

# CA Workload Automation iXp

## Administration Guide

Release 11.3.5, Third Edition

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## Contact CA Technologies

### Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

### Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to [techpubs@ca.com](mailto:techpubs@ca.com).

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.



## TABLE OF CONTENTS

1	INTRODUCTION .....	9
2	PHILOSOPHY .....	10
3	ARCHITECTURE .....	12
3.1	Processing Example.....	14
3.1.1	Data Refresh Cycle .....	14
3.1.2	On-Demand Activity.....	14
3.1.3	Log File Retrieval .....	14
3.2	Security .....	15
4	INSTALLATION .....	17
4.1	Overview .....	17
4.2	Components .....	17
4.2.1	iXp Daemon .....	17
4.2.2	iXp Client.....	18
4.2.3	iXp Agent .....	18
4.3	Basic System Requirements .....	18
4.3.1	iXp Daemon .....	18
4.3.2	iXp Client.....	19
4.3.3	iXp Agent .....	19
4.4	Server Pre-Installation Checklist .....	19
4.4.1	Example Server Pre-Install Checklist Form .....	21
4.5	Installing iXp.....	22
4.5.1	Configuring/Installing JRE .....	22
4.5.2	Configuring/Installing Tomcat.....	23
4.5.3	Installing the iXp Server .....	23
4.5.4	Installing the iXp Agents .....	26
4.5.4.1	Installing Java Agent on UNIX/Linux .....	26
4.5.4.2	Starting Java Agent on UNIX/Linux.....	28
4.5.4.3	Installing Java Agent on Windows.....	29
4.5.4.4	Starting Java Agent on Windows .....	31
4.5.4.5	Installing PERL Agent .....	32
4.5.4.6	Copying the Script .....	32
4.5.4.7	Loading the PERL Script .....	32
4.5.4.8	Starting the PERL Agent.....	34
4.5.5	Installing the iXp Client CLI .....	35
4.6	Opening the iXp Admin Tool .....	37
4.7	Post-Installation Checklist.....	38
4.8	Installation Troubleshooting.....	39
4.8.1	Common Installation Problems.....	39
4.8.2	Pathology: Symptoms and Solutions .....	40
5	iXp ADMIN TOOL.....	41
5.1	iXp Server Settings .....	41
5.2	CA Workload Automation AE Instance Configuration .....	44
5.2.1	Configuring for Oracle RAC .....	52
5.2.2	Validate the Instance Configuration.....	53

5.3	User Authentication .....	53
5.3.1	Single Sign-On.....	53
5.3.1.1	IP Address .....	54
5.3.1.2	Host Names.....	55
5.3.1.3	Domain.....	56
5.3.2	iXp User/Password.....	57
5.3.3	iXp CLI Authentication.....	59
5.4	Users and Groups.....	60
5.4.1	Groups.....	60
5.4.1.1	Member .....	61
5.4.1.2	Privilege .....	62
5.4.1.3	Using Filters for Security.....	66
5.4.1.4	Account History .....	70
5.4.2	Users .....	70
5.4.2.1	General.....	72
5.4.2.2	Group Membership .....	73
5.4.2.3	Privilege .....	74
5.4.2.4	Account History .....	75
5.4.2.5	Create a New User .....	75
5.4.2.6	Copy User .....	76
5.4.2.7	Edit User .....	77
5.4.2.8	Remove/Rename User .....	77
5.4.2.9	Undo Changes.....	77
5.4.2.10	User Message.....	77
5.4.2.11	ixp Admin User.....	77
5.4.3	Validate the Privileges.....	77
5.5	Migration .....	82
5.6	Administration Log.....	84
5.7	User Commands .....	85
5.7.1	Create or Edit User Commands .....	85
5.7.2	Interactive User Commands.....	88
5.8	Forecast.....	90
5.9	Message of the Day (MOTD).....	92
5.10	Clients.....	92
5.11	Pick Lists .....	93
5.12	Audit Trail.....	93
5.13	Run Log Files .....	95
5.13.1	Functional Overview.....	96
5.13.2	Configuration Settings .....	96
5.13.3	Resolving File Names.....	96
6	OTHER CLI UTILITIES .....	100
6.1	Server statistics .....	100
6.2	Forecast.....	101
6.2.1	Forecasting Job Runs .....	101
6.2.2	Forecasting Events .....	102
6.3	Currently Active Users .....	102

6.4	Job Information and Restart Instructions.....	103
6.5	Audit Report .....	104
7	MANAGING WORKLOAD MIGRATION.....	105
7.1	Scenario: How to Manage Workload Migration in CA Workload Automation iXp .....	105
7.1.1	Configure the Parameters of the CA Workload Automation AE Instances	108
7.1.1.1	Configure Two Instances with Identical Names on a UNIX/Linux iXp Server .....	108
7.1.1.2	Configure Two Instances with Identical Names on a Windows iXp Server 110	
7.1.2	Assign Security Privileges for Migration .....	111
7.1.3	Create an Exclusion Rule Set.....	113
7.1.4	Create Conversion Scripts.....	115
7.1.4.1	JIL Conversion Script .....	116
7.1.4.1.1	Run the Syntax Checker on the Generated JIL File .....	116
7.1.4.2	Global Variables Script .....	117
7.1.4.2.1	Extract Global Variable Names and Values to a JIL File .....	117
7.1.4.3	Calendars Script .....	118
7.1.5	Configure Migration Options.....	118
8	GLOSSARY.....	121
8.1	CA Workload Automation iXp Related Terms .....	121
8.2	CA Workload Automation AE Terms.....	122
8.3	Symbols in this Guide.....	123
8.3.1.1.1	Alternate color.....	123
8.3.1.1.1.1	Italic.....	123
8.4	Related Documents.....	124



# 1 INTRODUCTION

CA Workload Automation iXp is a Java™-based graphical interface that can be opened from Java Web Start. With CA Workload Automation iXp users can monitor, control, update, forecast, simulate, report on, and print CA Workload Automation AE job streams across multiple instances. The iXp Admin Tool lets you manage privileges for users by defining authorization roles.

The iXp Command Line Interface lets users view, report, control, create, update, and delete CA Workload Automation AE jobs. The commands interface with the CA Workload Automation iXp security model and do not require a local installation of the CA Workload Automation AE software.

The wizard-style migration assistant enables users to migrate jobs and other related objects from a Unicenter AutoSys JM 4.5.1 instance to a CA Workload Automation AE r11.3 or higher instance. Users can visualize, build, validate, and upload packages containing the appropriate set of jobs and their related global variables and calendars.

This guide assumes familiarity with CA Workload Automation AE. It also assumes that you have CA Workload Automation AE running and that you install CA Workload Automation iXp using the procedures described in the Chapter 4: *Installation*.

This **CA Workload Automation iXp Administration Guide** is intended for use with the companion **CA Workload Automation iXp User Guide**.

## 2 PHILOSOPHY

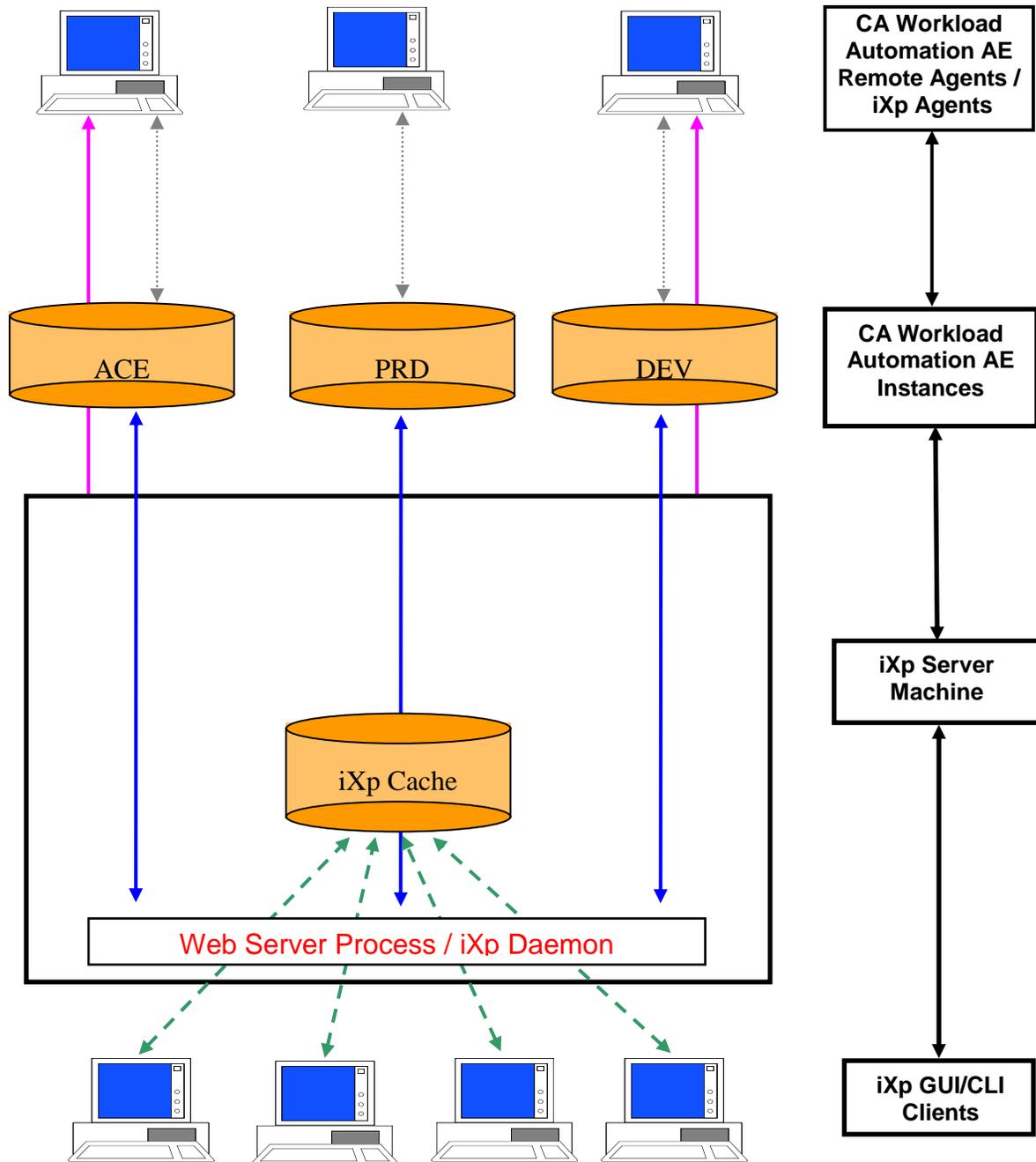
Workload Automation environments are rapidly transitioning to a self-service management mode. With CA Workload Automation iXp, CA Technologies, Inc. delivers the next generation in web-based graphical workload automation, as a secure and scalable solution. These guiding principles are central to the development of CA Workload Automation iXp:

- 1) The architecture should scale up and down. Users requiring minimal data should have minimal bandwidth requirements. Users requiring access to large volumes of data should expect quick response with conventional desktop hardware in a local area network.
- 2) The client should be easy to maintain. The only current requirement for the client to run iXp is to install the Java™ Plug-in. With respect to CA Workload Automation AE monitoring, the client does not require a CA Workload Automation AE client license. In addition, iXp administrators can configure user-defined commands that enable clients to perform custom server-side executions.
- 3) Management by exception is facilitated throughout iXp.
  - Alarms are selected to the top of the Console View.
  - Failures within boxes are visible while boxes are still running.
  - Sort by Status is available.
  - Impact analysis including critical path filtration facilitates response to exceptions.
- 4) Job filtration should be powerful and flexible. Efficient and intuitive filtration enables the defining of granular security roles and enables users to easily pinpoint subsections of job streams.
- 5) Management is consolidated across multiple instances and cross-instance relationships are depicted.
- 6) Management is consolidated across multiple database types.
- 7) Multi-threaded client architecture maintains access to the GUI during refreshes.

## Processing Example

- 8) Three tiered architecture minimizes the number of direct connections to a CA Workload Automation AE instance. Multiple users connect to one CA Workload Automation iXp Server.

# 3 ARCHITECTURE



ARCHITECTURE ELEMENT	DESCRIPTION
<b>iXp Daemon</b>	<p>This process runs on the iXp Server machine and is the only process that runs constantly. The iXp Daemon is a multi-threaded Java process that performs the following functions:</p> <ul style="list-style-type: none"> <li>• Collects all the relevant job data from the CA Workload Automation AE instances</li> <li>• Maintains the iXp Cache</li> <li>• Supplies the data to all the iXp clients</li> </ul> <p>The iXp Daemon runs as a servlet within a Web Application Server (for example, Tomcat).</p>
<b>iXp Cache</b>	<p>These highly compressed data files in proprietary binary format include all the CA Workload Automation AE data needed by the iXp Daemon and the iXp clients.</p>
<b>iXp Client</b>	<p>The iXp Client is the Java<sup>™</sup>-based GUI that can be opened on any Java-supported system, and the CLI that can be opened on supported systems.</p> <p>The GUI provides the capability to monitor, report, forecast, control and update job processing across the CA Workload Automation AE instances. Because the GUI is a Java application, there is no software installation required on the machine that will open the client.</p> <p>The CLI provides the capability to run CA Workload Automation AE commands, such as <i>sendevent</i>, <i>autorep</i>, <i>jil</i>, <i>autostatus</i>, and <i>job_depends</i>, from any machine without installing the CA Workload Automation AE client software.</p>
<b>iXp Agent</b>	<p>The iXp Agent is a Java program that runs on a CA Workload Automation AE Remote Agent. The iXp Agent enables iXp Clients retrieve the output files that CA Workload Automation AE jobs create.</p> <p>iXp also provides a PERL-based agent that has been deprecated. The iXp Daemon can start this program automatically when needed, or it can be started as a job</p>

ARCHITECTURE ELEMENT	DESCRIPTION
	<p>from CA Workload Automation AE. The iXp Server can install this program automatically; the iXp administrator can install it manually.</p> <p><b>Note:</b> <i>The iXp Agent is not required with CA Workload Automation AE r11.3 and higher.</i></p>

## 3.1 Processing Example

### 3.1.1 Data Refresh Cycle

The processing done by each component and the interaction between them during a normal data refresh cycle for the iXp Daemon and Client can be described as follows:

- 1) The iXp Daemon reads data from the CA Workload Automation AE database(s) for each instance.
- 2) It updates the iXp Cache with the newly fetched data.
- 3) The iXp Client contacts the web application server during its refresh cycle, and reads the iXp Cache for the data refresh. Since the iXp application is multi-threaded, it can service multiple client requests simultaneously, if needed.

### 3.1.2 On-Demand Activity

The processing done by each component and the interaction between them when an iXp Client performs an on-demand activity such as putting a job on hold can be described as follows:

- 1) The iXp Client contacts the web application server.
- 2) The web application server associates the request with a thread and asks it to perform the action to put the job on-hold.
- 3) The thread uses the *sendevent* command to perform the action and reports the status back to the web application server.
- 4) The web application server then reports the status back to the iXp Client.

