation location of the DB2 client directory. If you are using a local DB2 setup, you use the DB2 client that is part of the DB2 server installation. In this case, you need to specify the DB2 server directory.	The location is detected on your system and displayed as default directory.
DB2 instance host name	The host name of the DB2 instance in which the automation manager and operations console databases are located.	**Local DB2 setup:** The fully qualified host name of your system is displayed as default value. Do not change it to `localhost`! **Remote DB2 setup:** No default value is provided.
DB2 instance port number	The port number of the DB2 instance in which the automation manager and operations console databases are located. **Note:** When you install the end-to-end automation management component on AIX or Linux systems, the installation wizard can retrieve the valid DB2 instance port number automatically. If you opt not to use this function, or on Windows systems, the port number `50000` will be displayed in the entry field on the corresponding installation wizard panel, which is the default port number that is assigned to DB2 during the installation of DB2. However, if the port is not free, a different port number is assigned automatically, which is why you need to check if the default port number is correct. This is how you can determine the correct DB2 port number: • All operating systems: – The port number is displayed in the summary panel that appears when the DB2 installation is complete. – The port number can be determined using the **netstat** command. • **AIX**, **Linux**: The port number is listed in the file `/etc/services`.	50000

Table 38. DB2 data for local and remote DB2 setup (continued)

Parameter	Description	Default
Database instance owner name	The instance owner user ID of the DB2 instance in which the automation manager and operations console databases are located. In a local DB2 setup, this user ID will be used for creating the databases and tables. In a remote DB2 setup, the user ID will be used for creating tables. The user ID will be used by WebSphere Application Server to connect to the automation manager and operations console databases and to select, insert, delete, and update rows in tables.	**Windows**: `db2admin` **AIX, Linux**: `db2inst1`
Database instance owner password	The password for the instance owner user ID of the DB2 instance in which the automation manager and operations console databases are located.	No default value is provided
Automation manager database	Automation manager database for use by WebSphere Application Server. In a local DB2 setup, a database with this name will be created in the DB2 instance related to the specified instance owner. In a remote DB2 setup, a database with this name must already exist in the remote DB2 instance.	EAUTODB
Operations console database	Operations console database for use by WebSphere Application Server. In a local DB2 setup, a database with this name will be created in the DB2 instance related to the specified instance owner. In a remote DB2 setup, a database with this name must already exist in the remote DB2 instance and an alias must be defined to the local system.	OPCONDB

Installation parameters for WebSphere Application Server

The parameters listed in the following table must always be specified.

Table 39. WebSphere Application Server installation parameters

Parameter	Description	Default
WebSphere Application Server directory	The installation location of WebSphere Application Server. There must be exactly one installation of WebSphere Application Server on your system.	The location is detected on your system and displayed as default directory.
WebSphere Application Server profile	The WebSphere Application Server profile to be used for the automation manager and the operations console.	All existing profiles are detected on your system and displayed in a single-choice list.

Table 39. WebSphere Application Server installation parameters (continued)

Parameter	Description	Default
WebSphere Application Server name	The server to be used for the automation manager.	The server name is detected on your system and displayed as default value.

Installation parameters for LDAP

The parameters listed in the following table only need to be specified when you are using LDAP as the user registry.

Table 40. Installation parameters for LDAP

Parameter	Description	Default
LDAP server host name	The fully-qualified host name of the LDAP server that will be used by the operations console.	No default value is provided
LDAP server port	The port of the LDAP server that will be used by the operations console. The port number depends on whether SSL is used: • The default non-SSL port is 389 • The default SSL port is 636 **Note:** On the relevant installation wizard panel, port number 389 is always displayed as default value. If you will be using SSL, you must manually change the port number to the appropriate value.	389 (non-SSL)
LDAP admin bind DN	The user ID of the LDAP directory administrator in the distinguished name format. The operations console uses this ID to bind to the LDAP to retrieve user attributes, to create new users and groups in the LDAP, and to update user attributes. This ID is not required to be the LDAP admin DN, but rather an ID with sufficient authority for the use cases mentioned above. **Note:** Make sure to type the value in lower case, regardless of the case used in the distinguished name (DN). Example: `cn=ldapdb2`	No default value is provided
LDAP admin password	The password of the LDAP directory administrator.	No default value is provided
LDAP suffix	The LDAP directory DN suffix which the operations console uses for storing user and group data. Example: o=ibm.com	No default value is provided

Table 40. Installation parameters for LDAP (continued)

Parameter	Description	Default
Use SSL for LDAP	Indicates whether Secure Sockets Layer (SSL) communication is enabled for the LDAP server. Whether SSL is enabled or not determines which port number must be used for the LDAP port.	False
LDAP user prefix	The attribute name used for building the relative distinguished name (RDN) of user entries in the LDAP directory tree. The DN of user entries begins with this prefix. If the LDAP user object class is inetOrgPerson, this value is uid. This information is used to assemble the bind DN which is used by WebSphere Application Server to connect to the LDAP server in order to retrieve user attributes required for authentication.	uid
LDAP user suffix	The RDN of the user container entry in the LDAP directory tree.	ou=users
LDAP user object class	The object class used by the LDAP server to store user entries.	inetOrgPerson
Console admin group short name	The operations console administrator group name. The ISC administrator user is a member of this group.	iscadmins
LDAP group prefix	The attribute name used for building the relative distinguished name (RDN) of group entries in the LDAP directory tree. The DN of group entries begins with this prefix. If the LDAP group object class is groupOfUniqueNames, this value is cn.	cn
LDAP group suffix	The RDN of the group container entry in the LDAP directory tree.	ou=groups
LDAP group object class	The object class used by the LDAP server to store group entries.	groupOfUniqueNames
LDAP group member attribute	The property that specifies the attribute name of the membership attribute of group entries in the LDAP directory tree. If the LDAP group object class is groupOfUniqueNames, this attribute name is uniqueMember.	uniqueMember

Installation parameters for the operations console

The parameters listed in the following table must always be specified.

Table 41. Installation parameters for Integrated Solutions Console

Parameter	Description	Default
ISC administrator user	The user ID of the operations console administrator. During installation, the administrator is given access to all console modules. The user ID is added to the operations console administrator group. After the installation, the administrator can change the password and add other user IDs to the operations console administrator group. The user ID must comply with the following conditions: • The user ID must be unique. • The length is 3 to 20 characters. • A valid user ID may contain only the characters a-z, A-Z, period (.), hyphen (-), underscore (_), and double-byte character set (DBCS) characters. No other characters are permitted in this field. For example, diacritics, such as the umlaut, are not permitted. • If the user ID will also be used for authenticating the end-to-end automation manager (which is not recommended), additional restrictions apply (see "User credentials page" on page 125). If security with a DB2 database user registry is enabled, this user is created during the installation. If security with an LDAP user registry is enabled, this user must already exist in LDAP before the installation begins.	iscadmin
Password	The password of the operations console administrator. The password must comply with the following conditions: • The length is 5 to 60 characters. • A valid password may contain only the characters a-z, A-Z, period (.), hyphen (-), and underscore (_). No other characters are permitted in this field. For example, DBCS characters and diacritics, such as the umlaut, are not permitted. If security with a DB2 database user registry is enabled, the password is for a user which is created during installation. For this reason, the password must be confirmed. If security with an LDAP user registry is enabled, this password is for a user which must already exist before beginning the installation.	No default value is provided
Fully qualified host name	The fully qualified host name of the system where the operations console will be installed	The fully qualified host name is detected on your system and displayed as default value.

Table 41. Installation parameters for Integrated Solutions Console (continued)

Parameter	Description	Default
HTTP Port	The number of the HTTP port that the operations console will use. Select a port that is not being used by another process on the system. After the operations console is installed, you must include this port number in the URL for opening the console. The URL is composed of the protocol name, plus the fully-qualified host name, plus the port, plus ibm/console. This is an example of a full URL as it is needed for connecting to the operations console: `http://myhost.com:8421/ibm/console`	8421
HTTPS Port	The port that the operations console will use for secure HTTP transport (HTTPS). This value must not conflict with existing port assignments on the system. To enable HTTPS, you also must perform the procedure described as post-installation task in “Setting up SSL for the operations console” on page 113 after the operations console is installed.	8422
Bootstrap/RMI Port	The address for the bootstrap function and the port number for the Java Remote Method Invocation (RMI) connector on the operations console server. This value must not conflict with existing port assignments on the system.	8424
SOAP Port	The address for the Simple Object Access Protocol (SOAP) connector on the operations console server. This value must not conflict with existing port assignments on the system.	8425
Admin HTTP Port	The HTTP Administrative Console port on the operations console server. This value must not conflict with existing port assignments on the system.	8431
Admin HTTPS Port	The HTTPS Administrative Console secure port on the operations console server. This value must not conflict with existing port assignments on the system.	8432
SAS SSL ServerAuth Listener Address Port	The SAS SSL ServerAuth Listener Address port on the operations console server. This value must not conflict with existing port assignments on the system.	8439
CSIV2 SSL ServerAuth Listener Address Port	The CSIV2 SSL ServerAuth Listener Address port on the operations console server. This value must not conflict with existing port assignments on the system.	8440

Table 41. Installation parameters for Integrated Solutions Console (continued)

Parameter	Description	Default
CSIV2 SSL MutualAuth Listener Address Port	The CSIV2 SSL MutualAuth Listener Address port on the operations console server. This value must not conflict with existing port assignments on the system.	8441
Console Help Port	The port that the help system (based on Eclipse technology) will use to receive requests for help files. This value must not conflict with existing port assignments on the system.	8423
Register ISC server and ISC Help server as system service	To automatically restart the operations console and the console help server each time the system is restarted, these services can be registered as system services	Enabled
Console Service ID	To automatically restart the console server each time the operating system is restarted, specify this parameter. For Linux, the string must be 1 to 4 characters. The installation program checks the length of the value you specify. For AIX, the length must be 1 or more characters. For Linux and AIX, the operating system file `/etc/inittab` is edited directly to include the value you specify. The line that is added to the file has the following format: `service_ID:23:boot:isc_runtime_root/PortalServer/ bin/startISC.sh ISC_Portal ISCUSER ISCPASS` For Windows systems only: Set the value to a unique string. Valid characters are a-z, A-Z, and 0-9. The string must be 1 or more characters and the value is used to add a service to the operating system. If this parameter is specified, you must also specify the Console Help Service ID parameter.	CS01
Console Help Service ID	For Windows systems only: Set the value to a unique string. Valid characters are a-z, A-Z, and 0-9. The string must be 1 or more characters. The value is used to add a service to the operating system. If this parameter is specified, you also must specify the Console Service ID parameter. For AIX and Linux: The Console Help Service is started as part of the service defined by the Console Service ID parameter. The Console Help Service ID parameter is not shown.	HS01

Installation parameters for IBM Tivoli Enterprise Console

Optionally, you can use Tivoli Enterprise Console for monitoring end-to-end automation management events. The parameters listed in the following table are only required if you will be utilizing Tivoli Enterprise Console for end-to-end automation management.

Table 42. Installation parameters for IBM Tivoli Enterprise Console

Parameter	Description	Default
TEC host name	The name of the host where the Tivoli Enterprise Console server is installed.	localhost
TEC server port number	The port number for the Tivoli Enterprise Console server	5529

Note: When you TEC server runs on AIX or Linux, the TEC server port number must be set to `0`. For more information about utilizing Tivoli Enterprise Console for end-to-end automation management, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, chapter "Using Tivoli Enterprise Console with SA for Multiplatforms"

Name of the end-to-end automation domain

Table 43. Name of the end-to-end automation domain

Parameter	Description	Default
Automation domain name	The name of the end-to-end automation domain represented by this instance of the automation engine. The domain name must be unique and may not be used for any other automation domain. The characters used for the domain name are limited to the following ASCII characters: A-Z, a–z, 0-9, . (period), and _(underscore).	FriendlyE2E

What the installation CD contains

The end-to-end automation management component can be ordered from IBM as media pack or downloaded as an Electronic Software Distribution (ESD) image from an IBM software distribution download site.

There are multiple CDs for each supported platform.

This is what the CD labeled *IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component for <operating_system_name>* contains:

- The files for launching the installation wizard
- The readme file
- Directories containing the files required to install components that are embedded into the end-to-end automation management installation. These are:

Table 44. Directories on the product CD

Directory	Content
README	For example, copyright notices and license agreements
license	License key
DDL	Scripts for creating DB2 databases and tables when remote DB2 setup is used
<PLATFORM>[1]	Product installer and files needed for installing the product

Table 44. Directories on the product CD (continued)

Directory	Content
Note: 1. <PLATFORM> is one of the following: • AIX • PPC (Linux on POWER) • Windows • i386 (Linux on System x) • S390 (Linux on System z)	

Languages supported by IBM Tivoli System Automation

This section is only of interest for you if you want to use IBM Tivoli System Automation for Multiplatforms in a language other than English as shown in the following tables.

Table 45 shows which encodings are supported for the Linux distribution. If you are using the end-to-end automation adapter for the IBM Tivoli System Automation base component, note that new versions of Linux operating systems may not support all encodings, but UTF-8 encoding is always supported.

The following encodings are supported for the Linux distribution:

Table 45. Supported languages

Language	UTF-8	ISO-8859-1	EUC/GBK	Euro	GB18030/BIG5
German	de_DE.UTF-8	de_DE, de_DE.ISO-8859-1		de_DE@euro	
Spanish	es_ES.UTF-8	es_ES, es_ES.ISO-8859-1		es_ES@euro	
French	fr_FR.UTF-8	fr_FR, fr_FR.ISO-8859-1		fr_FR@euro	
Italian	it_IT.UTF-8	it_IT, it_IT.ISO-8859-1		it_IT@euro	
Japanese	ja_JP.UTF-8		ja_JP.eucJP		
Korean	ko_KR.UTF-8		ko_KR.eucKR		
Portugese/ Brazilian	pt_BR.UTF-8	pt_BR			
Simplified Chinese	zh_CN.UTF-8		zh_CN.GBK, zh_CN.GB2312		zh_CN.GB18030
Traditional Chinese	zh_TW.UTF-8				zh_TW.Big5, zh_TW

The following encodings are supported on the AIX distribution:

Language	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/BIG5
German	DE_DE	de_DE		
Spanish	ES_ES	es_ES		
French	FR_FR	fr_FR		
Italian	IT_IT	it_IT		

Language	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/BIG5
Japanese	JA_JP		ja_JP	Ja_JP
Korean	KO_KR		ko_KR	
Portugese/Brazilian	PT_BR	pt_BR		
Simplified Chinese	ZH_CN		zh_CN	Zh_CN
Traditional Chinese	ZH_TW		zh_TW	Zh_TW

Installation prerequisites

The following prerequisites must be satisfied before you can start the installation wizard for the end-to-end automation management component:

- WebSphere Application Server must be installed as described in "Installing WebSphere Application Server" on page 74. There must be no other WebSphere Application Server product installation on the same system. Security must be disabled in WebSphere Application Server.
- A DB2 server must be installed as described in "Installing a DB2 server" on page 69. The DB2 server instance must be running and accepting client connections.

  If you are using a local DB2 setup, the DB2 server instance should be empty or should at least not contain neither the automation manager database nor the operations console database from an earlier attempt to install a Tivoli System Automation for Multiplatforms component. Additionally, no other TCP/IP node must have been cataloged with a database alias that refers to an already existing automation manager or operations console database.
- If remote DB2 setup is used, a DB2 client must be installed on the same system as WebSphere Application Server as described in "Installing a DB2 client" on page 72.
- If LDAP is used as the user registry, an LDAP server must be configured as described in "Setting up an LDAP server" on page 76. The LDAP server must be running and accepting client connections.
- The user ID that is used to run the installer for the end-to-end automation management component must be able to run DB2 client code. This means that the DB2 environment must be made available for the user ID.

  For more information on setting up the DB2 environment, refer to Chapter 1. "Before creating a database" -> "Preparing to create a database" in *IBM DB2 Universal Database Administration Guide: Implementation*, Version 8.2 (SC09-4820).

  On Linux and AIX systems, the DB2 environment must be prepared in a way such that the DB2 environment is automatically available in every sub-shell that is opened. This is usually accomplished by extending a startup shell script. The user ID that is used to run the installed end-to-end automation management component must have the same DB2 environment setup.

  Attention:
  On Linux and AIX systems, this DB2 environment setup is not automatically done by a DB2 server or DB2 client installation and must be performed manually. If this is not done, the installation of the end-to-end automation management component will fail.

- The user ID that is used to run the installer for the end-to-end automation management component must have administrator authority.

  On Linux and AIX, this user ID is typically ″root″.

- When installing the end-to-end automation management component to an AIX or Linux system, you must ensure that an XWindows session is available for displaying the graphical installation wizard panels.

Installing the end-to-end automation management component

This section describes how to install the end-to-end automation management component. For the installation, you use a graphical installation program, the so-called installation wizard. The required steps are described below.

On the panels of the installation wizard, enter the data you have collected using the lists in section "Collecting the information you need to provide during installation" on page 79.

Notes:

1. Although the panels in this section show a Windows installation, the panels that are displayed for other operating systems have a similar appearance. Make sure to conform to the conventions of your platform when specifying directory locations, files names and so on.
2. In this section, only those panels are depicted on which user action is required.
3. The installation comprises two phases:
   a. In the pre-installation phase, you specify the installation parameters. This may take up to half an hour.
   b. The installation phase, which begins when you click the **Install** button on the last pre-installation panel, may take up to two hours to complete (depending on processor speed).
4. **Attention:** Do not cancel the installation after clicking **Install** on the last pre-installation panel. If you cancel an ongoing installation, the installation process may fail and you may need to clean up your system manually (see "Cleaning up from a failed installation" on page 208).

To install the end-to-end automation management component, perform these steps:

1. Make sure that all installation prerequisites are met (refer to "Installation prerequisites" on page 92).

   ---

2. Insert the following CD in the CD drive:

   IBM Tivoli System Automation Multiplatform V2.2.0 End-to-end component for <operating_system_name>

   There are multiple CDs. Be sure to use the one for your platform.

   ---

3. Change to the directory that contains the installation program. For the location of the directory, refer to "Packaging" on page 59.

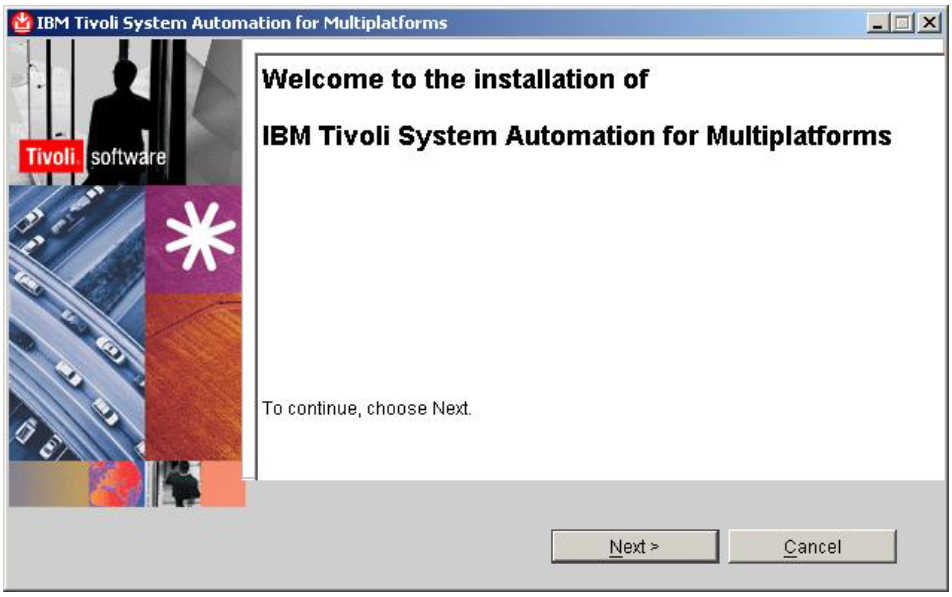
   ---

4. Launch the installation wizard by starting the following program from the current working directory:
   - **Windows**: `setup.exe`
   - **AIX, Linux**: `setup`

   When the wizard is launched successfully, the Welcome panel appears.

   ---

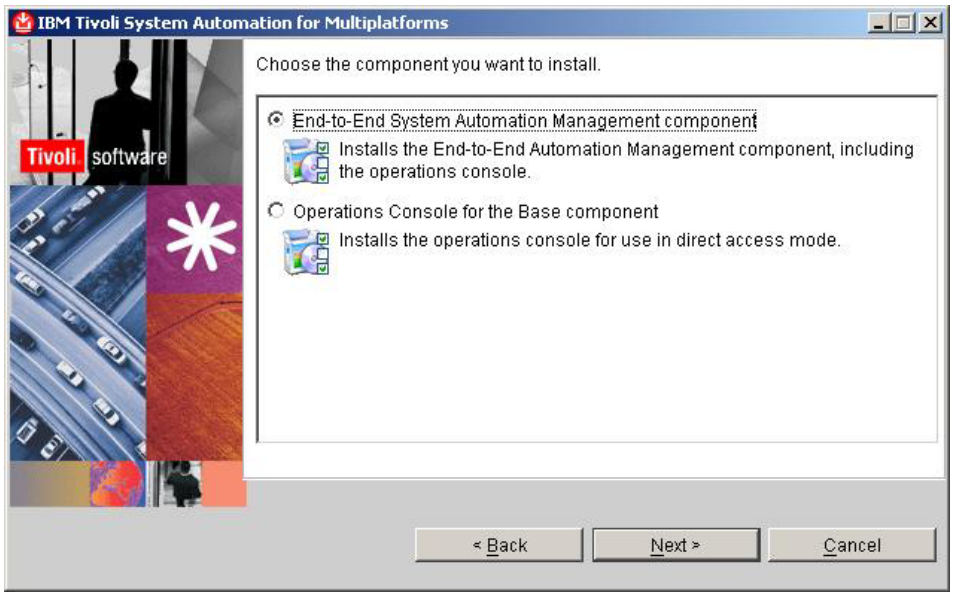
5. On the Welcome panel, click **Next** to display the License agreement panel.



6. Select **I accept the terms of the license agreement** and click **Next**.

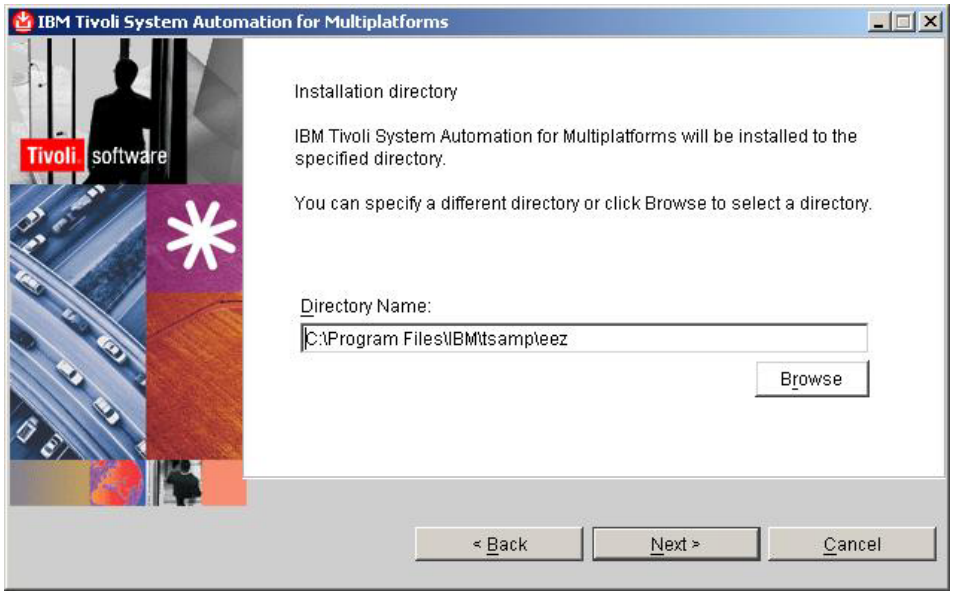
Note: After you click **Next**, the installation wizard checks whether the subdirectories ISC, EIF, and ISC are available in the directory in which the installation wizard program is located. If the subdirectories are not found, a panel is displayed that prompts you for the fully qualified path to the directory in which the subdirectories can be found.

7. Select **End-to-End System Automation Management component** and click **Next**.



8. Specify the directory where you want to install the end-to-end automation management component or accept the default location.

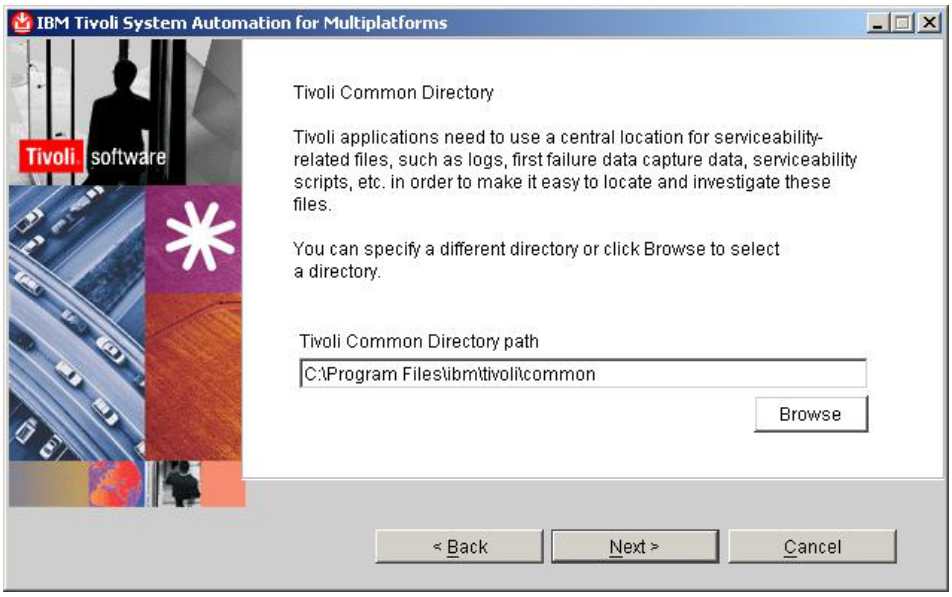
   Click **Next**.



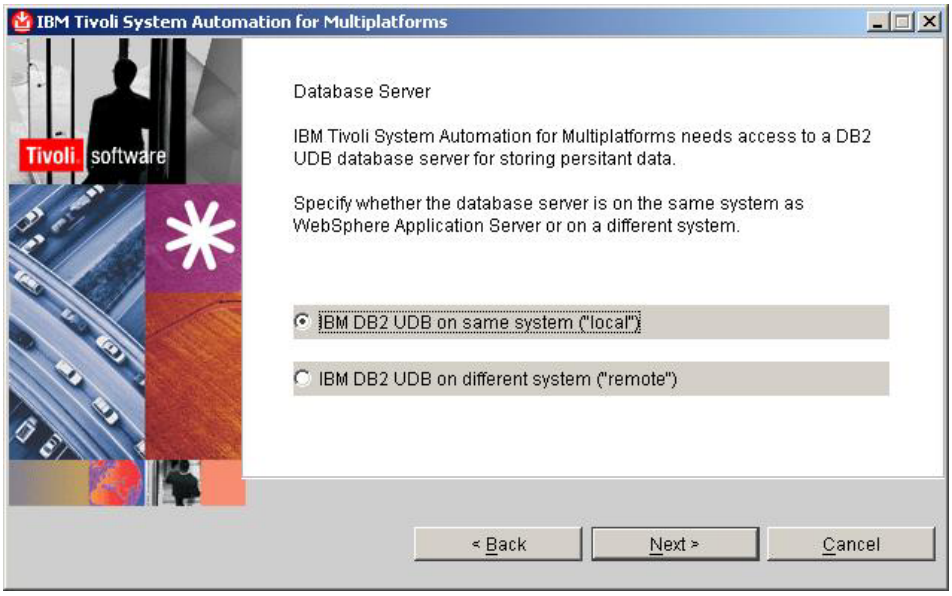
9. If the installation program detected a Tivoli Common Directory on your system, for example, because a Tivoli product is already installed, the directory must also be used for IBM Tivoli System Automation for Multiplatforms. In this case, the entry field that is displayed on this panel is write-protected.

   If the installation program did not detect a Tivoli Common Directory on your system, accept the default location or specify the directory to which the Tivoli log files are to be written.

   Click **Next**.



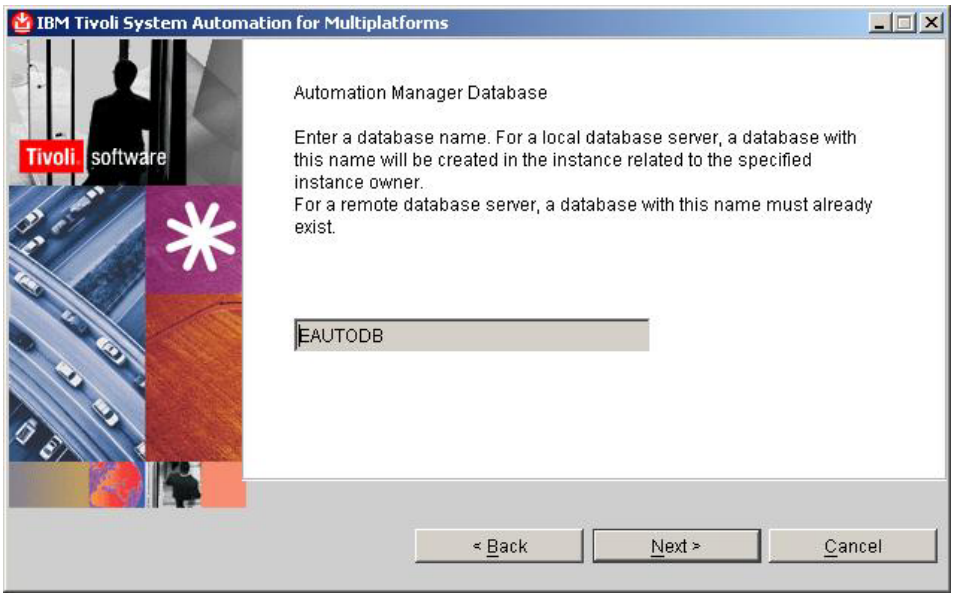
10. Select the DB2 setup type you are using and click **Next**.



11. Your actions on this panel depend on the type of DB2 setup you are using:
    - **Local DB2 setup:** Specify the automation manager database name you want to use or accept the default name.

      Click **Next** and proceed with step 12 on page 97.
    - **Remote DB2 setup:** Specify the name of the database you created for the automation manager.

      Click **Next** and proceed with step 14 on page 98.



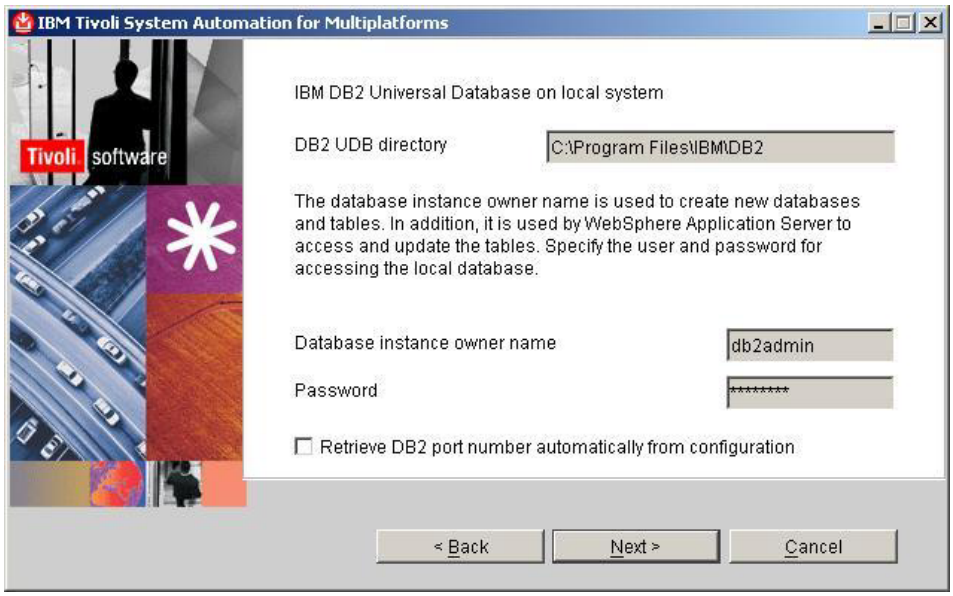
12. **This panel only appears when you are using a local DB2 setup.**

    AIX/Linux:

    a. Specify the name and password of the DB2 instance owner.
    b. Leave the check box on the panel selected to retrieve the correct DB2 port number automatically. If you clear the check box, you must specify the port number on the subsequent panel.
    c. Click **Next**.

    Windows:

    a. Specify the name and password of the DB2 instance owner.
    b. The DB2 port number cannot be retrieved automatically and the corresponding check box is disabled. You specify the DB2 port number on the subsequent panel.
    c. Click **Next**.



13. **This panel only appears when you are using a local DB2 setup.**

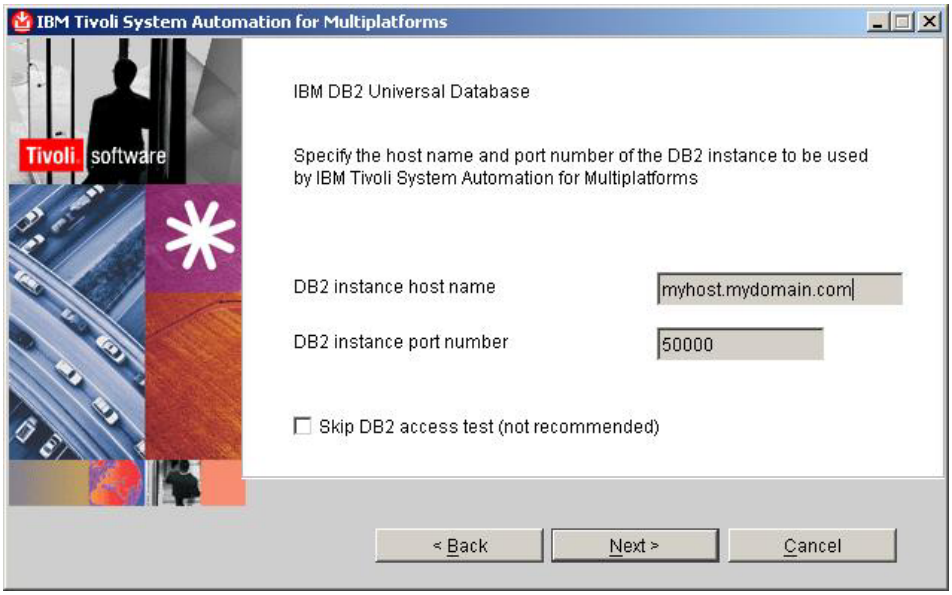
    The fully qualified host name of your system was detected by the installation program. The value is displayed in the field **DB2 instance host name**. Do not change the value to `localhost`!

    In the field**DB2 instance port number** the valid port number must be specified:

    - If the DB2 port number was retrieved automatically, the valid port number is displayed in the field.
    - If the DB2 port number was not retrieved automatically, the default port number (`50000`) is displayed. The actual DB2 port number may differ from the default, because a different port number is assigned automatically during DB2 installation if the default port is not free. Before you accept the default value, ensure that it is correct, or specify the valid port number.

    Click **Next** and proceed with step 16 on page 100.

    Note: After you click **Next,** the installation program checks whether the database can be accessed with the values you specified on the panel. If you want to skip the check, select the check box on the panel.



14. **This panel only appears when you are using a remote DB2 setup.**

    AIX/Linux:

    a. Specify the name and password of the DB2 instance owner.

    b. Leave the check box on the panel selected to retrieve the correct DB2 port number automatically. If you clear the check box, you must specify the port number on the subsequent panel.

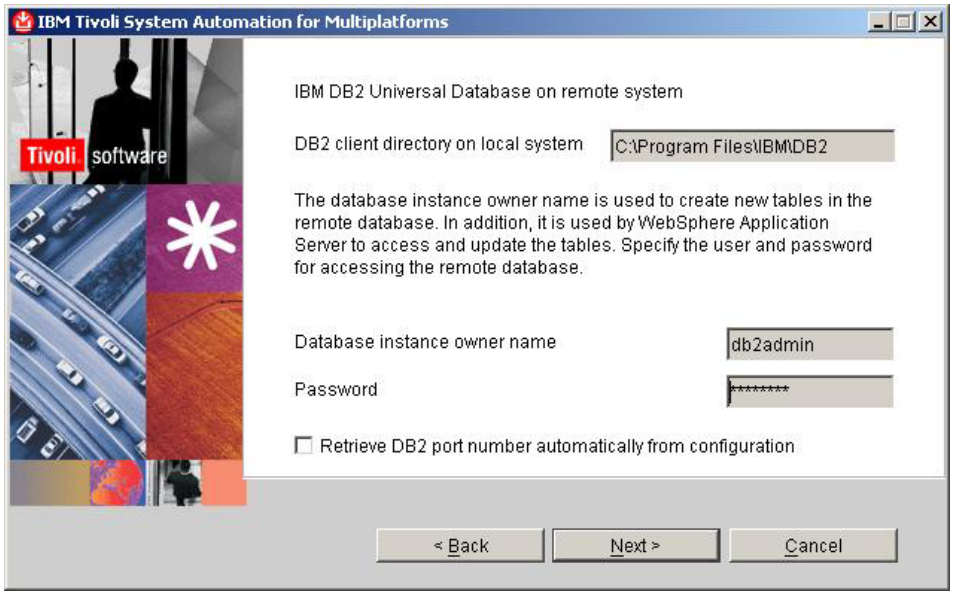
    c. Click **Next**.