### 3.1.3 Log File Retrieval

The processing done by each component and the interaction between them when an iXp Client requests retrieval of a log file (e.g. STDOUT) created by a

## Security

job running in Unicenter AutoSys JM r11 (or an older version) can be described as follows:

- 1) The iXp Client contacts the iXp Daemon via the web application server.
- 2) The iXp Daemon then requests the iXp Agent to read the appropriate log file and send the contents back to the iXp Server. If the iXp Agent is not running, then the iXp Daemon sends a message back to the Client indicating that the Agent is not running.
- 3) Once it receives the contents, the iXp Server sends the contents back to the requesting iXp Client. The iXp Client displays the contents in a browser window.

## 3.2 Security

There are two security methods available for controlling access to iXp, as follows:

- 1) Native iXp security.
- 2) Single Sign-On (SSO).

iXp provides a native multi-layered security model that encompasses data encryption, user authorization, and optional user authentication. The same security model is applied to the iXp GUI and the iXp CLI.

In the first model, user access to iXp requires validation of the user identity and password. All user identities and passwords are managed within iXp and have no relation to system/domain IDs and passwords.

In the second model, iXp leverages the user ID already authenticated to the Active Directory Domain or the local machine. This requires no user/password maintenance in iXp.

In either case, iXp security includes the following features:

- Data transmission between the server and client machines can be secured and encrypted through current secure HTTP technology. Also, the sensitive data stored by iXp is encrypted.
- User access to iXp requires validation of the user identity and password. All user identities and passwords are managed within iXp and have no relation to system IDs and passwords.

- Groups can be assigned to the iXp user identities to provide read, update, and control privileges for the CA Workload Automation AE objects.
- The security model is very dynamic and user and group policies can be changed on the fly. Changes immediately take effect and user logout is not required.
- The iXp administrator can easily manage the security policies through the iXp Admin Tool.

# 4 INSTALLATION

## 4.1 Overview

As a second-generation companion tool to CA Workload Automation AE, iXp is a Java™-based GUI that can be opened from Java Web Start. With the iXp GUI, users can monitor, control, update, forecast, simulate, report on and print the job processing environment across multiple CA Workload Automation AE instances from a single web browser window. Based on a true web-based 3-tiered architecture developed in Java™, iXp is highly scalable, efficient, fast and minimal in terms of impact on the network bandwidth and the CA Workload Automation AE repository.

The iXp Client CLI enables users to execute CA Workload Automation AE commands from any client machine without having to install the CA Workload Automation AE software. The iXp Client CLI interfaces with the iXp Security Model, hence providing secure access to the CA Workload Automation AE environment.

This section contains steps to install the iXp Server components on UNIX, Windows, and Linux Web Servers.

## 4.2 Components

As seen in the [Architecture](#) diagram, the product has two components that are executed on the iXp Server or iXp Client machines.

### 4.2.1 iXp Daemon

The iXp Daemon is the only persistent daemon in the iXp system. This process is installed on a Web Application Server and provides access to the different CA Workload Automation AE instance repositories. The iXp Daemon process is a multithreaded Java process that periodically reads job processing data from the different CA Workload Automation AE repositories and maintains the iXp Cache from which data is provided to the iXp Clients. The Web Application Server starts this process as a servlet. The main tasks of installation are:

- 1) Satisfying software prerequisites.
- 2) Installing iXp files.

- 3) Configuring iXp so it can communicate with all the CA Workload Automation AE instances to be managed.
- 4) Configuring user security.

## 4.2.2 iXp Client

iXp Client is the Java-based graphical interface that can be opened on any Windows or Linux system that supports JRE v1.6 or v1.7. The client provides the capability to monitor, report, forecast, control, and update job processing across the CA Workload Automation AE instances. Since the client is a Java application, no software installation is required on the machine where it is opened.

The iXp Client CLI can be installed on any supported system. We recommend that you install the Client CLI on those machines from which users want to run certain CA Workload Automation AE commands (e.g. `autorep`, `autocal_asc`, `sendevent`, `jil`). You do not need to install the CA Workload Automation AE Client software on machines where the iXp Client CLI is installed.

## 4.2.3 iXp Agent

The iXp Agent is a Java program that runs on a Unicenter AutoSys JM 4.5.1 or r11 Remote Agent. The iXp Agent lets iXp Clients retrieve the output files created by Unicenter AutoSys JM 4.5.1 jobs.

iXp also provides a PERL-based agent that has been deprecated. This program can be started automatically by the iXp Daemon when needed, or can be started as a job from Unicenter AutoSys JM 4.5.1. This program can be installed automatically by the iXp Server or manually by the iXp administrator.

**NOTE:** *The iXp Agent is not required with CA Workload Automation AE r11.3 and higher.*

## 4.3 Basic System Requirements

This section lists the system requirements for installing and running the iXp components. Some of the prerequisite software is already present on the machines when the operating system is loaded.

### 4.3.1 iXp Daemon

- 1) Tomcat v6 or v7

## Server Pre-Installation Checklist

- 2) JRE v1.6 or v1.7
- 3) PERL v5.1 or higher
- 4) 2 GB of disk space
- 5) 4 GB of available RAM
- 6) CA Workload Automation AE Full Client and configuration files for all instances of CA Workload Automation AE that will be accessed.

### 4.3.2 iXp Client

- 1) JRE v1.6 or v1.7
- 2) 1 GB of available RAM
- 3) 5 MB of disk space required if installing the iXp Client CLI

### 4.3.3 iXp Agent

- 1) JRE v1.6 or v1.7 (Optionally, PERL v5.1 or higher for the deprecated agent program)
- 2) The CA Workload Automation AE `sendevent`, `zql`, `xql` binaries are optional. They are needed if you want the iXp Daemon to automatically install and start the PERL-based iXp Agent.

## 4.4 Server Pre-Installation Checklist

The information required for installation is shown below. Fill in the right column with the values you will use during the installation process.

Hostname of the iXp Web Server	
IP Address of the iXp Web Server	
Port number of the Web Server process	
Secure or Standard Web Server process (http or https)	
Total Number of CA Workload Automation AE Instances that will be monitored	
Web Server Type and Version	

Location of Web Server webapps directory	
Directory for JRE binaries	
CA Workload Automation AE RDBMS Vendor	
Location and name of PERL v5.x executable	
CA Workload Automation AE Root Directory (AUTOSYS) on the Web Server	
Directory for CA Workload Automation AE Configuration Files (AUTOUSER) on the Web Server	
Value for Library Path environment variable (LD_LIBRARY_PATH or SHLIB_PATH or LIBPATH)	
Directory for Sybase interfaces file (SYBASE) on the Web Server	
Directory for Oracle tnsnames file (TNS_ADMIN) on the Web Server	
Oracle Home Directory (ORACLE_HOME) on the Web Server	
Root Directory for iXp files (IXP_HOME) on the iXp Server	
Root Directory for iXp files (IXP_HOME) on the iXp Clients and iXp Agents (for CLI and Agent program)	

### 4.4.1 Example Server Pre-Install Checklist Form

The same checklist with sample values filled in for your reference is shown here:

Hostname of the Web Server	venus
IP Address of the Web Server	192.168.200.19
Port number of the Web Server process	8080
Secure or Standard Web Server process (http or https)	Standard (http)
Total Number of CA Workload Automation AE Instances that will be monitored	3 (PRD, DEV, TST)
Web Server Type and Version	Tomcat v7
Location of Web Server webapps directory	/opt/tomcat7/webapps
Directory for JRE binaries	/opt/jre1.7/bin
CA Workload Automation AE RDBMS Vendor	Sybase
Location and name of PERL v5.x executable	/opt/perl5/bin/perl
CA Workload Automation AE Root Directory (AUTOSYS) on the Web Server	/opt/CA/WorkloadAutomationAE/autosys
Directory for CA Workload Automation AE Configuration Files (AUTOUSER) on the Web Server	/opt/CA/WorkloadAutomationAE/autouser
Value for Library Path environment variable (LD_LIBRARY_PATH or SHLIB_PATH or LIBPATH)	/opt/CA/WorkloadAutomationAE/autosys/lib:/opt/CA/CAlib
Directory for Sybase interfaces file (SYBASE) on the Web Server	/opt/sybase
Directory for Oracle tnsnames file (TNS_ADMIN) on the Web Server	N/A
Oracle Home Directory on the Web Server (ORACLE_HOME)	N/A
Root Directory where iXp files will be installed (IXP_HOME)	/opt/ca/ixp
Root Directory for iXp files (IXP_HOME) on the iXp Clients and iXp Agents (for CLI)	C:\ca\ixp

## 4.5 Installing iXp

### 4.5.1 Configuring/Installing JRE

Before installing the iXp Server, the Java environment on the machine needs to be present. The iXp Server needs the Java Runtime Environment (JRE) v1.6 or v1.7, 64-bit.

1. To check the version of Java on the server machine, run the following command from a command prompt:

```
% java -version
```

```
java version "1.7.0_05"  
Java(TM) SE Runtime Environment (build 1.7.0_05-b064)  
Java HotSpot(TM) 64-Bit Server VM (build 23.1-b034,  
mixed mode)
```

If the output of the command is similar to the sample above, then the required version of the Java environment is installed and set up correctly.

2. If the version of Java is not 1.6 or 1.7, or if the Java environment is not present, then it will be necessary to install the appropriate version. Typically, the `java` executable that was run above is in the `/usr/bin` directory on UNIX/Linux systems and `C:\Windows\System32` on Windows systems. On UNIX/Linux, it is a soft link to the real `java` executable in the directory where the Java environment resides. There is a possibility that the required version of Java is present on the server machine, but it is not present in the `PATH` of the user. Before installing the new version of Java, it may be helpful to search the server machine for any other versions of Java.

If the JRE has to be downloaded, the [java.oracle.com](http://www.oracle.com/technetwork/java/javase/downloads/index.html) website (or <http://www.oracle.com/technetwork/java/javase/downloads/index.html>) has download instructions for most platforms. If your platform is not listed, please contact CA Technologies, Inc. for appropriate download directions.

Once the JRE files have been located, put the directory in the `PATH` environment variable of the user that will install and run iXp. For example,

```
PATH=/opt/jre1.7/bin:$PATH; export $PATH (On UNIX/Linux)
```

## 4.5.2 Configuring/Installing Tomcat

Before installing the iXp Server, the Tomcat web application server needs to be present. The iXp server requires Tomcat v6 or v7.

If Tomcat is not present on the machine, it can be downloaded from the Apache Software Foundation (<http://tomcat.apache.org>).

**NOTE:** If the iXp server will be installed on a Windows machine, download the 32-bit/64-bit Windows Service Installer.

To install Tomcat on a UNIX/Linux machine, just extract the contents of the Tomcat tar file to the appropriate location. You can edit the “*conf/server.xml*” file under the base Tomcat directory to change the default parameters (port numbers, http mode).

To install Tomcat on a Windows machine, run the Windows Service installer, and make modifications to the default parameters as necessary (port numbers, login options).

The Tomcat process must be started as a user with the following privileges:

- Full privileges for the iXp home directory and its sub-directories.
- Edit and Exec Superuser capability on all Unicenter AutoSys JM and CA Workload Automation AE instances (Only if users will be performing job updates or sendevents through iXp).
- If the Unicenter AutoSys JM or CA Workload Automation AE instances are enabled with CA EEM, the Tomcat user must be defined in CA EEM with full privileges to all resources within each resource class related to those instances.

On Windows, you can configure the “Login” property of the Tomcat service to start as a user with these privileges.

## 4.5.3 Installing the iXp Server

The iXp software is delivered in the following two DVD image files:

- The ISO file for CA Workload Automation iXp CA Third Party Requirements
- The ISO file for CA Workload Automation iXp Release 11.3.5

To install the iXp Server, follow these steps:

- 1) Create the directory where all the iXp files will be stored (the iXp Root Directory), as defined in the Section 4.4 [Server Pre-Installation Checklist](#). Make sure the directory can store up to 2 GB of data.
- 2) Log in to the Web Server machine as the user that runs the web application server (Tomcat).
- 3) Mount the ISO file for CA Workload Automation iXp Third Party Requirements.
- 4) From the ISO image mount point, run the "installer.bat" (if Windows) or "installer.sh" (if UNIX).
- 5) You must agree to the EULA (End User License Agreement) to continue.
- 6) On UNIX/Linux, extract the tar file "ixp-thirdPartyLib-11.3.5.X.tar" from the ISO image to the "lib" directory under Tomcat. On Windows, extract the zip file "ixp-thirdPartyLib-11.3.5.X.zip" to the "lib" directory under Tomcat. In the filenames, X is the latest build number.
- 7) Mount the ISO image for CA Workload Automation iXp Release 11.3.5.
- 8) From the ISO image mount point, run the "installer.bat" (Windows) or "installer.sh" (UNIX).
- 9) You must agree to the EULA (End User License Agreement) to continue.
- 10) Set the following environment variables:

```
IXP_HOME=<Root Directory of the iXp files>
JAVA_OPTS="-Dixp.home=$IXP_HOME -Xms1500m -Xmx1500m"
JAVA_HOME=<Root Directory of Java>
CATALINA_HOME=<Root Directory of Tomcat>
PATH=$JAVA_HOME/bin:$PATH
```

For example,

```
% IXP_HOME=/export/home/ixphome; export IXP_HOME
% JAVA_OPTS="-Dixp.home=$IXP_HOME -Xms1500m -Xmx1500m"
% JAVA_HOME=/opt/jre1.7
% CATALINA_HOME=/opt/tomcat7
% PATH=$JAVA_HOME/bin:$PATH
% export JAVA_OPTS JAVA_HOME CATALINA_HOME PATH
```

## Installing iXp

11) On Windows, open the “Configure Tomcat” menu item from the Windows Start Menu. In this dialog, make the following changes:

- Under the “General” tab, change the “Startup type” to “Automatic” if appropriate.
- Under the “Log On” tab, if not performed earlier, change the service to run as a Windows user that has full Edit and Exec super user privileges to all the CA Workload Automation AE instances. If the CA Workload Automation AE environment is enabled with CA EEM, this user must be defined in CA EEM with full privileges to all resources within each resource class that relates to CA Workload Automation AE.
- Under the “Java” tab, add the following three lines to the “Java Options” item:

```
-Dixp.home=IXP_HOME  
-Xms1500m  
-Xmx1500m
```

where

IXP\_HOME= The root directory for iXp software. This value has to be specified in the Windows 8.3 format.

12) On UNIX/Linux, add the lines from step#10 to the login profile of the user that runs the web application server.

13) On UNIX/Linux, extract the tar file “ixp-distrib-11.3.5.X.tar” from the ISO image to the IXP\_HOME directory. On Windows, extract the zip file “ixp-distrib-11.3.5.X.zip” to the IXP\_HOME directory.

14) Go to the \$IXP\_HOME/webapps sub-directory and copy the iXp WAR file (ixp.war) to the appropriate directory of the servlet engine. For the above example, copy the file to /opt/tomcat7/webapps directory. If this directory has a previous iXp WAR file, then delete that file before copying this new file. Also, delete the /opt/tomcat7/webapps/ixp directory and all of its contents.

- 15) Restart the Web Application Server by running the command – “\$CATALINA\_HOME/bin/startup.sh” on UNIX/Linux machines or by starting the Tomcat service on Windows machines. Monitor the log files

\$IXP\_HOME/log/ixpDaemon.log

—and—

\$CATALINA\_HOME/logs/catalina.out

to make sure that iXp comes up without error.

## 4.5.4 Installing the iXp Agents

The iXp Agents run on the Remote Agent machines from which the iXp Clients will retrieve job log files. The iXp Agent can be installed at your convenience. The iXp distribution image includes the software to install the full client (which includes the iXp CLI and Agent), or only the iXp Agent. The software is located in the “install” sub-directory under the iXp root directory.

**NOTE:** *The iXp Agent is not required with CA Workload Automation AE r11.3 and higher.*

### 4.5.4.1 Installing Java Agent on UNIX/Linux

The software files for the full Client and Agent-only installation are “ixp-client-*RELEASE-PLATFORM*.tar” and “ixp-agent-*RELEASE-PLATFORM*.tar” respectively, where *RELEASE* is the version of iXp and *PLATFORM* is the OS platform for which the Agent has been compiled.

You need to copy the file appropriate for the Agent platform to the Agent machine.

Once the file has been copied to the Agent machine, follow these steps to install and configure the Agent:

- 1) Create a directory that will contain the Agent software.
- 2) Extract the contents of the TAR file to this directory.
- 3) Modify the Environment profile file for the user running the Agent program to include the following environment variables.

```
IXP_HOME=<Root Directory of Agent Software>; export  
IXP_HOME  
PATH=JAVABIN:$PATH; export PATH
```

## Installing iXp

where

*JAVABIN* is the directory that contains binaries for Java v1.6 or v1.7

- 4) If `$IXP_HOME/etc/ixp.conf` file does not exist, you can copy the sample file provided (`$IXP_HOME/etc/ixp.conf.sample`) to `ixp.conf`.

```
cp $IXP_HOME/etc/ixp.conf.sample $IXP_HOME/etc/ixp.conf
```

- 5) Edit the `ixp.conf` file to specify the location of the iXp Server.

```
IXP_SERVER_URL=PROTOCOL://IXPSERVERNAME:PORT
```

where

*PROTOCOL* is `http` or `https`, depending on the configuration  
*IXPSERVERNAME* is the name or IP address of the iXp Server machine

*PORT* is the Port number of the iXp Server process

For example,

```
IXP_SERVER_URL=http://venus:8080
```

- 6) Normally, CA Workload Automation AE jobs refer to certain environment variables when specifying the STDOUT/STDERR file names. Also, the default location of Remote Agent log files can be configured to be different than `/tmp`. We recommend that you create a file for each CA Workload Automation AE instance that specifies the values for such variables. That way, when users request log files that contain names of environment variables, the Agent will be able to substitute the appropriate values.

For each instance, create

`$IXP_HOME/agent/conf/$AUTOSERV.conf` files, where  
*\$AUTOSERV* = the 3 letter name for the CA Workload Automation AE instance.

For example,

```
$IXP_HOME/agent/conf/DEV.conf for the DEV instance.  
$IXP_HOME/agent/conf/TST.conf for the TST instance.
```

A sample of environment variables that you can specify in each file is as follows:

```
AUTOSYS=/opt/CA/WorkloadAutomationAE/autosys
AUTOUSER=/opt/CA/WorkloadAutomationAE/autouser
AutoRemoteDir=/opt/CA/WorkloadAutomationAE/tmp
LOGDIR=/opt/CA/WorkloadAutomationAE/logs
```

#### 4.5.4.2 Starting Java Agent on UNIX/Linux

After the iXp Agent has been configured as listed above, it has to be started so that the log files can be retrieved from this machine. You need to start the Agent only once per iXp Server. You can start the Agent in various ways.

- Create a CA Workload Automation AE job to start the Agent. You will need one job per Agent machine.
- Have the standard startup scripts for the machine start the Agent when the machine boots up.
- Start the Agent process by running the startup command in the background of an interactive UNIX command window.

The Agent can be run in one of the following two ways:

- A persistent process that will only stop if it encounters a fatal error, or if the iXp Server is not available for more than 30 minutes.
- A timed process that will gracefully finish when the specified duration is reached. It will also stop if it encounters a fatal error, or if the iXp Server is not available for more than 30 minutes.

The syntax to run the iXp Agent is as follows:

```
$IXP_HOME/bin/ixagent SERVER_URL AGENT_MACHINE
DURATION
```

where

`SERVER_URL` = The URL connection string for the iXp Server

`AGENT_MACHINE` = The name of the local Agent machine that matches the name specified in the Run machine field of the CA Workload Automation AE job

`DURATION` = The time, in minutes, for which the Agent will keep on running. If you want to run it persistently, specify 0 (zero)

## Installing iXp

For example,

```
$IXP_HOME/bin/ixagent http://venus:8080 neptune 0
```

This will run the agent as a persistent process, and it will connect to the iXp server running on `venus` over port 8080. The agent will pick up all log file requests for jobs that ran on machine `neptune`.

```
$IXP_HOME/bin/ixagent http://venus:8080 neptune.ca.com 10080
```

This will run the agent for 7 days, and it will pick up all log file requests for jobs that ran on machine `neptune.ca.com`.

**NOTE:** You will need to run multiple executions of the Agent concurrently if you have jobs running on the same machine but using different hostnames, DNS aliases, short and fully qualified names.

### 4.5.4.3 Installing Java Agent on Windows

The software files for the full Client and Agent-only installation are "`ixp-client-RELEASE-win.zip`" and "`ixp-agent-RELEASE-win.zip`" respectively, where `RELEASE` is the version of iXp.

You need to copy the appropriate software image file to the Windows Agent machine.

Once the file has been copied to the Agent machine, follow these steps to install and configure the Agent:

- 1) Create a directory that will contain the Agent software.
- 2) Extract the contents of the ZIP file to this directory.
- 3) Modify the System Environment so that the following environment variables are present when the Agent process is started. You will have to select the **Control Panel ► System ► Advanced ► Environment Variables** menu option to do this.

```
IXP_HOME=<Root Directory of Agent software>  
PATH=JAVABIN;%PATH%
```

- 4) If `%IXP_HOME%\etc\ixp.conf` file does not exist, you can copy the sample file provided (`%IXP_HOME%\etc\ixp.conf.sample`) to `ixp.conf`.

```
copy %IXP_HOME%\etc\ixp.conf.sample
%IXP_HOME%\etc\ixp.conf
```

5) Edit the `ixp.conf` file to specify the location of the iXp Server.

```
IXP_SERVER_URL=PROTOCOL://IXPSERVERNAME:PORT
```

where

PROTOCOL = `http` or `https`, depending on the configuration  
IXPSERVERNAME = Name or IP Address of the iXp Server machine  
PORT = Port number of the iXp Server process

For example,

```
IXP_SERVER_URL=http://venus:8080
```

The `IXP_SERVER_URL` environment variable overrides the `ixp.conf` file. If this variable (optional: `IXP_SERVER_URL_2`) is set, the value in the `ixp.conf` file is ignored. This simplifies the use of multiple iXp environments.

6) Normally, CA Workload Automation AE jobs refer to certain environment variables when specifying the `STDOUT/STDERR` file names. Also, the default value for the Remote Agent logging directory is stored within the CA Workload Automation AE Remote Agent configuration only. We recommend that you create a file for each CA Workload Automation AE instance that specifies the values for such variables. That way, when users request log files that contain names of environment variables, the Agent will be able to substitute the appropriate values.

For each instance, create `%IXP_HOME%\agent\conf\%AUTOSERV%.conf` files, where `%AUTOSERV%` = the 3 letter name for the CA Workload Automation AE instance.

For example,

```
%IXP_HOME%\agent\conf\DEV.conf for the DEV instance.
%IXP_HOME%\agent\conf\TST.conf for the TST instance.
```

A sample of environment variables that you could specify in each file is as follows:

```
AUTOSYS=C:\Progra~1\CA\Unicen~1.DEV\autosys
AUTOUSER=C:\Progra~1\CA\Unicen~1.DEV\autouser
```

## Installing iXp

```
AutoRemoteDir=C:\Progra~1\CA\Unicen~1.DEV\tmp  
LOGDIR=C:\Progra~1\CA\Unicen~1.DEV\logs
```

**NOTE:** You have to specify at least the AutoRemoteDir environment variable, or else the iXp Agent will be unable to retrieve the Remote Agent log files.

### 4.5.4.4 Starting Java Agent on Windows

After the iXp Agent has been configured as listed above, it has to be started so that the log files can be retrieved from this machine. You need to start the Agent only once per iXp Server. You can start the Agent in the following way:

- Create a CA Workload Automation AE job to start the Agent. You will need one job per Agent machine.

**NOTE:** Since the Agent will run as a CA Workload Automation AE job, you have to restart the CA Workload Automation AE Remote Agent service so that the new environment variables can be passed to the Remote Agent.

The Agent can be run in one of the following two ways:

- A persistent process that will only stop if it encounters a fatal error, or if the iXp Server is not available for more than 30 minutes.
- A timed process that will gracefully finish when the specified duration is reached. It will also stop if it encounters a fatal error, or if the iXp server is not available for more than 30 minutes. If you choose this method, specify the date/time conditions for the job such that the job runs every day and has start\_mins of 5 minutes. That way, when the Agent finishes, the job will restart the Agent within 5 minutes.

The syntax to run the iXp Agent is as follows:

```
%IXP_HOME%\bin\ixagent.exe SERVER_URL AGENT_MACHINE  
DURATION
```

where

SERVER\_URL = The URL connection string for the iXp Server

AGENT\_MACHINE = The name of the local Agent machine that matches the name specified in the Run machine field of the CA Workload Automation AE job

DURATION = The time, in minutes, for which the Agent will keep on running. If you want to run it persistently, specify 0 (zero)

For example,

```
%IXP_HOME%\bin\ixagent.exe http://venus:8080 neptune 0
```

This will run the agent as a persistent process, and it will connect to the iXp server running on `venus` over port 8080. The agent will pick up all log file requests for jobs that ran on machine `neptune`.

```
%IXP_HOME%\bin\ixagent.exe http://venus:8080 neptune.ca.com 10080
```

This will run the agent for 7 days, and it will pick up all log file requests for jobs that ran on machine `neptune.ca.com`.

**NOTE:** You will need to run multiple executions of the Agent concurrently if you have jobs running on the same machine but using different hostnames, DNS aliases, short and fully qualified names.

#### 4.5.4.5 Installing PERL Agent

If any machine on which you want to run the iXp Agent does not have JRE v1.6 or v1.7, but has PERL v5.6.x or higher installed, then you can run the deprecated iXp Agent. The PERL script for the iXp Agent can be installed manually on every system or automatically by the iXp Daemon when needed.

#### 4.5.4.6 Copying the Script

The Agent Script is provided with the iXp distribution. The file “`IXP_HOME/etc/runlog/ixpagent.pl`” is the Agent Script. You can copy this script to each machine and then run it to start the iXp Agent.

#### 4.5.4.7 Loading the PERL Script

The Agent Script can also be loaded as a database table on any relational database. The advantage of this mechanism is that the script can be extracted to any machine by using a database command, rather than copying the file (as per the previous section). By default, you can use the CA Workload Automation AE database on each instance.

**NOTE:** If you copied the PERL script on to the Remote Agent machines, you can skip this section.

## Installing iXp

The following steps will load the Agent Script in to the database of choice:

- 1) `cd $IXP_HOME/etc/runlog`
- 2) Load the script using the appropriate command for the database type.

For **Oracle** databases, use the following command:

```
zql -u <User> -p <Password> -s <TNS_ALIAS> -f  
ixpagent.zql
```

For **Sybase** databases, use the following command:

```
isql -U <User> -P <Password> -S <Dataserer> -i  
ixpagent.sql
```

For **SQL Server** databases, use the following command:

```
osql -U <User> -P <Password> -S <Dataserer> -i  
ixpagent.sql
```

where

<User>	- The Database login user ID
<Password>	- The Database login password
<TNS_ALIAS>	- Oracle Database name
<Dataserer>	- Sybase Dataserer or SQL Server name

The above commands will create a table called “IXP\_AGENT” on the database provided. The rows inside this table shall contain the actual PERL script of the iXp Agent.

If the iXp Server machine does not have a database client, then copy the `IXP_HOME/etc/runlog/ixpagent.sql` file to any machine that has a database client and is configured to reach the database, and run the above command from that machine. For example, you can copy the file to the Unicenter AutoSys JM scheduler and run the above commands from there.

#### 4.5.4.8 Starting the PERL Agent

We recommend that the iXp Agent should be installed manually. After the script has been loaded in a database, the Agent is ready for installation on Remote Agent machines.

- 1) Extract the script from the database by running the following command on the machine from which the script was loaded.

**NOTE:** If you copied the PERL script on to the Remote Agent machines, you can skip this step.

For **Oracle** databases, use the following command:

```
zql -u <User> -p <Password> -s <TNS_ALIAS> -qh -c
"select text from ixp_agent order by line" >
ixpagent.pl
```

For **Sybase** or **SQL Server** databases, use the following command:

```
xql -U <User> -P <Password> -S <Datasever> -qh -c
"select text from ixp_agent order by line" >
ixpagent.pl
```

- 2) Copy the extracted script to a directory on every Remote Agent machine. In the above case, the file "ixpagent.pl" that was created by extracting the information from the database needs to be copied to each Remote Agent machine.

- 3) Run the script as follows:

```
perl <FILE> http://<iXpServer>:<PORT> <Hostname>
<Duration>
```

where

<FILE>	- The full path and name of ixpagent.pl
<iXpServer>	- The name of the iXp Server machine
<PORT>	- The Port number for Tomcat on iXp Server
<Hostname>	- The name of the iXp Agent machine
<Duration>	- The amount of time (in minutes) that the iXp Agent script will stay running.

## Installing iXp

For example,

```
perl C:\temp\ixpagent.pl http://venus:8080 neptune  
600
```

The above command will have the iXp Agent running for 600 minutes before exiting. While the Agent is running, iXp Clients can retrieve log files from the Agent machine.

**Tip:** We recommend that you create two (2) jobs per Remote Agent machine in your environment. The first job performs the SQL extract and the second job runs the extracted PERL script. You can set up the second job to run after the SUCCESS of the first job and after its own completion. By doing this, you do not need to copy the Agent file to each machine, as the first job for each machine will extract the code from the database.