    Windows:

    a. Specify the name and password of the DB2 instance owner.

    b. The DB2 port number cannot be retrieved automatically and the corresponding check box is disabled. You specify the DB2 port number on the subsequent panel.

c. Click **Next**.



---

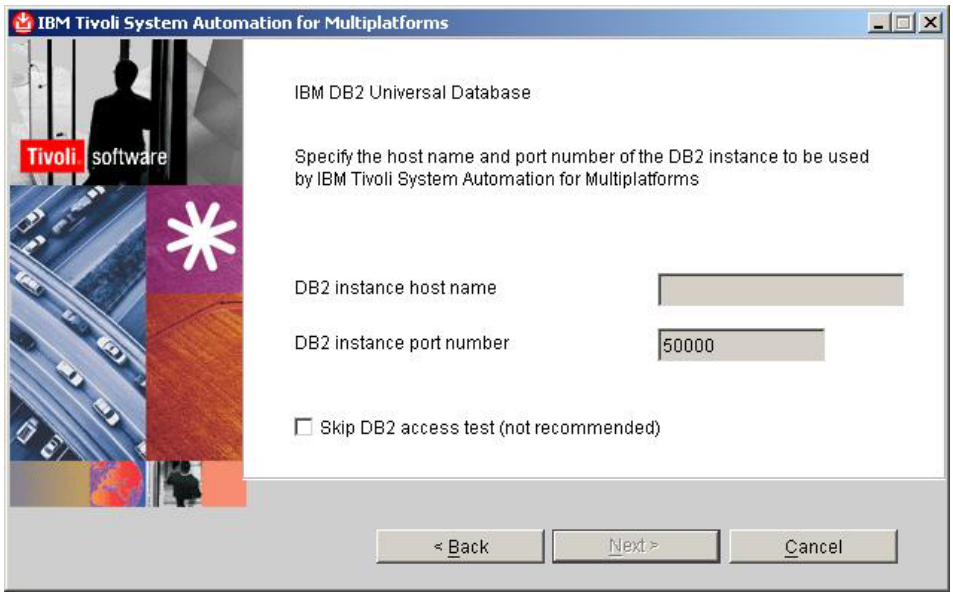
15. **This panel only appears when you are using a remote DB2 setup.**

    In the field **DB2 instance host name**, specify the fully qualified host name of the system where the DB2 server is installed.

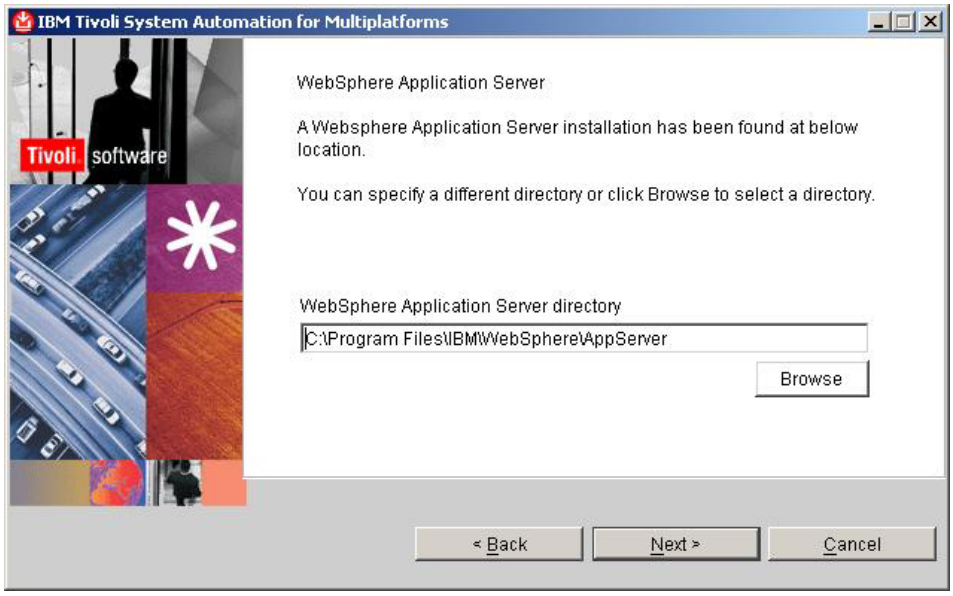
    In the field**DB2 instance port number**, the valid port number must be specified:

    - If the DB2 port number was retrieved automatically, the valid port number is displayed in the field.
    - If the DB2 port number was not retrieved automatically, the default port number (`50000`) is displayed. The actual DB2 port number may differ from the default, because a different port number is assigned automatically during DB2 installation if the default port is not free. Before you accept the default value, ensure that it is correct, or specify the valid port number.

    Note: After you click **Next,** the installation program checks whether DB2 can be accessed with the values you specified on the panel. If you want to skip the check, select the check box on the panel.

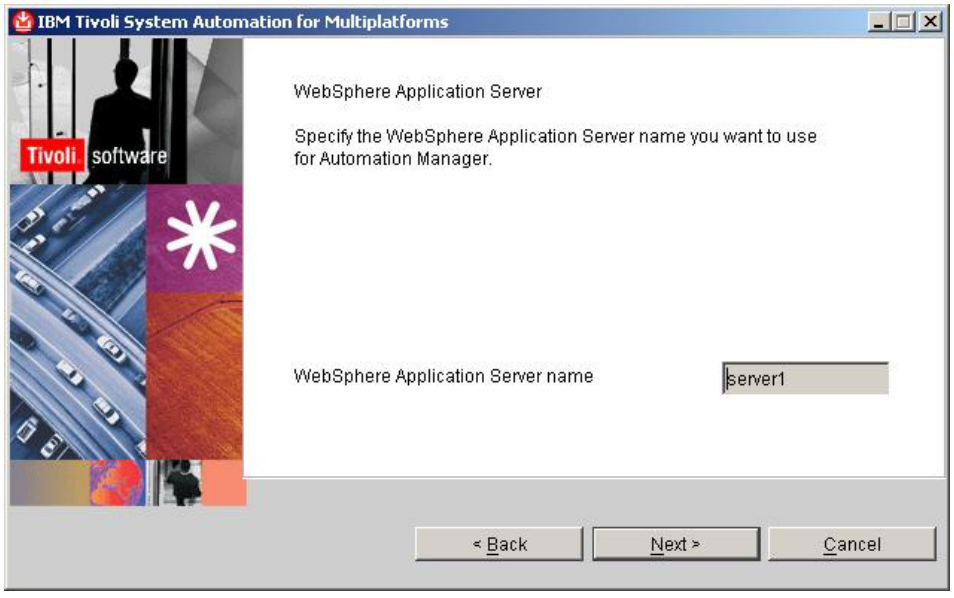


16. The installation directory of WebSphere Application Server is detected on your system and displayed. Click **Next**.

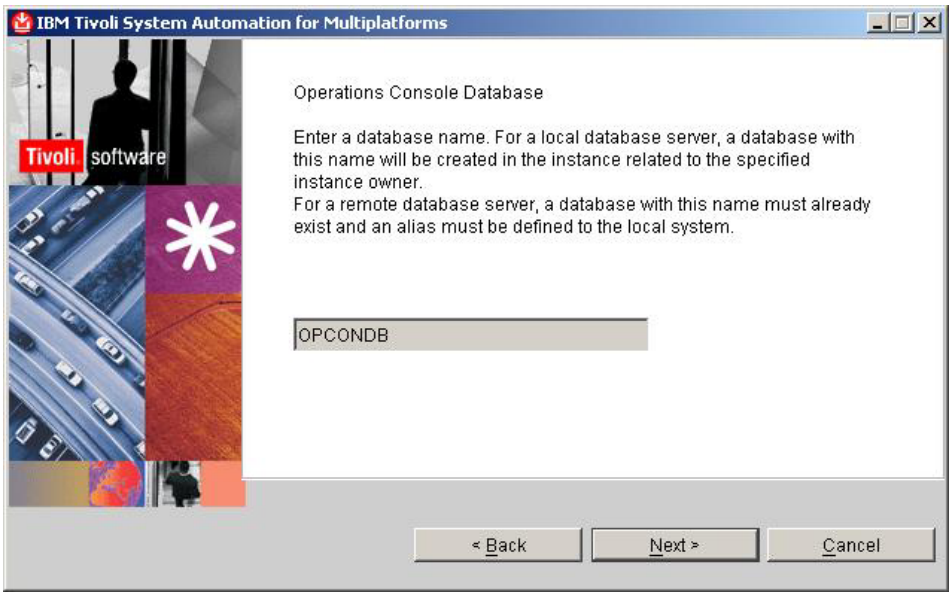


17. The existing WebSphere Application Server profiles are detected on your system and displayed. Select the profile you want to use and click **Next**.

18. Specify the WebSphere Application Server name you want to use or accept the default name. Click **Next**.



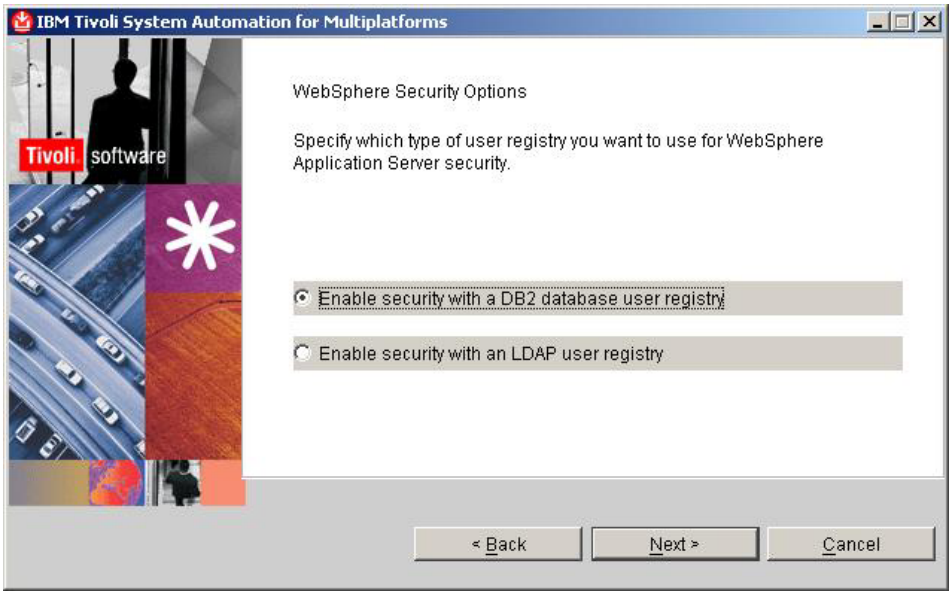
19. Your actions on this panel depend on the type of DB2 setup you are using:
    - **Local DB2 setup:** Specify the operations console database name you want to use or accept the default name and click **Next**.
    - **Remote DB2 setup:** Specify the name of the database alias you cataloged for the operations console and click **Next**.



20. Select the type of user registry you are using:
    - You are using a DB2 database as the user registry:

      Select the appropriate radio button, click **Next**, and proceed with step 21.
    - You are using an LDAP directory as the user registry:

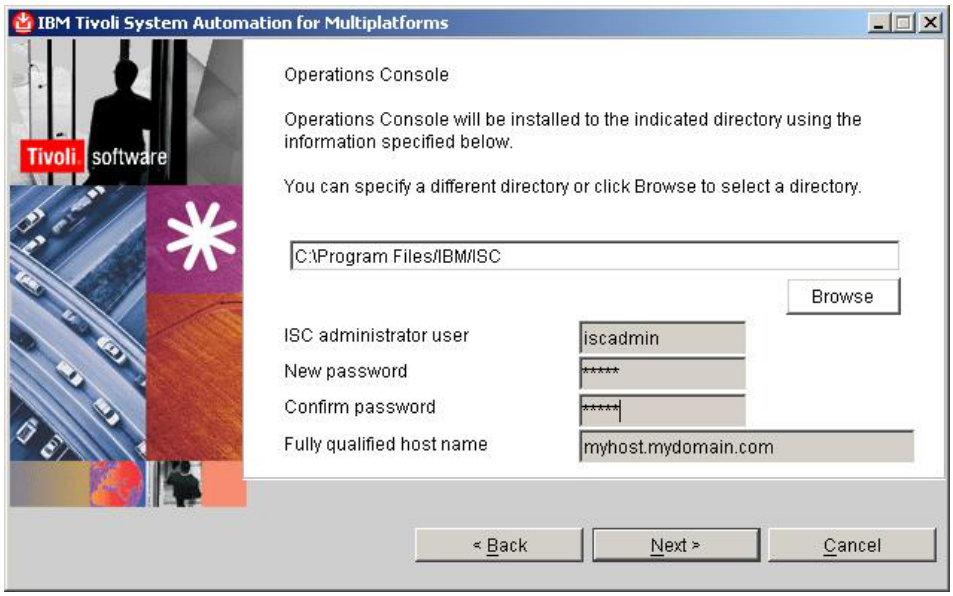
      Select the appropriate radio button, click **Next**, and proceed with step 22 on page 103.



21. **This panel only appears if you are using a DB2 database as the user registry.**

    Choose a user ID and password for the Integrated Solutions Console administrator. If you specify an operations console installation directory other than the default, note that the length of the installation path must be 32

characters or less (for further restrictions, refer to Table 37 on page 82). Click **Next**, and proceed with step 26 on page 105.

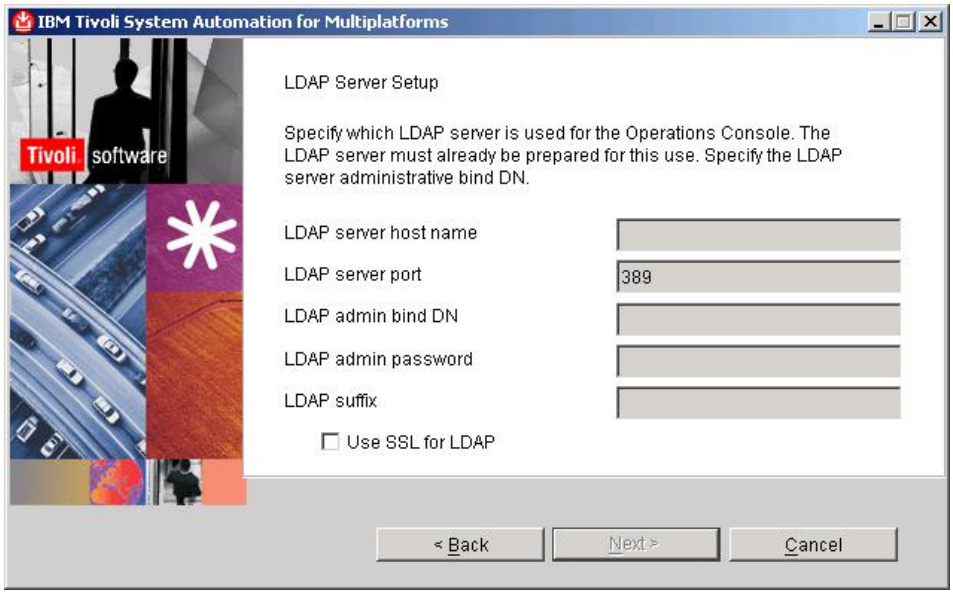


22. **This panel only appears if you are using LDAP as the user registry.**

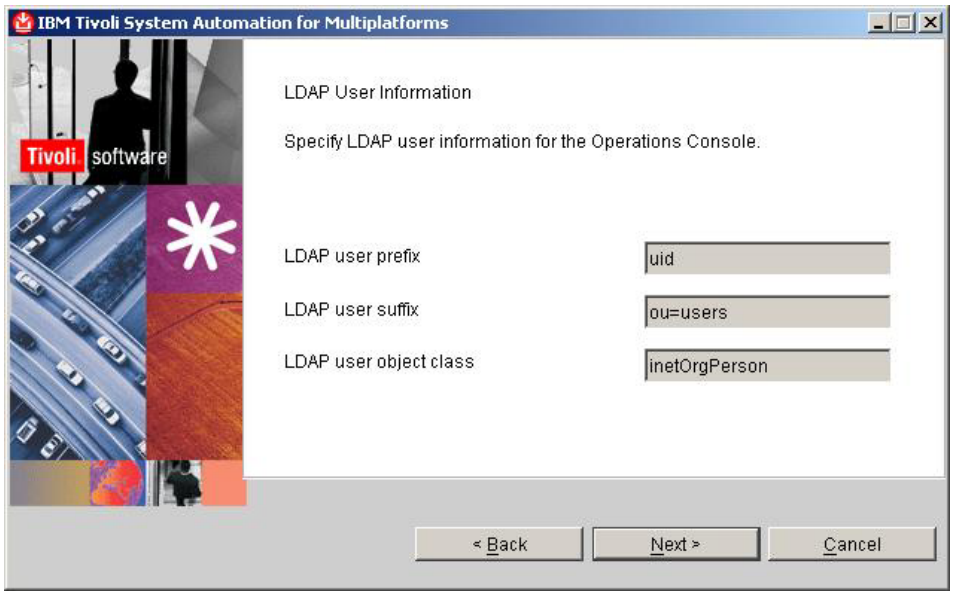
    Specify the LDAP-specific data you have collected (refer to the table in "Installation parameters for LDAP" on page 85. In the table, the parameters are listed in the sequence in which you must specify them on this and the subsequent panels).

    Note: On the panel, port number 389 is always displayed as default value for the LDAP server port, regardless of whether or not you are using SSL. If you will be using SSL, you must manually change the port number to the appropriate value.

    Click **Next**.

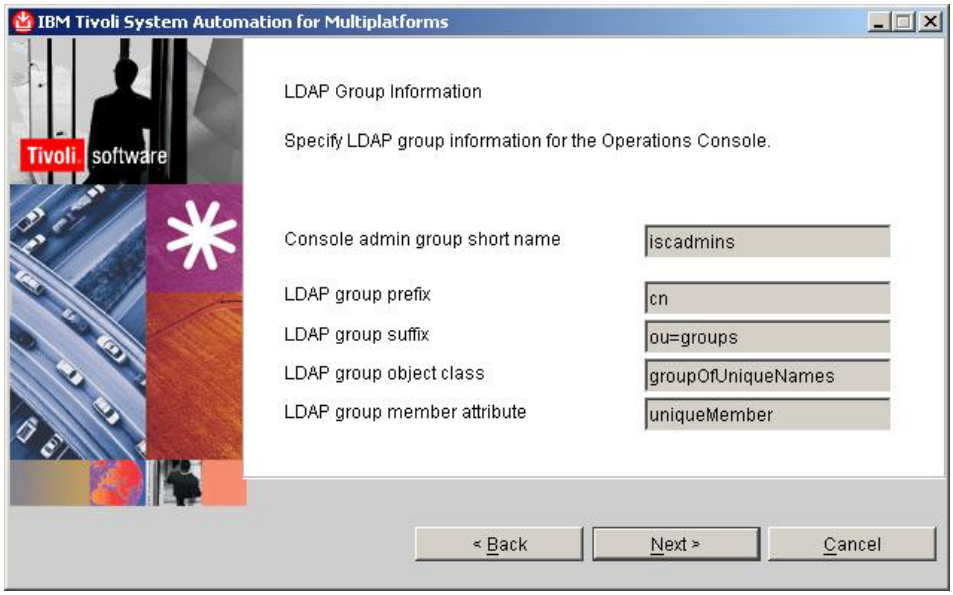


23. **This panel only appears if you are using LDAP as the user registry.**
Specify the LDAP-specific data you have collected (refer to the table in "Installation parameters for LDAP" on page 85). Click **Next**.



---

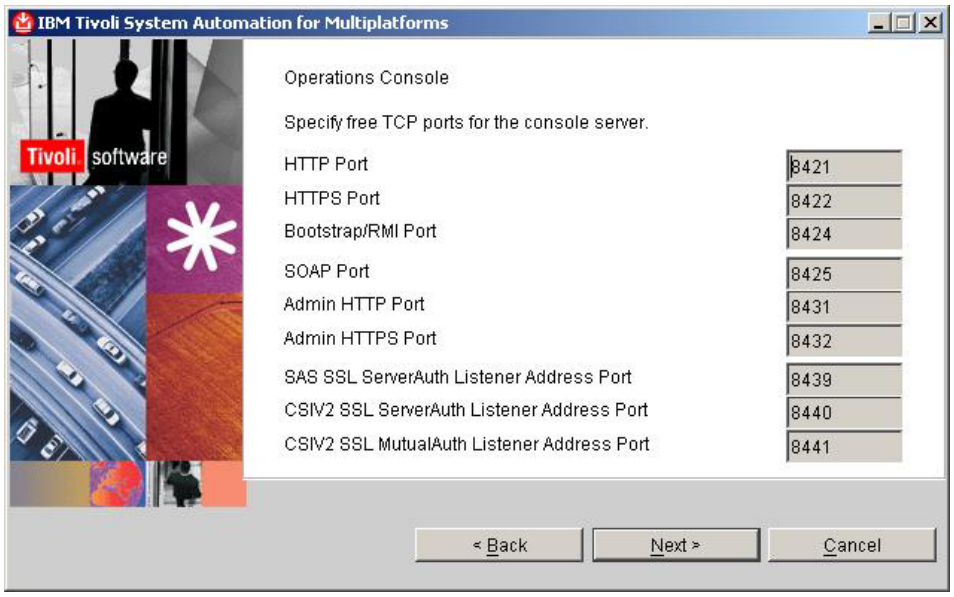
24. **This panel only appears if you are using LDAP as the user registry.**
Specify the LDAP-specific data you have collected (refer to the table in "Installation parameters for LDAP" on page 85). Click **Next**.



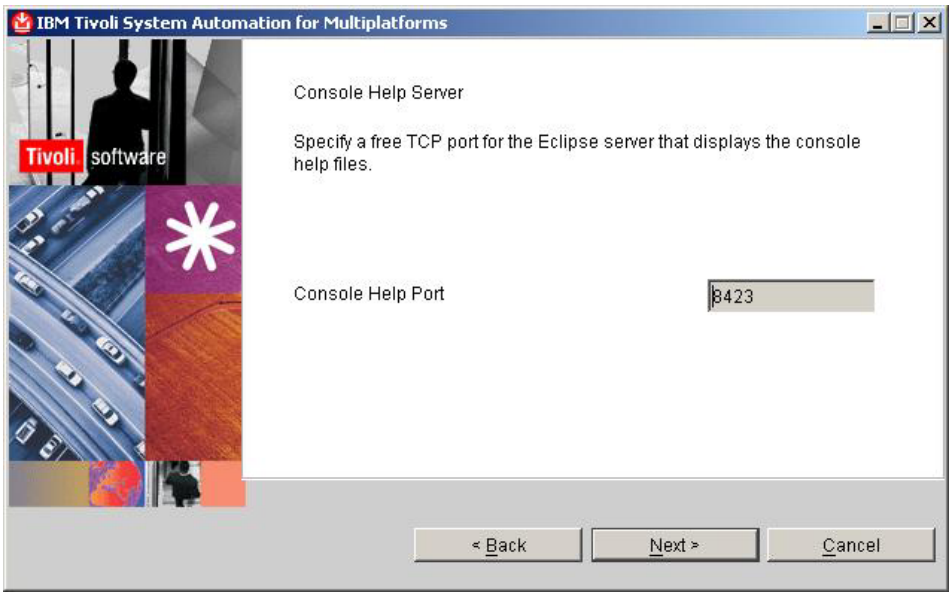
---

25. **This panel only appears if you are using LDAP as the user registry.**
Specify the user ID and password of the Integrated Solutions Console administrator user. If you specify an operations console installation directory other than the default, note that the length of the installation path must be 32 characters or less (for further restrictions, refer to Table 37 on page 82). Click **Next**.

26. Specify the ports you want to use for the operations console or accept the default values (refer to "Installation parameters for the operations console" on page 86 for detailed information) and click **Next**.

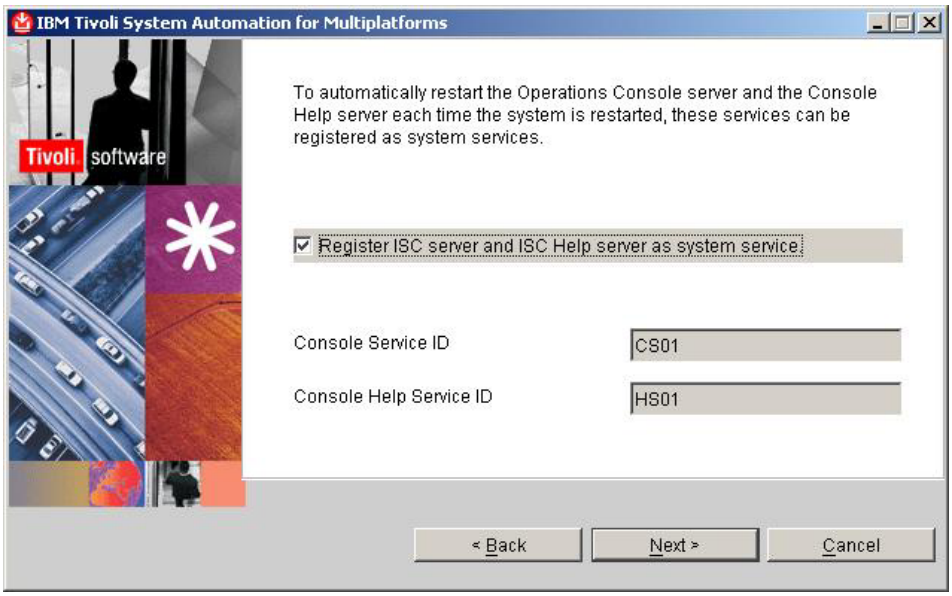


27. Specify the port number for the console help server or accept the default value and click **Next**.



28. If you want to register the operations console server and the console help server as system services, specify service IDs or accept the default service IDs and click **Next**.

    For more information, refer to "Installation parameters for the operations console" on page 86.

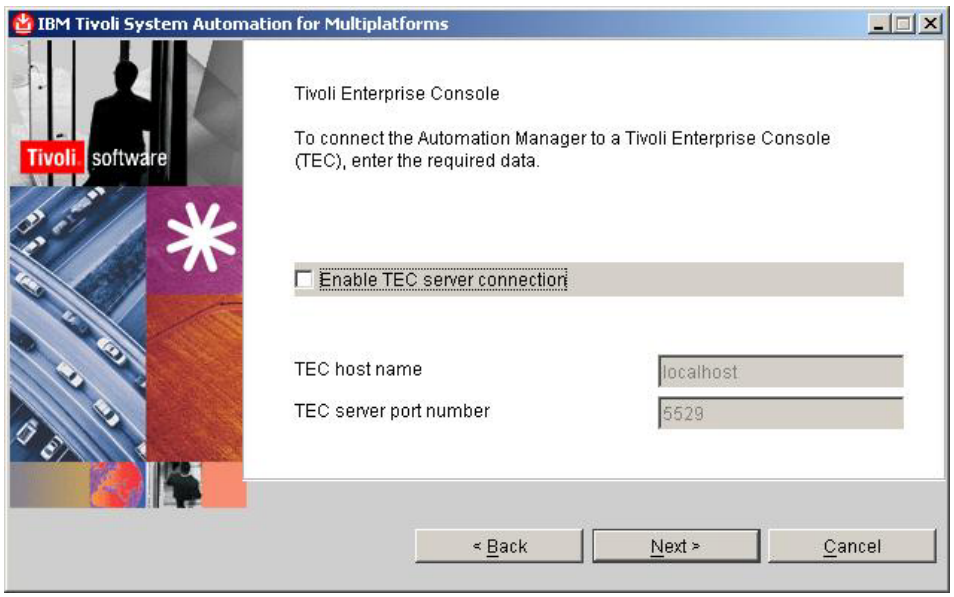


29. If you want to use Tivoli Enterprise Console to display end-to-end automation management events:
    - Select **Enable TEC server connection**
    - In the field **TEC host name**, specify the host name of the console server.
    - In the field **TEC server port number**, specify the port number of the console server:
      - **Windows:** Accept the default value that is displayed in the field (5529)

– **AIX/Linux:** Set the value to `0`

Click **Next**.

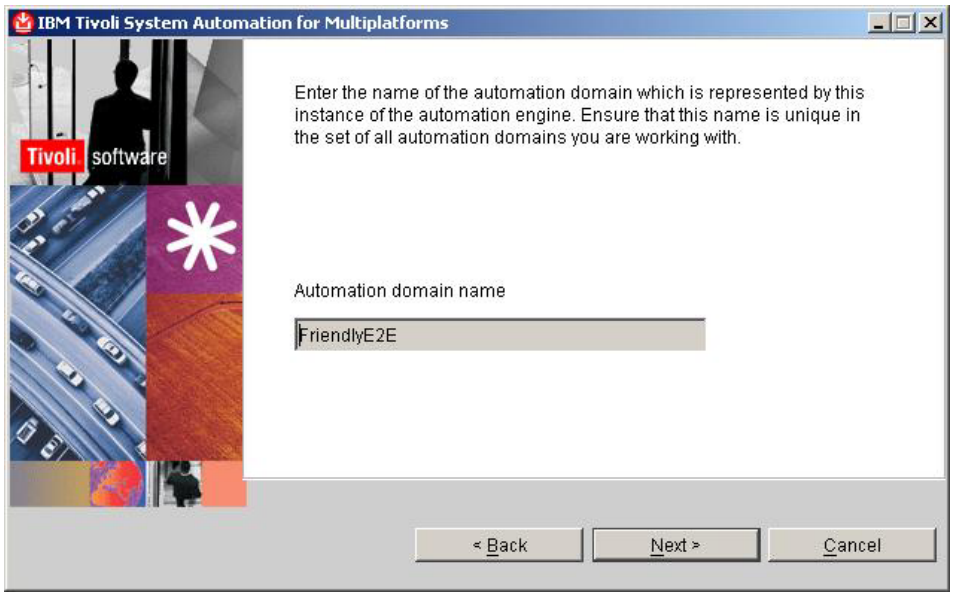
Note: You can also enable the connection using the WebSphere Application Server administrative console after the installation of the end-to-end automation management component is complete. This is described in the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, in section "Using Tivoli Enterprise Console with SA for Multiplatforms".



---

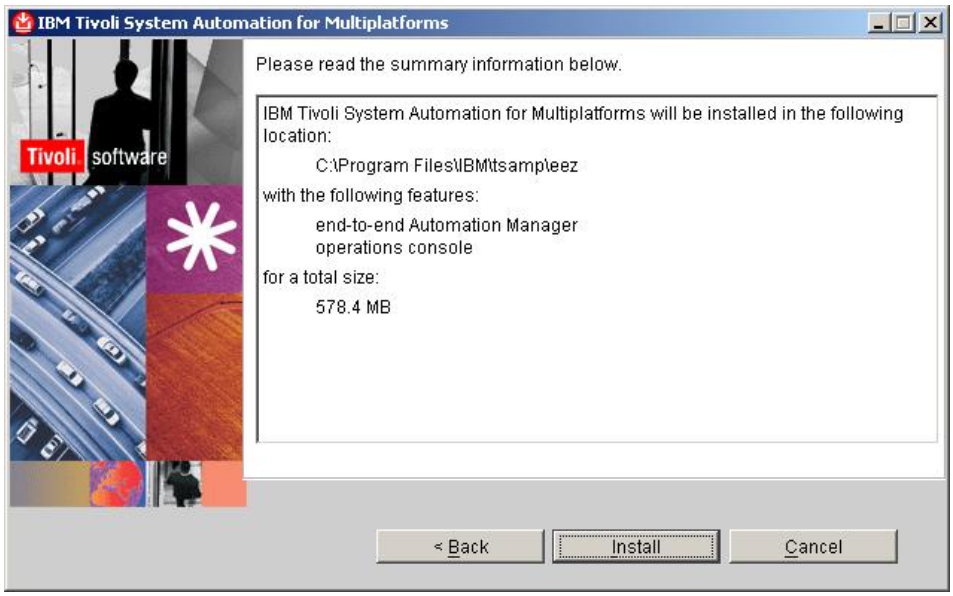
30. Specify the end-to-end automation domain name you want to use or accept the default name and click **Next**.

Note: Accept the default domain name ("FriendlyE2E") if you want to use the sample end-to-end automation management environment to familiarize yourself with end-to-end automation management and the operations console. For more information, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Getting started".



31. When you have specified all required information on the wizard panels, a summary panel appears. Click **Install**. The installation wizard begins installing the end-to-end automation management component. The installation can take considerable time to complete. While installation tasks are performed, the progress bar may appear to stall.

    Attention: Do not cancel the installation after clicking **Install**. If you cancel an ongoing installation, the installation process may fail and you may need to clean up your system manually (see "Cleaning up from a failed installation" on page 208).

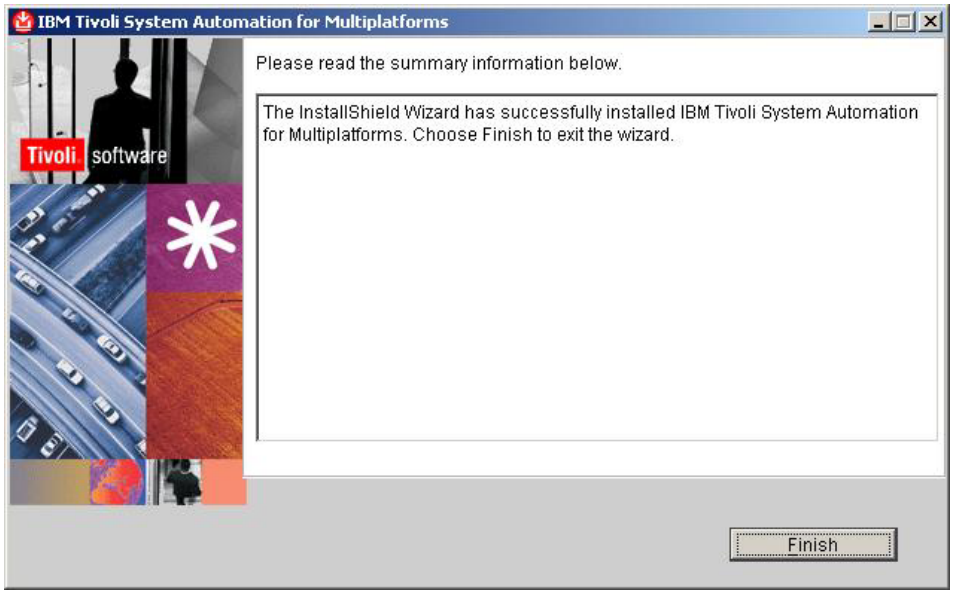


Note: During the installation, the following login window may appear:

You can safely ignore the window, no input is required. The window disappears automatically after some time and the installation completes successfully. The installation also completes successfully if you do enter information on the panel and click **OK**, or if you click **Cancel** to close the window.

---

32. When the end-to-end automation management component was installed successfully, a summary panel appears. Click **Finish** to close the installation wizard. For information on verifying the installation, refer to "Verifying the installation" on page 110.



Note: If problems were encountered during the installation, an error panel appears before the summary panel is displayed. In such a case, do this:

- On the error panel, click **Next**.
- On the summary panel that appears, click **Finish**.
- Use the log files that were created by the installation program to analyze and resolve the problems. For more information on the log files, refer to "Using the installation log files" on page 210.

Verifying the installation

Automation manager

To verify that the automation manager was installed successfully, complete the tasks described in the following sections.

End-to-end automation database

Perform these steps to verify that the end-to-end automation database and the database tables were created successfully:

1. Ensure that DB2 is running.
2. Open the DB2 Control Center.
3. Navigate to Databases and expand the folder.
4. Expand EAUTODB.
5. Click Tables. The following database tables must be listed:
   - EEZAUTOMATIONACCESS
   - EEZAUTOMATIONRELATION
   - EEZDOMAINSUBSCRIPTION
   - EEZOPERATORDOMAINFILTER
   - EEZOPERATORDOMAINPREFERENCES
   - EEZOPERATORHIDDENDOMAIN
   - EEZRESOURCESUBSCRIPTION

Automation J2EE Framework

Perform these steps to verify that the automation J2EE framework was installed successfully:

1. In a Web browser window, specify the address `http://<your_host_name>:<your_was_admin_console_port>/admin` to display the WebSphere Application Server administrative console.