**Tip:** If you end up creating a job that performs the SQL extract, we recommend that you create a limited database user ID that has permissions to read the IXP\_AGENT table. That way, exposing the database user ID and password will not compromise your current security model.

### 4.5.5 Installing the iXp Client CLI

The iXp Client GUI is a Java application and does not require any installation. The client machine requires JRE v1.6 or v1.7 installed.

The iXp Client CLI is a set of commands that can be installed on any machine, including the iXp GUI clients. These commands enable authorized users to run CA Workload Automation AE commands such as autocal\_asc, autorep, autostatus, jil, job\_depends, sendevent from their client machines. The client machines do not need to install the CA Workload Automation AE software.

Administrators need to set up authorizations for users running these commands. This can be done from the iXp Admin Tool.

The iXp Client CLI software is in a single file named `ixp-client-RELEASE-PLATFORM.tar` (UNIX/Linux) or `ixp-client-RELEASE-win.zip` (Windows). The software is located in the "install" subdirectory under the iXp root directory on the iXp Server machine.

Create the directory where the iXp files will be stored (the iXp Root Directory on iXp Client), as defined in the Section 4.4 [Server Pre-Installation Checklist](#). Make sure the directory can store up to 5 MB of data.

- 1) Log in to the Client machine and extract the files from the software image to the iXp Root Directory.

For example, as per the sample checklist, this would be the `C:\ca\ixp` directory.

- 2) Edit the `IXP_HOME\etc\ixp.conf` file and add a line that provides the connection information for the iXp Server.

The line to add is as follows:

```
IXP_SERVER_URL=http://IXP_SERVER:PORT
```

where

IXP\_SERVER = Name or IP address of iXp Server machine  
PORT = The HTTP port of the iXp Web Server

For example, as per the sample checklist,

```
IXP_SERVER_URL=http://venus:8080
```

If there is an alternate iXp server running for high availability, then an additional line can be added in the file to provide its connection information to the CLI.

```
IXP_SERVER_URL_2=http://IXP_SERVER_2:PORT
```

where

IXP\_SERVER\_2 = Name or IP address of the alternate iXp Server machine  
PORT = The HTTP port of the alternate iXp Web Server

For example,

```
IXP_SERVER_URL_2=http://mercury:8081
```

Alternatively, the above two lines can be set as environment variables `IXP_SERVER_URL` and `IXP_SERVER_URL_2`, rather than in the file. If the values are set as environment variables, then they take precedence over the lines in the file.

- 3) Have the user set two environment variables before executing the commands: `IXP_HOME` and `AUTOSERV`. `IXP_HOME` gets set to the Root

## Opening the iXp Admin Tool

Directory on the Client machine where the iXp CLI is installed, and `AUTOSERV` gets set to the CA Workload Automation AE Instance name for which the command is being executed. These can be set beforehand or at runtime.

For example, as per the sample checklist,

```
IXP_HOME=C:\ca\ixp
AUTOSERV=DEV
```

- 4) Now, to run the commands, the users can go to `IXP_HOME/bin` directory. More information about the commands is provided in the **CA Workload Automation iXp User Guide**.

## 4.6 Opening the iXp Admin Tool

You can open the iXp Admin Tool using Java Web Start on your iXp Client machine. Pass in the appropriate URL as specified by your Pre-Install Checklist as an argument to Java Web Start. Using the working example, run the following command on your Client machine:

```
javaws http://MACHINE:PORT/ixp/AdminTool.jnlp
```

where

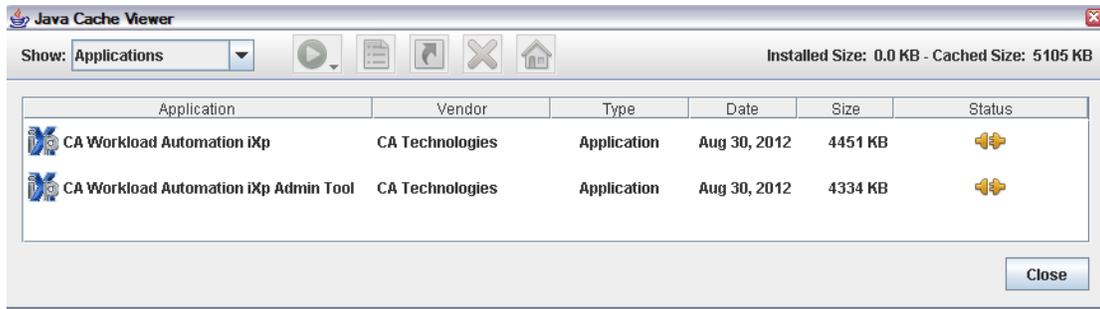
<code>MACHINE</code>	= Name of the iXp Server machine
<code>PORT</code>	= Port number of the Web server (e.g. 8080)

For example:

```
javaws http://venus:8080/ixp/AdminTool.jnlp
```

You will be prompted with a Security Warning. Click `Always` and `Run` to continue opening the iXp Admin Tool. The first time you open the application, Java Web Start has to upload the application image, so you may experience some delay if you have a busy network. This initial upload only occurs the first time you open an application through Java Web Start or when software upgrades occur. Once loaded you should see the login prompt.

Creating a shortcut on your desktop is recommended for opening Java Web Start. When you use Java Web Start for the first time, it prompts you to do that. After doing so, subsequent opening of iXp can be done by using the desktop shortcut or by opening the Java Application Viewer using the command "`javaws -viewer`".



At the iXp login prompt, enter the user “ixpAdmin” and the default password “ixpAdmin”. You will be prompted to change the password for this user. Select a new password that is at least 8 characters long, and has one special (non-alphanumeric) character, one uppercase letter, and one numeric character.

The MOTD format supports HTML 3 and pictures saved on your local Tomcat server.

- 1) To provide information about the CA Workload Automation AE Instances, to configure additional users, and set up the iXp Authentication policy, see Chapter 5: [iXp ADMIN TOOL](#).
- 2) If there are any errors during the installation, see Section 4.8 [Installation Troubleshooting](#) for solutions.
- 3) Open the iXp Application using Java Web Start. Since this is the first time you are opening the application, on the iXp Client machine run a command similar to the one for the iXp Admin Tool.

```
javaws http://venus:8080/ixp/iXp.jnlp
```

- 4) Provide the login information and, once authenticated, the iXp monitoring and control application will be opened.

## 4.7 Post-Installation Checklist

After installation according to the above steps, the following items need to be done or verified to assure full functionality of iXp clients.

A Web browser must be in the PATH variable on the client or the location of the browser must be provided in the IXP_HOME/dat/user/<username>/props file	√
JRE v1.6 or v1.7 is needed on the machine to run the iXp UI.	√

<p>The ID that the Web Application Server runs under needs to have JIL update privilege in CA Workload Automation AE, if users are going to be performing JIL updates through iXp. Typically, that ID is the same as the CA Workload Automation AE Edit SuperUser ID.</p>	√
---	---

## 4.8 Installation Troubleshooting

### 4.8.1 Common Installation Problems

- 1) IXP\_HOME environment variable is not set correctly.
- 2) Database URLs are incorrect.
- 3) JAVA\_OPTS environment variable is not set correctly.
- 4) Database user password is incorrect.
- 5) Database user permissions are incorrect.
- 6) The Tomcat options for Java are not set correctly.

## 4.8.2 Pathology: Symptoms and Solutions

<b>SYMPTOM/PROBLEM</b>	<b>CAUSE/SOLUTION</b>
"Undefined User" error message.	The system/AD user has not been defined to iXp yet. Log in as "iXp Admin" and set up the user.
"Invalid Password" error message.	Possible typo in login screen. Retype password.
Web Application Server does not start iXp Daemon	JAVA_OPTS variable may be incorrect. Reset the JAVA_OPTS variable, and restart the web server.
No jobs visible within iXp application and SQL exceptions in iXpDaemon. log file.	Database URLs are incorrect. Correct the database URLs, as described in this chapter.
"permission denied" errors in iXpDaemon. log file.	User permissions are incorrect. Solution: correct them.
"unauthorized access" errors in iXpDaemon. log file.	Database user password is incorrect. Solution: correct it.
Java Web Start window does not show the icons for iXp or Admin Tool	There is a problem with the URL specification or the web server is not running.
English version of iXp appears on your French or Italian operating system.	Cause may be the locale variable is not set on your system. Solution: set the locale variable on your system.

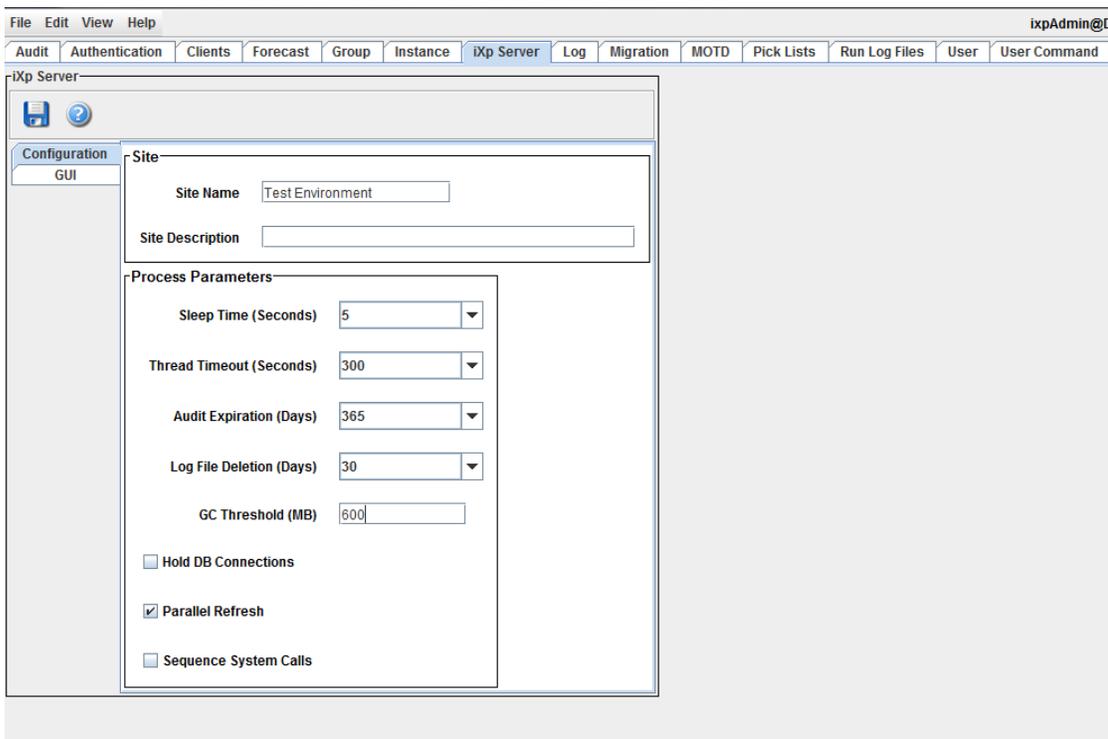
# 5 iXp ADMIN TOOL

The iXp Administration Tool (“Admin Tool”) allows the iXp administrator to control and monitor security, user permissions, user commands, and connections to CA Workload Automation AE. iXp Admin Tool functions manage authentication and authorization policies for end users.

The iXp Admin Tool can be accessed only by designated iXp administrators.

## 5.1 iXp Server Settings

The Chapter 4: *Installation* should get you to the point where you can see the iXp Admin Tool interface as follows:



The tabs at the top of the iXp Admin Tool allow the administrator to view, enter or modify information pertaining to a particular area. The data within each tab has to be saved individually. For example, clicking the Save button on the Configuration tab would save only the iXp Server information.

The following table explains the fields listed in the **Configuration** section. This section enables you to specify some general information, and server-level configuration parameters.

<b>iXp Server Configuration Fields</b>	<b>Description</b>
<b>Site Name</b>	Name of the site running iXp software. The site name will be shown in the Tree view of the main GUI. The site name must be at least 4 characters long.
<b>Site Description</b>	Description of the iXp Server site.
<b>Sleep Time</b>	The time, in seconds, that the iXp Daemon will sleep after each series of data retrieval from the CA Workload Automation AE instances. The recommended value is between 1 and 10 seconds, depending on the processing power of the iXp Server machine. The default value for this setting is five (5) seconds.
<b>Thread Timeout</b>	A central thread monitors all the threads of the iXp Daemon. If any of the threads has not finished its work within the value specified here, iXp will start reporting timeout errors. Setting a low value here may be too restrictive on the daemon, and a high value would not have any use. On average, no thread should take more than 5 minutes to finish its work.
<b>Audit Expiration</b>	iXp will maintain an online audit for the number of days specified here. After that, the audit files will be archived. The default value is 30 days.
<b>Log File Deletion</b>	iXp Daemon logs will be kept for the number of days specified here. After that they will be deleted. The default value is 30 days.
<b>GC Threshold</b>	Available memory is constantly checked and if below the Threshold, GC (Garbage Collection) is requested from the Java VM immediately. This means a high Threshold causes GC to occur more often, which could degrade performance. Suggested setting for GC Threshold is about 33% or less of the Tomcat -Xmx setting.
<b>Hold DB Connections</b>	If this option has been selected, each of the daemon threads that reads data from its CA Workload Automation AE instance will keep the database connection open. This reduces the processing overhead on the server and the database. By default, this option is turned off.

## iXp Server Settings

<b>iXp Server Configuration Fields</b>	<b>Description</b>
<b>Parallel Refresh</b>	If this option has been selected, the daemon will retrieve data from multiple CA Workload Automation AE instances concurrently. This speeds up the data refresh cycle on the server. By default, this option is selected.
<b>Sequence System Calls</b>	Enable this option to limit the iXp Server to perform user actions sequentially. This setting can be useful for servers with limited RAM.