   Typically, the default port number of the WebSphere Application Server administrative console is 9060.
2. On the login panel, enter the user ID and password of the Integrated Solutions Console administrator.
3. Navigate to Applications —> Enterprise Applications. The list of installed applications must contain the following entries:
   - EventServer
   - EventServerMdb
   - EEZEAR

Verifying that DB2 accepts WebSphere Application Server requests

Perform the following task to verify that DB2 accepts WebSphere Application Server requests:

1. In a Web browser window, specify the address `http://<your_host_name>:<your_was_admin_console_port>/admin` to display the WebSphere Application Server administrative console.

   Typically, the default port number of the WebSphere Application Server administrative console is 9060.
2. On the login panel, enter the user ID and password of the Integrated Solutions Console administrator.

3. Navigate to **Resources —> JDBC providers —> DB2 Universal JDBC Driver (XA) —> Data sources —> EAUTODBDS**. Click **Test connection** to verify that DB2 accepts WebSphere Application Server requests. If the test is successful, the following message comes up:

   ```
   Test connection for data source EAUTODBDS was successful.
   ```

   If the test fails, check if the DB2 port number specified for **EAUTODB** is correct (for more information, refer to the "Troubleshooting" appendix in the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "WebSphere Application Server cannot connect to DB2".

Automation engine

Perform these steps to verify that the automation engine was installed successfully:

1. Issue the command **eezdmn -?**. When the installation of the automation engine was successful, the list of available command options is displayed.

   Note: You can also use any of the other **eezdmn** command options to verify the installation of the automation engine. As long as you do not receive an exception, any message you receive verifies that the automation engine is installed correctly. For a complete list of the **eezdmn** command options, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, chapter "Using the command-line interface of the automation engine".

Operations console

Perform the following steps to verify that the operations console feature was installed successfully:

1. In a Web browser window, specify the address `http://<your_host_name>:<your_isc_port>/ibm/console` to display the Login panel of Integrated Solutions Console. The default ISC port is 8421.

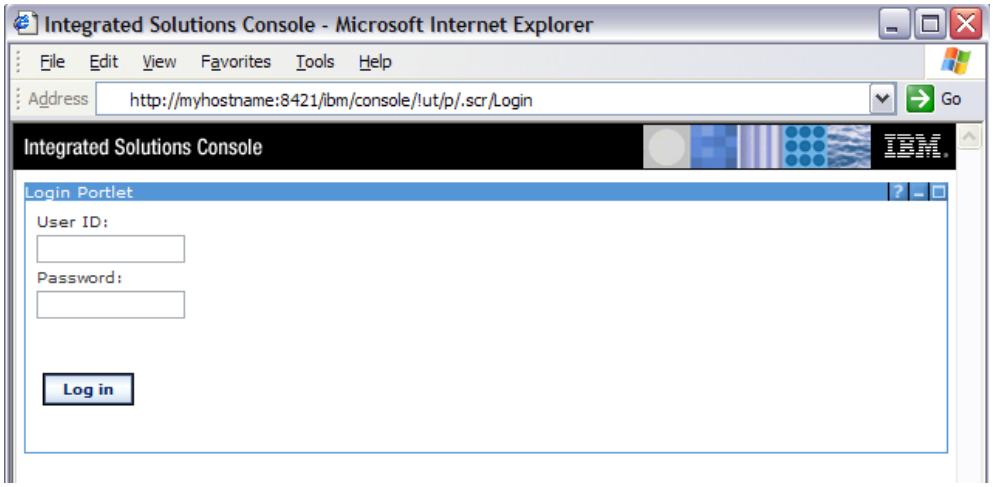


Figure 6. Log in panel of Integrated Solutions Console

2. Type the Integrated Solutions Console user ID and password that you specified during the installation and click **Log in**. The Welcome panel is displayed. On the Work Items page, you should see these entries:
   - Integrated Solutions Console

- Tivoli System Automation for Multiplatforms

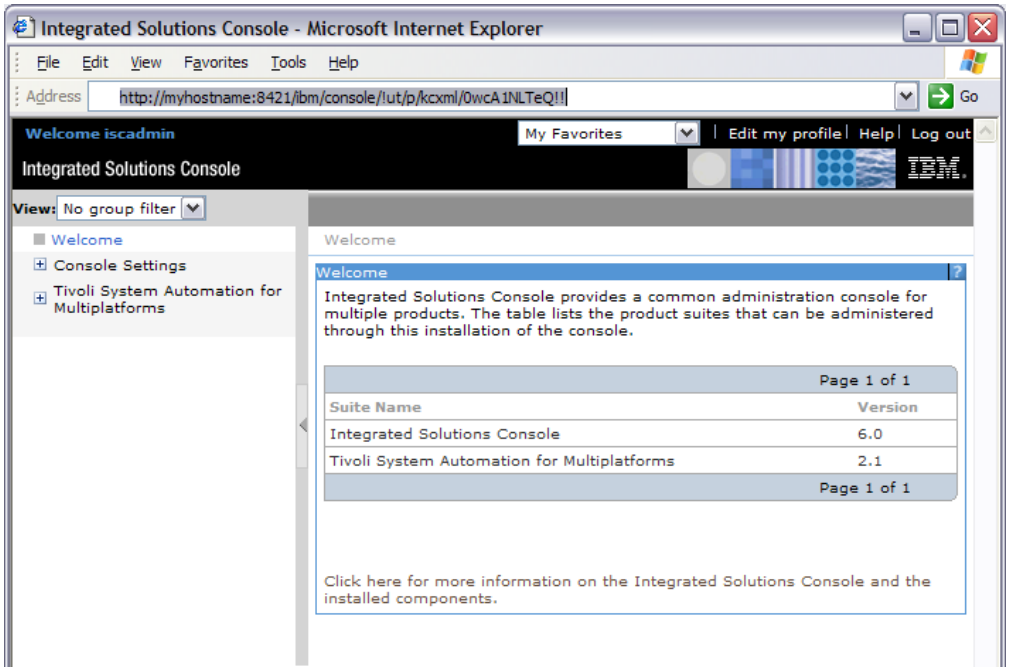


Figure 7. Welcome panel of Integrated Solutions Console

3. Expand the folder Tivoli System Automation for Multiplatforms.
4. Click **SA operations console**. When the panel for connecting to the operations console is displayed, the installation of the operations console was successful.

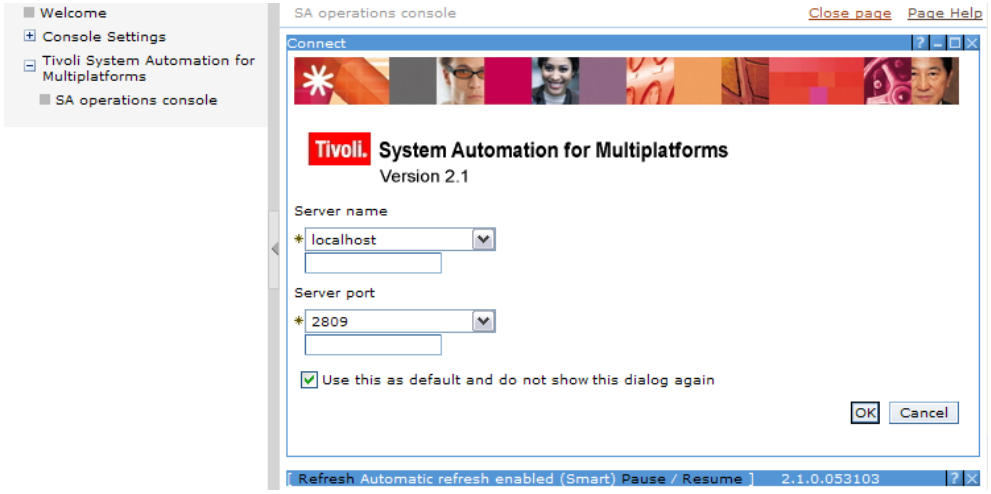


Figure 8. Panel for connecting to the operations console

5. To verify that communication can be established between the operations console and the automation J2EE framework, click **OK** on the Connect panel. The verification is successful when the operations console appears.

Post-installation tasks

When you have verified the installation of the end-to-end management component, you need to perform a number of post-installation tasks:

- When the end-to-end automation component is installed, only the user ID iscadmin is authorized for the operations console, where it has unlimited authority. To create and authorize additional users, you must perform the tasks described the following chapter of the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*:
  - "Post-installation tasks for administrators"
- You must enable the end-to-end automation manager to access the first-level automation domains.

  To do this, you must specify the user credentials for the first-level domains on the User credentials page of the configuration dialog.
  "Invoking the configuration dialog" on page 121 describes how you launch the configuration dialog. For detailed information about the User credentials page, refer to the online help of the configuration dialog.
- Before users can work with the SA for Multiplatforms operations console, you must complete the following tasks regardless of whether the users will be using the operations console in end-to-end automation mode or first-level automation mode:
  - Create and authorize users. For more information, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Creating and authorizing users in Integrated Solutions Console".
- To get end-to-end automation management operational, you must complete the following tasks:
  - Create and activate an automation policy. This is described in the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, in chapters "Creating and modifying policies" and "Working with policies".

Setting up SSL for the operations console

This is an optional post-installation task to allow for secure HTTP transport (HTTPS) between client browsers and the operations console.

To set up SSL for Integrated Solutions Console, perform the following procedure:

1. Configure the Web server to support HTTPS. If you are doing this in a production environment, you need to obtain a certificate from a certificate authority. For testing purposes, you can use IKEYMAN to generate a self-signed certificate. Refer to the WebSphere Application Server documentation for detailed instructions.

   ---

2. Add the virtual host defined in the Web server to the Web server virtual host alias list. Add a host alias for the SSL port that the Web server uses. To create the settings, perform the following steps:
   a. Use a text editor to open the following file:

      ```
      <was_root>/profiles/default/config/cells/<cell>/virtualhosts.xml
      ```

where <was_root> is the WebSphere Application Server installation directory, and <cell> is the name of the WebSphere Application Server cell for the operations console installation.

---

b. Add the following element before the ending element </host:VirtualHost> for the virtual host named default_host. Add the element to the list of aliases:

```
<aliases xmi:id="HostAlias_x" hostname="*" port="alias_port"/>
```

where x is the next number in the HostAlias sequence and alias_port is the value specified for the HTTPS Port parameter.

---

c. Save the file.

---

3. Edit the ConfigService.properties file in

```
isc_runtime_root/PortalServer/shared/app/config/services
```

where isc_runtime_root is the operations console installation directory.

Change the following parameters:

```
redirect.login.ssl = true
redirect.logout.ssl = true
host.port.https = alias_port
```

where alias_port is the port number used for the virtual host alias that you specified in step 2 on page 113.

---

4. Set the security constraints for the console URL. To do so, perform the following steps:

a. Use an editor to open the file web.xml. It is located in the following directory:

```
<was_root>/profiles/default/config/cells/<cell>/
          applications/wps.ear/deployments/wps/wps.war/WEB-INF
```

where <was_root> is the WebSphere Application Server installation directory, and <cell> is the name of the WebSphere Application Server cell for the operations console installation.

---

b. In the web.xml file, change the <security-constraint> element for the console URL to use HTTPS as shown in the following example:

```
<security-constraint id="SecurityConstraint_1">
     <web-resource-collection id="WebResourceCollection_1">
        <web-resource-name></web-resource-name>
        <url-pattern>/console/*</url-pattern>
        <http-method>DELETE</http-method>
        <http-method>GET</http-method>
        <http-method>POST</http-method>
        <http-method>PUT</http-method>
    </web-resource-collection>
     <auth-constraint id="AuthConstraint_1">
        <description></description>
        <role-name>All Role</role-name*gt;
     </auth-constraint>
     <user-data-constraint id="UserDataConstraint_4">
```

```
            <transport-guarantee>CONFIDENTIAL</transport-guarantee>
            <!-- replace NONE with CONFIDENTIAL  -->
        </user-data-constraint>
    </security-constraint>
```

5. From a command prompt, change to the following directory:
   `<isc_runtime_root>/PortalServer/config`

   where `<isc_runtime_root>` is the operations console installation directory.

6. Edit the file `wpconfig.properties` and set the PortalAdminPwd parameter to your console administrator user ID's password.

7. Run the following command from the command line:
   `WPSconfig.bat|sh init action-deploy-setupisc-ssl`

8. From a command prompt, change to the following directory:
   `<isc_runtime_root>/PortalServer/bin`

   where `<isc_runtime_root>` is the operations console installation directory.

9. Run the following command from the command line:
   Windows:
   `stopISC.bat ISC_Portal iscadmin iscpass`
   AIX, Linux:
   `./stopISC.sh ISC_Portal iscadmin iscpass`

   where `iscadmin` is the console administrator user ID and `iscpass` is the console administrator user ID's password.

10. Run the following command from the command line:
    Windows:
    `startISC.bat ISC_Portal`
    AIX, Linux:
    `./startISC.sh ISC_Portal`

11. Test your changes by launching the home page of the console in a Web browser. The login page that is displayed is not secure. However, when you click **Log in**, the credentials are encrypted and the session is directed to a secure connection.

Modifying the LTPA settings

After the installation of the end-to-end automation management component, you should check whether the LTPA settings are appropriate for your environment.

During installation, the following LTPA parameters are automatically set in WebSphere Application Server:

- LTPA Password is set to the password of the Integrated Solutions Console administrator user ID

- LTPA Timeout is set to 120 minutes

  LTPA Timeout is a security-related timeout. Because this timeout is absolute, a user will be logged out and forced to log in to Integrated Solutions Console again when the LTPA timeout is reached even if the user is working with the operations console at the time.

To change the LTPA settings (for example, password and timeout) you use the WebSphere Application Server administrative console. On the administrative console, select **Security —> Global Security —> Authentication mechanism —> LTPA**.

Modifying the HTTP session timeout

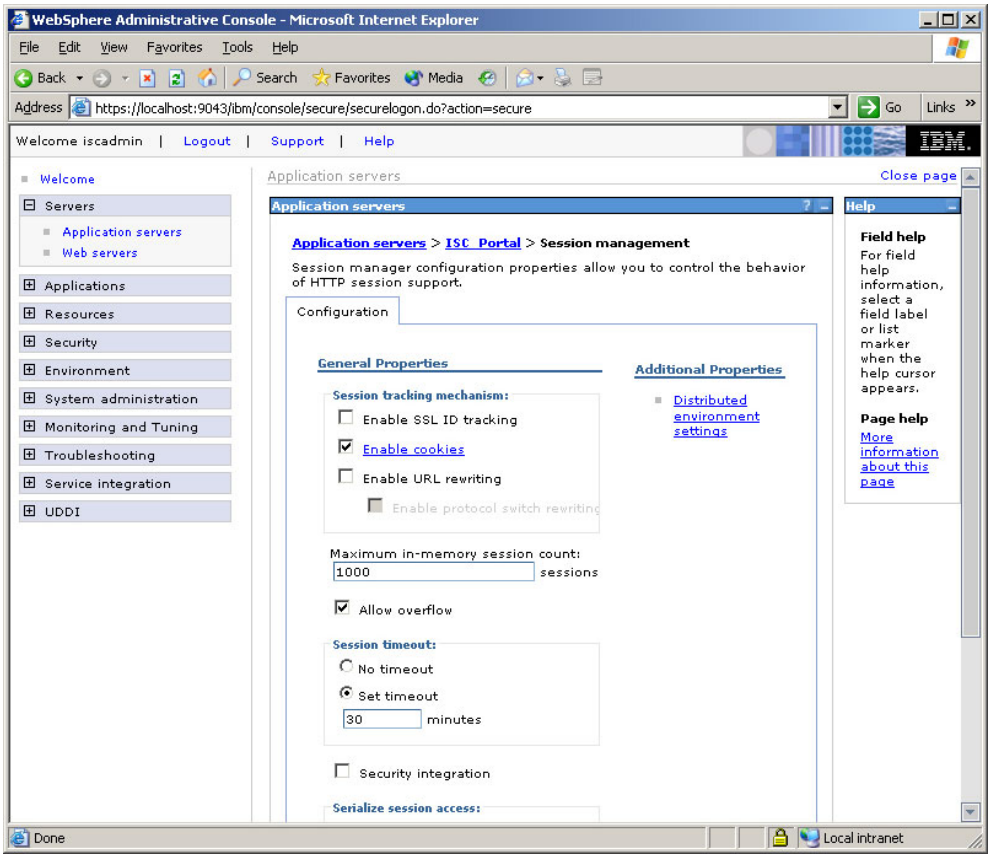
After the installation of the end-to-end automation management component, you should check whether the setting of the HTTP session timeout is appropriate for your environment.

The HTTP session time is an activity timeout. The value to which the HTTP session timeout is set defines after how many minutes of inactivity a user is logged out automatically.

During installation, the HTTP session timeout is set to 30 minutes.

To change the value, you use the WebSphere Application Server administrative console.

On the administrative console, select **Servers —> Application servers —> ISC_Portal —> Web container settings —> Session Management**:



Configuring how many users can connect to the automation manager using the operations console

During the installation of the end-to-end automation management component, a default value is set that defines how many users can simultaneously connect to the automation manager using the operations console. You can change the current setting by changing the **Maximum connections** value for the EEZTopicConnectionFactory from the WebSphere Application Server administrative console (**Resources —>Resource adapters —> SIB JMS Resource Adapter —>J2C connection factories —> EEZTopicConnectionFactory —> Connection pool properties**).

If **Maximum connections** is set to 0, the number of concurrent connections that can be established is allowed to grow infinitely. If the specified number of maximum connections has been reached, the next connection attempt using the operation console will show the following error message:

```
EEZU0011E:
Unable to set up the event path between the operations console
and the management server:
CWSIAD005E: The JCA runtime failed to allocate a connection.
```

Chapter 8. Upgrading the end-to-end automation management component from release 2.1

If the end-to-end automation management component 2.1 is already installed, you can upgrade to release 2.2. The minimum release level required for upgrading is 2.1.1.0. If a lower release level is installed, you must first upgrade to level 2.1.1.0 by installing service.

To perform the upgrade to release 2.2, you use the following files:

- **AIX/Linux:** `update`
- **Windows:** `update.exe`

To find the `update` file on the product CD or in the product archive, refer to the description of the `setup` file in "Packaging" on page 59. The location of the `update` and `setup` files is identical.

To launch the update wizard, invoke the `update` file. Follow the instructions on the wizard panels to upgrade the end-to-end automation management component to release 2.2. No further migration actions are required.

Chapter 9. Configuring the end-to-end automation manager

The basic configuration of the end-to-end automation manager is performed during the installation of the end-to-end automation management component. The configuration properties are in properties files. To browse or change the properties, you use the configuration dialog. You should not edit the properties files.

This chapter describes how you invoke the dialog and provides an overview of the pages of the dialog. Detailed information about the configuration dialog and the configuration properties is available in the online help of the dialog.

Invoking the configuration dialog

Before you begin:

The user ID you use to invoke the dialog must meet the following requirements:

- It must be in same group as the user ID you used for installing the end-to-end automation management component. The group permissions for `cfgeezdmn.sh` must be set to EXECUTE.
- The user ID must have read-write permissions on the following directory:
  - **Windows:** `<EEZ_INSTALL_ROOT>/cfg`
  - **AIX and Linux:**`/etc/<EEZ_INSTALL_ROOT>/cfg`

Perform the following step to invoke the configuration dialog:

1. Log in to the system where end-to-end automation management is installed.

---

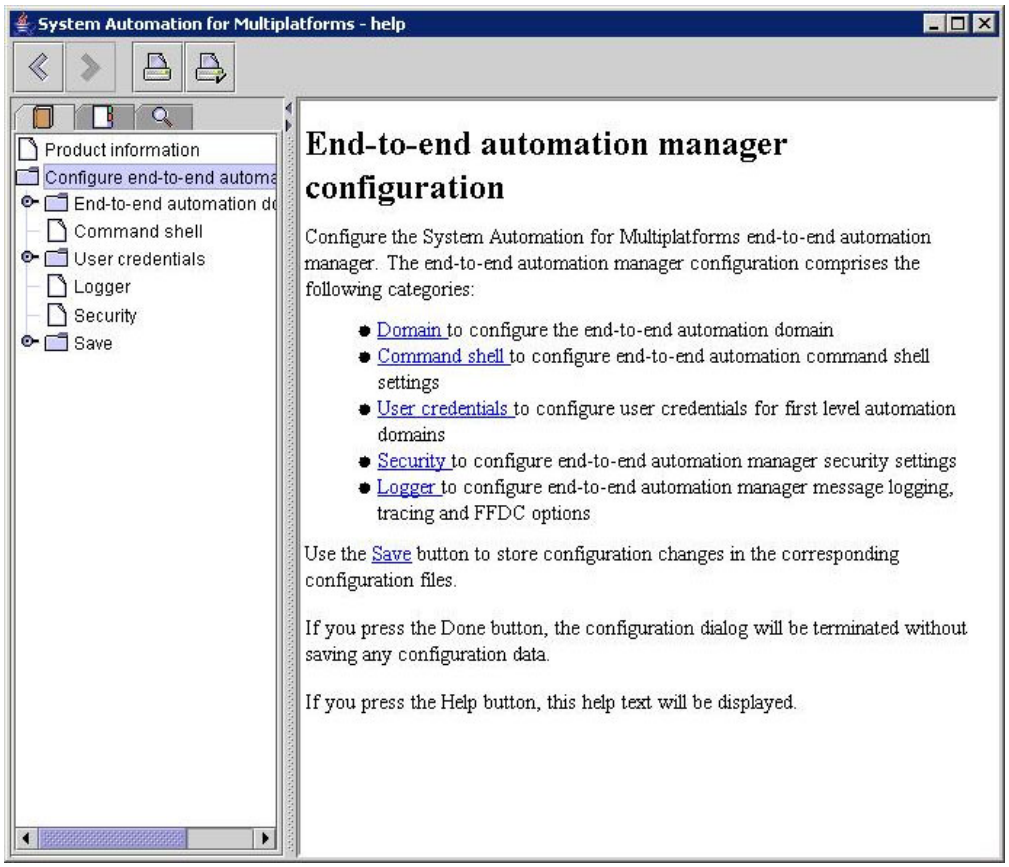
2. To launch the dialog, enter the following command:
   - **Windows**: `cfgeezdmn.bat`
   - **AIX** and **Linux**: `cfgeezdmn`

   The configuration dialog is displayed.

After you have changed any of the configuration properties, you must activate the new settings by invoking the command **eezdmn** with the option -reconf. For more information about the command **eezdmn** and its options, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*, section "Using the command-line interface of the automation engine".

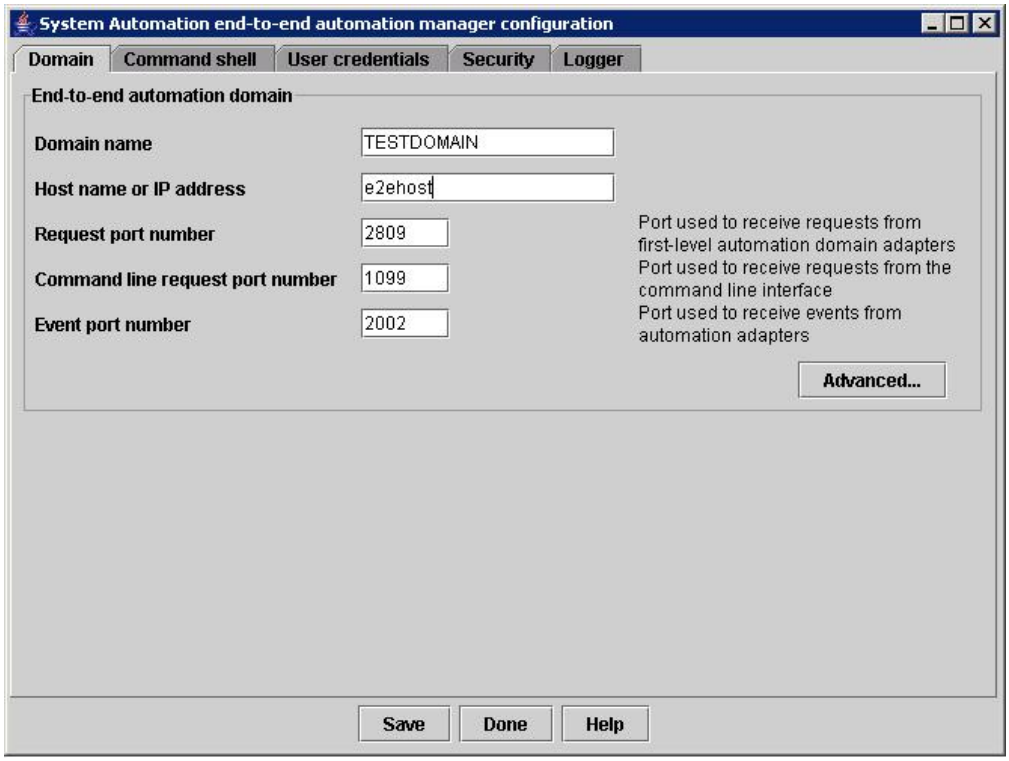
Using the configuration dialog

The following sections provide an overview of the pages that are available in the configuration dialog. Detailed information about the configuration dialog and the properties you can configure is available in the online help of the dialog. Click the **Help** button on a page of the dialog to launch the online help:



Domain page

Use the page to browse or change the configuration properties of the end-to-end automation domain.



Fields on the Domain page:

Domain name
The name of the end-to-end automation domain. The name specified here must be identical with the name specified in each XML policy file for the domain in the element `<AutomationDomainName>`. The characters used for the domain name are limited to the following ASCII characters: A-Z, a–z, 0-9, . (period), and _(underscore).

Host name or IP address
Name or IP address of the system that host the end-to-end automation manager.

Request port number
The port on which the automation engine receives all requests from the automation manager.

Command line request port number
The port on which the automation engine receives command line interface requests.

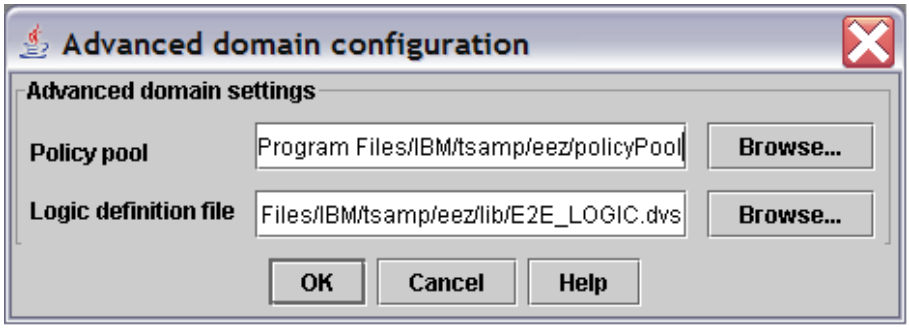
Event port number
The port on which the EIF message converter listens for events from the first-level automation domains. The port number specified here must match the port number specified in the properties files of the automation adapters on the first-level automation domains (property `eif-send-to-port`).

For SA for Multiplatforms, this is the Event port specified in the adapter configuration dialog.

Buttons on the Domain page:

Advanced

Click **Advanced** to bring up the Advanced domain settings panel:



Use the Advanced panel to specify the paths to the policy pool directory and to the logic definition file.

When you click **Browse**, you can select the paths in the selection panel that appears.

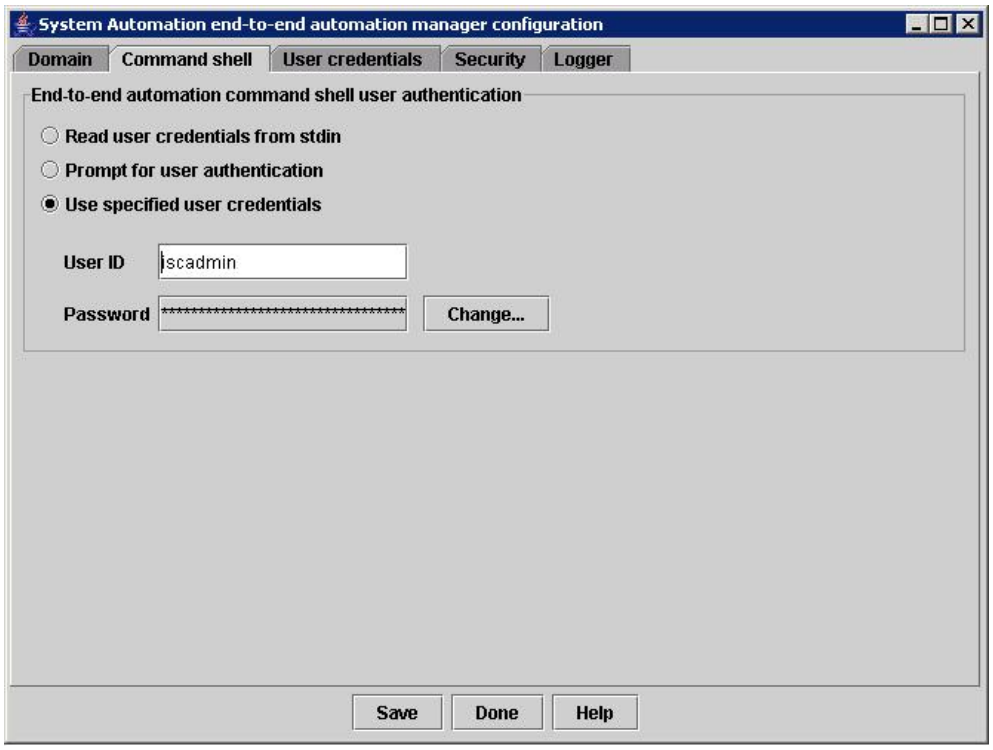
The paths to the policy pool directory and to the logic definition file must follow the same naming rules as the Installation Directory Name (see Table 37 on page 80).

Save Click **Save** to save your changes.

Done Click **Done** to close the dialog.

Help Click **Help** to open the dialog help.

Command shell page



The end-to-end automation manager requires authentication when a user invokes the end-to-end automation manager command shell. By default, users are always prompted for their user credentials. On the Command shell page you have the choice between these authentication modes:

Read user credentials from stdin
In this mode, users must always specify their user credentials in the shell window.

Prompt for user authentication
In this mode, users are always prompted for their credentials unless they specify them when they invoke the command shell.

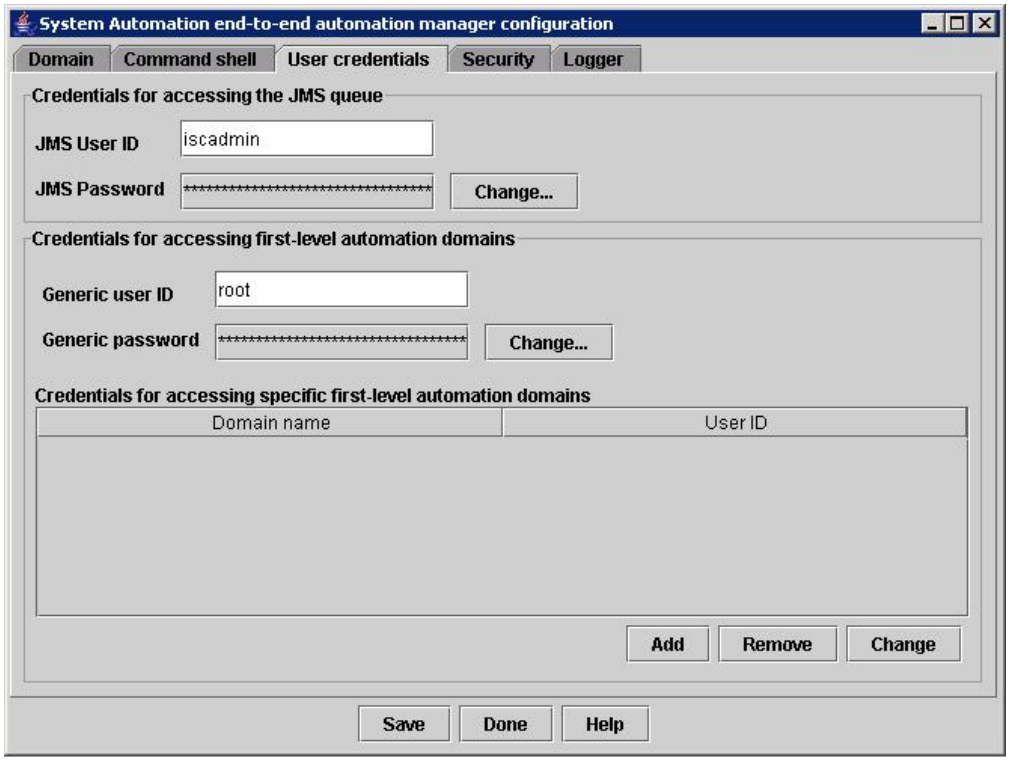
Use specified user credentials
In this mode, a shared user ID is used for authentication, which prevents users from being prompted for their credentials when they invoke the command shell.

You specify the shared user ID and the corresponding password in the fields **User ID** and **Password**. Note that only the following ASCII characters can be used for the user ID: A-Z, a–z, 0-9, and _(underscore).

To change the password, click **Change**.

User credentials page

Use the page to browse or change the user credentials of the end-to-end automation manager. The automation manager uses these credentials to authenticate itself. The characters used for all credentials entered on this page are limited to the following ASCII characters: A-Z, a–z, 0-9, and _(underscore).



Fields on the User credentials page:

JMS User ID
The user ID that is used to access the JMS queue of the end-to-end automation manager.

JMS Password
The password for the JMS user ID.

Generic user ID
The user ID the automation manager uses to authenticate itself to a first-level automation domain when no credentials are specified for the domain in **Credentials for accessing specific first-level automation domains**.

Generic password
The password for the generic user ID.

Credentials for accessing specific first-level automation domains
User IDs and passwords for specific domains. Use the **Add**, **Remove** and **Change** buttons to create or modify the credentials of a first-level automation domain.

Buttons on the User credentials page:

Change
Click Change to open a dialog on which you can change the password.

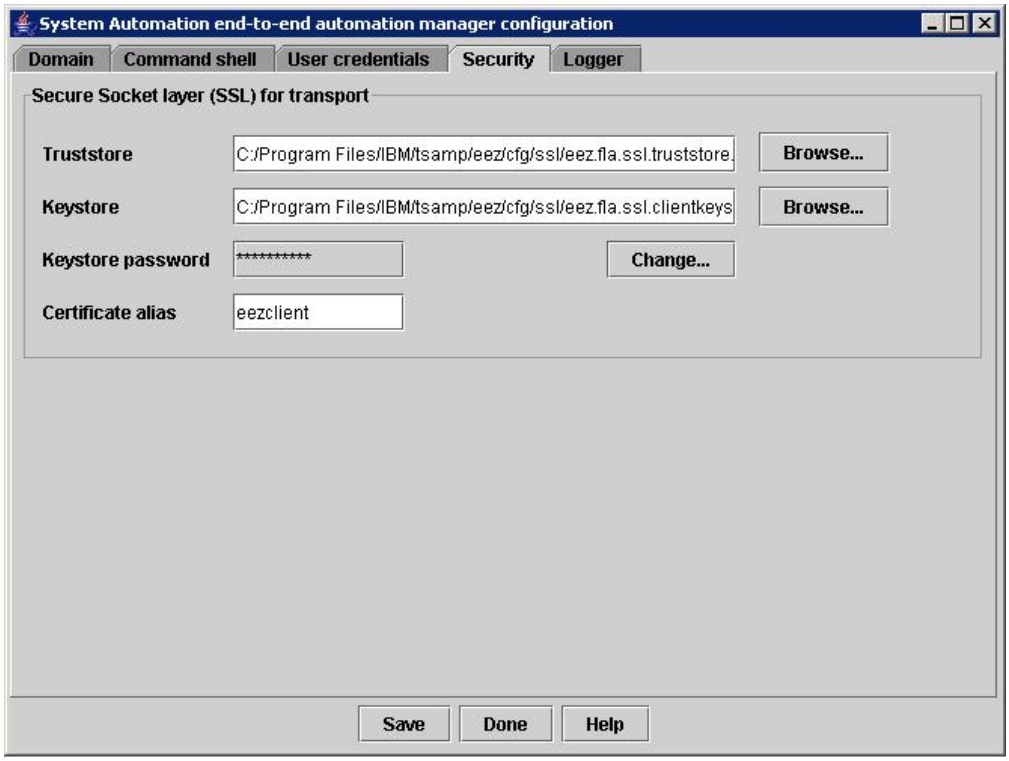
Save Click **Save** to save your changes.

Done Click **Done** to close the dialog.

Help Click **Help** to open the dialog help.

Security page

Use the page to browse and change the configuration properties for the SSL connection to the first-level automation domains.



Fields on the Security page:

Truststore
The fully qualified file name of the truststore file that is used for SSL. The truststore path name must follow the same naming rules as the Installation Directory Name (see Table 37 on page 80).

Keystore
The fully qualified file name of the keystore file that is used for SSL. The keystore path name must follow the same naming rules as the Installation Directory Name (see Table 37 on page 80).

Keystore password
The password of the keystore file.

Certificate alias
The alias name of the certificate to be used by the server. The characters used for the certificate alias are limited to the following ASCII characters: A-Z, a–z, 0-9, and _(underscore).

Buttons on the Security page:

Browse
Click **Browse** to display a panel where you can select the file.

Change
Click **Change** to display a panel where you can change the keystore password.

Save Click **Save** to save your changes.

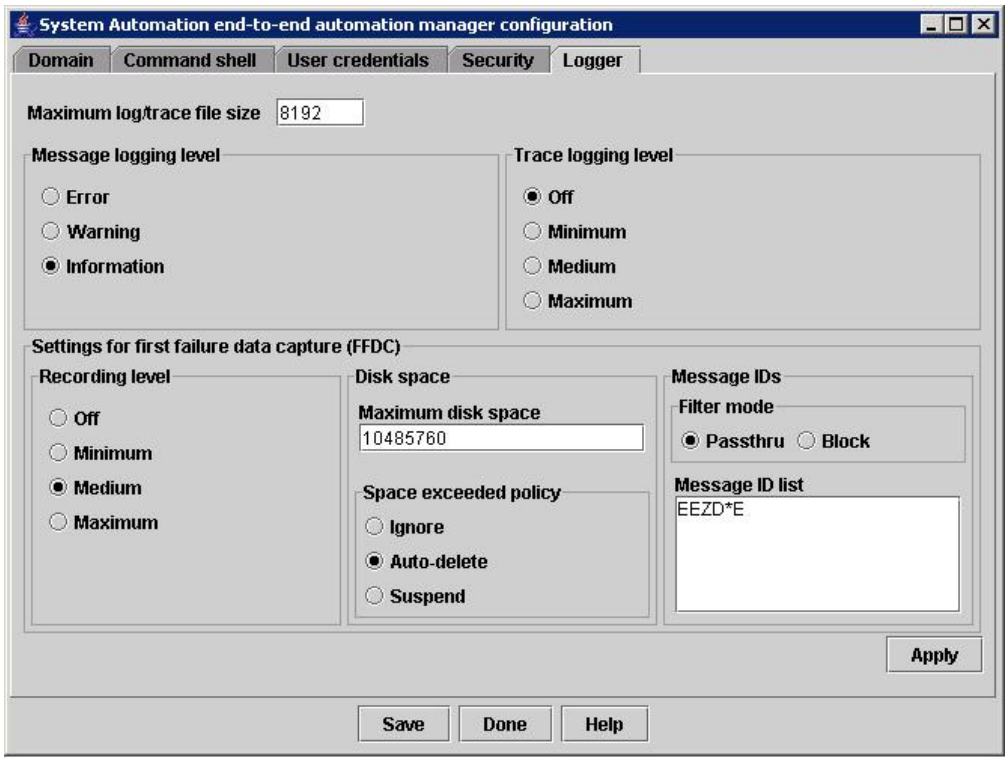
Done Click **Done** to close the dialog.

Help Click **Help** to open the dialog help.

Logger page

Use the Logger page to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the properties file.



On the Logger page, you can perform the following tasks:

Changing the settings permanently

Perform these steps:

1. Make the required changes on the page.
2. Click **Save**.

Results:

The settings in the properties file are updated. You must restart the automation engine using the command **eezdmn -reconf** for the changes to take effect.

Changing the settings temporarily

Perform these steps after ensuring that the automation engine is running:

1. Make the required changes on the page.
2. Click **Apply**.

Results:

The new settings take effect immediately. They are not stored in the properties file. If the automation engine is not running, you receive an error message.

Reverting to the permanent settings

Perform the following steps to revert to the permanent settings in the properties file, or when you are unsure which settings are currently active:

1. Invoke the configuration dialog and open the Logger page. The Logger page displays the values that are currently set in the properties file.
2. Click **Apply** to activate the settings.

Results:
The settings take effect immediately.

Controls and fields on the Logger page:

Maximum log/trace file size
: The file size in kilobytes.

Message logging level:

Error
: Logs messages on the error level.

Warning
: Logs messages on the error and warning levels.

Information
: Logs messages on the error, warning and informational levels.

Trace logging level:

Off
: Collects no trace information.

Minimum
: Collects trace information on the error level.

Medium
: Collects trace information on the error and warning levels.

Maximum
: Provides the message and trace logs and collects additional information on the error, warning, and informational level.

First failure data capture (FFDC) settings:

- Recording level:

  Off
  : Collects no FFDC information.

  Minimum
  : Provides the message and trace logs and collects additional information on the error level.

  Medium
  : Provides the message and trace logs and collects additional information on the error and warning level.

  Maximum
  : Provides the message and trace logs and collects additional information on the error, warning, and informational level.

- Disk space:

  Maximum disk space
  : Specifies the maximum disk space in bytes used by FFDC traces which are written into the FFDC trace directory. The default space is 10485760 (10MB).

  Space exceeded policy
  : Select what to do if the maximum disk space is exceeded.

- Message IDs:

  Filter mode
  : Initiates the tracing of FFDC data depending on the message IDs listed in 'Message ID list'.

Message ID list:

Specifies the message IDs which cause the tracing of the FFDC data. Wildcards like *E, meaning all error messages, are allowed.

Chapter 10. Installing and uninstalling service

Installing service

Installing service means applying corrective service fix packs to release 2.2.0 of IBM Tivoli System Automation for Multiplatforms or upgrading the software release level from release 2.2.0. In this documentation, the service fix packs that you use for updating the end-to-end automation management component are referred to as product fix packs.

Note: For some product fix packs, specific interim fixes or fix packs for WebSphere Application Server are required. In such a case, these fixes are available at the location from which you download the product fix pack. They must be installed **before** the product fix pack is installed. Detailed instructions for installing the fixes are provided in the release notes.

Do not install any WebSphere Application Server interim fixes or fix packs that are not mentioned in the release notes unless you are explicitly advised to do so by Tivoli System Automation support.

Product fix packs and interim fixes are delivered as:

- Self-extracting archives for Windows and AIX
- Archives in TAR-format for Linux

Where to obtain fix packs

Read the release notes to find out which fix packs are required for a release update. The release notes are available on the IBM Tivoli System Automation home page at:

`www.ibm.com/software/tivoli/products/sys-auto-linux/`

On the page, click **Technical Documentation** to display the list of available documentation.

The archives can be downloaded from the IBM Tivoli System Automation support site at:

`www.ibm.com/software/sysmgmt/products/support/IBMTivoliSystemAutomationforLinux.html`

Archive naming conventions

Naming convention for product fix pack archives:

`2.2.0-TIV-SAE2E-<platform>-FP<fix_pack_number>.<archive_type>`

Naming convention for WebSphere Application Server interim fix archives:

`2.2.0-TIV-SAWAS-<platform>-FP<fix_pack_number>.<archive_type>`

where

- `<platform>` represents the platform on which the end-to-end automation management component is installed
- `<fix_pack_number>` represents the fix pack number
- `<archive_type>` represents the platform-specific file extension of the archive

Example:
This is the tar archive that is used to install product fix pack 1 for IBM Tivoli System Automation for Multiplatforms 2.2 on Linux on POWER platforms:

`2.2.0-TIV-SAE2E-PPC-FP0001.tar`

Naming conventions of the update installer location

The location at which you find the update wizard program for installing the product fix pack after unpacking an archive has the following syntax:

`EEZ22<mf>E2E<platform>/<platform>/<update_wizard_file>`

where

- `<mf>` represents modification level and fix level. For example, for fix pack 2210, the directory is named `EEZ2210`.
- `<platform>` represents the platform on which the end-to-end automation management component is installed
- `<update_wizard_file>` represents the update wizard program you use to install the product fix pack

Example:
This is where you find the update wizard after the Linux on POWER archive for fix pack 1 for SA for Multiplatforms 2.2 is unpacked:

`EEZ2210E2EPPC/ppc/update`

Usage instructions for the platform-specific archives

These are the archives for applying service to the end-to-end automation management component.

Windows

Table 46. Windows platforms

Archive name	Description
`2.2.0-TIV-SAE2E-WIN-FP<fix_pack_number>.exe`	The archive is self-extracting. This is where you find the update installer program after unpacking the product fix pack archive: `EEZ22<mf>E2EWindows/Windows/update.exe`
`2.2.0-TIV-SAWAS-WIN-FP<fix_pack_number>.exe`	The archive is self-extracting. For information about installing WebSphere Application Server interim fixes, refer to the release notes.

AIX

Table 47. AIX platforms

Archive name	Description
`2.2.0-TIV-SAE2E-AIX-FP<fix_pack_number>.bin`	The archive is self-extracting. This is where you find the update installer program after unpacking the product fix pack archive: `EEZ22<mf>E2EAIX/AIX/update`

Table 47. AIX platforms (continued)

Archive name	Description
2.2.0-TIV-SAWAS-AIX-FP<fix_pack_number>.bin	The archive is self-extracting. For information about installing WebSphere Application Server interim fixes, refer to the release notes.

Linux on System x

Table 48. Linux on System x

Archive name	Description
2.2.0-TIV-SAE2E-I386-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: EEZ22<mf>E2EI386/i386/update
2.2.0-TIV-SAWAS-I386-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. For information about installing WebSphere Application Server interim fixes, refer to the release notes.

Linux on POWER

Table 49. Linux on POWER

Archive name	Description
2.2.0-TIV-SAE2E-PPC-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: EEZ22<mf>E2EPPC/ppc/update
2.2.0-TIV-SAWAS-PPC-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. For information about installing WebSphere Application Server interim fixes, refer to the release notes.

Linux on System z

Table 50. Linux on System z

Archive name	Description
2.2.0-TIV-SAE2E-S390-FP<fix_pack_number>.tar	For extracting the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: EEZ22<mf>E2ES390/s390/update
2.2.0-TIV-SAWAS-S390-FP<fix_pack_number>.tar	For information about installing WebSphere Application Server interim fixes, refer to the release notes.

Steps for installing a product fix pack

Before you begin:

- Product fix packs are always cumulative.
- Release 2.2.0 must be installed before any product fix pack can be installed.
- To install a product fix pack, you must have root authority.

To install a product fix pack, perform the following steps:

1. Check the release notes to find out which archives are required.
2. Download the archives from the SA for Multiplatforms support site:
   - Archives for WebSphere Application Server fixes:
     Follow the download instructions provided in the release notes.
   - Archives for product fix packs:
     Typically, one archive is provided for each platform. Download the archive to a temporary directory.
3. If fixes for WebSphere Application Server must be installed, unpack and install the fixes as described in the release notes.
4. Unpack the product fix pack archive to a temporary directory. For information about how to unpack the archive for your platform, refer to "Usage instructions for the platform-specific archives" on page 132.
5. Before performing the subsequent steps, check the release notes for additional or deviating installation instructions.
6. Change to the directory in which the update wizard program is located. For information on where to find the update wizard program, refer to "Usage instructions for the platform-specific archives" on page 132.
7. Launch the update wizard.

   When the wizard is launched successfully, the Welcome panel appears.
8. Follow the instructions on the wizard panels to install the product fix pack.

Uninstalling service

Uninstalling service means that you have to uninstall the complete end-to-end automation management component as described in Chapter 11, "Uninstalling the end-to-end automation management component," on page 135. After the uninstall procedure is complete, you need to reinstall the component and install the required service level (fix pack level).

Chapter 11. Uninstalling the end-to-end automation management component

This section describes how to uninstall the end-to-end automation management component. An uninstallation program is provided that removes the components that were installed by the installation wizard.

Launching the graphical uninstallation program on Windows

To launch the uninstallation program on Windows, you can either issue the command `<EEZ_INSTALL_ROOT>/_uninst/uninstaller.exe` at a command prompt or perform the following steps:

1. Open the Control Panel (**Start —> Settings —> Control Panel**).

2. On the Control Panel, open **Add/Remove Programs**.

3. On the Add/Remove Programs panel, select **End-to-End Automation Management component of Tivoli System Automation for Multiplatforms** and click **Change/Remove**. This brings up the Welcome panel of the uninstallation program.

Launching the graphical uninstallation program on AIX and Linux

To launch the uninstallation program on AIX and Linux, enter the following command in a shell:

```
<EEZ_INSTALL_ROOT>/_uninst/uninstaller.bin
```

This brings up the Welcome panel of the uninstallation program.

Using the uninstallation program

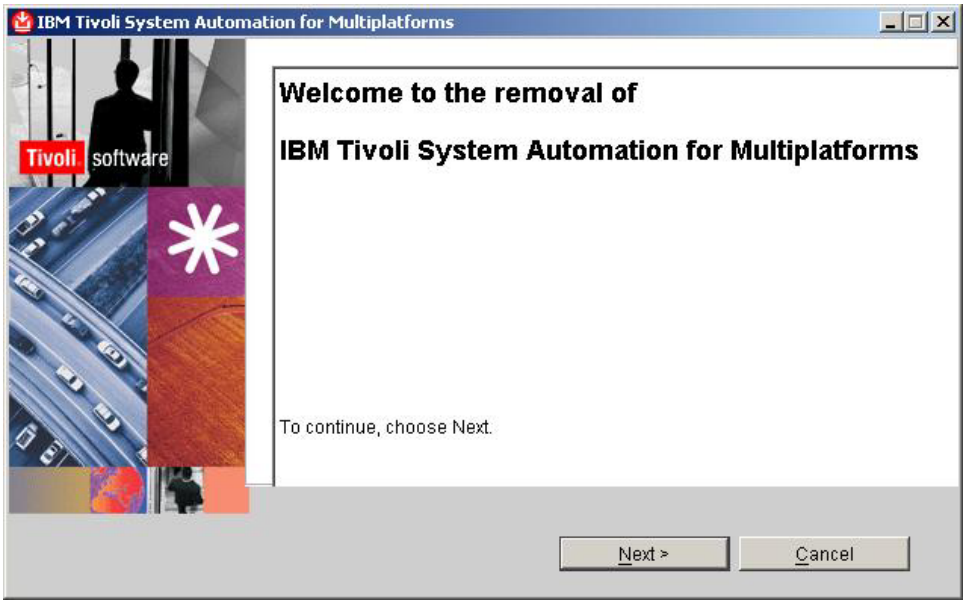
Before you begin:

- Before starting the uninstallation of the end-to-end automation management component, make sure that the automation engine, the Integrated Solutions Console server, and the WebSphere Application Server "server1" are stopped. For information on how to stop the components, refer to the following sections in the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*:
  - To stop the automation engine, refer to section "Using the command-line interface of the automation engine".
  - To stop the Integrated Solutions Console server, refer to section "Starting and stopping the operations console".
  - To stop WebSphere Application Server, refer to section "Starting and stopping WebSphere Application Server".
- During uninstallation, a number of panels may appear prompting you to confirm that specific files are to be deleted. Make sure that the files should be deleted before confirming the deletion.

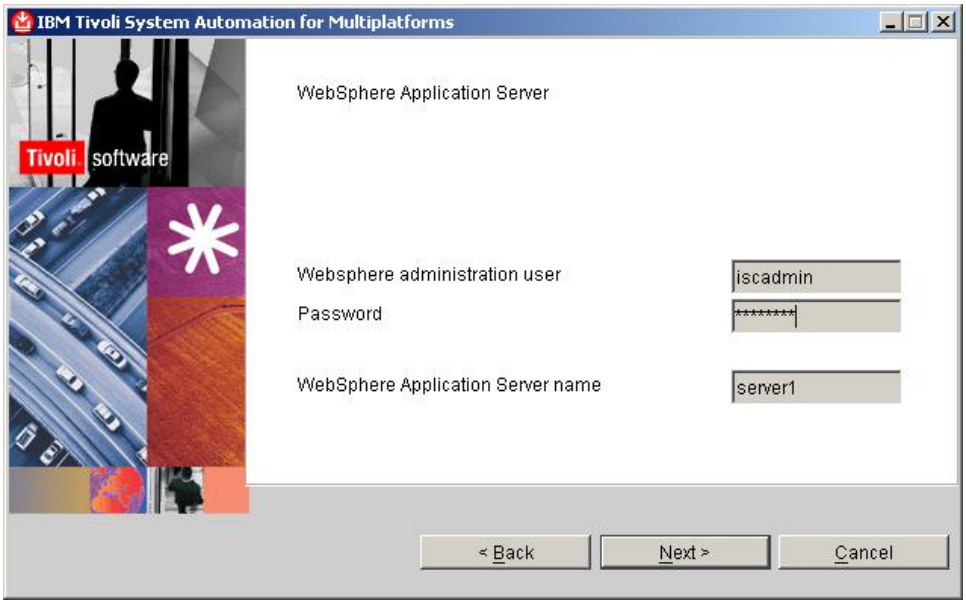
Perform the following steps to uninstall the end-to-end automation management component:

1. Launch the uninstallation program as described in the sections above.

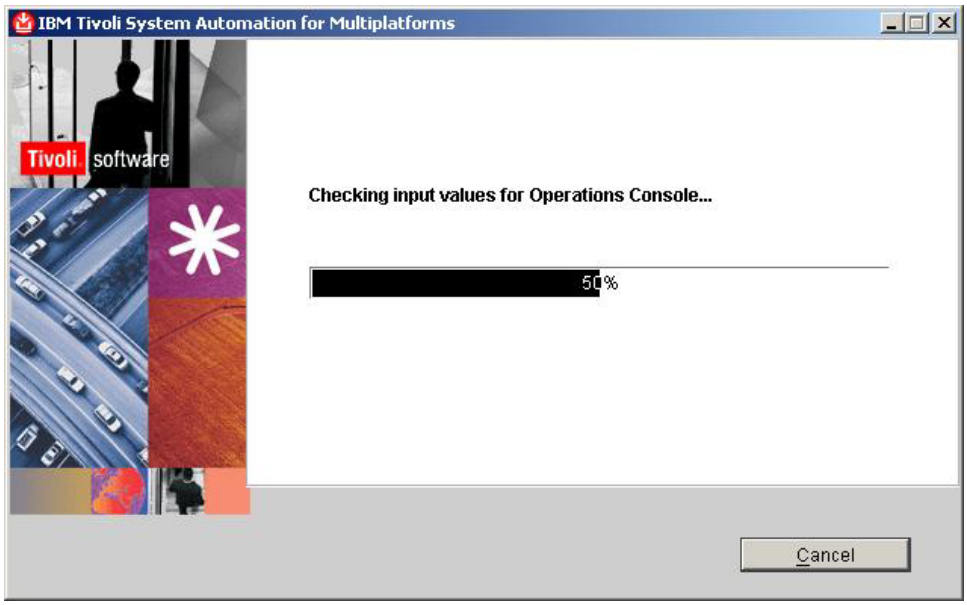
2. On the Welcome panel of the uninstallation program, click **Next**.



3. In the fields **WebSphere administration user** and **Password**, type the user ID and password of the Integrated Solutions Console administrator user. Click **Next**.

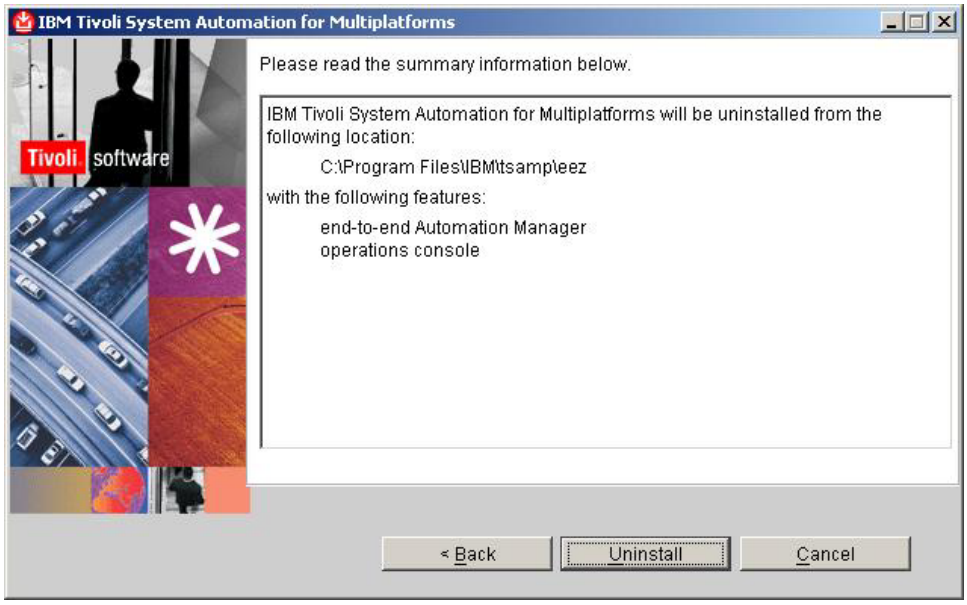


4. Some information panels are displayed while the uninstallation program checks your system for the information it needs for the uninstall. The following figure shows an example.

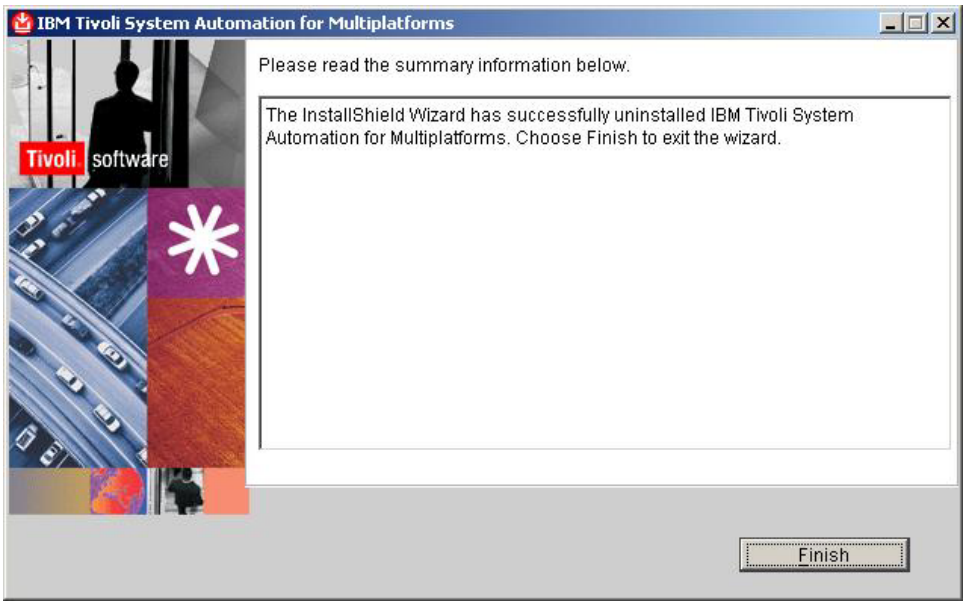


5. When all required information has been detected, a confirmation panel appears. To start the uninstallation, click **Uninstall**.

   Note that the uninstallation can take considerable time to complete. Use the progress indicators that are displayed throughout the uninstallation to monitor the progress.



6. When the uninstallation is complete, a summary panel is displayed. On the panel, click **Finish**.



Note: If problems were encountered during the uninstallation, an error panel appears before the summary panel is displayed. In such a case, do this:

- On the error panel, click **Next**.
- On the summary panel that appears, click **Finish**.
- Use the log files that were created by the uninstallation program to analyze and resolve the problems. For more information on the log files, refer to "Using the installation log files" on page 210.

Part 3. Installing and configuring the end-to-end automation adapters

Chapter 12. Overview

The chapters in this section describe how you install and configure the automation adapters for IBM Tivoli System Automation for Multiplatforms:

- Chapter 13, "Configuring the end-to-end automation adapter of the base component of IBM Tivoli System Automation for Multiplatforms," on page 143 describes how you configure the automation adapter for the base component. The adapter is installed automatically when you install the base component.
- Chapter 14, "Installing and configuring the HACMP adapter," on page 161 describes how you install and configure the HACMP adapter, which is shipped with the end-to-end automations management component.
- Chapter 15, "Installing and configuring the MSCS adapter," on page 177 describes how you install and configure the HACMP adapter, which is shipped with the end-to-end automations management component.

Chapter 13. Configuring the end-to-end automation adapter of the base component of IBM Tivoli System Automation for Multiplatforms

The following sections describe how to configure the end-to-end automation adapter of the base component.

You need to configure the end-to-end automation adapter when you use the end-to-end automation management component of IBM Tivoli System Automation for Multiplatforms or if you want to operate automated resources directly from an operations console. (For information about the end-to-end automation management component, see the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*).

Note: To use the base component operations console or end-to-end automation management, base component object names and their text fields, for example, group names, resource names, and descriptions, must not contain the following characters: **"** (double quotation mark), **'** (single quotation mark), **;** (semicolon), **$** (dollar sign), / (slash)

End-to-End Automation can be used to automate the operation of resources within heterogeneous environments (called first level automation domains) that each have a local automation technology of their own. A first level automation domain is defined as resources managed by IBM Tivoli System Automation. Each first-level domain is connected to the end-to-end automation manager or an operations console by an end-to-end automation adapter.

The purpose of the automation adapter is to

- Monitor resources within its first-level automation domain
- Propagate resource attribute changes to the end-to-end automation manager.
- Start and stop resources within the first-level automation domain by requests of the end-to-end automation manager or an operator.
- Provide information for resources that are available within the first-level automation domain.

The end-to-end automation adapter uses the Tivoli Event Integration Facility (EIF) to communicate with the end-to-end automation manager.

The online helps provided with the System Automation for Multiplatforms end-to-end automation adapter configuration dialog also provide useful information about using and configuring the end-to-end automation adapter.

The following figure shows in which environments the end-to-end automation adapter can work and what needs to be configured for the end-to-end automation adapter:

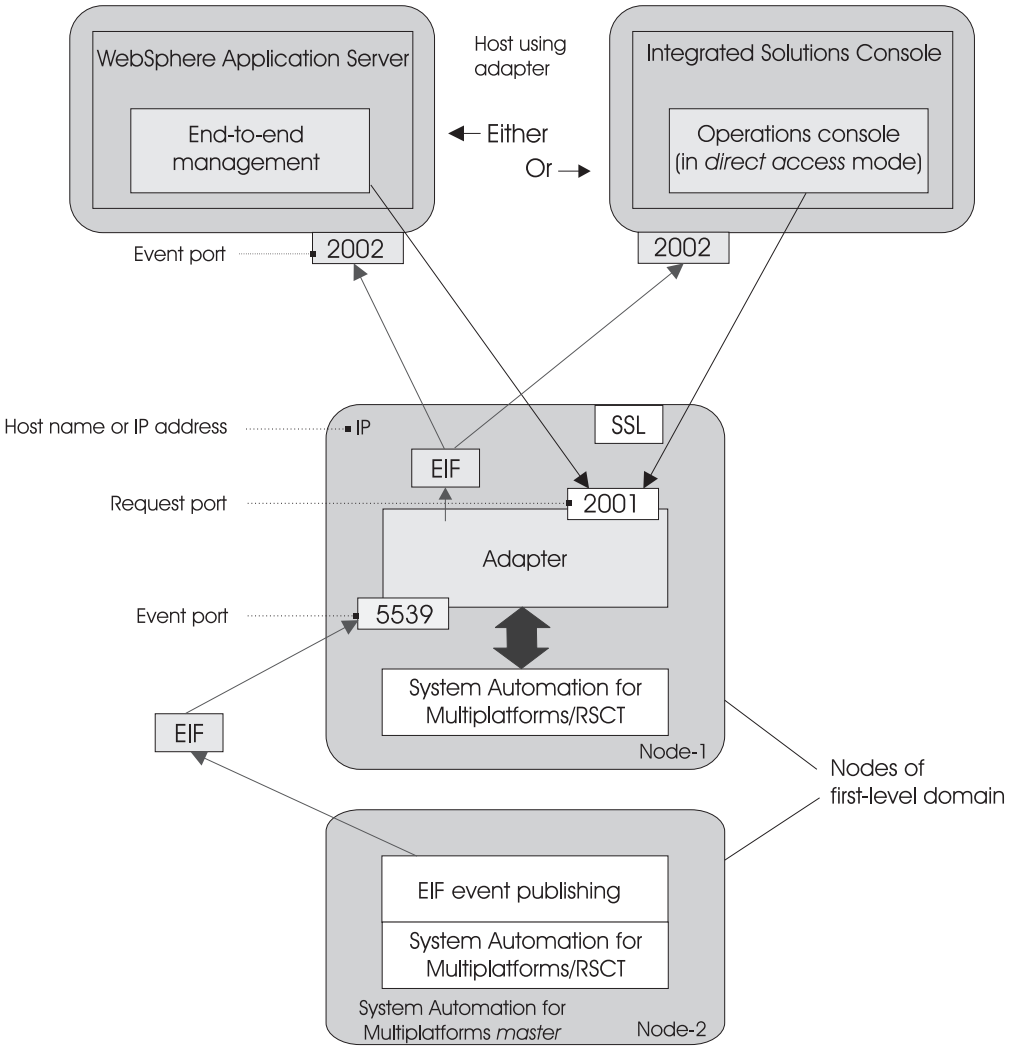


Figure 9. Overview of the environment the end-to-end automation adapter works on

Figure 9 shows that you have two adapter configuration alternatives which are mutually exclusive:

- You can configure the adapter for the operations console of the base component of IBM Tivoli System Automation. In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as *direct access mode*.
- If the end-to-end automation management component is installed, you can configure the adapter for end-to-end automation management. This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode, or if you want to use the operations console in first-level automation mode. For more information on end-to-end automation management and these console modes, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*.

Automating the end-to-end automation adapter

If the IBM Tivoli System Automation for Multiplatforms cluster consists of more than one node, the end-to-end automation adapter must be automated. (For a description of how this can be achieved, refer to "**Automation** tab" on page 150.)

When the adapter is automated, it can run on any node that is online in the cluster. This is necessary because the adapter is connected to two components as shown in Figure 9 on page 144:

1. The event publisher, which sends events to the adapter, for example, if the state of a resource changes. The event publisher runs on the master node. The master node can change at any time, for example, if a node goes down or a severe error condition occurs. This would be no problem if the adapter only received events from the event publisher because the event publisher will silently move to another node. However, the adapter also communicates with the so-called *host using the adapter*.
2. The host using the adapter, which is either the operations console of the base component or the end-to-end management for the end-to-end automation management component of IBM Tivoli System Automation. The adapter both sends events on resource changes to the host using the adapter and receives requests from the host using the adapter.

This means that the adapter must be able to always receive requests from both the host using the adapter and from the event publisher. To achieve this, the event publisher and the host using the adapter must access the adapter over a unique IP address which must be entered on the automation tab as described in "**Automation** tab" on page 150. This IP address must be requested from the system administrator.

This is what can happen if the adapter is running on the master node but has not been automated:

1. If the node on which the adapter runs goes down, the host using the adapter cannot access it anymore. Therefore it is not possible to learn how the automated resources behaved.
2. Although resources change their state, the operations console or end-to-end management may not show these changes. Select 'Refresh' to get the most recent state in the operations console displayed. The reason of this behavior is that the event publisher silently moved to another node.

The following sections describe how to configure and work with the end-to-end automation adapter.

Invoking the System Automation for Multiplatforms configuration dialog

The end-to-end automation adapter can be configured with the *cfgsamadapter* utility.

Notes:

1. The *cfgsamadapter* utility is an X-application and must be used from a workstation with Xserver capabilities. This could be one of your cluster nodes, if the X11 optional feature is installed on that node.
2. On AIX systems the end-to-end automation adapter installation requires that Java 1.4 in the 32-bit version is installed. Also on AIX systems SSL/SSH

packages must be installed and the sshd subsystem must be running to be able to complete the 'Replication' task of the adapter configuration.

3. To use the `System Automation for Multiplatforms adapter configuration` dialog you must be logged on to the system with the user ID `root` or you must have write access to the directories `/etc/opt/IBM/tsamp/sam/cfg` and `/etc/Tivoli`.

Issue the **cfgsamadapter** command to invoke the `System Automation for Multiplatforms adapter configuration` dialog. The main panel of the dialog is displayed:

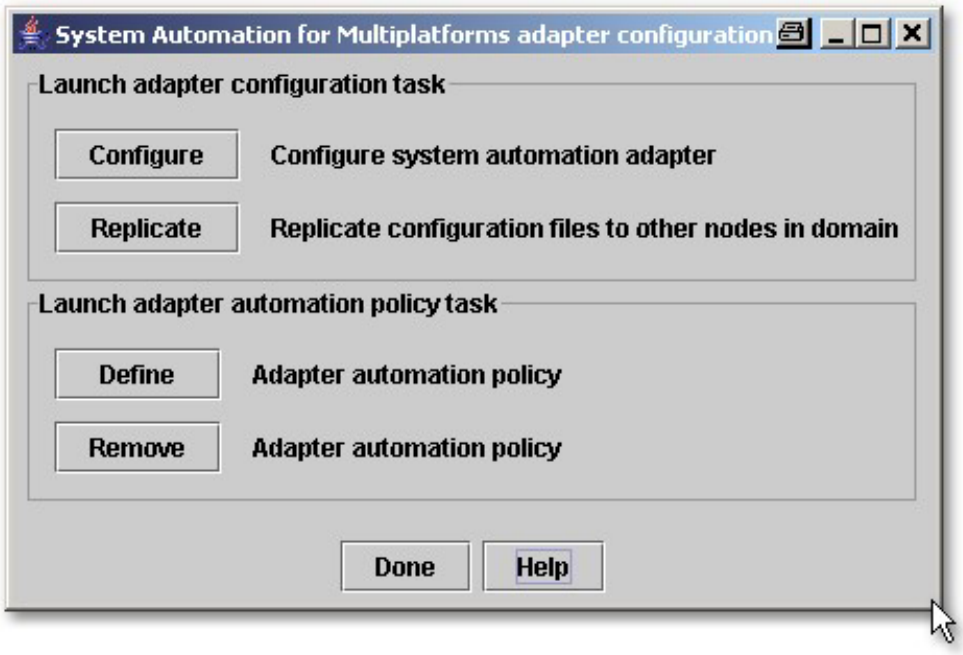


Figure 10. Main panel of the configuration dialog

This dialog lets you perform the following tasks:

1. Configuring the end-to-end automation adapter (see page 146)
2. Replicating the end-to-end automation adapter configuration files to other nodes (see page 157)
3. Defining the end-to-end adapter automation policy which results in the creation of resources to automate the adapter (see page 158)
4. Removing the end-to-end adapter automation policy (see page 159)

Configuring the end-to-end automation adapter

Pressing the `Configure` button leads you to the panel shown below where you can select several tabs described in the following sections.
In the following description the expression '**Host using adapter**' either means end-to-end automation management or direct access operations console.

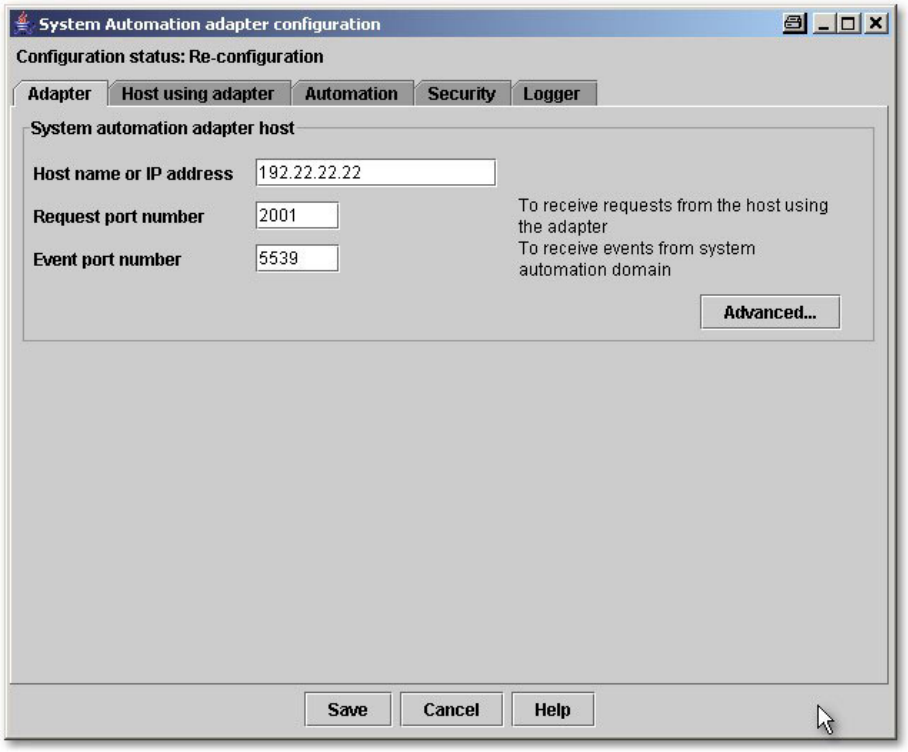


Figure 11. System Automation for Multiplatforms end-to-end adapter configuration

Adapter tab

Selecting the adapter tab lets you configure the adapter host.