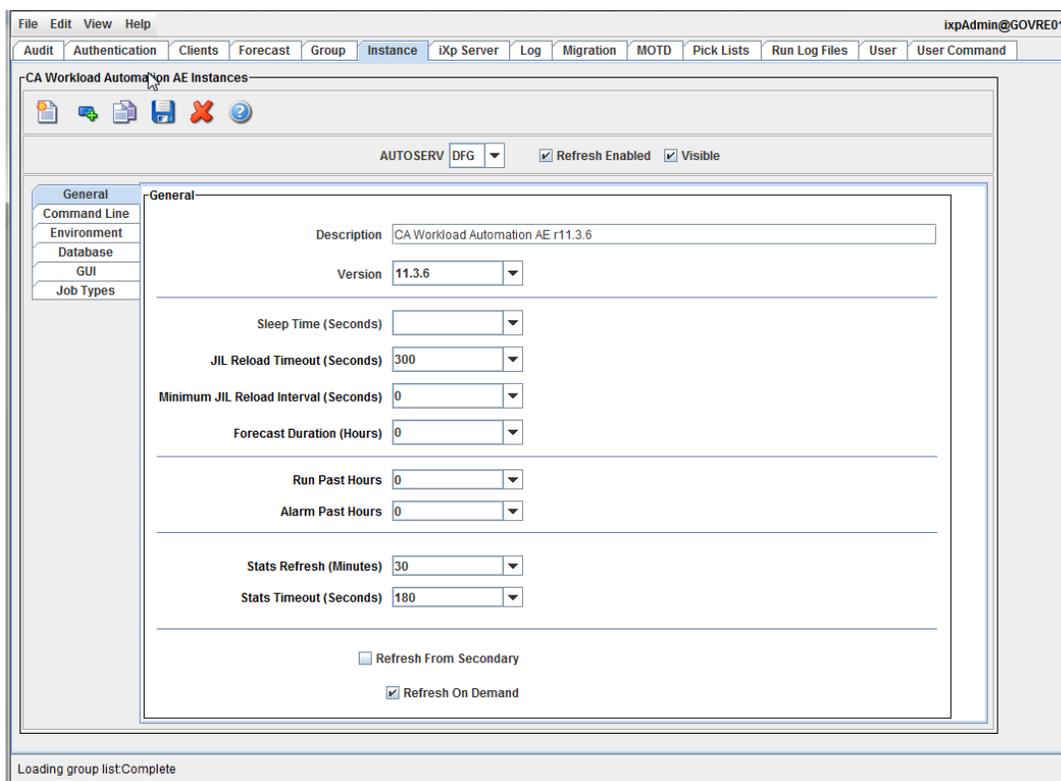
The **GUI** tab controls instance monitoring and GUI idle timeout.

<b>iXp Server GUI Attributes</b>	<b>Description</b>
<b>Enable instance monitor</b>	The instance monitor is an icon, at the bottom left corner of the GUI, which signifies the status of CA Workload Automation AE instances. The check boxes enable this feature for all users or for administrators only.
<b>Pause client refresh</b>	If a user does not perform any action in iXp, the refresh will automatically pause after the specified number of minutes. A pop-up window informs the user, and when the user clicks "OK" the automatic refresh resumes.

Click the Save  icon to save the configuration. The Help  icon opens the Help dialog that provides similar information as above.

## 5.2 CA Workload Automation AE Instance Configuration

Select the **Instance** tab in the iXp Admin Tool to enter the CA Workload Automation AE Instance configuration area.



Each CA Workload Automation AE instance to be accessed from iXp has to be set up here. The Copy Instance button can be used to create an identical AUTOSERV instance connection with a new instance name. Once copied, just the unique information should be changed.

The toolbar at the top provides the buttons to manage the data displayed on this tab.

Tool Bar Icon	Field	Description
	New Instance	Specify the information for a CA Workload Automation AE instance not previously configured.

Tool Bar Icon	Field	Description
	New External Instance	Specify information for an MVS-based instance not previously configured.
	Copy Instance	Copy the information from a configured Instance to a new Instance.
	Save	Save the information.
	Delete	Delete the Instance configuration.
	Help	Open the Help Dialog.

The Instance tab has 5 subsections. Each section can be accessed from the menu on the left-hand side of the tab.

The following table explains the fields listed in the **General** section. This section enables you to specify how much Run Data and Alarm data will be stored on the iXp Server, and other time-out related settings.

Field	Description
<b>AUTOSERV</b>	The CA Workload Automation AE instance name, as denoted by the AUTOSERV environment variable.
<b>Refresh Enabled</b>	Used to enable or disable the iXp Daemon data retrieval process from the instance. If disabled, the iXp Daemon will not read any data from the instance until it has been enabled.
<b>Visible</b>	Select this check box to make this instance appear in the GUI. If you clear this check box, this instance is only accessible from iXp Admin Tool. It will not appear anywhere in the GUI. A report that runs against multiple instances will not show information for the invisible instance. A report that only references the invisible instance will give an error.
<b>Version</b>	The Version of CA Workload Automation AE for this Instance. The default is Release 11.3.6.
<b>Sleep Time</b>	The numbers of seconds that the iXp Daemon will be idle between data refresh cycles. The default value for this setting is Server Sleep Time – 1 second.

<b>Field</b>	<b>Description</b>
<b>JIL Reload Timeout</b>	Number of seconds to wait before reload of JIL based on job time stamp changes.
<b>Minimum JIL Reload Interval</b>	Minimum number of seconds to wait for JIL reloads, irrespective of the amount of changes being made.
<b>Forecast Duration</b>	Specifies if the iXp Forecasting Engine should generate a real-time forecast of upcoming events and runs, based on the current state of the CA Workload Automation AE instance. If this value is set to non-zero, then on every Instance refresh cycle, the iXp Server will generate a forecast for the next X hours, where X is the value specified here. The default is 0.
<b>Run Past Hours</b>	The iXp Daemon will retrieve all the runs within the CA Workload Automation AE instance that either started, or ended in the time frame set by this field. If set to 0 (zero), the iXp Daemon will not retrieve any run data for the instance, until the value is changed. The lower value here, the faster the performance of the server.
<b>Alarm Past Hours</b>	If the value for this field is set to 0 (zero), the iXp Daemon will not retrieve any alarms from the instance. If the value is set to any value greater than 0 (zero), then the iXp Daemon will retrieve all the alarms from the instance. This setting is "loosely enforced", meaning that the current setting plus 24-hours worth of alarms are retrieved.
<b>Stats Refresh</b>	Dictates how often the iXp Daemon retrieves and calculates the CA Workload Automation AE performance statistics for the particular instance. Typically, it is 30 to 45 minutes.
<b>Stats Timeout</b>	Number of seconds after which server statistics collector process will timeout.
<b>Refresh from Secondary Connection</b>	If the CA Workload Automation AE instance has Dual Servers, the iXp Daemon would retrieve the data from the Primary Server. If this option is selected, the iXp Daemon will retrieve data from the Secondary database. This may be useful in case of network problems or database issues.
<b>Refresh On Demand</b>	If this option is selected, the iXp Daemon will try to retrieve CA Workload Automation AE data at the most optimal point in its refresh cycle. This ensures that the iXp Cache features more recent job status information. If you have a busy iXp Server and fast-performing

## CA Workload Automation AE Instance Configuration

Field	Description
	database servers, we recommend that you turn this option ON.

The following table explains the fields listed in the **Command Line** section. You can specify the Date Format that is used for this CA Workload Automation AE instance, and alternate “jil” and/or “sendevent” commands.

Field	Description
<b>Sendevent Shell Command</b>	By default, iXp uses “/bin/sh” or “cmd /c” when executing the <code>sendevent</code> command on the iXp server. You can specify an alternate shell command here (e.g. ssh).
<b>JIL Shell Command</b>	By default, iXp uses “/bin/sh” or “cmd /c” when executing the <code>jil</code> command on the iXp server. You can specify an alternate shell command here (e.g. ssh).
<b>Sendevent Command</b>	iXp uses “ <code>sendevent</code> ” as the default command to use when performing certain actions. You can specify a new command here, and iXp will pass all the <code>sendevent</code> parameters to the command specified here, instead of passing them to the “ <code>sendevent</code> ” command.
<b>JIL Command</b>	iXp uses “ <code>jil</code> ” as the default command to use when modifying, creating job and override definitions. You can specify an alternate command here, and iXp will pass the JIL file to this command instead.
<b>Date Format</b>	The Date Format, as specified within CA Workload Automation AE, for this instance. This field is needed for proper functioning of “ <code>sendevent</code> ”. The value for this field must be identical to what has been specified within the CA Workload Automation AE configuration file/registry.

The following table explains the fields listed in the **Environment** section. You can specify the values for all the CA Workload Automation AE related environment variables here.

<b>Field</b>	<b>Description</b>
<b>AUTOSYS</b>	Path to AUTOSYS directory on the iXp Server. If the CA Workload Automation AE Remote Agent has not been installed on the iXp Server, leave this field blank.
<b>AUTOUSER</b>	Path to AUTOUSER directory on the iXp Server, if the CA Workload Automation AE Remote Agent has been installed on the machine.
<b>ORACLE_HOME</b>	Value of the ORACLE_HOME environment variable on the iXp Server. This value is not needed with Unicenter AutoSys JM r11 and higher versions.
<b>SYBASE</b>	Value of the SYBASE environment variable on the iXp Server. This value is not needed with Unicenter AutoSys JM r11 and higher.
<b>TNS_ADMIN</b>	Value of the TNS_ADMIN environment variable on the iXp Server. This is needed by the CA Workload Automation AE client to locate the database connection information. This value is not needed with Unicenter AutoSys JM r11 and higher.
<b>LD_LIBRARY_PATH/ SHLIB_PATH/ LIBPATH</b>	Value of the applicable environment variable that is required to locate the CA Workload Automation AE libraries.

The information provided in the checklist for AUTOSYS, AUTOUSER, SYBASE, TNS\_ADMIN, ORACLE\_HOME, LD\_LIBRARY\_PATH, SHLIB\_PATH, LIBPATH, and TZ environment variables is applied to each instance of CA Workload Automation AE that is configured.

The following table explains the fields listed in the **Database** section. The fields in this section specify the connection information to the CA Workload Automation AE database.

The Primary Connection and Secondary Connection values mirror the CA Workload Automation AE convention for Primary and Secondary Event Servers.

Field	Description
<b>Database Vendor</b>	Name of the supplier of the CA Workload Automation AE database (Oracle, SQL Server, Sybase). Oracle is the default.
<b>JDBC Driver</b>	Java™ DataBase Connection driver. The drop-down lists the options for Sybase, Oracle, and SQL Server drivers.
<b>Schema Owner</b>	The owner of the DB schema being used by CA Workload Automation AE— needed only for Oracle (typically "aedbadmin" or "mdbadmin")
<b>URL</b>	The database connection parameters used by the JDBC driver.
<b>User</b>	The database user for the connection.
<b>Password</b>	The password for the database user.
<b>Re-enter</b>	Re-enter the password for verification.
<b>DSQUERY</b>	The name of the Sybase Dataserver or the ORACLE TNS alias.
<b>Row Prefetch</b>	The number of rows that is fetched at a time by the Oracle JDBC driver when performing any database query. The default value is 10. If you notice that the iXp server is experiencing slow data retrieval times, we recommend that you set it to 1000.

In addition to these values, the following information about each database is needed:

JDBC Driver

oracle.jdbc.driver.OracleDriver	(Oracle)
net.sourceforge.jtds.jdbc.Driver	(Sybase)
net.sourceforge.jtds.jdbc.Driver	(MS SQL Server)

## URL

jdbc:oracle:thin:@HOST:PORT:SID (Oracle)  
jdbc:jtds:sybase://HOST:PORT/DATABASE (Sybase)  
jdbc:jtds:sqlserver://HOST:PORT/DATABASE (MS SQL Server)

## User/Password

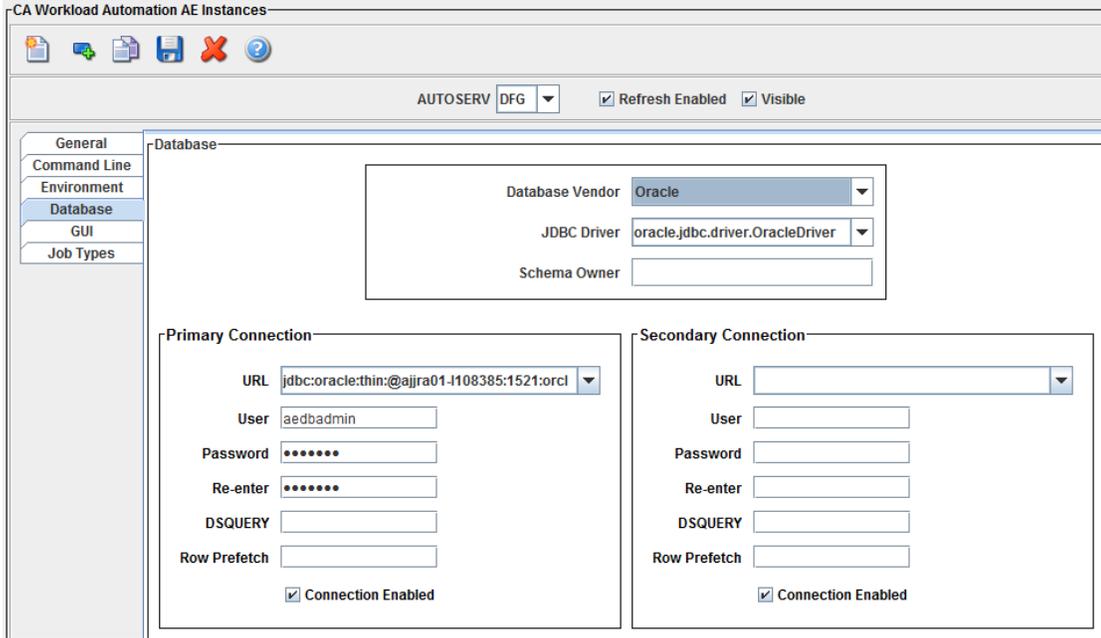
DBUSER (All)  
DBPASS (All)

where

HOST =	Hostname or IP Address of the machine where the autosys RDBMS resides
PORT =	Port number for the database
SID =	The Oracle SID or Global Service Name for the Oracle instance that the database is on
DATABASE =	The name of the Sybase or MS SQL Server database where the CA Workload Automation AE data for the instance is stored. This parameter needs to be used only when the name of the database is not the same as the default database for the DBUSER.
DBUSER =	The database user that has <u>read</u> permissions on all CA Workload Automation AE tables and <u>update</u> permissions on the alarm table. Typically, this is the database user autosys.
DBPASS =	The password of the database user DBUSER.

The **Connection Enabled** check box allows the administrator to disable a DB connection (clear the check box) when a database is down for maintenance or a rollover has occurred. If all the DBs are disabled (Connection Enabled check box is cleared), then the GUI Instance Status Monitor will show the instance as "Disabled".

# CA Workload Automation AE Instance Configuration



The following table explains the fields listed in the **GUI** section. You can use this section to customize how the CA Workload Automation AE job data for this instance is shown in the iXp GUIs.

Field	Description
<b>Console Background</b>	You can specify the color that will be used to highlight the jobs of this CA Workload Automation AE Instance, in the iXp Console View. The default is “No Highlight”.
<b>Timezone</b>	The timezone value for this instance. This value can be displayed whenever start times or end times for jobs belonging to this instance are shown.
<b>Time Format</b>	The format that will be used to display the dates, times, and timezone for the run data for jobs of this instance.
<b>Current Time</b>	Shows a sample display of date/time, for the chosen value in the “Time Format” field.
<b>Enable Server Statistics for All Users</b>	If this option is selected, all iXp Users will be able to view the iXp Server Statistics Graph for their instances.
<b>Enable Server Statistics for iXp Administrators Only</b>	If this option is selected, then only iXp administrators will be able to view the iXp Server Statistics Graph for their instances.
<b>Maximum Alarm Response Length</b>	The total number of characters allowed in the response field when acknowledging or closing an alarm. The header

Field	Description
	data that iXp automatically adds for each alarm response is included in this value. This value should not exceed 127 characters.