Host name or IP address
: Host name of the node where the adapter runs if the adapter is not automated.

  If you select to automate the adapter, the value is updated automatically with the value you specify in the field **Adapter IP address** on the **Automation** tab (see "**Automation** tab" on page 150). In this case, do not change the value in the field.

Request port number
: The port on which the end-to-end automation adapter listens for requests from the end-to-end management host. The default port is '2001'.

Event port number
: The port on which the end-to-end automation adapter listens for events from the first level automation manager. The default port is '5539'.

Clicking on the `Advanced` button lets you specify the adapter run time behavior:

Adapter stop delay
: Delays stopping of the end-to-end automation adapter for the specified number of seconds. This gives the adapter a chance to

deliver the domain leave event properly. The default value is 5, the value ranges between 3 through 60. You may need to increase this value on slow systems.

Remote contact activity interval
: Defines the time after which the end-to-end automation adapter stops if there is no communication with the **host using the adapter**. Setting this parameter to 0 means that the adapter continues to run and never stops. The default value is 360 seconds.

Initial contact retry interval
: During this period (in minutes) the end-to-end automation adapter tries to contact the **host using the adapter**. This continues until it succeeds or the specified time has elapsed. The default value 0 means that the adapter tries contacting the **host using the adapter** forever.

EIF reconnect attempt interval
: If the connection to the **host using the adapter** was interrupted, this specifies the time the end-to-end automation adapter waits until it tries to reconnect. The default value is 30 seconds.

Host using adapter tab

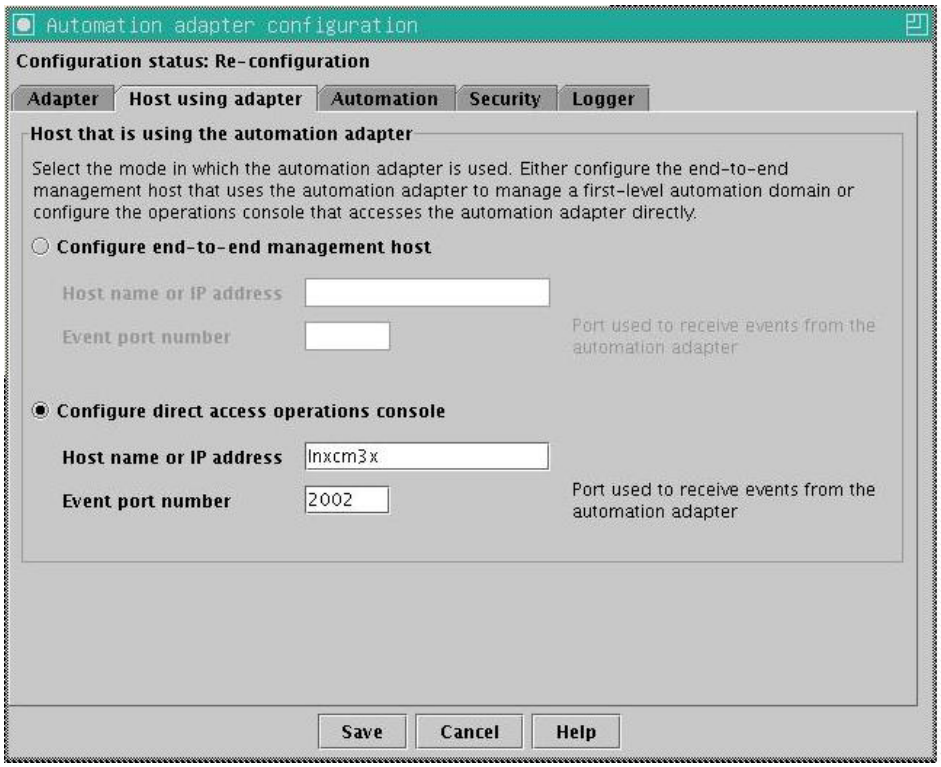


Figure 12. Host using the adapter

The end-to-end automation adapter can be used in two modes:

1. Configure the end-to-end management host which uses the adapter to manage a first level domain.
2. Configure the operations console that directly accesses the adapter.

Both modes are mutually exclusive.

Configure end-to-end management host:

Host name or IP address
: The name or the IP address of the host on which the end-to-end automation manager runs.

Event port number
: The port on which the end-to-end automation manager listens for events from the end-to-end automation adapter. The default port is '2002'.

Configure direct access operations console:

Host name or IP address
: The name of the IP address of the host on which the operations console runs.

Event port number
: The port on which the operations console listens for events from the end-to-end automation adapter. The default port is '2002'.

Automation tab

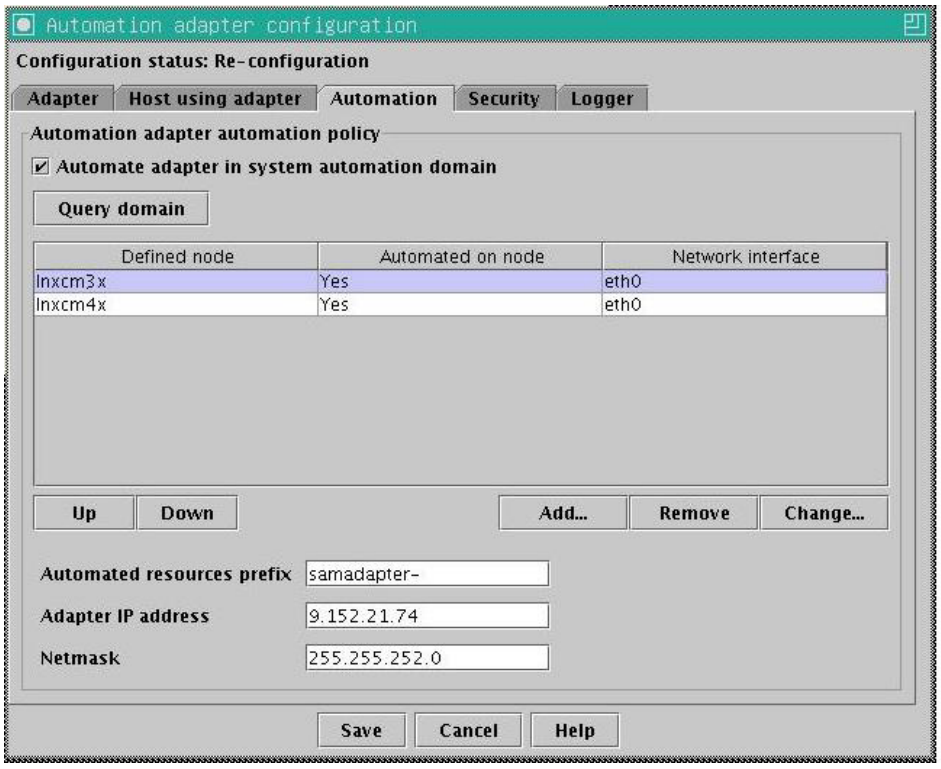


Figure 13. Automating the adapter

This tab lets you configure the adapter automation policy. This allows you to make the end-to-end automation adapter highly available, meaning that if the node on which the adapter runs breaks down, the adapter will be restarted on another node in the domain.

Note: All nodes where the adapter can run must be accessible using the same user ID and password.

Automate adapter in system automation domain
: Select this check box if the end-to-end automation adapter is running in an RSCT peer domain with more than one node. See the section which discusses automation on tab 145.

Query domain
: Provided that the node on which the configuration dialog runs is in the RSCT peer domain, this queries the current automation policy. If the domain is online, all nodes that are online are shown in the 'Defined nodes' table. This table provides the following information:

  - Defined node

    If the RSCT peer domain is online, all nodes that are online are shown here
  - Automated on node

    Indicates if the end-to-end automation adapter should be automated on this node.
  - Network interface

Name of the network interface used for requests from the **host using the adapter**.

The buttons at the bottom of the table let you perform the following:

- Up

  Moves the selected node one position up in the node sequence. The position determines the order in which automation selects the node on which the end-to-end automation adapter may run.

- Down

  Moves the selected node one position down in the node sequence. The position determines the order in which automation selects the node on which the end-to-end automation adapter may run.

- Add

  Displays the 'Add node for adapter automation' panel which lets you define the name of the node to be added, determine if the node is to be added to automation of the adapter, and lets you enter the name of the network interface.

- Remove

  Removes the selected node from the list. This means that the end-to-end automation adapter must not be started on that node.

- Change

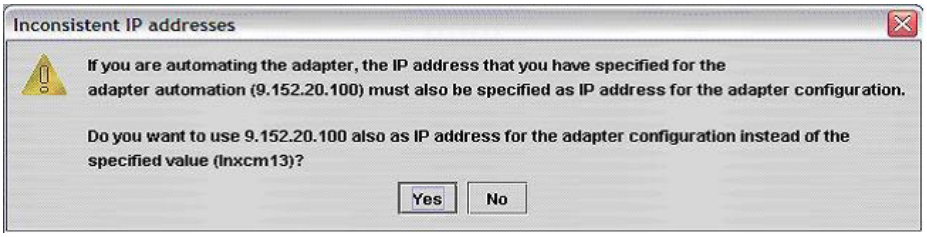
  Displays the 'Change node for adapter automation' panel which lets you change the name of the node, add or remove the node from automation of the adapter, and lets you change the name of the network interface.

Automated resources prefix
: This shows the prefix of the resource or resource groups names in the automation policy.
The prefix can be changed.
It is restricted to ASCII characters; the following characters cannot be used: " (double quote), ' (single quote), **;** (semicolon), $ (dollar), / (slash)
Note that if the end-to-end adapter policy has been defined using this existing prefix, you must remove this policy before changing the prefix.
For more information about defining the adapter automation policy, refer to "Defining the end-to-end adapter automation policy" on page 158.

Adapter IP address
: Regardless on which node it runs, the end-to-end automation adapter uses this address to listen for requests and receive requests from the end-to-end management server. It is an IP address which will be used as a ServiceIP resource to automate the adapter. You must obtain this IP address from your network administrator and it must neither be a real host address nor *localhost*.

Netmask
: Request a value from your network administrator.

Note: When you click **Save** after specifying an IP address in the field **Adapter IP address**, the following message may be displayed:



The message informs you that the IP addresses on the Adapter tab and on the Automation tab differ and asks you to confirm that the IP address on the Adapter tab is to be updated with the value you specified on the Automation tab. Click **Yes** to confirm the change.

Security tab

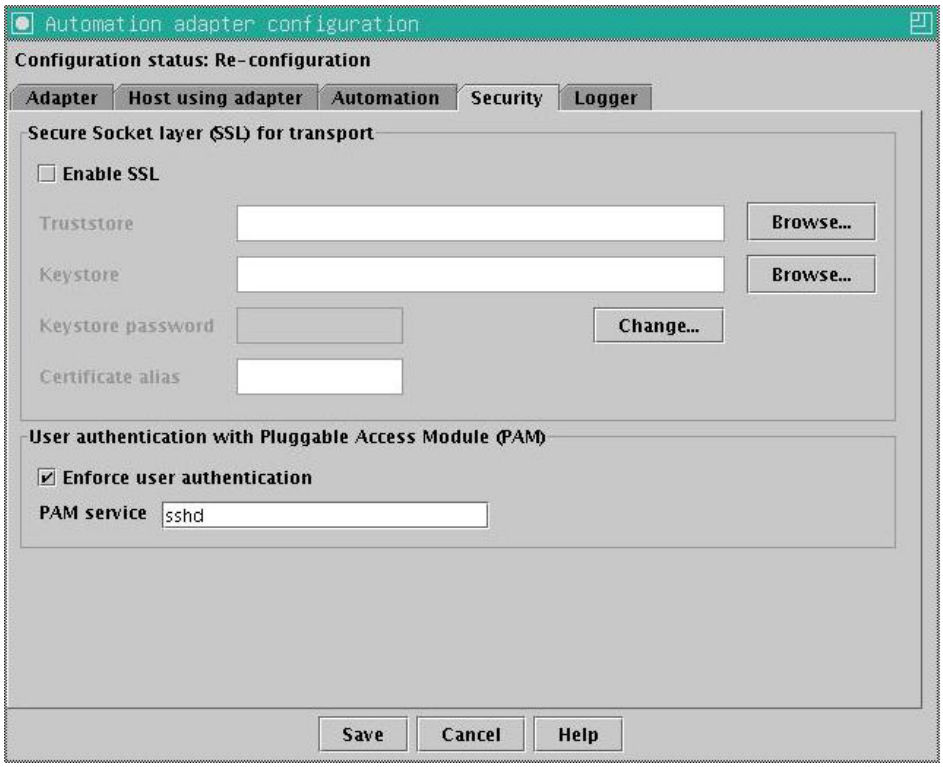


Figure 14. Configuring the adapter security

This tab lets you configure the security for the interface between the end-to-end automation adapter and the end-to-end management host.

Select the `Enable SSL` check box if you want to use the `Secure Socket layer (SSL)` protocol. If checked, the following entry fields must be completed.

Truststore
: Name of the truststore file used for SSL.

Keystore
: Name of the keystore file used for SSL.

Keystore password
: Password of the keystore file. The password is required if a keystore file was specified.

Keystore alias
: Alias name of the certificate to be used by the server. If not specified the keystore file must contain only one entry which is the one to be used.

Also select the `Enforce user authentication` check box to enable the authentication of the user with `Pluggable Access Module (PAM)`.

PAM Service
: The name of a file in the directory `/etc/pam.d` (SUSE), or an entry in file `/etc/pam.d` (RedHat), or an entry in file `/etc/pam.conf` (AIX), which determines which checks are made to authenticate a user. If you have AIX 5.2, you may have to perform the steps described for AIX 5.2 in Chapter 1, “Installing the base component,” section “Preparing for installation” on page 6.

Logger tab

Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.

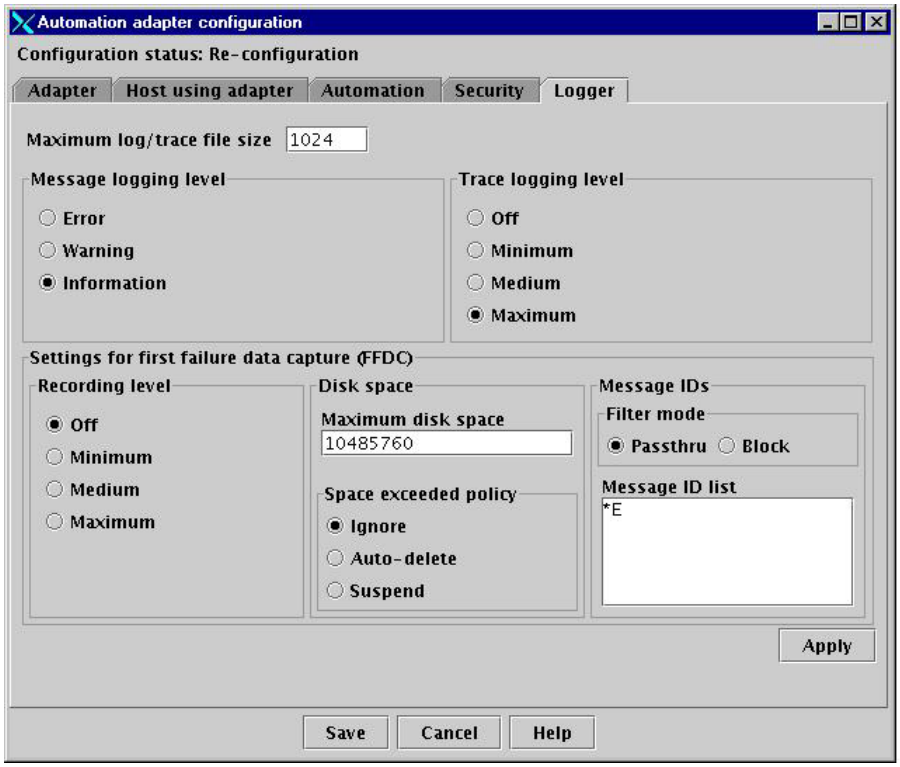


Figure 15. Adapter logging and trace information

On the Logger tab, you can perform the following tasks:

Changing the settings permanently

Perform these steps:

1. Make the required changes on the tab.
2. Click **Save**.

Results:

The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

Changing the settings temporarily

Perform these steps after ensuring that the adapter is running:

1. Make the required changes on the tab.
2. Click **Apply**.

Results:

The new settings take effect immediately. They are not stored in the configuration file. If the adapter is not running, you receive an error message.

Reverting to the permanent settings

Perform the following steps to revert to the permanent settings in the configuration file, or when you are unsure which settings are currently active for the adapter:

1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

Results:
The settings take effect immediately. If the adapter is not running, you receive an error message.

Controls and fields on the Logger tab:

Maximum log/trace file size
: The file size in kilobytes.

Message logging level:

Error	Logs messages on the error level.
Warning	Logs messages on the error and warning levels.
Information	Logs messages on the error, warning and informational levels.

Trace logging level:

Off	Collects no trace information.
Minimum	Collects trace information on the error level.
Medium	Collects trace information on the error and warning levels.
Maximum	Provides the message and trace logs and collects additional information on the error, warning, and informational level.

First failure data capture (FFDC) settings:

- Recording level:

Off	Collects no FFDC information.
Minimum	Provides the message and trace logs and collects additional information on the error level.
Medium	Provides the message and trace logs and collects additional information on the error and warning level.
Maximum	Provides the message and trace logs and collects additional information on the error, warning, and informational level.

- Disk space:

  Maximum disk space
  : Specifies the maximum disk space in bytes used by FFDC traces which are written into the FFDC trace directory. The default space is 10485760 (10MB).

  Space exceeded policy
  : Select what to do if the maximum disk space is exceeded.

- Message IDs:

  Filter mode
  : Initiates the tracing of FFDC data depending on the message IDs listed in 'Message ID list'.

Message ID list:

Specifies the message IDs which cause the tracing of the FFDC data. Wildcards like *E, meaning all error messages, are allowed.

Saving the configuration

Click **Save** on the configuration dialog to save your changes to the adapter configuration files. Upon completion, the configuration update status panel appears, showing the list of configuration files that were updated. This is depicted in Figure 16.

Notes:

1. When you changed the Adapter IP address on the Automation tab, the message described in the note on page 151 may be displayed. Click **Yes** to confirm the change and to save the new configuration to the configuration files.
2. When entries are missing or a value you have entered is out of range (for example, a port number), an error message is displayed.

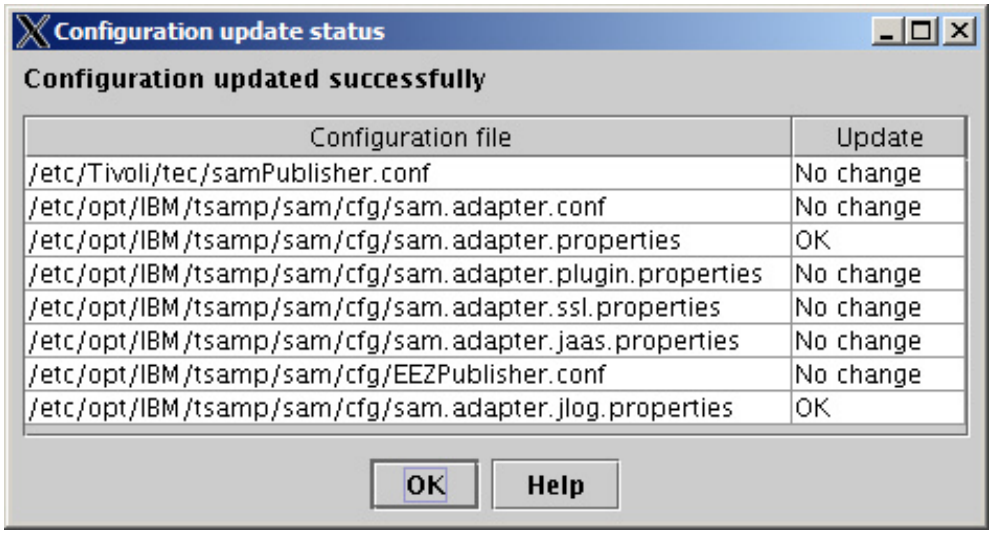


Figure 16. Configuration update status panel

Replicating the end-to-end automation adapter configuration files to other nodes in the domain

Click **Replicate** on the main panel of the configuration dialog (see Figure 10 on page 146). The following panel is displayed:

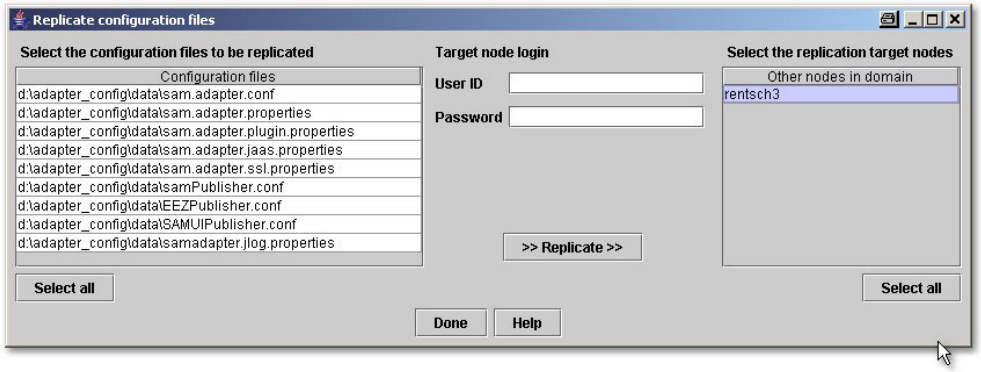


Figure 17. System Automation for Multiplatforms replicate configuration files panel

Use this panel to distribute (replicate) the end-to-end automation adapter configuration itself or configuration updates to other nodes in the RSCT peer domain:

1. Select the configuration files you want to replicate or click **Select all** to select all configuration files in the list.
2. Enter the user ID and password for the target nodes you want to replicate the files to.
3. Click **Select all** below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
4. Start the replication by clicking **Replicate**.

When the replication is complete, a panel shows the replication status of each configuration file for each target node.

Defining the end-to-end adapter automation policy

Clicking **Define** on the main panel of the configuration dialog (see Figure 10 on page 146) will create the resources with the resource name (Resource-/group prefix) as described on page 151. Note that if automated resources with the same name existed, they will be removed before creation of the new ones.

If you specified, for example, the resource-/group prefix name **samadapter**, the resource group `samadapter -rg`, and the resources and relationships shown in the following table will be created.

Resource name	Resource class	Description
samadapter-rg	IBM.ResourceGroup	The resource group that comprises all automated resources.
samadapter	IBM.Application	The samadapter application itself.
samadapter-ip	IBM.ServiceIP	The virtual IP address on which the adapter can be accessed from the end-to-end management host and the EIF event publisher.
samadapter-nieq	IBM.Equivalency	The available network interfaces on each node.
samadapter-on-ip	IBM.ManagedRelationship	The dependency of samadapter on the IP address.
samadapter-ip-on-nieq	IBM.ManagedRelationship	The dependency of the IP address on the network interface.

Note: Activating or deactivating a policy for the IBM Tivoli System Automation for Multiplatforms base component using the **sampolicy** command may remove existing definitions for the end-to-end adapter automation policy, or definitions that are referenced by an end-to-end automation policy. For example, the definition of a resource that is referenced in an end-to-end automation policy may be removed when a new policy for the base component is activated.

Therefore, it is recommended that you first save the currently active policy using the **sampolicy -s** command, edit the XML output file, and finally activate the changed policy. When editing the policy, you must make sure that all definitions for end-to-end adapter automation are preserved and that none of your changes has an undesired effect on the currently active end-to-end automation policy.

For detailed information, see the description of the **sampolicy** command in the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.

Removing the end-to-end adapter automation policy

Clicking **Remove** on the main panel of the configuration dialog (see Figure 10 on page 146) will remove the resources shown in the preceding table. Note that you should remove the end-to-end adapter automation policy before you change the Resource-/group prefix name as described on page 151.

If the end-to-end automation adapter is still running, the automated resource group is stopped. Then the resources are removed.

Chapter 14. Installing and configuring the HACMP adapter

The following topics describe how to install and configure the HACMP adapter.

Installing the HACMP adapter

Packaging

The HACMP adapter is shipped with the end-to-end automation management component. The name of the installp package name you use for installing the adapter is **hac.adapter**. This is where you find the installation package:

- **CD:**

  You install the adapter from the CD "Tivoli System Automation for Multiplatforms - End-to-End component, Automation Adapters all platforms". The installation package is available in the installation source directory `EEZ2200Adapter/EEZEEZ2200HACMP/AIX`.

- **Electronic distribution:**

  If you obtain the end-to-end automation management component through electronic distribution, you use the following archive to install the HACMP adapter:

  – Deliverable name: `C9483ML.bin`

  – Installation source directory: `EEZ2200Adapter/EEZ2200HACMP/AIX`

Installation prerequisites

Note that the HACMP adapter can only be connected to an end-to-end automation management component V2R2 or later.

The system on which you are installing the adapter must meet the following installation prerequisites:

- Required minimum HACMP release level: 5.3.0.5 (PTF5)
- AIX Java 32-bit runtime: `/usr/java14`
- The HACMP adapter must not run on a node in the RSCT peer domain. If the node on which the adapter is to run formerly was a node of an RSCT peer domain, the following actions must be taken prior to installing the adapter:
  1. The environment variable CT_MANAGEMENT_SCOPE, which is set to 2 for the RSCT peer domain, must be unset.
  2. The RSCT registry must be cleared using the command `/usr/sbin/rsct/install/bin/recfgct`

Using SMIT to install the adapter

You find the package in the following directory on the CD: `EEZ2200HACMP/AIX`

Package name: `hac.adapter`. Use the SMIT interface to install the adapter.

The HACMP adapter installation directory is `/opt/IBM/tsamp/eez/hac`

Note: Do not change the installation directory or the configuration directory (`/etc/opt/IBM/tsamp/eez/hac/cfg`). Otherwise, the HACMP adapter cannot be run because it relies on fixed paths.

After installing the adapter it must be configured as described in the remaining sections of this chapter.

Automating the HACMP adapter

If the HACMP cluster consists of more than one node, the HACMP adapter must be automated for the following reasons:

- The host using the adapter must be able to reach the adapter always through the same service IP without reconfiguration.
- If the node on which the adapter runs goes down or the HACMP cluster services on that node are stopped, the adapter must move to another available node in the cluster to resume the connection with the host using the adapter.

For more information about automating HACMP adapters using the adapter configuration dialog, see "**Automation** tab" on page 167.

Configuring the HACMP adapter

The following figure shows in which environments the HACMP adapter can work and what needs to be configured for the adapter.

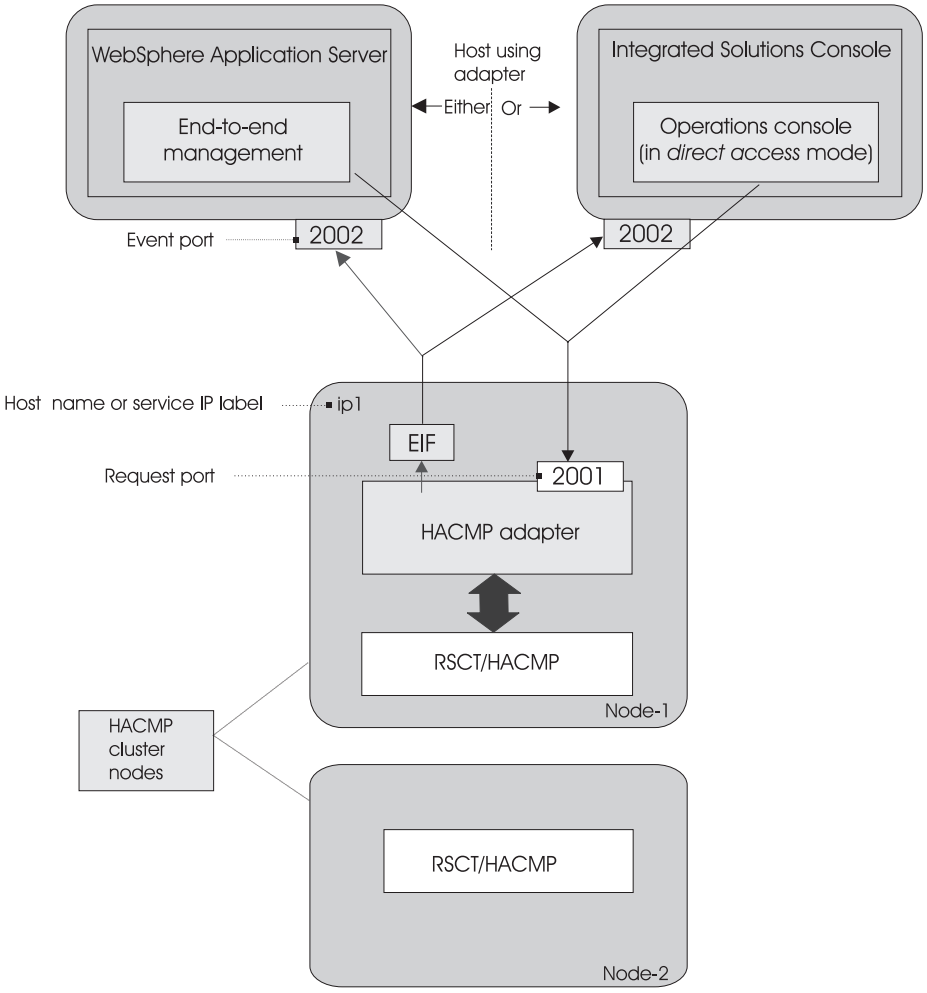


Figure 18. Configuration alternatives for the HACMP adapter

Figure 18 on page 162 shows that you have two adapter configuration alternatives which are mutually exclusive:

- You can configure the adapter for the operations console of the base component of IBM Tivoli System Automation. In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as *direct access mode*.
- If the end-to-end automation management component is installed, you can configure the adapter for end-to-end automation management. This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode or if you want to use the operations console in first-level automation mode. For more information on end-to-end automation management and these console modes, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*.

Invoking the HACMP adapter configuration dialog

The HACMP adapter can be configured with the *cfghacadapter* utility.

Notes:

1. The *cfghacadapter* utility is an X-application and must be used from a workstation with Xserver capabilities. This could be one of your cluster nodes, if the X11 optional feature is installed on that node.
2. The adapter installation requires that Java 1.4 in the 32-bit version is installed. SSL/SSH packages must be installed and the sshd subsystem must be running to be able to complete the 'Replication' task of the adapter configuration.
3. To use the HACMP adapter configuration dialog you must be logged in to the system with the user ID `root` or you must have write access to the directory `/etc/opt/IBM/tsamp/eez/hac/cfg`.

Issue the **cfghacadapter** command to invoke the configuration dialog.

The main panel of the dialog is displayed:

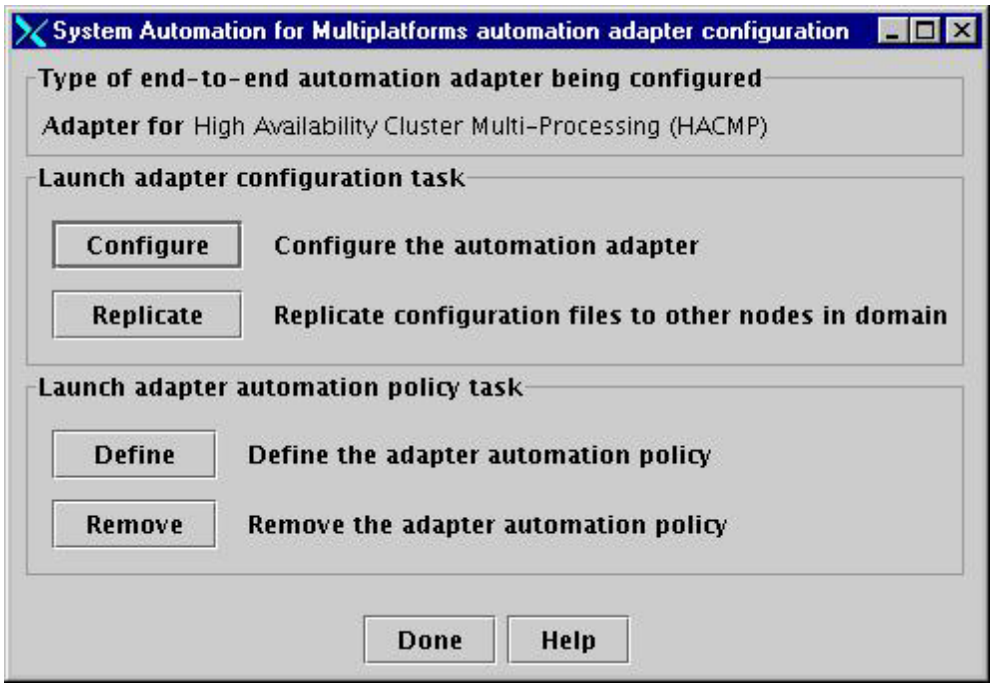


Figure 19. Main panel of the HACMP adapter configuration dialog

The dialog lets you perform the following tasks:

1. Configure the HACMP adapter.
2. Replicate the HACMP adapter configuration files to other nodes.
3. Define the HACMP adapter automation policy to create the resources required to automate the adapter.
4. Remove the HACMP adapter automation policy.

Using the HACMP adapter configuration dialog

On the main panel, click **Configure** to display the configuration panel.
In the following description the expression **Host using adapter** refers to either end-to-end automation management or the direct access operations console.

Adapter tab

Selecting the adapter tab lets you configure the adapter host.

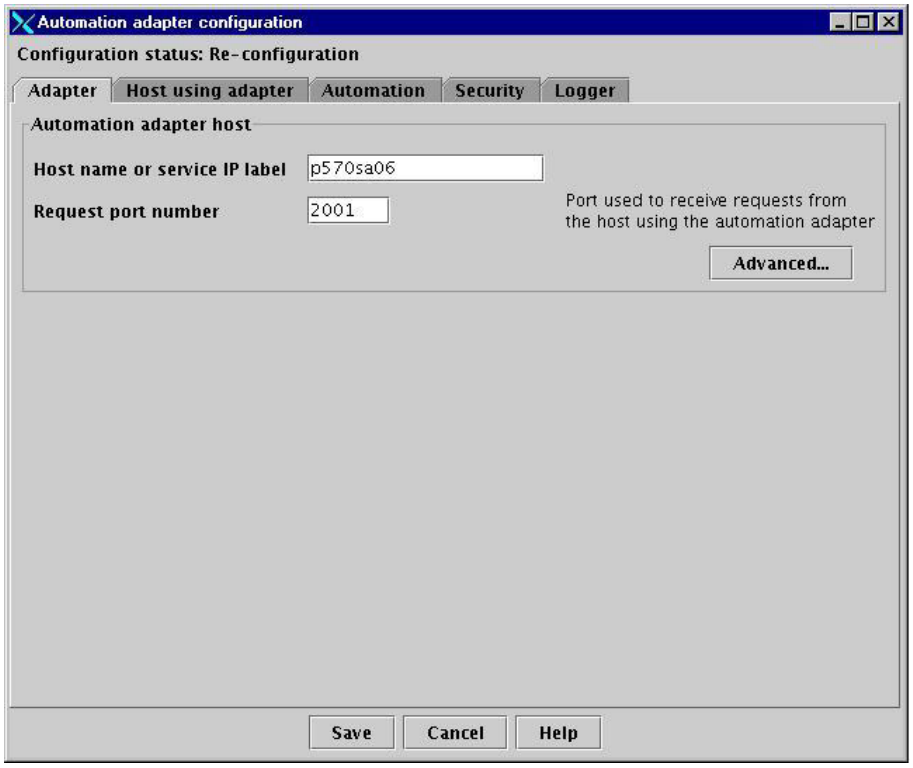


Figure 20. Adapter tab of the HACMP adapter configuration dialog

Fields and controls on the Adapter tab:

Host name or IP address
: Host name or service IP label of the node where the adapter runs.

  On initial invocation, the field contains the value the command **hostname** would return.

  If you are automating the adapter, leave the value unchanged. The value will be updated automatically with the value you specify in the field **Service IP label** on the **Automation** tab (see "**Automation** tab" on page 167).

Request port number
: The port on which the HACMP adapter listens for requests from the end-to-end management host. The default port is '2001'.

Clicking **Advanced** lets you specify the adapter run time behavior:

Adapter stop delay
: Delays stopping of the HACMP adapter for the specified number of seconds. This gives the adapter a chance to deliver the domain leave event properly. The default value is 5, the value ranges between 3 through 60. You may need to increase this value on slow systems.

Remote contact activity interval
: Defines the time after which the HACMP adapter shuts down if there is no communication with the **host using the adapter**, which periodically contacts the adapter to check if the adapter is still running.

Make sure that the interval specified in this field is a multiple of the check interval. The default value is 360 (seconds). A value of 0 means that the HACMP adapter never shuts down.

Initial contact retry interval
: During this period (in minutes) the HACMP adapter tries to contact the **host using the adapter** until it succeeds or the specified time has elapsed. The default value is 0, which means that the adapter tries to contact the **host using the adapter** forever.

EIF reconnect attempt interval
: If the connection to the **host using the adapter** was interrupted, this specifies the time the HACMP adapter waits until it tries to reconnect. The default value is 30 seconds.

Host using adapter tab

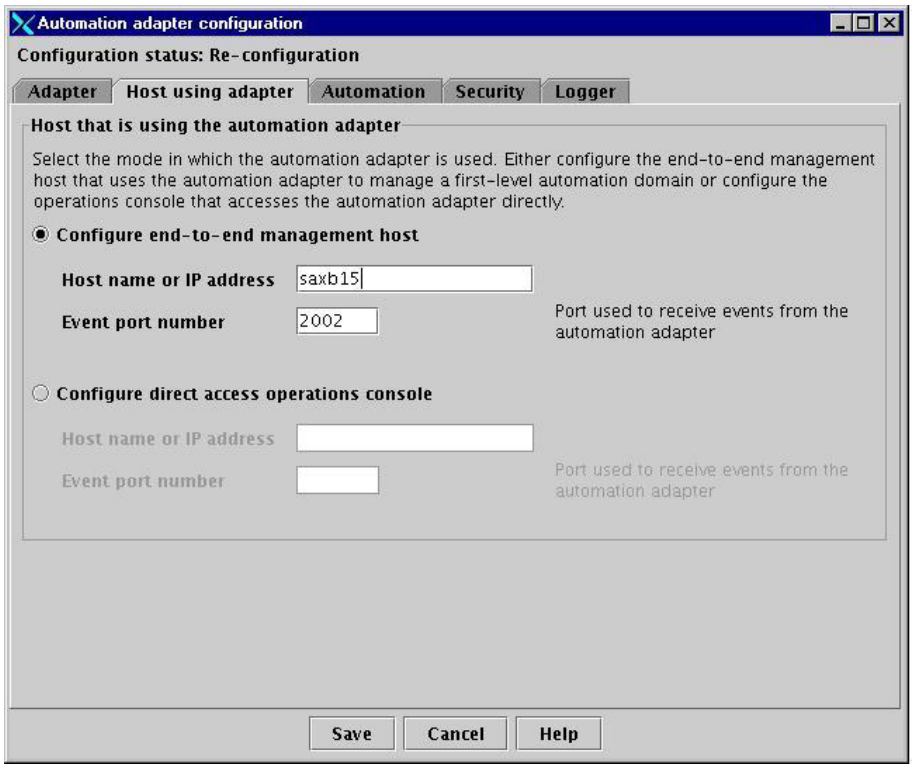


Figure 21. Host using adapter tab of the HACMP configuration dialog

On the Host using adapter tab you specify the host that is using the adapter, which can be either:

- The host where the end-to-end automation engine is running. In this case, the end-to-end automation manager uses the adapter to operate the cluster you are configuring as one of its first-level automation domains.
- The host where the base component operations console is installed. In this case, the operations console uses the adapter in direct access mode to operate the cluster you are configuring.

Fields and controls on the Host using adapter tab:

Configure end-to-end automation management host:

Host name or IP address
: The name or service IP label of the host on which the end-to-end automation manager runs.

Event port number
: The port on which the end-to-end automation manager listens for events from the HACMP adapter. The default port is '2002'.

Configure direct access operations console:

Host name or IP address
: The name or service IP label of the host on which the operations console runs.

Event port number
: The port on which the operations console listens for events from the HACMP adapter. The default port is '2002'.

Automation tab

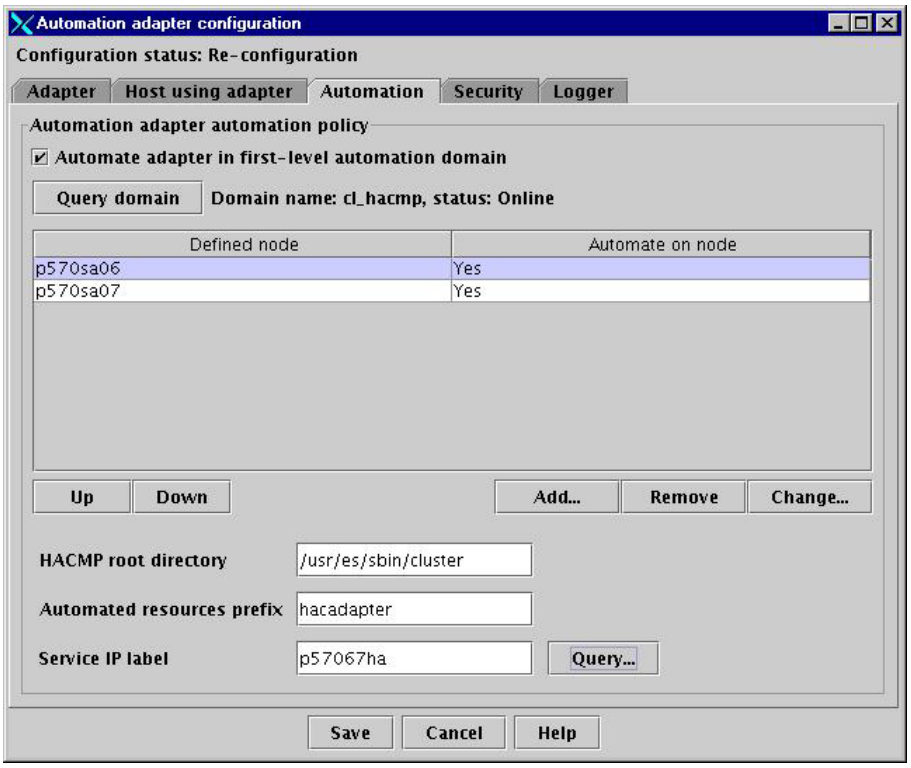


Figure 22. Automation tab of the HACMP configuration dialog

This tab lets you configure the adapter automation policy. This allows you to make the HACMP adapter highly available.

Note: All nodes where the adapter can run must be accessible using the same user ID and password.

Fields and controls on the Automation tab:

Automate adapter in first-level automation domain
: Select this check box (see also "Automating the HACMP adapter" on page 162).

Query domain
: If the configuration dialog runs on a node in the HACMP cluster, click **Query domain** to query the current automation policy from the HACMP cluster. If the automation policy for the adapter is not yet defined but the cluster is up, at least all nodes that are online are shown in the **Defined nodes** table. This table provides the following information:

  - Defined node

    The list of defined nodes.
  - Automated on node

    Indicates if the adapter is automated on this node.

  The buttons at the bottom of the table let you perform the following tasks:

  - Up

    Moves the selected node one position up in the node sequence. The position determines the order in which automation selects the node on which the adapter may run.
  - Down

    Moves the selected node one position down in the node sequence. The position determines the order in which automation selects the node on which the adapter may run.
  - Add

    Displays the 'Add node for adapter automation' panel which lets you define the name of the node to be added and determine if the node is to be added to automation of the adapter.
  - Remove

    Removes the selected node from the list. This means that the adapter must not be started on that node.
  - Change

    Displays the 'Change node for adapter automation' panel. On the panel, you can do this:

    – Prevent the adapter from running on a node by deselecting the check box **Automate adapter on node**.
    – Add a node even if it does not exist in the HACMP cluster or is offline at the time.
    – Remove a node.

HACMP root directory
: Shows the HACMP root directory.

Automated resources prefix
: The prefix that is used to compose the names of the resource group, application, and application monitor in the automation policy.
  The resource names will appear in the resource table on the operations console. The prefix can be changed. It is restricted to ASCII characters; the following characters cannot be used: " (double quote), ' (single quote), **;** (semicolon), $ (dollar), / (slash)
  Note that if the HACMP adapter policy has been defined using the current prefix, you must remove this policy before changing the prefix.

For more information about defining the adapter automation policy, refer to “Defining the HACMP adapter automation policy” on page 174.

Service IP label

The Service IP label is an entry in `/etc/hosts` that represents a service IP label. It must be different from the host name of any node in the HACMP cluster. It should be requested from the network administrator as a "service IP label" or "alias" for all nodes in the HACMP cluster and must have been created (for example, using the SMIT interface) before you invoke the configuration dialog.

The HACMP adapter will listen on the service IP label for requests from the host using the adapter, regardless on which node it runs.

Security tab

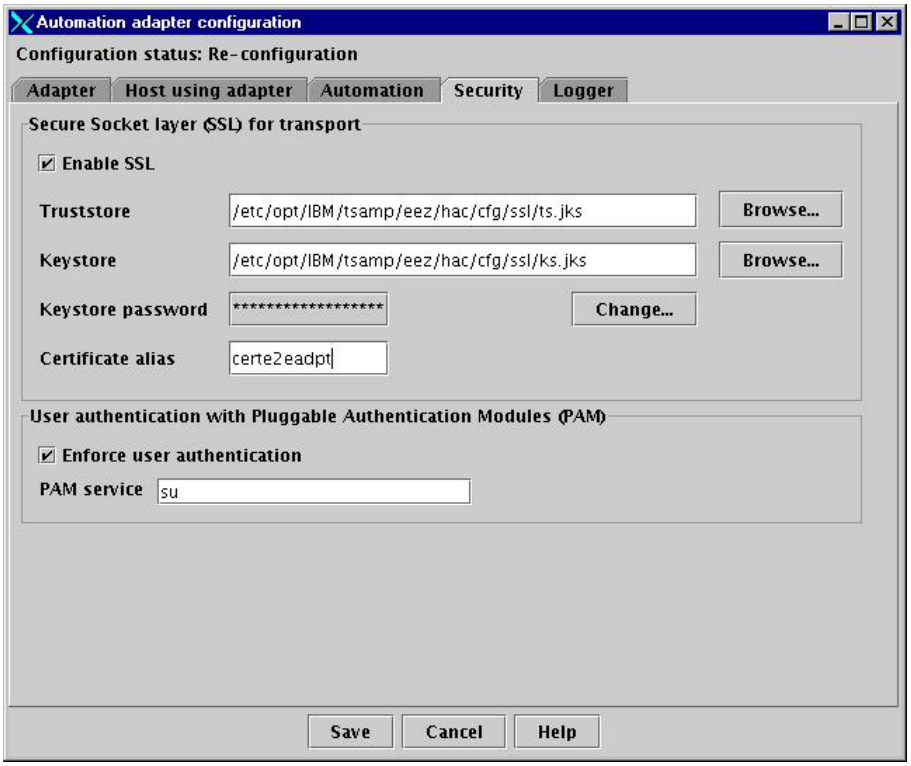


Figure 23. Security tab of the HACMP configuration dialog

The security tab lets you configure the security for the interface between the HACMP adapter and the end-to-end automation management host.

Fields and controls on the Security tab:

Select the `Enable SSL` check box if you want to use the `Secure Socket layer (SSL)` protocol. If checked, the following entry fields must be completed.

Truststore
: Name of the truststore file used for SSL. Click **Browse** to select a file.

Keystore
: Name of the keystore file used for SSL. Click **Browse** to select a file.

Keystore password
: Password of the keystore file. The password is required if a keystore file was specified. To change the keystore password, click **Change**.

Keystore alias
: Alias name of the certificate to be used by the server. If not specified the keystore file must contain only one entry which is the one to be used.

The `Enforce user authentication` check box enables user authentication with the `Pluggable Access Module (PAM)`. This check box is selected by default. It should only be deselected for test purposes when user authentication is not required.

PAM Service
: Is the name of a file in the directory `/etc/pam.conf` that determines which modules are called to authenticate a user. The default value is `su`, which checks users as if they were trying to execute the command **su**.

Logger tab

Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.

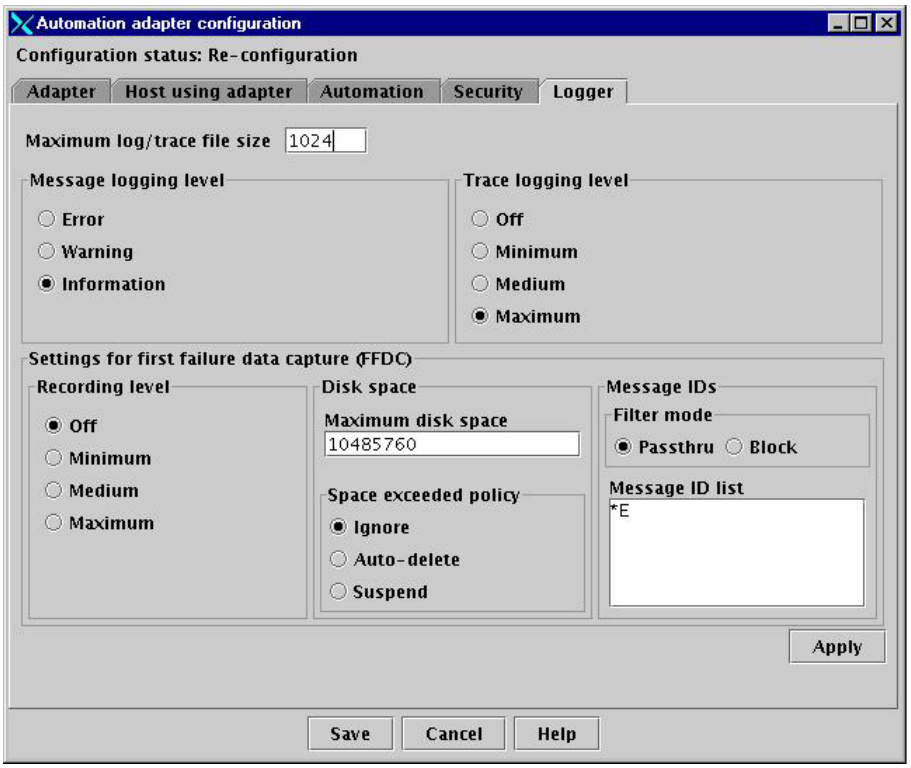


Figure 24. HACMP configuration dialog: Logger tab

On the Logger tab, you can perform the following tasks:

Changing the settings permanently
: Perform these steps:

1. Make the required changes on the tab.
2. Click **Save**.

Results:
The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

Changing the settings temporarily

Perform these steps:

1. Make the required changes on the tab.
2. Click **Apply**.

Results:
The new settings take effect immediately. They are not stored in the configuration file. If the adapter is not running, you receive an error message.

Reverting to the permanent settings

Perform the following steps to revert to the permanent settings in the configuration file, or when you are unsure which settings are currently active for the adapter:

1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

Results:
The settings take effect immediately. If the adapter is not running, you receive an error message.

Controls and fields on the Logger tab:

Maximum log/trace file size
: The maximum file size in kilobytes that each log file can reach before it rolls over.

Message logging level:

Error
: Logs messages on the error level.

Warning
: Logs messages on the error and warning levels.

Information
: Logs messages on the error, warning and informational levels.

Trace logging level:

Off
: Collects no trace information. (Not recommended.)

Minimum
: Collects trace information on the error level. Only severe error situations are traced. This is the default setting.

Medium
: Collects trace information on the error and warning levels.

Maximum
: Provides the message and trace logs and collects additional information on the error, warning, and informational level. Required for testing and problem determination.

First failure data capture (FFDC) settings:

- Recording level:

  Off
  : Collects no FFDC information.

Minimum
: Provides the message and trace logs and collects additional information on the error level.

Medium
: Provides the message and trace logs and collects additional information on the error and warning level.

Maximum
: Provides the message and trace logs and collects additional information on the error, warning, and informational level.

- Disk space:

  Maximum disk space
  : Specifies the maximum disk space in bytes used by FFDC traces which are written to the FFDC trace directory. The default space is 10485760 (10MB).

  Space exceeded policy
  : Select what to do if the maximum disk space is exceeded:

    Ignore
    : Issue warnings, but do not enforce the FFDC disk space quota.

    Auto-delete
    : Automatically delete FFDC files, oldest first, until the directory is below the limit. This is the default setting.

    Suspend
    : Halt further FFDC actions until the directory is manually cleaned up.

- Message IDs:

  Filter mode
  : Initiates the tracing of FFDC data depending on the message IDs listed in **Message ID list**.

  Message ID list
  : Specifies the message IDs that are to trigger tracing, depending on the filter mode. Wildcards, for example, *E (for all error messages), are allowed.

Saving the configuration

Click **Save** on the configuration dialog to save your changes to the adapter configuration files. Upon completion, the Configuration update status panel appears, showing the list of configuration files that were updated.

Notes:

1. If the service IP label specified on the Automation tab does not match the host specified on the Adapter tab, you are prompted for input. On the panel that appears, click the button **Adapter automation**.
2. If you made changes on the Automation tab, a message appears reminding you that automation resources for the HACMP adapter must be defined.

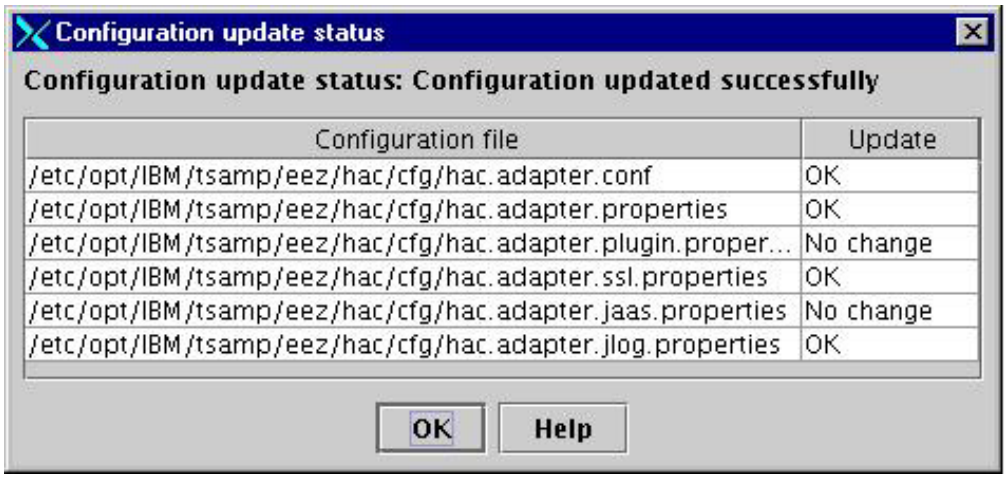


Figure 25. Configuration update status panel of the HACMP configuration dialog

Replicating the HACMP adapter configuration files to other nodes in the domain

After configuring an HACMP adapter on a node, you use the **Replicate** function to propagate the changes to the other nodes in the HACMP cluster. To use the Replicate function, go to the main panel of the configuration dialog and click **Replicate**. The Replicate configuration files panel is displayed:

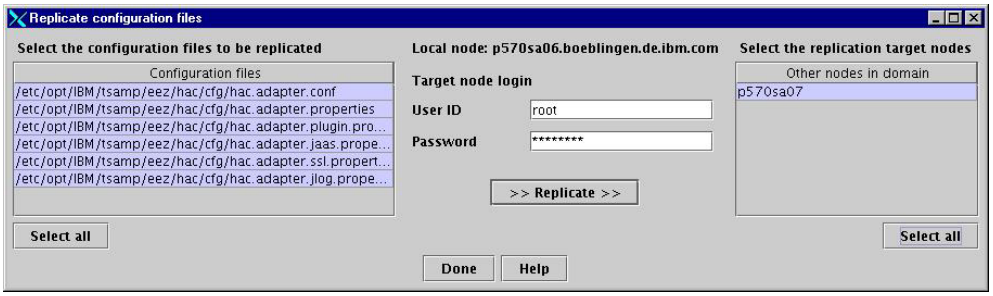


Figure 26. Replicate configuration files panel of the HACMP adapter configuration dialog

Use this panel to distribute (replicate) the HACMP adapter configuration itself or configuration updates to other nodes in the HACMP cluster:

1. Select the configuration files you want to replicate or click **Select all** to select all configuration files in the list.
2. Enter the user ID and password for the target nodes you want to replicate the files to.
3. If the user ID and password you specified are valid on all nodes, you can click **Select all** below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
4. Start the replication by clicking **Replicate**.

Replication may take a while. During replication, the button is indented and grayed-out. When the replication is complete, a panel shows the replication status of each configuration file for each target node:

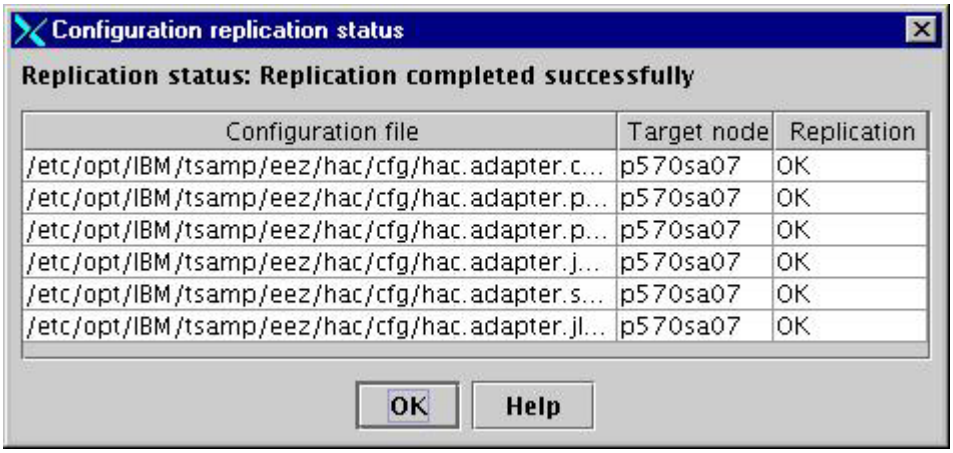


Figure 27. Replication status panel

Defining the HACMP adapter automation policy

If definitions for the automation of the HACMP adapter have been made, clicking **Define** on the main panel of the configuration dialog will create the resources with the resource name (Resource-/group prefix) as described on page 168. Note that if automated resources with the same name already exist, they are removed before the new resources are created.

If you used the default resource name prefix, the following resources will be defined or queried:

Table 51. Resources in the HACMP adapter automation policy

Resource class	Resource name	Description
IBM.HacmpResourceGroup	hacadapter_rg	The resource group that comprises all automated resources.
IBM.HacmpApplication	hacadapter	Commands: hacadapter start, hacadapter stop
IBM.HacmpAppMonitor	hacadapter_mon	Command: hacstatus
IBM.HacmpServiceIP	<service_ip_label> value	The label of the service IP on which the host using the adapter accesses the adapter.This value is not defined but just queried and, therefore, not removed.

When you click **Define**, the button may stay indented for minutes until the resources have been removed, the cluster is synchronized, the new resources are created, and the cluster is synchronized again. The dialog will not repaint after it has been covered and uncovered. Eventually, the results of the commands are displayed in a pop-up window.

Removing the HACMP adapter automation policy

You typically use the Remove function **before** you change the name prefix of the automated resources (see page 168). When the adapter is automated and you

deselect the check box **Automate adapter in system automation domain** on the Automation tab, you receive a message reminding you to remove the automated resources for the adapter.

Clicking **Remove** on the main panel of the configuration dialog will remove the resources shown in Table 51 on page 174. If the HACMP adapter is still running, it is stopped before the automated resources are removed.

When you click **Remove**, the button may stay indented for minutes until resources have been removed and the cluster has been synchronized. Eventually, the results of the commands are displayed in a pop-up window.

Verifying the HACMP adapter configuration

You can use the **clstat** command to verify that the HACMP adapter is running:

1. Open PuTTy sessions with the nodes on which the HACMP adapter may run.
2. In each session, type `/usr/es/sbin/cluster/clstat`
3. The status screen depicted below should be displayed:
   - `Resource Group: hacadapter_rg` (if the prefix is 'hacadapter') in `State: On line`
   - `Interface: p57067ha` (in the example configuration) associated with the service IP label of the same name in `State: UP`

```
clstat - HACMP Cluster Status Monitor
               -------------------------------------

Cluster: hacp57067      (1137142142)
Mon Feb 20 14:15:16 MET 2006
               State: UP               Nodes: 2
               SubState: STABLE

        Node: p570sa06          State: UP
           Interface: p570sa06 (0)              Address: 9.152.20.176
                                                State:   UP
           Interface: p57067ha (0)              Address: 9.152.24.195
                                                State:   UP
           Resource Group: hacadapter_rg        State:  On line

        Node: p570sa07          State: UP
           Interface: p570sa07 (0)              Address: 9.152.20.177
                                                State:   UP
********************** f/forward, b/back, r/refresh, q/quit *********
```

Chapter 15. Installing and configuring the MSCS adapter

The following topics describe how to install and configure the MSCS adapter.

Installation and configuration roadmaps

Before you install the MSCS adapter, you must decide whether you want to make the adapter highly available, which is strongly recommended. The roadmaps provided in this section give an overview of the steps you need to perform to install and configure the adapter depending on your high-availability decision.

Roadmap for highly available adapters

If you are making your adapter highly available, which is highly recommended, perform the following steps:

1. Plan and prepare for the installation and configuration of the MSCS adapters (see "Planning and preparing for the MSCS adapter" on page 178).

   _____

2. Use the installation wizard to install the adapter on one node in the cluster and generate a response file (see "Using the installation wizard to install the MSCS adapter" on page 179).

   _____

3. To ensure that uniform installation parameters are used, use the response file to install the adapters on the remaining nodes. Response-file driven installation can be performed in silent mode (see "Installing the adapter in silent mode" on page 181) or in interactive mode using the installation wizard (see "Using the installation wizard to install the MSCS adapter" on page 179).

   _____

4. Configure the adapter on one of the cluster nodes using the adapter configuration dialog (see "Configuring the MSCS adapter" on page 182).

   _____

5. To ensure that uniform configuration parameters are used, replicate the adapter configuration files to the remaining nodes (see "Replicating the configuration files to other nodes" on page 188).

   _____

6. Create the MSCS resources needed for making the adapter highly available.

   _____

7. Verify the installation and configuration (see "Verifying the installation and configuration" on page 195).

   _____

Roadmap for adapters that are not highly available

If you are not making your adapter highly available, perform the following steps:

1. Plan and prepare for the installation and configuration of the MSCS adapter (see "Planning and preparing for the MSCS adapter" on page 178).

   _____

2. Use the installation wizard to install the adapter on a cluster node (see "Using the installation wizard to install the MSCS adapter" on page 179).

3. Configure the adapter using the adapter configuration dialog (see “Configuring the MSCS adapter” on page 182).

4. Verify the installation and configuration (see “Verifying the installation and configuration” on page 195).

Planning and preparing for the MSCS adapter

Packaging

The MSCS adapter is shipped with the end-to-end automation management component. This is where you find the installation file:

- **CD:**

  You install the adapter from the CD "Tivoli System Automation for Multiplatforms - End-to-End component, Automation Adapters all platforms". This is where you find the installation wizard file (`setup.exe`) on the CD:

  `EEZ2200Adapter\EEZ2200MSCS\Windows\setup.exe`

- **Electronic distribution:**

  If you obtain the end-to-end automation management component through electronic distribution, you use the following archive to install the MSCS adapter:
  `C9484ML.exe`
  To extract the archive, run the executable. The resulting directory structure is identical to that on the CD. This is where you find the installation wizard file (`setup.exe`) when you have extracted the archive:

  `EEZ2200Adapter\EEZ2200MSCS\Windows\setup.exe`

Installation prerequisites

Note that the MSCS adapter can only be connected to an end-to-end automation management component V2R2 or later.

The system on which you are installing the adapter must meet the following installation prerequisites:

- Windows Server 2003 Enterprise Edition with Service Pack 1 or later
- 32-bit systems only
- System must be an MSCS node
- System must not be a domain controller, or local user IDs must be permitted on the domain controller
- 64 MB RAM is required for running the MSCS adapter service
- 40 MB RAM is required for running the adapter configuration dialog
- Disk space requirements:
  - 140 MB for MSCS adapter installation
  - Typically, 6 MB is sufficient during normal operation, however, up to 250 MB may be required for service-related files in the Tivoli Common Directory (log files, FFDC files)

Planning and preparing for high availability

Making the MSCS adapter highly available using MSCS is highly recommended but not required. To prepare for making an adapter highly available, do this:

- Obtain a virtual IP address:
  - The MSCS adapter will use this IP address for incoming connections
  - MSCS will make the virtual IP address available on the appropriate MSCS node
- If desired, obtain a network name:
  - If you specify the network name in the MSCS adapter configuration, the name will be published to the end-to-end automation server
  - The end-to-end automation server will use this network name for connecting to the MSCS adapter
  - MSCS will associate this network name with the virtual IP address on the DNS server that is configured in the Microsoft Windows domain

Installation directories

For the MSCS adapter installation directory and the Tivoli Common Directory, the following restrictions apply:

- The MSCS adapter installation directory name must not include the DBCS space character. The SBCS space character is supported.
- Tivoli Common Directory:

  When specifying a directory other than the default, observe the following restrictions:
  - The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
  - The colon character is allowed only once, immediately following the drive letter. For example, `C:\<directory_name>` is allowed, but `C:\<directory_name>:<directory_name>` is not allowed.
  - The space character and the underscore character (_) are allowed.

Installing the MSCS adapter

You have the following options to install an MSCS adapter:

- You use the installation wizard to install the adapter.
- You generate a response file when you use the installation wizard on a node. You can then use the response file in one of two ways to install the adapter on other nodes:
  - You launch the installation wizard using the response file as input. The values in the response file will appear in the fields on the wizard panels and can be changed.
  - You can install the adapter in silent mode on the remaining nodes of the cluster if you are making the adapter highly available, in which case the values in the response file apply to all nodes.

Using the installation wizard to install the MSCS adapter

This section describes how you install the MSCS adapter using the installation wizard. For information on silent mode, see “Installing the adapter in silent mode” on page 181.

Note: The MSCS adapter requires the Windows service `JaasLogon`. `JaasLogon` is part of the IBM Java Runtime Environment, which is installed during adapter installation. If the service is already installed on the system, it will be replaced during adapter installation.

Perform the following steps to install the adapter:

1. Log in as a local user. The user ID must have administrator privileges. Note that installation will be denied if you are logged in with a domain user ID.

   ---

2. Launch the installation wizard. You have the following options:
   - To launch the installation wizard without generating a response file, use the file:

     ```
     setup.exe
     ```

     When you launch the wizard in this way, the values that are displayed on the wizard panels are either default values or values that were detected on your system.
   - To launch the installation wizard, generating a response file, use the following command:

     ```
     setup.exe -V responseFile=<response_file_name>
     ```

     where `<response_file_name>` is the fully qualified name of the response file to be generated, for example:

     ```
     C:\response.txt
     ```

     When you launch the wizard in this way, the values that are displayed on the wizard panels are either default values or values that were detected on your system.
   - To launch the installation wizard using a response file as input, use the following command:

     ```
     setup.exe -options <response_file_name>
     ```

     When you launch the wizard in this way, the fields on the wizard panels are filled in with the values from the response file.

   When you have launched the wizard, click **Next** on the Welcome panel to display the license agreement.

   ---

3. Select **I accept the terms in the license agreement** to agree to the license agreement. Click **Next**. The Installation directory panel is displayed.

   ---

4. Specify the directory where you want to install the adapter or accept the default location. Click **Next** to display the Tivoli Common Directory panel.

   ---

5. If the installation program did not detect a Tivoli Common Directory on your system, accept the default location or specify a different directory. If a Tivoli Common Directory was detected on your system, the directory is displayed and cannot be changed.

   Click **Next** to display the Microsoft Cluster Adapter service user panel.

   ---

6. Specify the user ID and password for the user who is to run the adapter. The user ID must be authorized to connect to MSCS, retrieve MSCS objects, bring MSCS resources and groups online and offline, and suspend and resume MSCS

nodes. It is recommended that you use a domain user ID. The default is the user ID used for running MSCS itself, which is the Windows service "Cluster Service".

Click **Next** to display the summary panel.

---

7. Check the values on the summary panel and click **Install** to start the installation.

---

8. While the adapter is being installed, a progress panel is displayed.

   When the installation is complete, an installation summary panel is displayed, on which you can verify the success of the installation.

   If problems occur, check the applicable installation log files for more information. Click **Finish** to close the installation wizard.

Installing the adapter in silent mode

This section describes how you install the adapter in silent mode, using a response file you generated during wizard-driven installation. For information on how to generate a response file and how to use it as input for a wizard-driven installation, see "Using the installation wizard to install the MSCS adapter" on page 179.

To install the MSCS adapter in silent mode, use the following command:

```
setup.exe -options <response_file_name> -silent
```

Note that response files contain password information and should be deleted when they are no longer needed.

The following example shows a typical response file:

```
#
# Aug 22, 2006 1:02:54 PM
#
# This response file contains the required values for an installation,
# uninstallation or update of
# IBM Tivoli System Automation for Multiplatforms MSCS Adapter.
#

# Set to 'true' to accept the terms of the license agreement,
# otherwise set to 'false'.
# Note that the product will not be installed if set to 'false'.
-V LICENSE_ACCEPT_BUTTON="true"

# IBM Tivoli System Automation for Multiplatforms MSCS Adapter will be
  installed to the specified directory.
-P installLocation="C:\Program Files\IBM\tsamp\eez\mscs"

# Tivoli Common Directory path
-V TCD_LOC="C:\Program Files\IBM\tivoli\common"

# Microsoft Server Cluster Adapter service user ID and password
-V SERVICE_UID="IBM.local\Administrator"

-V SERVICE_PWD="mscs"
```

Configuring the MSCS adapter

You use the adapter configuration dialog to configure your MSCS adapter. If your MSCS adapter is highly available, you always configure the adapter on one node and replicate the configuration file to the remaining cluster nodes as described in "Replicating the configuration files to other nodes" on page 188.

You have two configuration alternatives which are mutually exclusive:

- You can configure the adapter for the operations console of the base component of IBM Tivoli System Automation. In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as *direct access mode*.
- If the end-to-end automation management component is installed, you can configure the adapter for end-to-end automation management. This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode, or if you want to use the operations console of the end-to-end automation management component in first-level automation mode. (For more information on end-to-end automation management and these console modes, refer to the *IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide*.)

Invoking the MSCS adapter configuration dialog

To invoke the configuration dialog, issue the following command:

```
cfgmscsadapter.bat
```

The file is located in the adapter installation directory, in the subdirectory `bin`. The default directory is

```
C:\Program Files\IBM\tsamp\eez\mscs\bin
```

The main panel of the configuration dialog is displayed:

Using the MSCS adapter configuration dialog

On the main panel, click **Configure** to display the configuration panel.

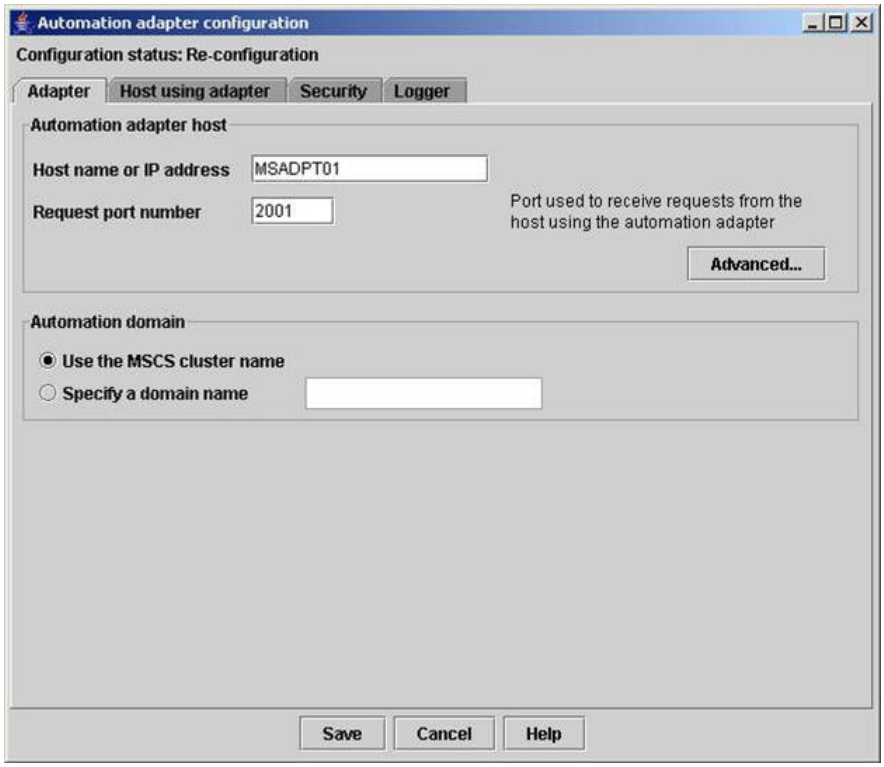


Figure 28. MSCS adapter configuration panel

Adapter tab

Use the Adapter tab (see Figure 28) to make the following specifications:

- Field **Host name or IP address**:
  - If the MSCS adapter *is highly available*, specify the network name or IP address you obtained as described in "Planning and preparing for high availability" on page 179.
  - If the MSCS adapter is *not* highly available, specify the IP address or host name of the system on which the adapter is running.
- Field **Request port number**: Specify the number of the port on which the adapter is listening and which is contacted by the end-to-end automation manager or the base component operations console.
- In the **Automation domain** section, specify the domain name by which the Microsoft Server Clustering (MSCS) cluster is published to the end-to-end automation manager or the base component operations console. If you specify a domain name, ensure that it is unique.