**NOTE:** We recommend that you create all the needed CA Workload Automation AE instance information first, before creating user definitions.

**IMPORTANT!** Restart the iXp Web Application Server (Tomcat) after all the CA Workload Automation AE instances have been created.

**NOTE:** You also have to restart the iXp Tomcat server every time you add a new CA Workload Automation AE instance.

The following table explains the fields listed on the Job Type tab:

Field	Description
<b>Only Permit...</b>	When selected, users are only allowed to define Unicenter AutoSys JM 4.5.1 job types through ixjil (from the command line) and <b>File ► CLI ► jil</b> .

## 5.2.1 Configuring for Oracle RAC

If your CA Workload Automation AE instance is setup with Oracle RAC, you can define the database connection information in iXp to leverage this configuration.

To set up iXp with Oracle RAC, perform the following tasks:

1. Copy the database connection information from the Oracle “tnsnames.ora” file on the CA Workload Automation AE server machine.
2. Paste the database connection information in the “URL” field under the “Database” subtab in the “Instance” tab of the iXp Admin Tool.

For example, the database connection URL can be as follows:

```
jdbc:oracle:thin:@(DESCRIPTION
=(LOAD_BALANCE=on)(FAILOVER=on)(ADDRESS_LIST =(ADDRESS =
(PROTOCOL = TCP)(HOST = orasvr1)(PORT = 1521))(ADDRESS =(PROTOCOL
```

```
= TCP)(HOST = orasvr2)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME = ORCL)(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC))))
```

## 5.2.2 Validate the Instance Configuration

Once the Instance has been defined and the Tomcat server has been restarted, you can verify its configuration by performing the following steps:

1. Open the iXp client, and log in as “ixpAdmin”.
2. Click the Instance name in the Tree View, right-click and select “Expand” option to see the top-level jobs of this instance.
3. Select any job that is shown for this instance, and select the **Edit ► Edit Jobs** menu option to see its definition in the Job Editor.
4. Verify that the Console View is showing the Start and End Time information in the appropriate time format and time zone.

## 5.3 User Authentication

Click the **Authentication** tab at the top of the iXp Admin Tool window to configure the authentication policy for iXp. You have to specify the user authentication model for users opening the Client GUI.

By default, iXp is configured to authenticate users based on Single Sign-On mode. The other option is to use internally stored user name and password based authentication.

From this tab, you can also enable the iXp Client CLI and specify the authentication model for users executing the commands.

### 5.3.1 Single Sign-On

This is the default authentication model. With this mode, users do not have to enter a username and password when they open the GUI. The iXp Client GUI will recognize users based on their Domain or OS authentication.

The MOTD format supports HTML 3 and pictures saved on your local Tomcat server.

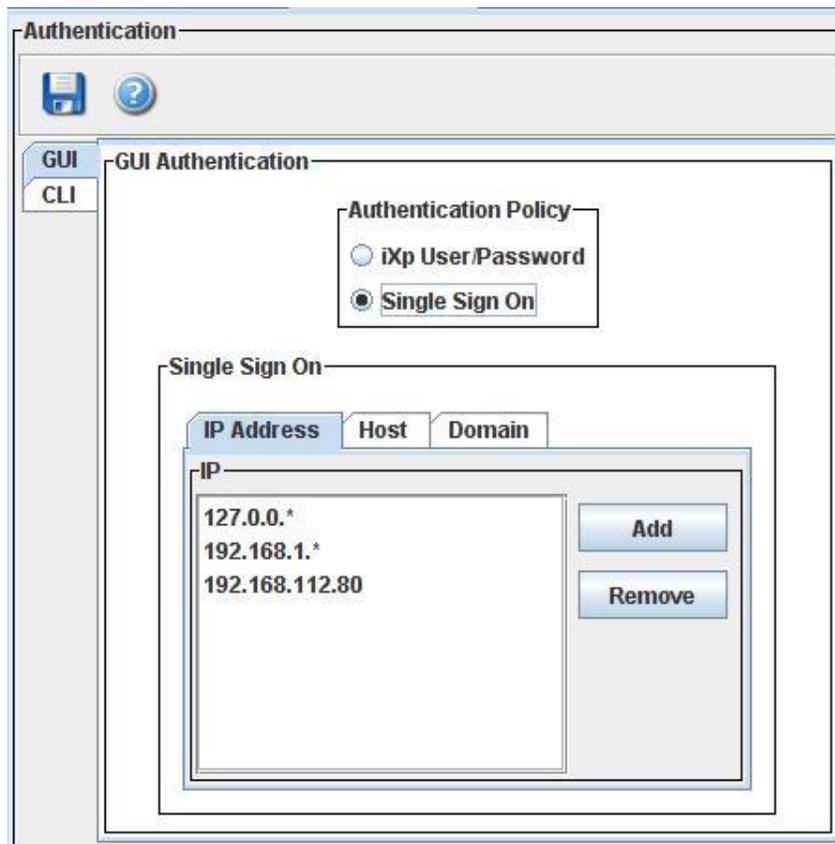
Under this method, you can provide a list of valid IP Addresses, Host names, and Windows Domain names. Users that are not authenticated to the valid Domain, or whose iXp Client machines are not within the list of valid IP Addresses **or** host names, will be unable to open the GUI.

### 5.3.1.1 IP Address

You can provide a list of IP Address strings that will cover all valid iXp Client machines. By default, access is enabled from any IP address (“\*”).

You can provide multiple lists of valid IP Addresses, and you can use wildcards or ranges for any of the values. For example,

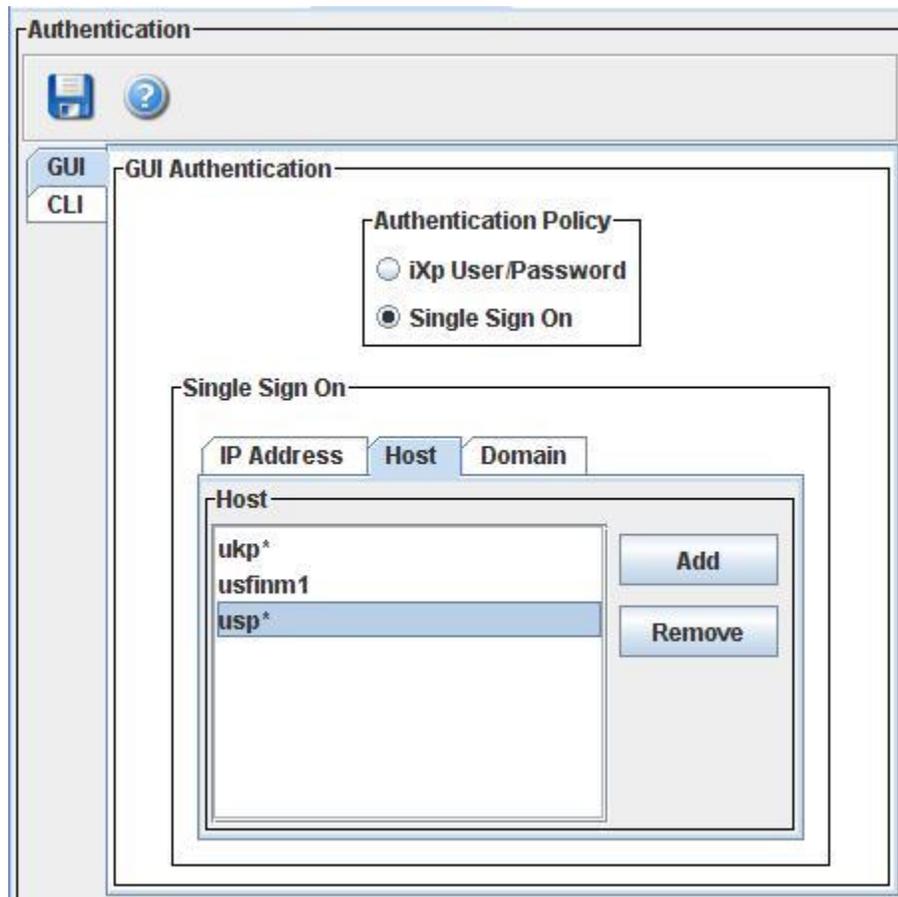
```
192.*.*.*  
19.68.5.10-200  
10.1.86.*  
*
```



If an iXp Client machine matches any one of the specified IP Address lists, then only it will pass the IP Address check.

### 5.3.1.2 Host Names

You can provide a list of host name strings that will cover all valid iXp Client machines. The list of host names is needed along with the list of IP Addresses. A valid iXp Client machine has to pass both the checks. By default, access is enabled from any host name (“\*”).



You can provide multiple lists of valid host names and you can use wildcards for any values. For example,

```
ukp*
usp*
usfinm1
*
```

If the host name of an iXp Client machine matches any of the specified host name lists, it will pass the host name check.

### 5.3.1.3 Domain

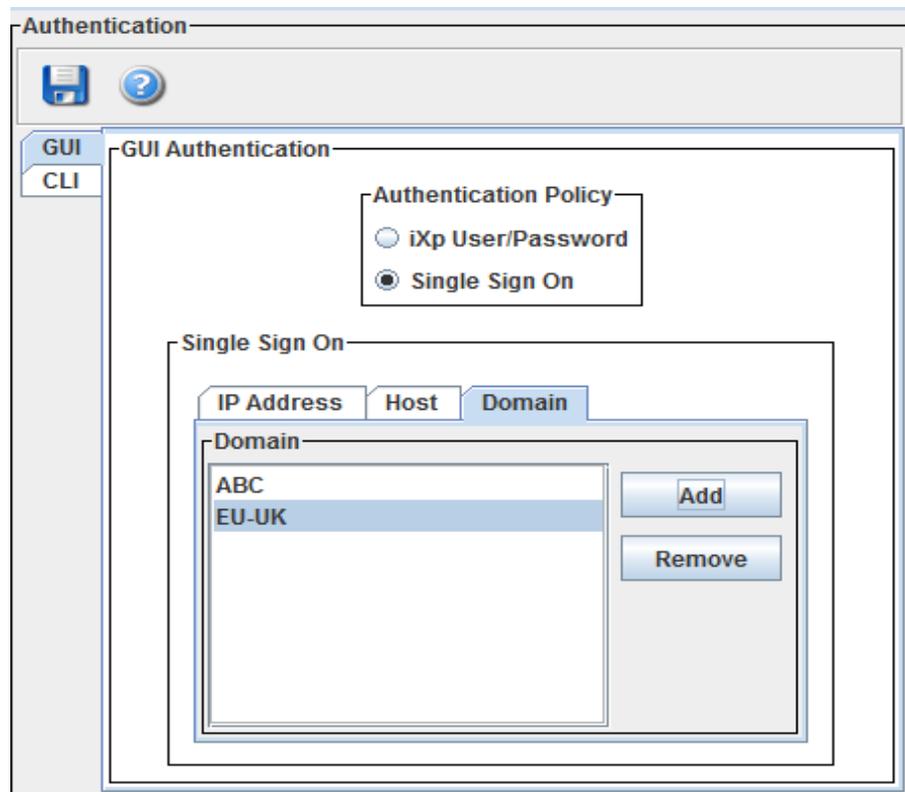
This field is used to validate the Domain or OS authentication of a user. You can provide a list of Domains or host names that will cover all valid user authentications. The domain names are case-sensitive. By default, access is enabled from any domain (“\*”).

If a user is logging on to a Windows Active Directory, NT Domain, or local Windows machine, you can provide the names of valid Domains and local machine names. If a user logs on to a Domain not listed, or logs on to the local machine not listed, then the user will not be authorized to open the iXp GUI.

If a user is logging on to a UNIX/Linux machine, then you have to provide the names of valid machines. In this case, the list of machines could match the list of Host names provided earlier.

For example,

```
CA
us*
*
```



Once a user has logged on from a valid client, and has authenticated to a valid Domain or machine, the user will be able to open the iXp GUI. The user will not be asked to provide a password, since the authentication has passed all checks.

### 5.3.2 iXp User/Password

This is an alternate authentication mode for users opening the iXp GUI. Each user has to be set up with a username and password within iXp. The user name is of your choice, though we recommend that you use names that already exist for users within your domain. You can specify the password policies and other account settings here if you select this option.

The screenshot shows the 'Authentication' tab in the iXp Administration Tool. The window has a title bar with tabs for 'Audit', 'Authentication', 'Clients', 'Forecast', 'Group', 'Instance', and 'iXp Server'. Below the title bar, there are icons for a floppy disk and a question mark. The main content area is titled 'Authentication' and contains a sub-section 'GUI Authentication'. Within 'GUI Authentication', there is an 'Authentication Policy' section with two radio buttons: 'iXp User/Password' (which is selected) and 'Single Sign On'. Below this, there is an 'iXp User/Password' section with five input fields for configuration: 'Maximum Incorrect Entries' (10), 'Maximum Days' (365), 'Minimum Days' (0), 'Unique Entries' (3), and 'Maximum Account Idle Days' (365). On the left side of the window, there are tabs for 'GUI' and 'CLI'.

The following table provides details on the fields for which information has to be provided:

<b>Field</b>	<b>Value</b>
Maximum Incorrect Entries	The maximum number of incorrect password entries allowed before the account is automatically Suspended. The default value is 1000 tries.
Maximum Days	The number of days after which the password for any user has to be reset.
Minimum Days	After setting a password, users cannot change that password for the number of days specified here. Administrators can still change the password from the iXp Admin Tool. The default value is 0 days.
Unique Entries	A new password cannot match the last X number of passwords. The default value is 3.
Maximum Account Idle Days	If an iXp User account does not have any user or administrator activity for the number of days specified here, the account will be automatically Suspended by the iXp Daemon. The default value is 365 days.