Clicking **Advanced** lets you specify the adapter runtime behavior:

Adapter stop delay
: Delays stopping of the MSCS adapter for the specified number of seconds. This gives the adapter a chance to deliver the domain leave event properly. The default value is 5, the value ranges from 3 through 60. You may need to increase this value on slow systems.

Remote contact activity interval
: Defines the time after which the MSCS adapter stops if there is no

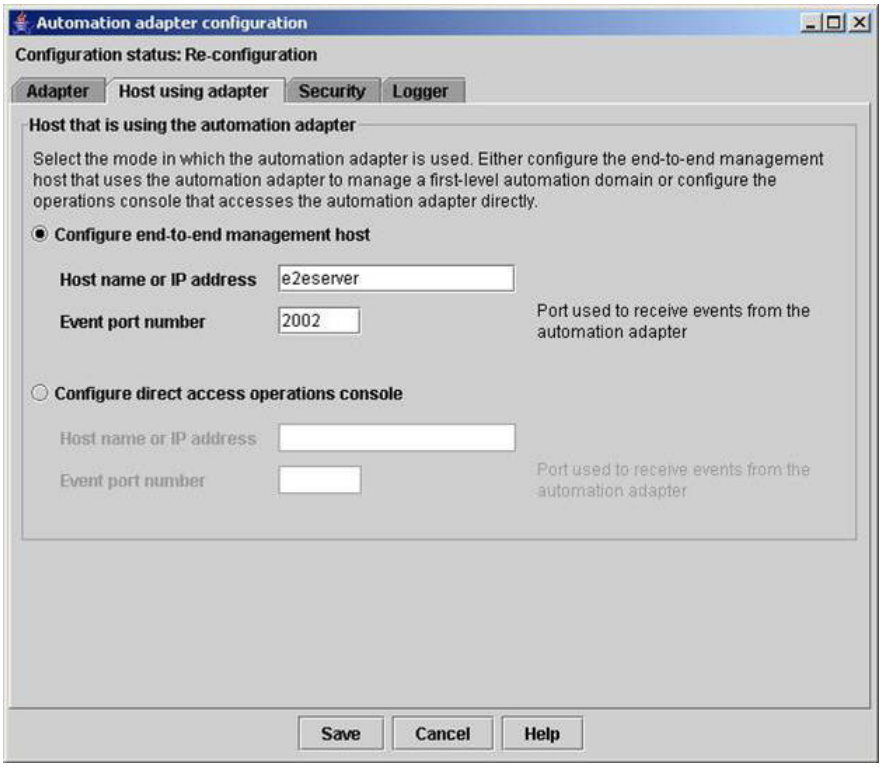
communication with the **host using the adapter**. Setting this parameter to 0 means that the adapter continues to run and never stops. The default value is 360 (seconds).

Initial contact retry interval
: During this period (in minutes) the MSCS adapter tries to contact the **host using the adapter**. This continues until it succeeds or the specified time has elapsed. The default value 0 means that the adapter tries contacting the **host using the adapter** forever.

EIF reconnect attempt interval
: If the connection to the **host using the adapter** was interrupted, this specifies the time the MSCS adapter waits until it tries to reconnect. The default value is 30 seconds.

Host using adapter tab

Use the Host using adapter tab to determine whether the adapter connects to an end-to-end automation management host or a base component operations console, and specify the required information.



Configure end-to-end automation management host:

Host name or IP address
: The name or the IP address of the host on which the end-to-end automation manager runs.

Event port number
: The port on which the end-to-end automation manager listens for events from the MSCS adapter. The default port is '2002'.

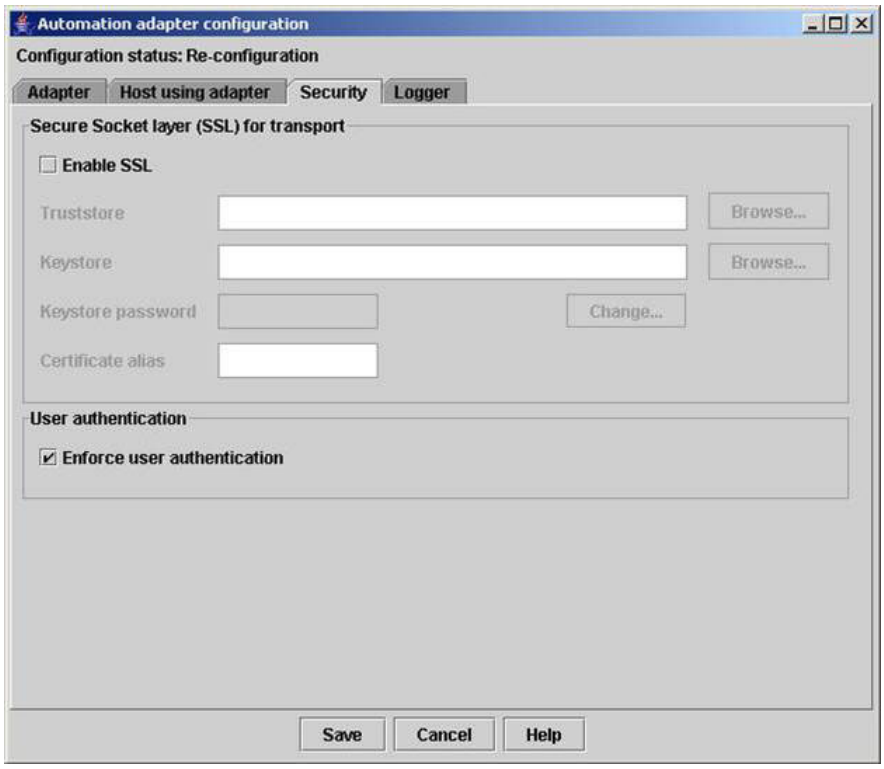
Configure direct access operations console:

Host name or IP address
: The name of the IP address of the host on which the operations console runs.

Event port number
: The port on which the operations console listens for events from the MSCS adapter. The default port is '2002'.

Security tab

Use the Security tab to configure security for the interface between the MSCS adapter and the end-to-end automation management host.



Select the **Enable SSL** check box if you want to use the Secure Socket layer (SSL) protocol. If checked, the following fields must be completed:

Truststore
: Name of the truststore file used for SSL.

Keystore
: Name of the keystore file used for SSL.

Keystore password
: Password of the keystore file. It is required if a keystore file was specified.

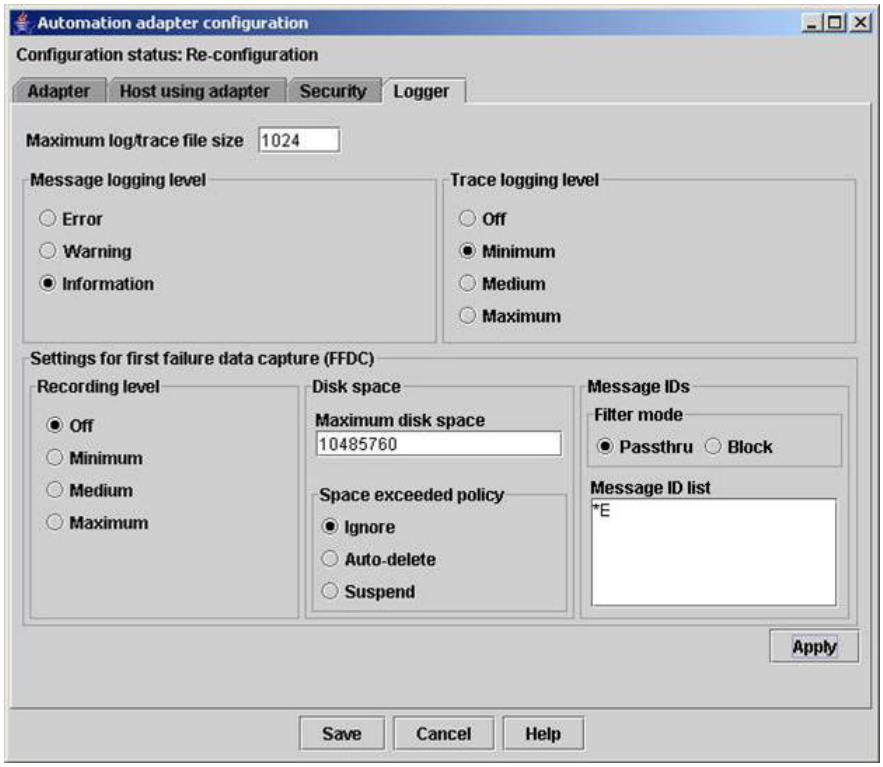
Keystore alias
: Alias name of the certificate to be used by the server. If not specified, the keystore file must contain only one entry which is the one to be used.

It is recommended that you select the corresponding check box to enforce user authentication.

Logger tab

Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.



On the Logger tab, you can perform the following tasks:

Changing the settings permanently

Perform these steps:

1. Make the required changes on the tab.
2. Click **Save**.

Results:

The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

Changing the settings temporarily

Perform these steps after ensuring that the adapter is running:

1. Make the required changes on the tab.
2. Click **Apply**.

Results:

The new settings take effect immediately. They are not stored in the configuration file. If the adapter was not running, you receive an error message.

Reverting to the permanent settings

Perform the following steps to revert to the permanent settings in the configuration file, or when you are unsure which settings are currently active for the adapter:

1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

Results:
The settings take effect immediately. If the adapter is not running, you receive an error message.

Controls and fields on the Logger tab:

Maximum log/trace file size
: The file size in kilobytes.

Message logging level:

Error
: Logs messages on the error level.

Warning
: Logs messages on the error and warning levels.

Information
: Logs messages on the error, warning and informational levels.

Trace logging level:

Off
: Collects no trace information.

Minimum
: Collects trace information on the error level.

Medium
: Collects trace information on the error and warning levels.

Maximum
: Provides the message and trace logs and collects additional information on the error, warning, and informational level.

First failure data capture (FFDC) settings:

- Recording level:

  Off
  : Collects no FFDC information.

  Minimum
  : Provides the message and trace logs and collects additional information on the error level.

  Medium
  : Provides the message and trace logs and collects additional information on the error and warning level.

  Maximum
  : Provides the message and trace logs and collects additional information on the error, warning, and informational level.

- Disk space:

  Maximum disk space
  : Specifies the maximum disk space in bytes used by FFDC traces which are written into the FFDC trace directory. The default space is 10485760 (10MB).

  Space exceeded policy
  : Select what to do if the maximum disk space is exceeded.

- Message IDs:

  Filter mode
  : Initiates the tracing of FFDC data depending on the message IDs listed in 'Message ID list'.

  Message ID list:
  : Specifies the message IDs which trigger the tracing of the FFDC data. Wildcards like *E, meaning all error messages, are allowed.

Saving the configuration

Click **Save** to save your settings to the adapter configuration files. Upon completion, the configuration update status panel appears, showing the list of configuration files that were updated.

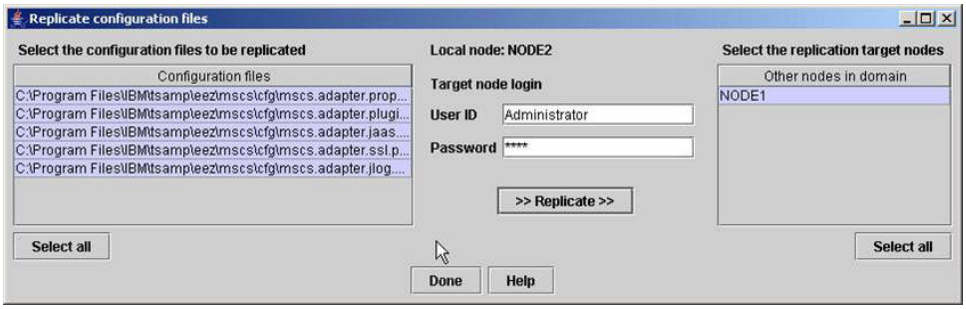
Note: If you change the configuration while the adapter is running, you must restart the adapter for the changes to take effect.

Replicating the configuration files to other nodes

If your MSCS adapter is highly available, you must replicate the configuration files to the other cluster nodes.

Perform the following steps:

1. Open the main panel of the adapter configuration dialog and click **Replicate**. The following panel is displayed:



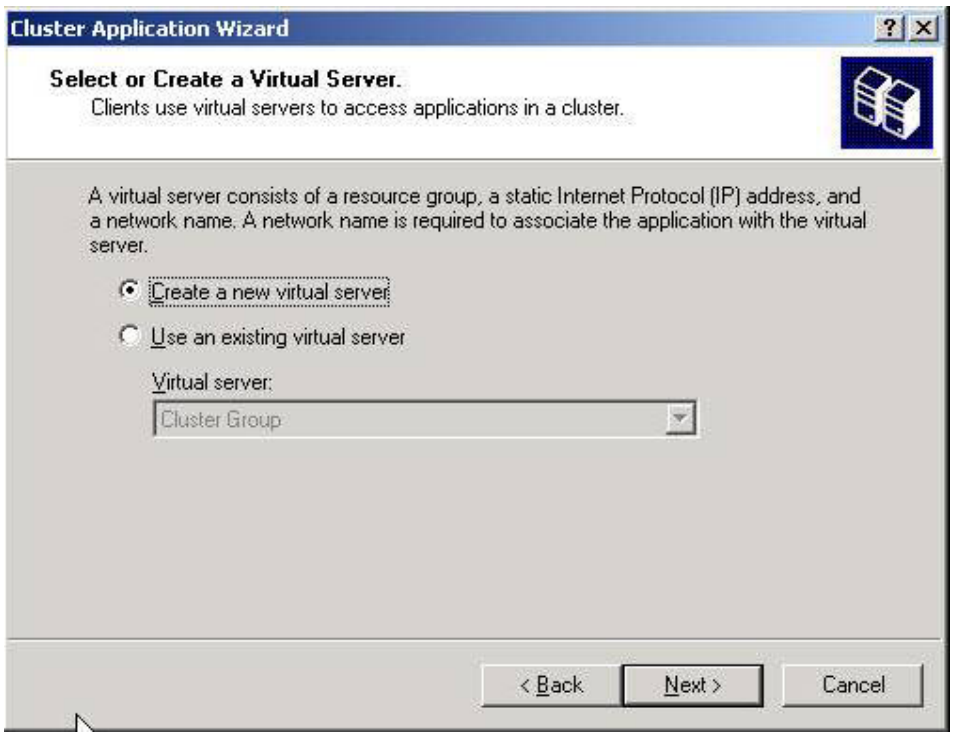
2. On the replication panel, replicate the configuration files to the other cluster nodes:
   a. Select the configuration files you want to replicate, or click **Select all** below the configuration file list to select all files in the list.
   b. In the **Target node login** section, specify a local or domain user ID that is valid on all target nodes. For a local user ID, the specified password must be valid on all target nodes. Domain user IDs must be specified in the form `<user_ID>@<domain_name>`.
   c. Click **Select all** below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
   d. Click **Replicate** to start the replication.

When the replication is complete, a panel shows the replication status of each configuration file for each target node.

Providing high availability for the MSCS adapter

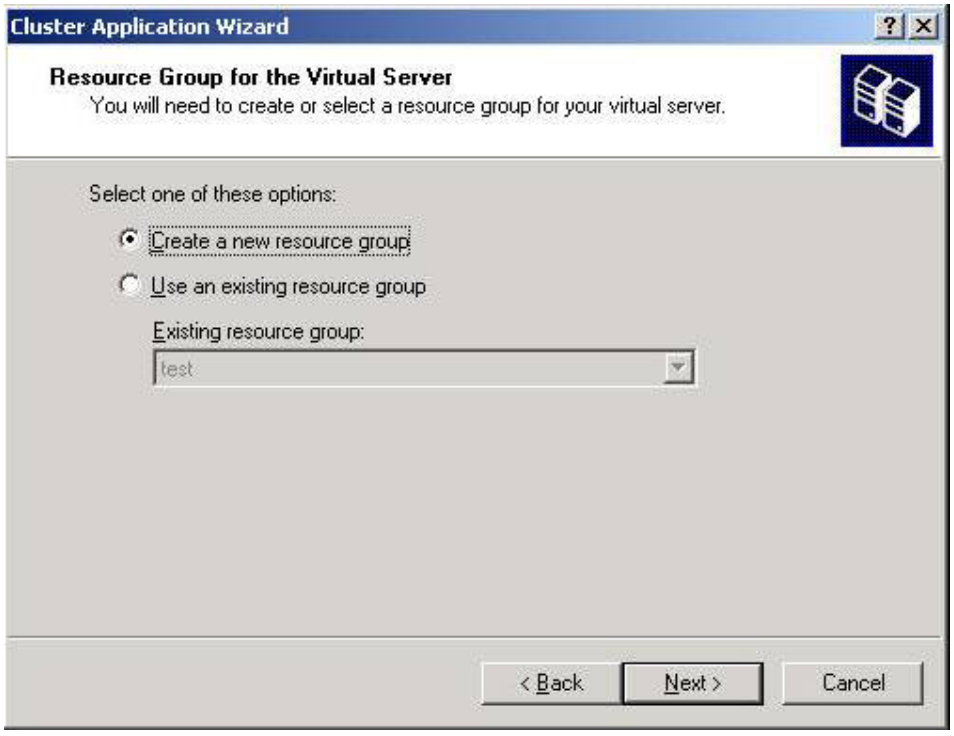
Perform the following steps:

1. Open the Microsoft Cluster Administrator. Launch the Cluster Application Wizard from the **File** menu. On the Welcome panel, click **Next**. The following panels displays:



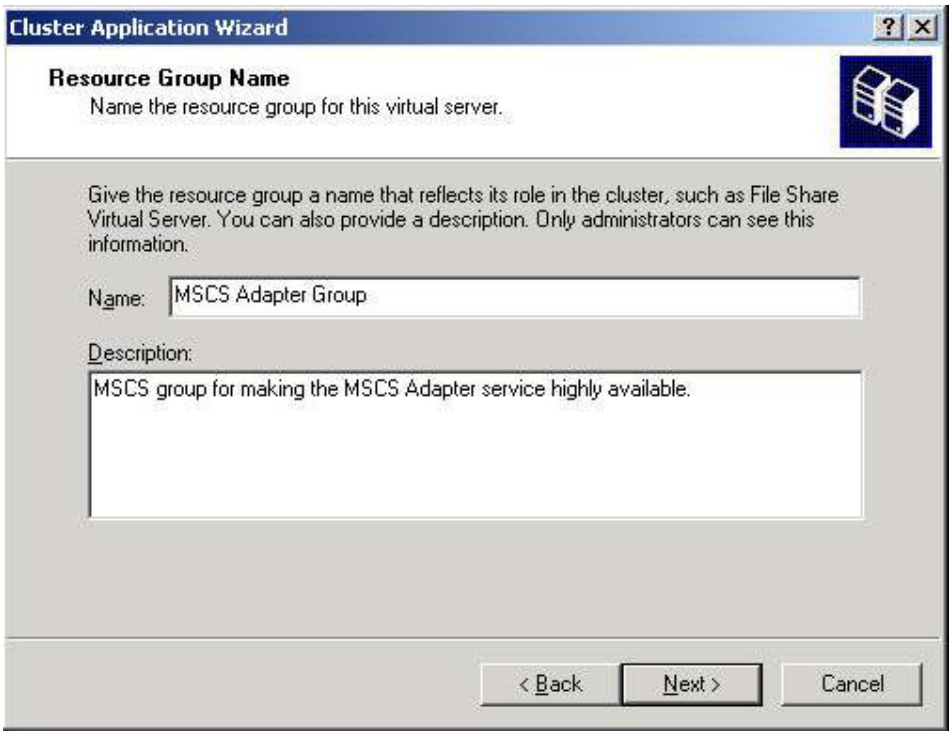
2. It is recommended that you select **Create a new virtual server** to create or assign dedicated resources to the MSCS adapter service resources, for example, the virtual IP address.

   Click **Next**. The following panel is displayed:

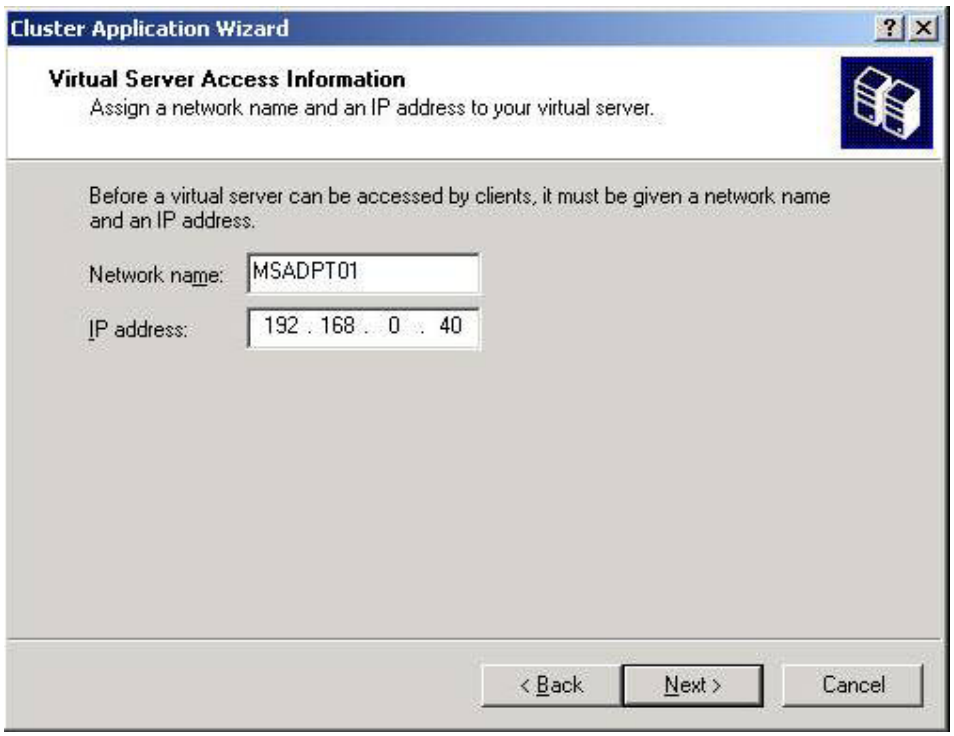


3. Define a new group or identify an existing group representing the MSCS adapter as virtual server. In the following steps, this group is referred to as "virtual server group". You should choose the group containing the quorum resource. If you choose a different group, this group should only contain resources for making the MSCS adapter service highly available.

   Click **Next**. The Resource Group Name panel is displayed:



4. On the Resource Group Name panel, specify a group name and a description. Click **Next**. The Virtual Server Access Information panel is displayed:



5. On the Virtual Server Access Information panel, specify a valid new network name under which the MSCS adapter will be reachable. It must be ensured that the operations console or automation manager to which the MSCS adapter will connect is able to resolve this network name.

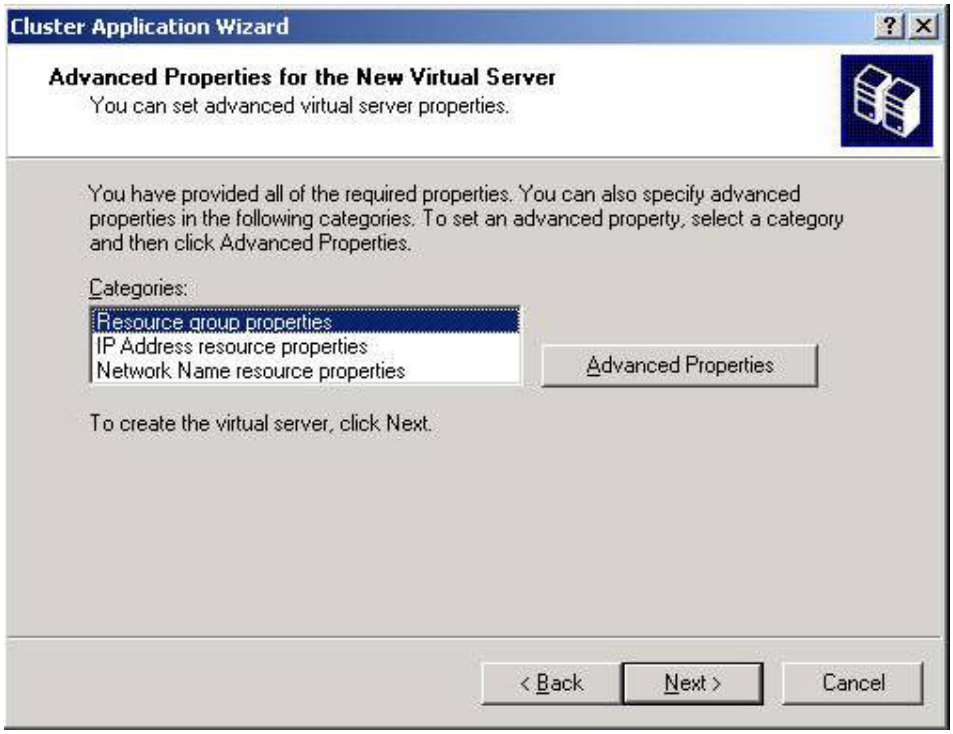
   If you do not want to use a network name for the MSCS adapter, specify a dummy name and remove it later.

   Specify a valid IP address on which the MSCS adapter can be reached. It must be ensured that the operations console or automation manager to which the MSCS adapter will connect is able to reach the virtual IP address.

   Do not specify the IP address shown in the screen capture because it belongs to the private IP address space.

   If the MSCS adapter *is highly available*, specify the network name or IP address you obtained as described in "Planning and preparing for high availability" on page 179.

   Click **Next** to display the Advanced Properties panel:



---

6. Click **Advanced Properties** to view or modify the properties of the selected MSCS group or resource. Typically the default settings are appropriate but should be checked for correctness and completeness.

   Click **Next** to continue.

---

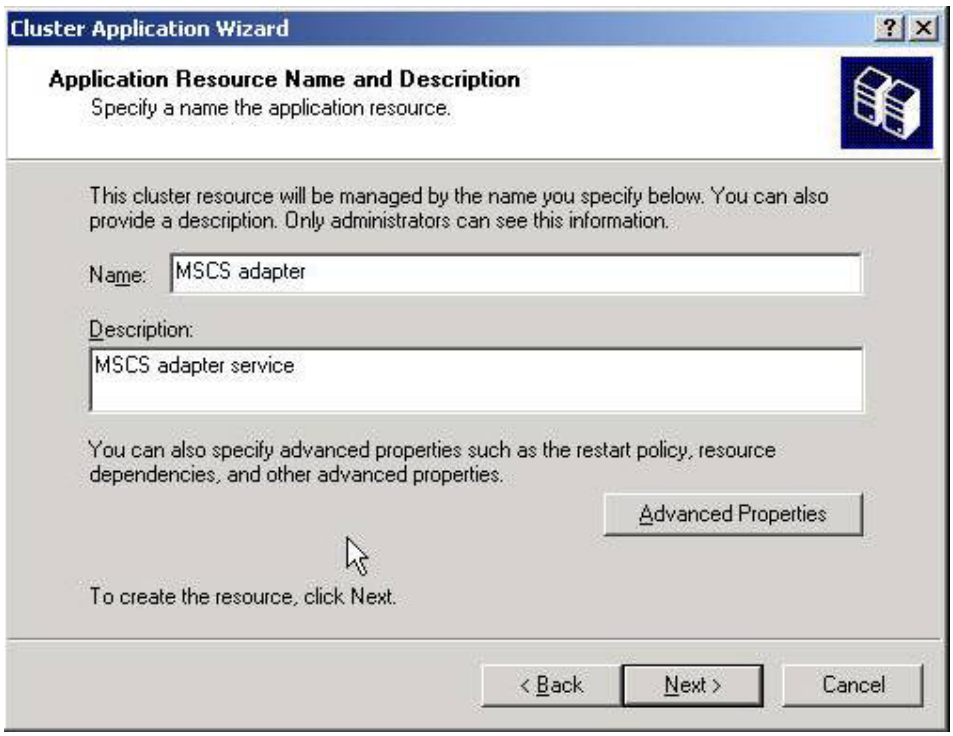
7. On the Create Application Cluster Resource panel, select to create a cluster resource for your application now.

   Click **Next** to continue.

---

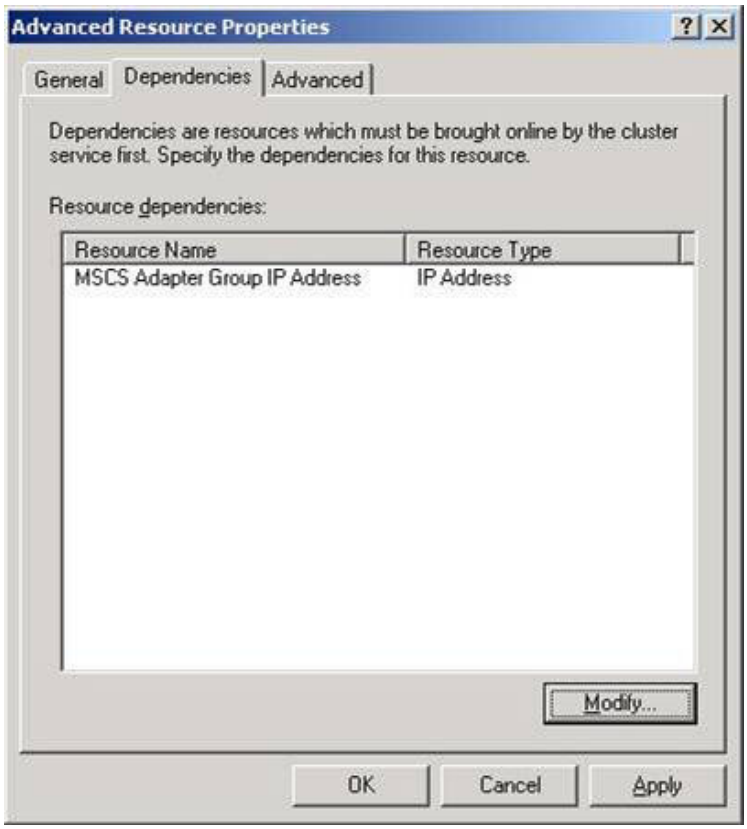
8. On the Application Resource Panel, select **Generic Service** from the drop-down list. An MSCS resource of type Generic Service is used to make the service highly available, because the MSCS adapter runs as Windows service.

   Click **Next** to display the following panel:



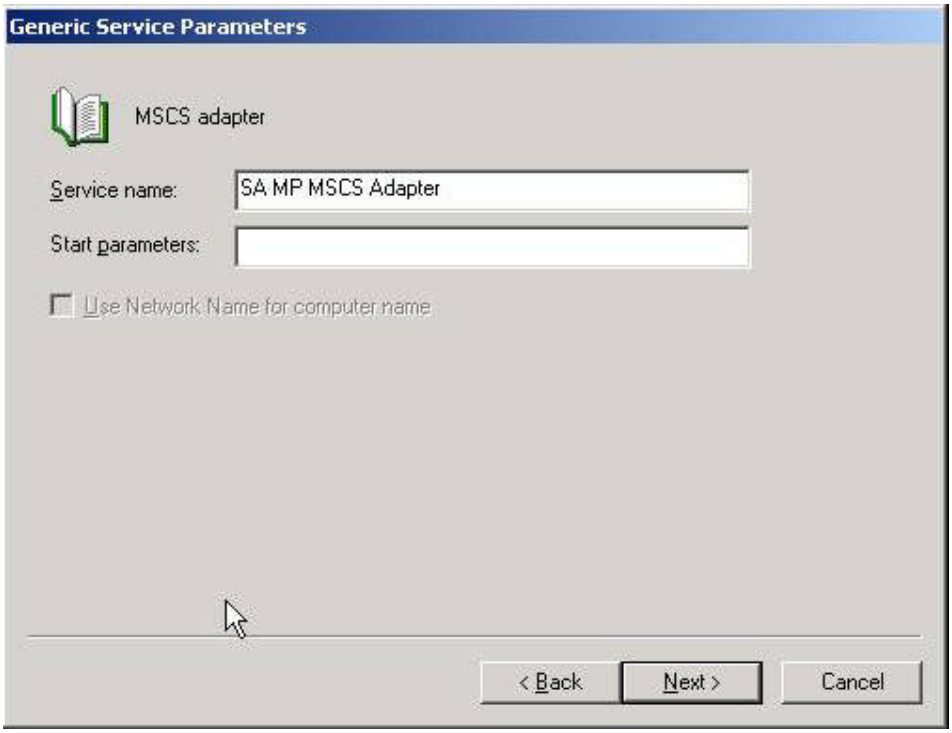
9. Specify an adapter name and a description.

10. Click **Advanced Properties** and open the Dependencies page.



11. On the Dependencies page, do this:
    - If you do not want to define a network name for the MSCS adapter, add a dependency on the “IP Address” resource.
    - If you want to define a network name for the MSCS adapter, add a dependency on the “Network Name” resource.

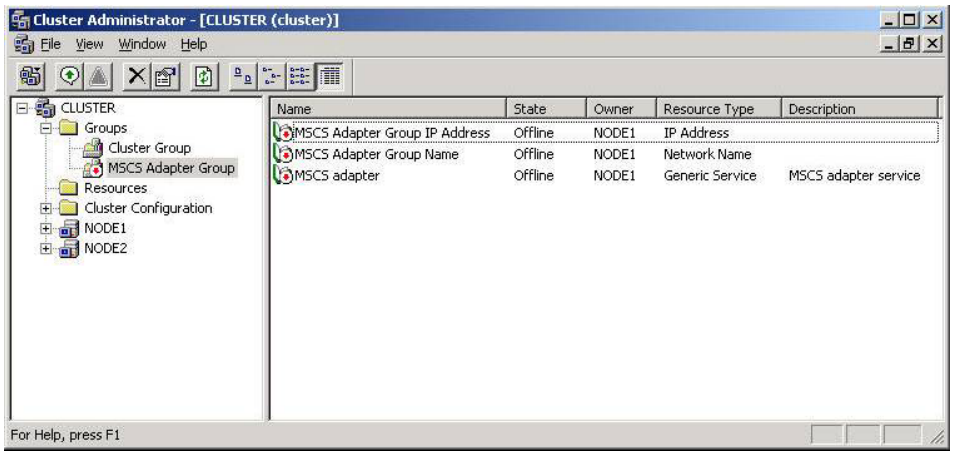
12. Display the Generic Service Parameters panel, type the service name "SA MP MSCS Adapter" in the Service name field. Leave the Start parameters field empty and click **Next**.



13. On the Registry Replication panel that displays, no entries are required. Click **Next**.

14. On the completion panel, verify that the configuration settings are correct, and click **Finish** to save the configuration.

15. If you do not want to use a network name for the MSCS adapter, you can delete it now using the Cluster Administrator:



Verifying the installation and configuration

Perform the following steps to verify that the adapter is installed and configured correctly:

The adapter is highly available:

1. Start the MSCS adapter using MSCS and check if the domain joins.
2. Fail the adapter over to all MSCS nodes and check if the domain joins.

The adapter is not highly available:

- Start the MSCS adapter using the Services plug-in from the Microsoft Management Console and check if the domain joins.

Uninstalling the MSCS adapter

Perform the following steps:

1. Make sure that the MSCS adapter service is stopped before starting the uninstallation.

   Note that MSCS may try to restart or fail the MSCS adapter service over to another MSCS node if you stop the service manually.

   If the MSCS adapter service is highly available, you must take the MSCS adapter group offline.

2. Open the Windows Control Panel and use Add or Remove Programs to uninstall the adapter.

Part 4. Appendixes

Appendix A. Troubleshooting the installation of the base component operations console

Use this section for troubleshooting problems you experience when installing or configuring the base component operations console.

Cleaning up from a failed installation

If the installation was canceled after the installation was started by clicking **Install**, or if the installation failed, you may have to clean up your system manually. Depending on the phase in which the installation was canceled, different clean-up actions may be required:

The installation was canceled before the installation of Integrated Solutions Console began

An automatic roll-back is performed. Typically, no or only minor clean-up actions are required. Retry the installation. If the installation fails, perform the actions described below and restart the installation.