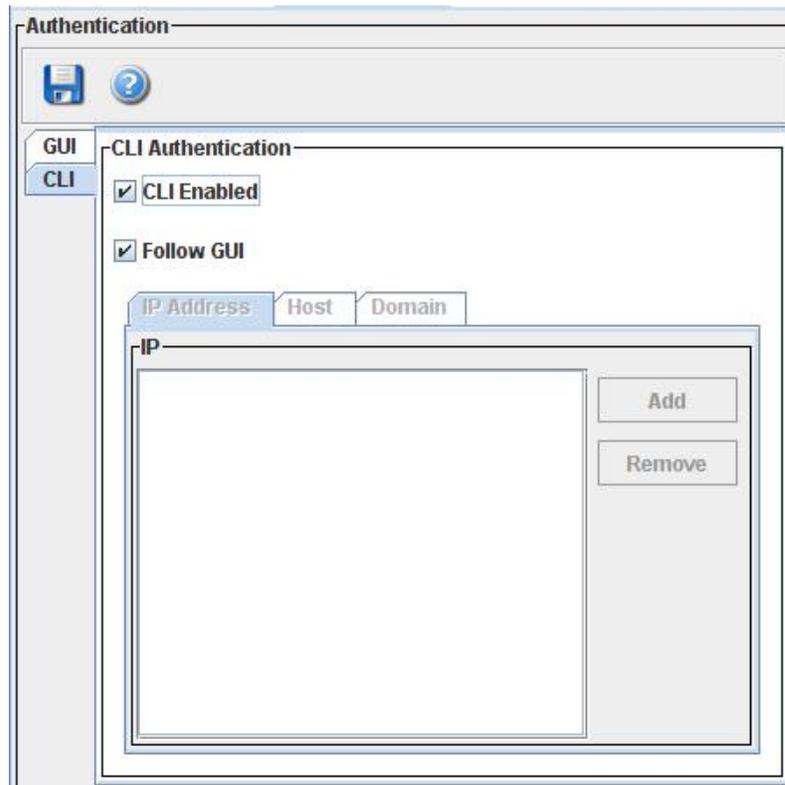
When you choose this authentication model, users have to enter a user name and password every time they open the GUI.

### 5.3.3 iXp CLI Authentication

By default, the iXp Client CLI is enabled. Users can install the CLI, and use the commands unless you disable it in iXp Admin Tool. If the CLI is enabled, users will be able to execute commands directly from the iXp GUI (**File►CLI**).

By default, the CLI is enabled to follow the same authentication fields as the GUI. For the CLI, there is no option to choose iXp User/Password based authentication.

If you chose the Single Sign-On authentication option for the GUI, you can elect to follow the values specified for the GUI authentication. In that case, the CLI has to be opened from machines that are valid for the GUI and has to be opened by users authenticated to the same Domains and hosts specified for the GUI.



If you do not want to follow the same settings as the GUI, then you have to clear the “Follow GUI” check box and specify the list of valid IP Addresses, Host names, and Domains. The same options exist here as they do for the GUI.

For more information about user authentication, see Section 5.3 [User Authentication](#).

Once the user authentication has been set up, you now have to set up authorizations for each valid user.

**NOTE:** Without valid authorization policies, users will not be able to open the GUI or CLI, even after successful authentication.

## 5.4 Users and Groups

Once the authentication policy has been defined, privileges have to be assigned to users. Users that do not have any privileges will not be able to open the iXp GUI or the CLI.

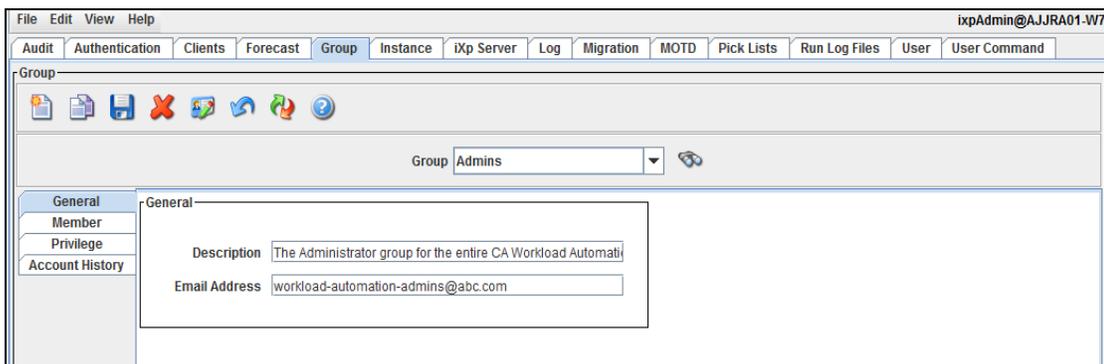
You can assign privileges to users in two ways:

- 1) Assign privileges to Groups and assign Group memberships to each user.
- 2) Assign privileges directly to users, with or without Group memberships. These privileges would be in addition to any other privileges the user inherits from its group membership.

### 5.4.1 Groups

You can create Groups and assign privileges to each group. Users can be members of multiple groups. The privileges for each user will be the combined privileges of all of their groups.

Select the **Group** tab at the top of the iXp Admin Tool window to maintain group definitions.



To find an existing Group, you can select it by using the drop-down list in the Group name area, or click the Search button to open a wild-card based Search dialog.

## Users and Groups



To create a new Group, click the **New Group** icon on the toolbar.



Click the Copy Group icon to copy an existing group, including its memberships and privileges.



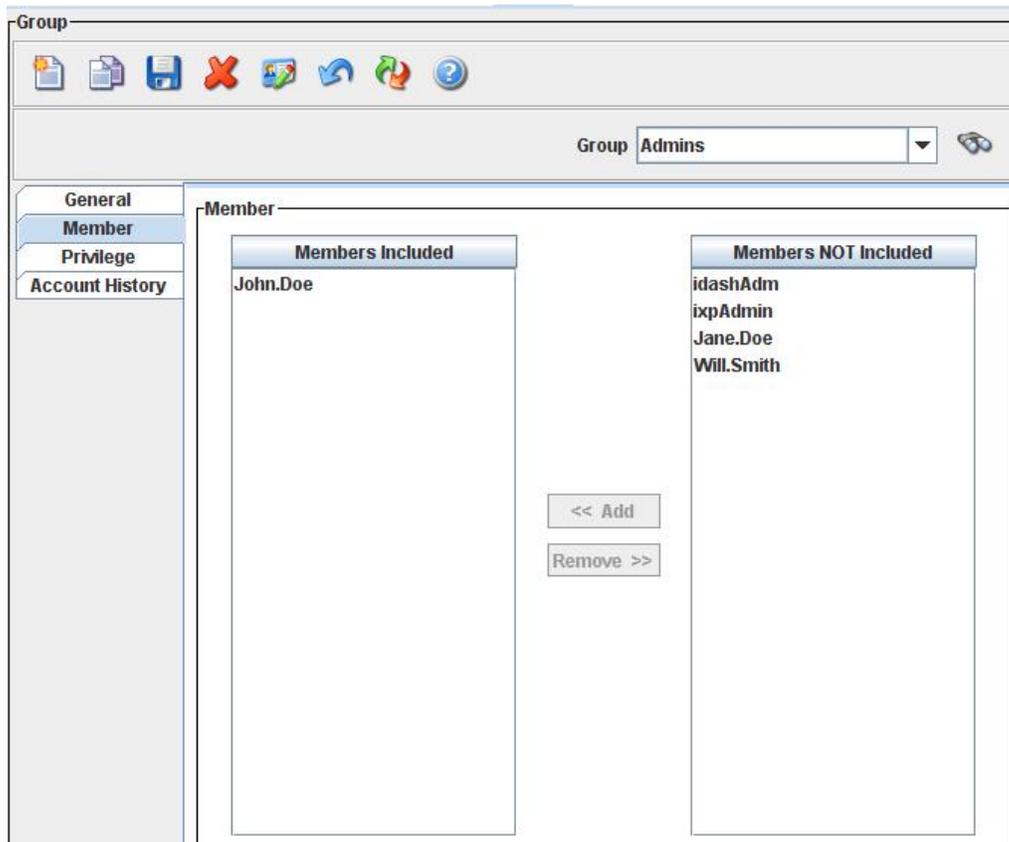
Click the Rename Group icon to rename an existing group.

**NOTE:** The group name cannot include any spaces.

The left-hand side shows multiple tabs. The first tab “General” provides an area to enter a description and an email address for the group. This information is strictly for viewing only.

### 5.4.1.1 Member

This tab enables you to assign membership to this group.



To add members, select the users from the “Members NOT Included” area and click the “Add” button.

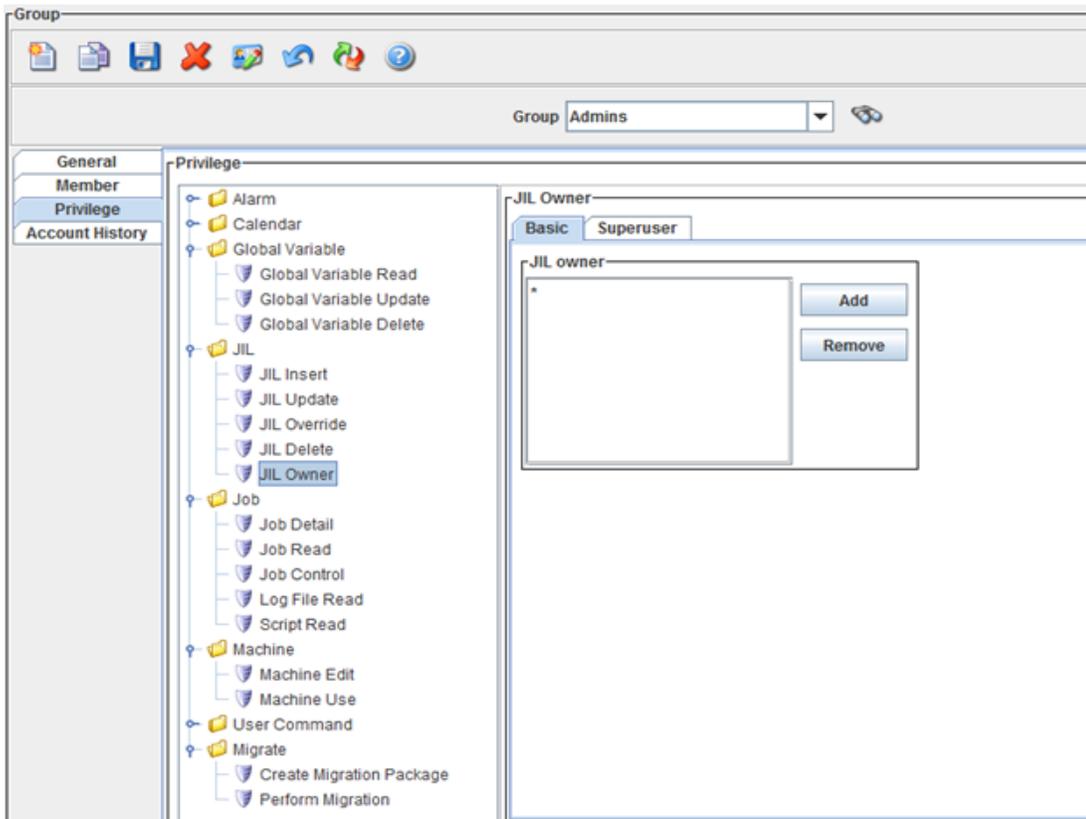
To remove members, select the users from the “Members Included” area and click the “Remove” button.



You can click the “Save” button at any time to save the current Group definition.

### 5.4.1.2 Privilege

This is the tab where you assign the privileges for this Group. All members of this group will then inherit these privileges. When you change the privileges for any group, all the members will immediately get the new set of privileges.



Note the search  icon beside the list of Filters NOT Included. This can be used to find a particular filter by name.

Each Group can be assigned different levels of authorizations, depending on its function. By default, each Group gets created with “read-only” privileges for every CA Workload Automation AE job.

## Users and Groups

The privileges are classified in to multiple categories: Alarm, Calendar, Global Variables, JIL, Jobs, User Command, and Migrate. You can expand each category and see the individual privileges.

The following table explains all of the categories and their individual privileges:

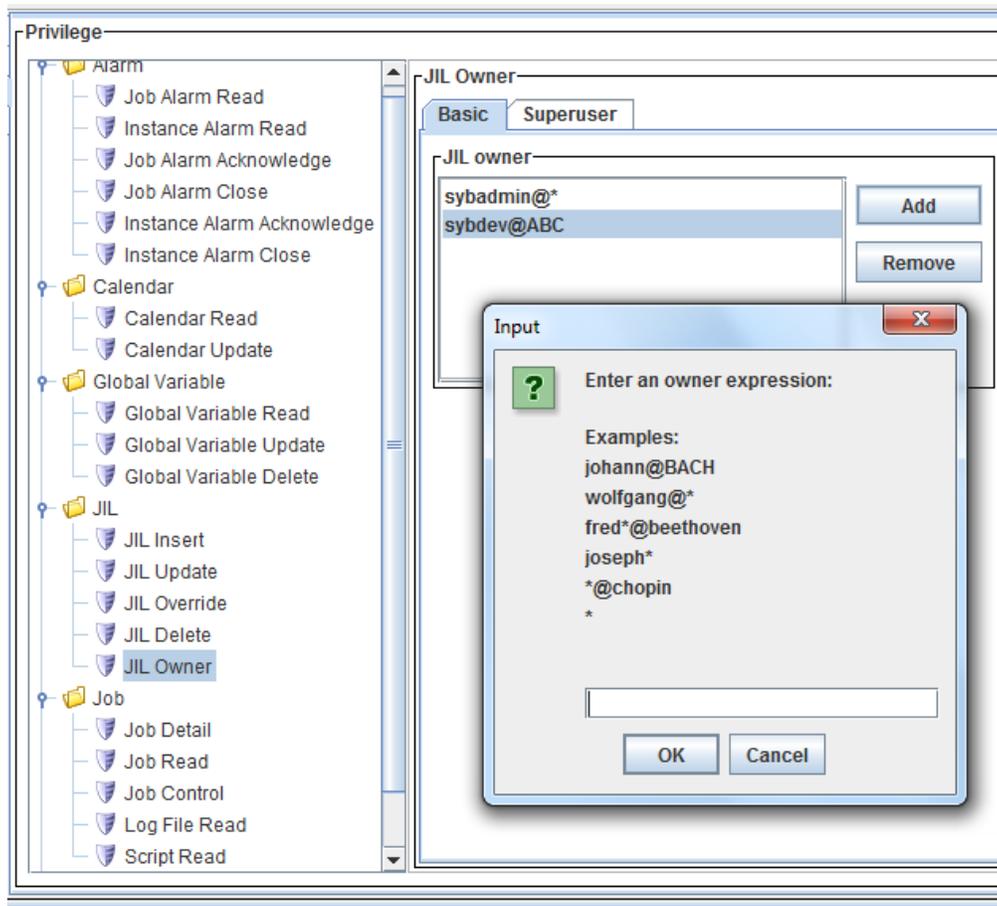
Category	Privilege	For the Jobs matching the filters, Users can
<b>Alarm</b>	Job Alarm Read	<ul style="list-style-type: none"> <li>✓ See the Alarm Dialog</li> <li>✓ View the job-related CA Workload Automation AE Alarms subject to Job Detail privilege</li> </ul>
	Instance Alarm Read	<ul style="list-style-type: none"> <li>✓ See the Alarm Dialog</li> <li>✓ View the non-job related CA Workload Automation AE Alarms for instances covered by the Job Read privilege.</li> </ul>
	Job Alarm Acknowledge	<ul style="list-style-type: none"> <li>✓ Acknowledge the CA Workload Automation AE Alarms in the iXp Alarm Dialog.</li> </ul>
	Job Alarm Close	<ul style="list-style-type: none"> <li>✓ Close the CA Workload Automation AE Alarms in the iXp Alarm Dialog.</li> </ul>
	Instance Alarm Acknowledge	<ul style="list-style-type: none"> <li>✓ Acknowledge non-job related CA Workload Automation AE Alarms.</li> </ul>
	Instance Alarm Close	<ul style="list-style-type: none"> <li>✓ Close non-job related CA Workload Automation AE Alarms.</li> </ul>
<b>Calendar</b>	Calendar Read	<ul style="list-style-type: none"> <li>✓ View all the Calendars for the Instance(s) included that match the given expressions.</li> </ul>
	Calendar Update	<ul style="list-style-type: none"> <li>✓ Create, or modify any of the Calendars for the Instance(s) included that match the given expressions.</li> </ul>
<b>Global Variable</b>	Global Variable Read	<ul style="list-style-type: none"> <li>✓ View any Global Variables for the Instance(s) included that match the given expression(s).</li> </ul>