The installation was canceled during the installation of Integrated Solutions Console and the installation of Integrated Console failed

Typically, no or only minor clean-up actions are required. Retry the installation. If the installation fails, perform the actions described below and restart the installation.

The installation was canceled during the installation of Integrated Solutions Console and the installation of Integrated Console completed

Retry the installation. If the installation fails, perform the actions described below and restart the installation.

The installation was canceled after the installation of Integrated Solutions Console completed successfully

Typically, no or only minor clean-up actions are required. Retry the installation. If the installation fails, perform the actions described below and restart the installation.

Cleaning up a Windows system from a failed installation

Perform the following steps:

1. Stop Integrated Solutions Console if the corresponding script is available:

   ```
   <isc_home>\PortalServer\bin\stopISC.bat ISC_Portal <iscadmin uid> <iscadmin pw>
   ```

2. Delete the following directories if they exist:

   ```
   <isc_home>
   <tsamp_root>
   ```

   Use the following commands:

   ```
   del /S /F /Q  <isc_home>
   del /S /F /Q  <tsamp_root>
   ```

   Examples:

   ```
   del /S /F /Q c:\Program Files\IBM\ISC
   del /S /F /Q c:\Program Files\IBM\tsamp
   ```

3. Additional deletions that may be required:

   ```
   del /S /F /Q c:\Program Files\Common Files\InstallShield\Universal\eez
   del /S /F /Q c:\Program Files\IBM\tivoli\common\eez
   ```

Cleaning up an AIX or Linux system from a failed installation

Perform the following steps:

1. Stop Integrated Solutions Console if the corresponding script is available:

   ```
   <isc_home>/PortalServer/bin/stopISC.sh ISC_Portal <iscadmin uid> <iscadmin pw>
   ```

2. Delete the following directories if they exist:

   ```
   <isc_home>
   <EEZ_INSTALL_ROOT>
   ```

   Use the following command:

   ```
   rm -rf <isc_home> <EEZ_INSTALL_ROOT>
   ```

   Example:

   ```
   rm -rf /opt/IBM/ISC /opt/IBM/tsamp/eez
   ```

3. Additional deletions that may be required:

   ```
   rm -rf /tmp/ISC* /tmp/Portal* /tmp/e2e* /tmp/event* /tmp/isc*\
          /tmp/install* /tmp/ismp* /tmp/wps* /tmp/xml* /tmp/serial*\
          /tmp/WP_Fix* /tmp/specFile /tmp/efixes
   ```

Using the installation log files

Installation log file directories

The following table lists the directories to which installation log files are written during the installation.

Table 52. Location of the installation log files

Location

Installation directory of the operations console:
`<EEZ_INSTALL_ROOT>`
 	
Default directory:
Windows:
`C:\Program Files\IBM\tsamp\eez`
AIX/Linux:
`/opt/IBM/tsamp/eez`

Installation log directory of the operations console:
Windows:
`<EEZ_INSTALL_ROOT>\install\logs`
AIX/Linux:
`<EEZ_INSTALL_ROOT>/install/logs`

Table 52. Location of the installation log files (continued)

Location
System temporary directory: **Windows:** %TEMP% Typically, this is: C:\Documents and Settings\<user_name>\Local Settings\temp where <user_name> is the user ID that is used for running the installer **AIX/Linux:** When the environment variable $TEMP is set, the directory specified in the environment variable. Typically, this is: /tmp When the environment variable is not set, the logs are written to the directory /tmp.
WebSphere Application Server profile log directory: **Windows:** <isc_home>\AppServer\profiles\default\logs **AIX/Linux:** <isc_home>/AppServer/profiles/default/logs

Installation log files

The tables in the following sections list the log files that are written during the installation of the operations console:

- Section "Pre-installation phase log files" lists the log files that are written in the pre-installation phase, that is, before you click the **Install** button in the installation wizard.
- Section "Installation phase log files" on page 202 lists the log files that are written in the installation phase, that is, after you click the **Install** button in the installation wizard.

In the tables, the following acronym is used:

ISC Integrated Solutions Console is the application server in which the operations console runs

Pre-installation phase log files

During the pre-installation phase, that is, before you click the **Install** button in the installation wizard, various log files are created:

- **e2ewizard.log**

  This is the first log file the installation wizard creates. Use it as the first source of information if you encounter problems during the pre-installation phase.

  The file is located in the system temporary directory (refer to Table 52 on page 200).

  At the beginning of the installation phase, after you click the Install button in the installation wizard, the contents of the file are copied to the installation log file e2einstaller.log (refer to "Installation phase log files" on page 202).

- **Task-specific pre-installation log files**

During the pre-installation phase, the installation wizard initiates numerous tasks. The messages that are generated while the tasks are performed are logged in task-specific log files.

To find out the names and locations of these log files, refer to the log file `e2ewizard.log`. It contains references that let you identify and locate these log files.

Installation phase log files

During the installation phase, that is, after you click the **Install** button, various log files are created:

- **`e2einstaller.log`**

  This is the log file to which the installation wizard logs information during the installation phase. Use it as the first source of information if you encounter problems during the installation phase.

  The file is located in the installation directory of the operations console (refer to Table 52 on page 200).

  The file is created at the beginning of the installation phase. The contents of the pre-installation phase log file `e2ewizard.log` are copied to the file.

- **Task-specific installation-phase log files**

  During the installation phase, the installation wizard initiates numerous tasks. The messages that are generated while the tasks are performed are logged in task-specific log files.

  To find out the names and locations of these log files, refer to the log file `e2einstaller.log`. It contains references that let you identify and locate these log files.

- **Installation log files in the system temporary directory** (refer to Table 52 on page 200).

  Table 53. Installation logs in the system temporary directory

Log file name	Description
`ISCAction.log`	This log file is written while the ISC installer checks whether there is already an ISC installed in the WebSphere Application Server.
`ISCRuntime.rsp`	This response file contains all the information that was passed to the Integrated Solutions Console installer.
`ISCRuntimeConfig.properties`	This properties file contains all the information used by the Integrated Solutions Console installer.
`ISCRuntimeInstallProgress.properties`	This properties file contains a progress indicator for a running Integrated Solutions Console installation. For a completed installation, it contains the information whether the installation was successful.
`ISCRuntimeInstall.log`	The main log file for the Integrated Solutions Console installation. Calls the following sub-installation tasks: ISCPreInstallConfigTask ISCPostInstallConfigTask.

Table 53. Installation logs in the system temporary directory (continued)

Log file name	Description
ISCPreInstallConfigTask.log	Installs WebSphere Portal. Called by ISCRuntimeInstall.
wpsinstalllog.txt	Log file for WebSphere Portal installation.
ISCPostInstallConfigTask.log	Prepares the installation of Integrated Solutions Console and performs the installation. Called by ISCRuntimeInstall.
PortalBasicConfig.log	Prepares WebSphere Portal for the installation of Integrated Solutions Console. Called by ISCPostInstallConfigTask.
ISCUpdatePorts.log	Updates the ports of the Integrated Solutions Console Portal server. Called by ISCPostInstallConfigTask.
ISCEnableSecurityDB.log	Enables WebSphere Application Server security. The log file is written when DB2 is used as the user registry. Called by ISCPostInstallConfigTask.
ISCEnableSecurityLDAPNew.log	Enables WebSphere Application Server security. The log file is written when LDAP is used as the user registry. Called by ISCPostInstallConfigTask.
ISCSetupISCXml.log	Changes the WebSphere Portal configuration settings. Called by ISCPostInstallConfigTask.
PortalDeployConfig.log	Changes the Integrated Solutions Console configuration settings. Called by ISCPostInstallConfigTask.
WP_Fixes.log	Installs the WebSphere Application Server fixes needed by WebSphere Portal and Integrated Solutions Console. Called by ISCPostInstallConfigTask.
PortalPostConfig.log	Changes the Integrated Solutions Console configuration settings. Called by ISCPostInstallConfigTask.
ISCDeploy_AdminComponents	Contains return codes of deploy operations.

Procedures for troubleshooting an installation

If the installation fails, the installation wizard displays an error message. The error message either describes the cause of the failure or points you to the log file that you need to analyze to resolve the problem.

When an error occurs, immediately archive the installation log files (see "Using the log file collector utility"). This ensures that the original log files are retained, which is important should you need to contact IBM Support, and you can use the archive for your own troubleshooting activities.

An error occurred in the pre-installation phase

When the error occurred in the pre-installation phase, that is, before the **Install** button was clicked, perform the following steps:

1. Use the log file collector utility to archive the log files (see "Using the log file collector utility") and use the archive in the subsequent steps.
2. View the log file `e2ewizard.log`
3. Search for error indications
4. View all additional log files that are written in the pre-installation phase and search for error indications. The names and locations of the additional log files appear in the file `e2ewizard.log`. The files are also listed in "Pre-installation phase log files" on page 201.

An error occurred in the installation phase

When the error occurred in the installation phase, that is, after the **Install** button was clicked, perform the following steps:

1. Use the log file collector utility to archive the log files (see "Using the log file collector utility") and use the archive in the subsequent steps.
2. View the file `e2einstaller.log`
3. Search for error indications, for example, unexpected return codes (RC) or exceptions. Search for the strings ″RC″ and ″Exception″. Locate the first problem that occurred.
4. Check for previous or subsequent messages that may explain why the problem occurred.
5. Check whether the failed step creates an additional log file. If this is the case, view the relevant log file. The names and locations of the additional log files appear in the file `e2einstaller.log`. The files are also listed in "Installation phase log files" on page 202.
6. Repeat the procedure for each log file.

Using the log file collector utility

When an error occurs, use the you log file collector utility to collect the log files that were written during the installation. The utility generates an archive that you can use for your own troubleshooting activities and send to IBM Support if you cannot resolve the error.

Perform these steps to run the log file collector utility:

1. Change the directory to `<EEZ_INSTALL_ROOT>/install`.
2. Issue the following command:
   Windows: **e2einstallerlogs**
   AIX/Linux: **e2einstallerlogs.sh**

   Note: If Java is not available on the system, you must specify the path to the JAR tool, which is available on the operations console installation CD, when you invoke the log file collector utility.

   Examples:

   - **Windows:**

     ```
     e2einstallerlogs d:\EEZ2200E2EWindows\Windows\ISC\RuntimeExt\ewase\windows\java\bin\jar
     ```

- **AIX/Linux:**

  ```
  e2einstallerlogs.sh <cd_mount_point> /EEZ2200E2EAIX/AIX/ISC/RuntimeExt/ewase/aix/java/bin/jar
  ```

Result:

The installer log archive is created in the directory from which you invoked the collector utility. The name of the archive has the following format:

```
e2einstallerlogs_<timestamp>.zip
```

where `<timestamp>` is a concatenation of the current date and the time at which the collector utility was invoked.

Gathering information for IBM Support

If you cannot resolve an installation problem, send the installation log file archive to IBM support (see "Using the log file collector utility" on page 204).

Appendix B. Troubleshooting the installation of the end-to-end automation management component

Use this section for troubleshooting problems you experience when installing or configuring the end-to-end automation management component.

Installation wizard cannot find WebSphere Application Server on the system

The installation program for SA for Multiplatforms uses InstallShield to install code. InstallShield uses the `vpd.properties` file to track products that it installs.

WebSphere Application Server also uses InstallShield. WebSphere Application Server must be installed on the system before end-to-end automation management can be installed. If the installation wizard of Tivoli System Automation for Multiplatforms does not detect WebSphere Application Server on the system but you did install it, check whether the file `vpd.properties` exists and correct its contents.

This is where you find the `vpd.properties` file:

- **AIX**:

  In the root directory or in the directory `/usr/lib/objrepos`
- **Linux**:

  In the root directory
- **Windows**

  In installation directory of the operating system, for example, `C:\windows`

If you cannot locate the file, your WebSphere Application Server installation may be damaged, in which case you need to re-install WebSphere Application Server. For more information about the `vpd.properties` file, refer to the WebSphere Application Server Help System.

DB2 access test hangs

If the progress bar of the installation wizard stays at 98% for a long time during the DB2 access test, the test may be hung. The DB2 password may be expired. To resolve the problem, perform these steps:

1. End the installer. Because **Cancel** is not enabled at this point, you must end the installer using the Task manager (on Windows systems) or the **kill** command (on UNIX systems).
2. Check if the DB2 password is expired.
3. Renew the DB2 password.
4. Restart the installation.

The installation of the operations console fails

This may occur when an error is encountered during the creation of the operations console database. To check if this is the case, view the log file `ISCRuntimeInstall.log` and search for an error message like the one in the following example:

```
COM.ibm.db2.jdbc.DB2Exception: [IBM][CLI Driver] SQL30061N
The database alias or database name "OPCONDBD"
was not found at the remote node.  SQLSTATE=08004
```

The log file `ISCRuntimeInstall.log` is written to the system temporary directory (refer to Table 54 on page 210).

Login to Integrated Solutions Console fails

Symptom: You cannot log in to Integrated Solutions Console after the installation of the end-to-end automation management component is complete.

Cause: An incorrect DB2 instance port number was specified during the installation of the end-to-end automation management component.

Solution: Uninstall and reinstall the end-to-end automation management component.

Cleaning up from a failed installation

If the installation was canceled after the installation was started by clicking **Install**, or if the installation failed, you may have to clean up your system manually. Depending on the phase in which the installation failed or was canceled, different clean-up actions may be required:

The installation was canceled before the installation of Integrated Solutions Console began

An automatic roll-back is performed. Typically, no or only minor clean-up actions are required. Retry the installation. If the installation fails, perform the actions described below and restart the installation.

The installation was canceled during the installation of Integrated Solutions Console and the installation of Integrated Console failed

Typically, no or only minor clean-up actions are required. Retry the installation. If the installation fails, perform the actions described below and restart the installation.

The installation was canceled during the installation of Integrated Solutions Console and the installation of Integrated Console completed

Retry the installation. If the installation fails, perform the actions described below and restart the installation.

The installation was canceled after the installation of Integrated Solutions Console completed successfully

Typically, no or only minor clean-up actions are required. Retry the installation. If the installation fails, perform the actions described below and restart the installation.

Cleaning up a Windows system from a failed installation

Perform the following steps:

1. Stop the following components if the corresponding scripts are available:

- **End-to-end automation engine**

  Issue the following command:

  ```
  <EEZ_INSTALL_ROOT>\bin\eezdmn.bat -shutd
  ```

- **Integrated Solutions Console**

  Issue the following command:

  ```
  <isc_runtime_root>\PortalServer\bin\stopISC.bat ISC_Portal <iscadmin uid> <iscadmin pw>
  ```

- **WebSphere Application Server**

  Issue the following command:

  ```
  <was_root>\bin\stopServer server1 -username <iscadmin uid> -password <iscadmin pw>
  ```

2. Drop the databases if they exist (only required for a local DB2 setup)
   a. Log in as the DB2 database instance owner
   b. Drop the database:

      ```
      db2 drop database EAUTODB
      db2 drop database OPCONDBD
      ```

3. Delete the following directories if they exist:

   ```
   <isc_runtime_root>
   <tsamp_root>
   ```

   Use the following commands:

   ```
   del /S /F /Q  <isc_install_dir>
   del /S /F /Q  <tsamp_root>
   ```

   Examples:

   ```
   del /S /F /Q c:\Program Files\IBM\ISC
   del /S /F /Q c:\Program Files\IBM\tsamp
   ```

4. Additional deletions that may be required:

   ```
   del /S /F /Q c:\Program Files\Common Files\InstallShield\Universal\eez
   del /S /F /Q c:\Program Files\IBM\tivoli\common\eez
   ```

5. Remove and recreate the WebSphere Application Server profile (see "Post-installation tasks" on page 76).

Cleaning up an AIX or Linux system from a failed installation

Perform the following steps:

1. Stop the following components if the corresponding scripts are available:
   - **End-to-end automation engine**

     Issue the following command:

     ```
     <EEZ_INSTALL_ROOT>/bin/eezdmn.sh -shutd
     ```

   - **Integrated Solutions Console**

     Issue the following command:

     ```
     <isc_runtime_root>/PortalServer/bin/stopISC.sh ISC_Portal <iscadmin uid> <iscadmin pw>
     ```

   - **WebSphere Application Server**

     Issue the following command:

     ```
     <was_root>/bin/stopServer.sh server1 -username <iscadmin uid> -password <iscadmin pw>
     ```

2. Drop the databases if they exist (only required for a local DB2 setup)
   a. Log in as the DB2 database instance owner
   b. Drop the database:

      ```
      db2 drop database EAUTODB
      db2 drop database OPCONDBD
      ```

3. Delete the following directories if they exist:

```
<isc_runtime_root>
<EEZ_INSTALL_ROOT>
```

Use the following command:

```
rm -rf <isc_runtime_root> <EEZ_INSTALL_ROOT>
```

Example:

```
rm -rf /opt/IBM/ISC /opt/IBM/tsamp/eez
```

4. Additional deletions that may be required:

```
rm -rf /tmp/ISC* /tmp/Portal* /tmp/e2e* /tmp/event* /tmp/isc*\
       /tmp/install* /tmp/ismp* /tmp/wps* /tmp/xml* /tmp/serial*\
       /tmp/WP_Fix* /tmp/specFile /tmp/efixes
```

5. Remove and recreate the WebSphere Application Server profile (see "Post-installation tasks" on page 76).

Using the installation log files

Installation log file directories

The following table lists the directories to which installation log files are written during the installation of the end-to-end automation management component.

Table 54. Location of the installation log files

Location
Installation directory of the end-to-end automation management component: <EEZ_INSTALL_ROOT> Default directory: **Windows:** C:\Program Files\IBM\tsamp\eez **AIX/Linux:** /opt/IBM/tsamp/eez
Installation log directory of the end-to-end automation management component: **Windows:** <EEZ_INSTALL_ROOT>\install\logs **AIX/Linux:** <EEZ_INSTALL_ROOT>/install/logs
System temporary directory: **Windows:** %TEMP% Typically, this is: C:\Documents and Settings\<user_name>\Local Settings\temp where <user_name> is the user ID that is used for running the installer **AIX/Linux:** When the environment variable $TEMP is set, the directory specified in the environment variable. Typically, this is: /tmp When the environment variable is not set, the logs are written to the directory /tmp.

Table 54. Location of the installation log files (continued)

Location

WebSphere Application Server profile log directory:
Windows:
`<was_root>\profiles\<profile>\logs`
AIX/Linux:
`<was_root>/profiles/<profile>/logs`
where `<profile>` is the profile you specified in the installation wizard during the installation of the end-to-end automation management component (refer to step 17 on page 100).

Installation log files

The tables in the following sections list the log files that are written during the installation of the end-to-end automation management component:

- Section "Pre-installation phase log files" lists the log files that are written in the pre-installation phase, that is, before you click the **Install** button in the installation wizard.
- Section "Installation phase log files" on page 212 lists the log files that are written in the installation phase, that is, after you click the **Install** button in the installation wizard.

In the tables, the following acronyms appear:

ISC Integrated Solutions Console is the application server in which the operations console runs

CEI Common Event Infrastructure is part of the Tivoli Enterprise Console (TEC) server connection

EIF Event Instrumentation Framework is part of the Tivoli Enterprise Console (TEC) server connection

Pre-installation phase log files

During the pre-installation phase, that is, before you click the **Install** button in the installation wizard, various log files are created:

- **`e2ewizard.log`**

  This is the first log file the installation wizard creates. Use it as the first source of information if you encounter problems during the pre-installation phase.

  The file is located in the system temporary directory (refer to Table 54 on page 210).

  At the beginning of the installation phase, after you click the Install button in the installation wizard, the contents of the file are copied to the installation log file `e2einstaller.log` (refer to "Installation phase log files" on page 212).

- **Task-specific pre-installation log files**

  During the pre-installation phase, the installation wizard initiates numerous tasks. The messages that are generated while the tasks are performed are logged in task-specific log files.

  To find out the names and locations of these log files, refer to the log file `e2ewizard.log`. It contains references that let you identify and locate these log files.

Installation phase log files

During the installation phase, that is, after you click the **Install** button, various log files are created:

- **e2einstaller.log**

  This is the log file to which the installation wizard logs information during the installation phase. Use it as the first source of information if you encounter problems during the installation phase.

  The file is located in the installation directory of the end-to-end automation management component (refer to Table 54 on page 210).

  The file is created at the beginning of the installation phase. The contents of the pre-installation phase log file `e2ewizard.log` are copied to the file.

- **Task-specific installation-phase log files**

  During the installation phase, the installation wizard initiates numerous tasks. The messages that are generated while the tasks are performed are logged in task-specific log files.

  To find out the names and locations of these log files, refer to the log file `e2einstaller.log`. It contains references that let you identify and locate these log files.

- **Installation-phase log files in the WebSphere Application Server profile log directory or in the system temporary directory**

  The log files listed in Table 55 are written to either the WebSphere Application Server profile log directory or the system temporary directory or both (refer to Table 54 on page 210) during the installation phase:

  Table 55. Installation logs in the WebSphere Application Server profile log directory or in the system temporary directory

Log file name	Description
`events_install_msg.log`	CEI installation messages
`events_install_trc.log`	CEI installation traces
`events_db_install_msg.log`	CEI database configuration messages
`events_db_install_trc.log`	CEI database configuration traces

- **Installation log files in the system temporary directory** (refer to Table 54 on page 210).

  Table 56. Installation logs in the system temporary directory

Log file name	Description
`ISCAction.log`	This log file is written while the ISC installer checks whether there is already an ISC installed in the WebSphere Application Server.
`ISCRuntime.rsp`	This response file contains all the information that was passed to the Integrated Solutions Console installer.
`ISCRuntimeConfig.properties`	This properties file contains all the information used by the Integrated Solutions Console installer.

Table 56. Installation logs in the system temporary directory (continued)

Log file name	Description
ISCRuntimeInstallProgress.properties	This properties file contains a progress indicator for a running Integrated Solutions Console installation. For a completed installation, it contains the information whether the installation was successful.
ISCRuntimeInstall.log	The main log file for the Integrated Solutions Console installation. Calls the following sub-installation tasks: ISCPreInstallConfigTask ISCPostInstallConfigTask.
ISCPreInstallConfigTask.log	Installs WebSphere Portal. Called by ISCRuntimeInstall.
wpsinstalllog.txt	Log file for WebSphere Portal installation.
ISCPostInstallConfigTask.log	Prepares the installation of Integrated Solutions Console and performs the installation. Called by ISCRuntimeInstall.
PortalBasicConfig.log	Prepares WebSphere Portal for the installation of Integrated Solutions Console. Called by ISCPostInstallConfigTask.
ISCUpdatePorts.log	Updates the ports of the Integrated Solutions Console Portal server. Called by ISCPostInstallConfigTask.
ISCEnableSecurityDB.log	Enables WebSphere Application Server security. The log file is written when DB2 is used as the user registry. Called by ISCPostInstallConfigTask.
ISCEnableSecurityLDAPNew.log	Enables WebSphere Application Server security. The log file is written when LDAP is used as the user registry. Called by ISCPostInstallConfigTask.
ISCSetupISCXml.log	Changes the WebSphere Portal configuration settings. Called by ISCPostInstallConfigTask.
PortalDeployConfig.log	Changes the Integrated Solutions Console configuration settings. Called by ISCPostInstallConfigTask.
WP_Fixes.log	Installs the WebSphere Application Server fixes needed by WebSphere Portal and Integrated Solutions Console. Called by ISCPostInstallConfigTask.

Table 56. Installation logs in the system temporary directory (continued)

Log file name	Description
`PortalPostConfig.log`	Changes the Integrated Solutions Console configuration settings. Called by ISCPostInstallConfigTask.
`ISCDeploy_AdminComponents`	Contains return codes of deploy operations.

Procedures for troubleshooting an installation

If the installation fails, the installation wizard displays an error message. The error message either describes the cause of the failure or points you to the log file that you need to analyze to resolve the problem.

When an error occurs, immediately archive the installation log files (see "Using the log file collector utility" on page 215). This ensures that the original log files are retained, which is important should you need to contact IBM Support, and you can use the archive for your own troubleshooting activities.

An error occurred in the pre-installation phase

When the error occurred in the pre-installation phase, that is, before the **Install** button was clicked, perform the following steps:

1. Use the log file collector utility to archive the log files (see "Using the log file collector utility" on page 215) and use the archive in the subsequent steps.
2. View the log file `e2ewizard.log`
3. Search for error indications
4. View all additional log files that are written in the pre-installation phase and search for error indications. The names and locations of the additional log files appear in the file `e2ewizard.log`. The files are also listed in "Pre-installation phase log files" on page 211.

An error occurred in the installation phase

When the error occurred in the installation phase, that is, after the **Install** button was clicked, perform the following steps:

1. Use the log file collector utility to archive the log files (see "Using the log file collector utility" on page 215) and use the archive in the subsequent steps.
2. View the file `e2einstaller.log`
3. Search for error indications, for example, unexpected return codes (RC) or exceptions. Search for the strings ″RC″ and ″Exception″. Locate the first problem that occurred.
4. Check for previous or subsequent messages that may explain why the problem occurred.
5. Check whether the failed step creates an additional log file. If this is the case, view the relevant log file. The names and locations of the additional log files appear in the file `e2einstaller.log`. The files are also listed in "Installation phase log files" on page 212.
6. Repeat the procedure for each log file.

Using the log file collector utility

When an error occurs, use the you log file collector utility to collect the log files that were written during the installation. The utility generates an archive that you can use for your own troubleshooting activities and send to IBM Support if you cannot resolve the error.

Perform these steps to run the log file collector utility:

1. Change the directory to `<EEZ_INSTALL_ROOT>/install`.
2. Issue the following command:
   Windows: **e2einstallerlogs**
   AIX/Linux: **e2einstallerlogs.sh**

   Note: If Java is not available on the system, you must specify the path to the JAR tool, which is available on the end-to-end automation management component installation CD, when you invoke the log file collector utility.

   Examples:

   - **Windows:**

     ```
     e2einstallerlogs d:\EEZ2200E2EWindows\Windows\ISC\RuntimeExt\ewase\windows\java\bin\jar
     ```

   - AIX/Linux:

     ```
     e2einstallerlogs.sh <cd_mount_point> /EEZ2200E2EAIX/AIX/ISC/RuntimeExt/ewase/aix/java/bin/jar
     ```

Result:

The installer log archive is created in the directory from which you invoked the collector utility. The name of the archive has the following format:

`e2einstallerlogs_<timestamp>.zip`

where `<timestamp>` is a concatenation of the current date and the time at which the collector utility was invoked.

Gathering information for IBM Support

If you cannot resolve an installation problem, send the installation log file archive to IBM support (see “Using the log file collector utility”).

Appendix C. Troubleshooting the installation of the HACMP adapter

Use this section for troubleshooting problems you experience when installing or configuring the HACMP adapter.

HACMP adapter does not start

Possible causes:

- HACMP level is lower than 5.3.0.5

  To check, use: `lslpp –l cluster.es.server.utils`
- Cluster services have not been started

  Start the services using smitty: **hacmp** —> C-SPOC —> Manage...

HACMP adapter terminates

Cluster services terminated while the HACMP adapter was running
If the adapter is automated, it should restart automatically on next priority node where cluster services run.

Adapter attempts to start but terminates again
This may indicate that the adapter has not been configured correctly.

Adapter does not connect to the host

Make sure the firewall allows connections in both directions.

Check with netstart:

- whether the adapter listens on the request port (default port is `2001`)
- whether the end-to-end automation manager or the base component operations console listens on the event port (default port is `2002`)

HACMP adapter log files

Increasing the trace logging level

If your trace is not detailed enough to analyze a problem and the problem can be recreated, it may be useful to increase the trace logging level:

1. Invoke the adapter configuration dialog using **cfghacadapter**.
2. On the main panel of the configuration dialog, click **Configure**.
3. Select the Logger tab.
4. Set the **Trace logging level** to **Maximum**.
5. Click **Apply**. The new setting takes effect immediately.

For more information about the Logger tab, see “**Logger** tab” on page 170.

Log file locations

The HACMP adapter log files are located in the Tivoli Common Directory:

- Default location: `/var/ibm/tivoli/common`

- HACMP adapter-specific subdirectory structure in the Tivoli Common Directory:
  - `eez/ffdc` – Contains the First Failure Data Capture files (if the FFDC recording level is not set to Off in the adapter configuration dialog)
  - `eez/logs` – Contains the HACMP adapter trace file:
    - `traceFlatAdapter.log`

Appendix D. Troubleshooting the installation of the MSCS adapter

Use this section for troubleshooting problems you experience when installing or configuring the MSCS adapter.

MSCS adapter log files

This is where the adapter log files are located:

- Tivoli Common Directory

  Default location: `C:\Program Files\IBM\tivoli\common`

  MSCS adapter-specific subdirectory structure in Tivoli Common Directory:

  – `eez\ffdc` – Contains the First Failure Data Capture files (if the FFDC recording level is not set to Off in the adapter configuration dialog)

  – `eez\logs` – Contains the MSCS adapter log files:

    - `msgMSCSAdapter.log`
    - `traceMSCSAdapter.log` (if trace logging level is not set to Off)
    - `eventMSCSAdapter.log` (if trace logging level is not set to Off)

- The default adapter installation directory is `C:\Program Files\IBM\tsamp\eez\mscs`.

  Subdirectories and files used for troubleshooting:

  – The file `data\eez.release.information.txt` is created in the adapter installation directory when the MSCS adapter is started. It contains information about service applied to the MSCS adapter and about the configuration settings used.

  – The installation log files are located in the subdirectory `_inst_logs`.

MSCS adapter installation fails

If the installation wizard indicates a problem, check the installer output and the following files for error messages:

- The file `mscsinstaller.log` in the adapter installation directory
- The log files in the `_inst_logs` subdirectory of the adapter installation directory

Adapter configuration dialog problems occur

A problem occurs using the adapter configuration dialog

Problem determination:

- The file `cfgmscsadapter.bat` contains a command for launching the configuration dialog
- The file contains a duplicate of this command which enables diagnostic output (option **-DEBUG**)

The Apply button on the Logger page cannot be clicked

Possible cause: The MSCS adapter is not running.

Configuration files cannot be replicated

Possible causes:

- The MSCS cluster is not available.

- The cluster contains only a single node.

Replication fails with the message "Login on target node failed"

Possible cause: The domain user ID was not specified in the correct format, which is <user_ID>@<domain_name>.

MSCS adapter does not start

MSCS adapter does not start

Problem determination:

- The application event log should contain the message "The service SA MP MSCS Adapter has been started."
- In the configuration file cfg\mscs.service.properties, uncomment the property service-log-file, restart the service, and investigate the resulting file.

  Ensure to comment the property again before returning to normal operation.

The SA MP Adapter Service reports the status Started for some seconds and stops again

- Startup should be completed within 60 seconds.
- Refresh the view to see the actual status.

Problem determination:

- Investigate the MSCS adapter log file msgMSCSAdapter.log.
- If no error messages can be found, increase the trace logging level to Maximum and provide all logs to IBM support.

The file msgMSCSAdapter.log contains the message EEZA0061E indicating that the adapter failed to bind to a socket

Possible reason if the MSCS adapter service is made highly available using MSCS:

- The network name or virtual IP address used for the "Automation adapter host" is not available during adapter startup

Possible solution:

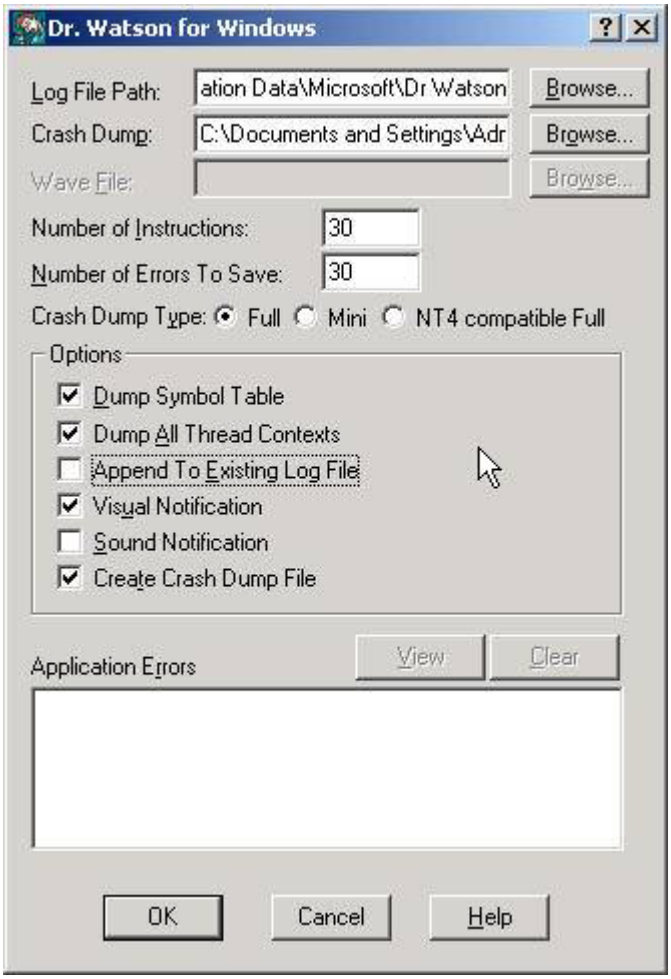
- Check the spelling of the network name or virtual IP address in the adapter configuration dialog.
- Check that there are appropriate "Network Name" / "IP Address" resources defined in MSCS and that they are working properly.
- Check that the MSCS adapter service resource has a dependency on the "Network Name" / "IP Address" resources in MSCS.

MSCS adapter terminates

The MSCS adapter services stops and the log files contain no related error messages. In particular, message "EEZA0104I" does not appear in the MSCS adapter log file msgMSCSAdapter.log. The message indicates that the MSCS adapter was successfully stopped.

Problem determination:

1. Search for javacore.*.txt files in the subdirectory lib.
2. Use Windows tool drwtsn32 to configure dump capturing. Use the following settings:



3. Try to recreate the MSCS adapter termination.
4. Provide the data to IBM support.

Domain does not join

The MSCS domain does not join within two minutes and the MSCS adapter service is no longer running

Problem determination:

- Investigate the MSCS adapter log file `msgMSCSAdapter.log`.
- If no problems can be found, increase the trace logging level to "Maximum" and provide all logs to IBM support.

The MSCS domain does not join within two minutes but the MSCS adapter service is running

Problem determination and possible causes:

- An invalid host name or IP address is specified for the end-to-end automation management server.
- The end-to-end automation management server cannot be reached from the system running the MSCS adapter. To check, use ping, telnet, and tracert commands.
- Determine the network name / IP address the MSCS adapter sends to the end-to-end automation management server:

- Increase the trace logging level at least to “Minimum”, restart the MSCS adapter, investigate the log file `eventMSCSAdapter.log`.
- Locate the latest adapter join event (“EVT_RSN=domainAdapterJoin”). The event contains the required information.

- The system running the MSCS adapter cannot be reached from the end-to-end server. To check, use ping, telnet, and tracert commands.

MSCS adapter uninstallation fails

Uninstaller indicates an uninstallation problem

This happens if the MSCS adapter service was still running during uninstallation.

Note: If the MSCS adapter service is made highly available using MSCS, MSCS may restart or fail over the service.

Uninstalling the MSCS adapter manually

Perform the steps in exactly this sequence:

1. Stop the MSCS adapter service and ensure that it is not restarted by MSCS on the system where the manual uninstallation is performed.
2. Manually remove the service by issuing the command:

   ```
   sc.exe delete "SA MP MSCS Adapter"
   ```
3. Manually remove the service JaasLogon by issuing the following commands:

   ```
   cd <adapter_installation_directory>\jre\bin
   JaasLogon.exe –remove
   ```
4. Delete the adapter installation directory.
5. If no other Tivoli System Automation product is installed on the system, you can delete the `eez` subdirectories of the Tivoli Common Directory.
6. Delete the directory `eezmscs` from `<Program_Files>\Common Files\InstallShield\Universal\`.

Appendix E. 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.

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
Mail Station P300
2455 South Road
Poughkeepsie New York 12601-5400
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, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS"

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

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

Trademarks

- IBM, AIX, DB2, HACMP, NetView, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere, and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both.
- Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, and service names may be trademarks or service marks of others.

Index

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

System Automation for Multiplatforms
Installation and Configuration Guide
Version 2.2

Publication No. SC33-8273-01

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 a fax to the following number: FAX (Germany): 07031+16-3456
  FAX (Other Countries): (+49)+7031-16-3456
- Send your comments via e-mail to: eservdoc@de.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
SC33-8273-01

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 Deutschland Entwicklung GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany

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

SC33-8273-01

Cut or Fold
Along Line

Program Number: 5724-M00

Printed in USA

SC33-8273-01