Category	Privilege	For the Jobs matching the filters, Users can
	Global Variable Update	✓ Change any Global Variables for the Instance(s) included that match the given expression(s).
	Global Variable Delete	✓ Delete any Global Variables for the Instance(s) included that match the given expression(s).
<b>JIL</b>	JIL Insert	✓ Create new jobs from the iXp GUI using Job Editor, or from the CLI using "ixjil".
	JIL Update	✓ Update jobs using the iXp GUI or CLI.
	JIL Override	✓ Issue one-time overrides using the iXp GUI or the CLI. ✓ Delete one-time overrides using the iXp GUI or CLI.
	JIL Delete	✓ Delete jobs using the iXp CLI.
	JIL Owner	✓ Assign a Job Owner when creating or updating jobs using the iXp GUI or CLI.
<b>Job</b>	Job Detail	✓ View and search job attributes such as command, owner, description. ✓ Also control Log read and Alarm read access.
	Job Read	✓ View Jobs and their statuses, details, run history, alarms ✓ View One-time Overrides ✓ Generate Historical and Forecast Run Reports.
	Job Control	✓ Issue any <code>sendevent</code> .
	Log File Read	✓ View Job Log, Job Profile, and Remote Agent log files subject to Job Detail privileges.
	Script Read	✓ View the Command Script file

## Users and Groups

Category	Privilege	For the Jobs matching the filters, Users can
		specified in the selected job's <code>command</code> attribute.
<b>Machine</b>	Machine Edit	<ul style="list-style-type: none"> <li>✓ Change or delete any Machine for the included Instances that match the given expressions.</li> <li>✓ Issue the <code>MACH_ONLINE</code> and <code>MACH_OFFLINE sendevent</code> commands.</li> </ul>
	Machine Use	<ul style="list-style-type: none"> <li>✓ Use any Machine for the included Instances that match the given expressions in a job's <code>machine</code> attribute.</li> </ul>
<b>User Command</b>	Job Command	<ul style="list-style-type: none"> <li>✓ Execute predefined Job User Commands.</li> </ul>
	Alarm Command	<ul style="list-style-type: none"> <li>✓ Execute predefined Alarm User Commands.</li> </ul>
	Context Free Command	<ul style="list-style-type: none"> <li>✓ Execute predefined Context-Free User Commands.</li> </ul>
<b>Migrate</b>	Create Migration Package	<ul style="list-style-type: none"> <li>✓ Open the migration assistant, and create and save workload packages.</li> </ul>
	Perform Migration	<ul style="list-style-type: none"> <li>✓ Open the migration assistant, and migrate workload packages.</li> </ul> <p><b>NOTE:</b> Administrators can migrate all packages created by any user if given this privilege. Other users can migrate only packages they created themselves.</p>

**NOTE:** In the Job Owner area, you can provide a list of owners that are allowed for each user. You can use wildcards (\*) in the owner names. If you specify just a wildcard, then the user will be allowed to specify any owner, other than "root". If you want to allow the user to specify "root" as a job owner, click the "Superuser" tab and enable that privilege.



Most of the privileges must be allocated a list of jobs. These lists are called “Filters” in iXp. The iXp administrator can assign any out-of-the-box filters provided with iXp, or create new filters and assign them. Users will be able to leverage their privileges only for those jobs that pass through the filters assigned for that privilege.

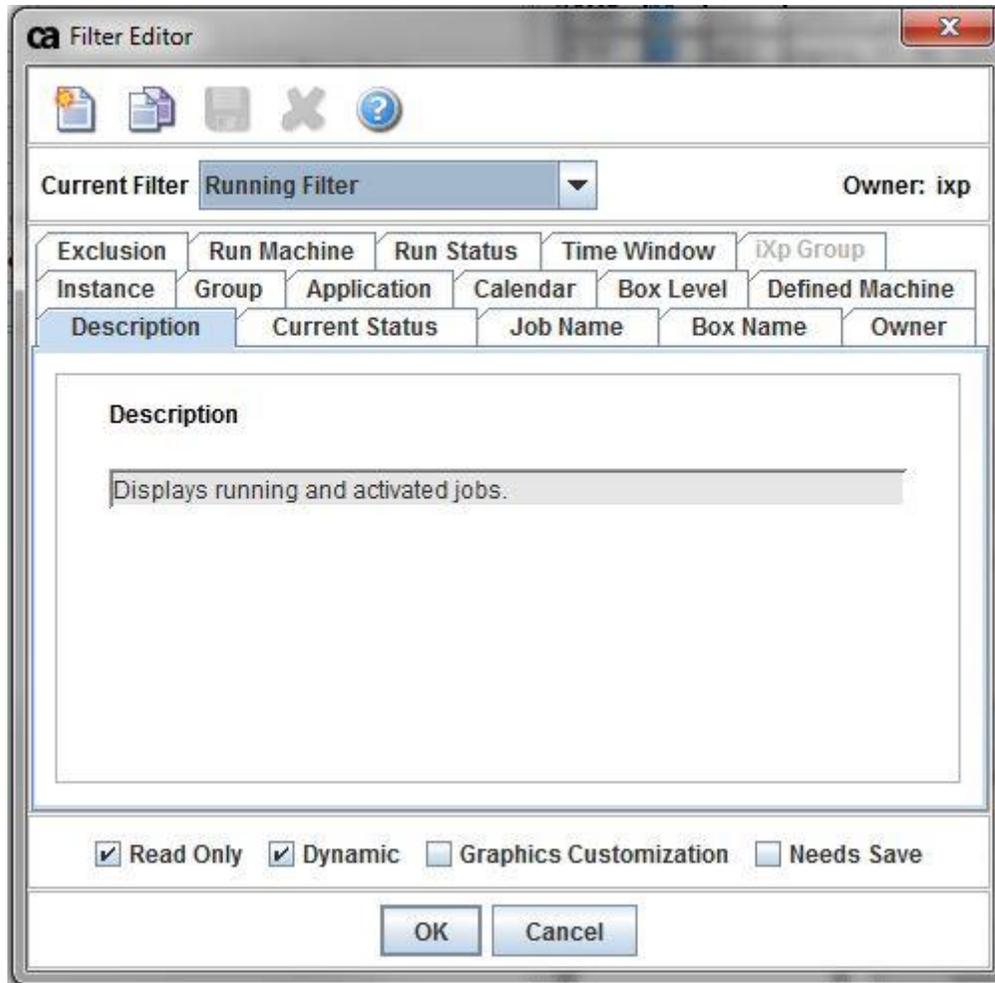
### 5.4.1.3 Using Filters for Security

Filters are used to create authorizations. Only the filters created by users with “Admin” privileges and the filters provided standard with iXp can be used for this purpose.

Each filter can include wildcards for any of the job attributes. The iXp Daemon dynamically generates a list of jobs based on the values assigned to each field in the filter definition.

To create new filters, select the **Edit ► Edit Filters** menu option to view the following Filter Editor window:

## Users and Groups



Click the New Filter icon to create a new filter. When you type in the name for the filter, remember that the name cannot include any spaces.

You can create a filter that includes jobs based on values for one or more attributes listed in this dialog. By default, each attribute will be ignored unless you explicitly provide a list of values.

The following table describes all the fields that can be used for a filter definition:

Filter Attribute	Description
<b>Description</b>	A text description for the filter being created. This is not the same as the description attribute of jobs.
<b>Current Status</b>	Only jobs with Statuses that are selected will satisfy the filter. If no statuses are selected, no jobs will pass the filter. By default, all current statuses are selected.

Filter Attribute	Description
<b>Job Name</b>	Each list entry can be a job_name, such as “Job_A”, or a wildcard expression, such as “Job_A*”. Note that “^” is a special character for delimiting instances. “Job_A” is equivalent to “Job_A^*”. This list will be applied to all types of jobs (Box, Command, and File Watcher).
<b>Box Name</b>	Each list entry can be the name of a Box Job. The name supports wildcard expressions. The filter will return all Box Jobs that match the name expressions <u>AND</u> all the jobs within them, including other box jobs.
<b>Owner</b>	Only jobs with owner that match these expressions will pass the filter. Entries may be a string, such as “root@pluto”, or a wildcard expression, such as “root@*”.
<b>Instance</b>	CA Workload Automation AE instance names, such as “ACE”, or wildcard expressions, such as “A*”.
<b>Box Level</b>	Box Level is the maximum number of box levels that will satisfy the filter. All jobs at a higher box level will be excluded.
<b>Defined Machine</b>	Each list entry can be a string, such as “pluto”, or a wildcard expression, such as “jup*”. A job satisfies the filter if it has at least one machine in its JIL "machine:" definition that matches any of the filter's wildcard expressions.
<b>Exclusion</b>	Each list entry can be a job_name, such as “Job_A”, or a wildcard expression, such as “Job_A*”. Jobs that match the names listed here or are within a Box job listed here will not pass through the filter.
<b>Run Machine</b>	Each list entry can be a string, such as “pluto”, or a wildcard expression, such as “pl*”. Only those jobs that have at least one execution on the machines listed here will pass through the filter. Only jobs having one or more historical run records on a run machine (or virtual machine) will pass the filter.
<b>Run Status</b>	Works in conjunction with the <b>Time Window</b> tab. Only those jobs that have historical or forecasted runs with a status selected here <u>AND</u> within the time frame selected in the Time Window tab will pass through the filter. By default, all run statuses are selected.
<b>Time Window</b>	“Future Hours” and “Past Hours” set bounds on the Run Status filter tab. Choosing “Ignore” for Past Hours means no recent

Filter Attribute	Description
	run history is required to pass the filter. Choosing “Ignore” for Future Hours means no forecasted execution is required to pass the filter.
<b>Group</b>	A filter can be assigned to one or more groups. When a filter gets assigned to groups, only the members of that group (and administrators) will be able to see the filter in their Shared Filter list. If a group has no members and the filter gets assigned to that group, only the administrators will be able to see that filter. Group members can use the filter, but not edit it. If a user is removed, all of that user’s filters will be deleted, including group filters.



You can also copy an existing filter; change some of its properties, and save it under a new name.

If any of the fields in the filter definition are left blank, those fields will be ignored when passing jobs through the filter. So, for example, if the Job Name field is blank, all job names will pass through the filter.

**NOTE:** When you assign filters to the “**JIL Insert**” or “**JIL Delete**” privilege, only the Job Name and Instance attributes are used. All other attributes are ignored. If the Job Name field is left blank, these privileges will be available for ALL jobs. You have to specify a list of values in the Job Name field in order to restrict this privilege.

Each filter also has some “informational” check boxes shown at the bottom of the Filter Editor dialog. These are for information only and cannot be changed by the user creating the filter.

Check Box	Description
<b>Read Only</b>	Indicates this filter is not owned by the current user and/or cannot be modified.
<b>Dynamic</b>	Indicates that jobs that will pass through this filter will depend on their job run information (e.g. Current Status)
<b>Graphics Configuration</b>	Indicates additional drill-down or drag-n-drop actions are associated with this filter.
<b>Needs Save</b>	Indicates that filter configuration changes have not yet been saved to the iXp Daemon.



Once you have created a filter as per your specifications, click the icon to save the filter definition. Only after saving the filter, it can be used for privileges.



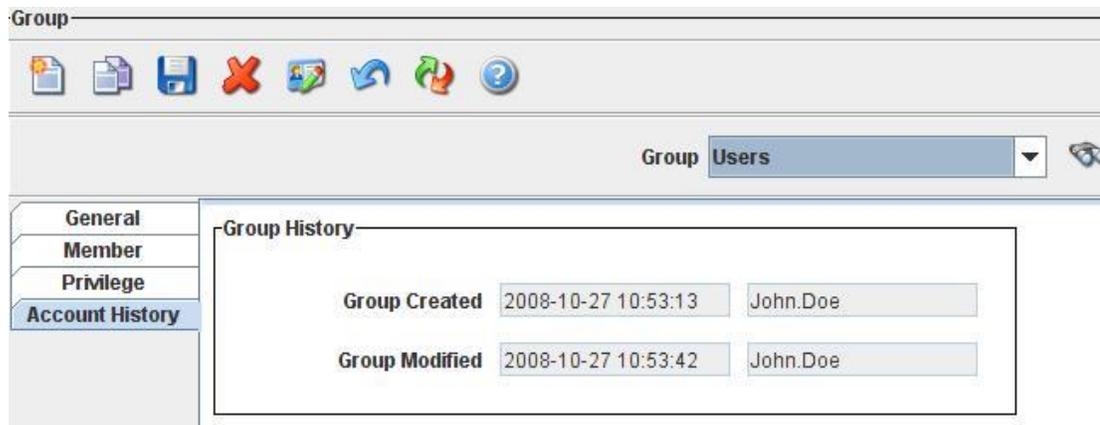
After saving a new filter, click the Reload Filters icon on the Group toolbar. This will import the newly saved filter in the list of filters available for assignment to privileges.



You can delete any of the existing filters by selecting the filter in the Filter Editor and clicking the delete icon.

#### 5.4.1.4 Account History

This tab shows creation and modification information about the Group.



Once you have created one or more Groups, you can now create users and assign group memberships to them.

#### 5.4.2 Users

Select the **User** tab to create users and their group memberships and/or privileges. Once users pass the Authentication tests, they can open the iXp Client GUI or the CLI **only** if they have been defined here.

## Users and Groups

The screenshot shows the 'User' management window. At the top, there is a toolbar with icons for file operations and help. Below the toolbar, a dropdown menu shows the selected user 'ixpAdmin'. On the left, a sidebar contains tabs for 'General', 'Group Membership', 'Privilege', and 'Account History'. The 'General' tab is active, displaying the following fields:

- Account Type: Admin (with an Edit button)
- Account Status: Active (with an Edit button)
- Account Expiration: (with an Edit button)
- Description: (text input field)
- Email Address: (text input field)
- Password: (text input field) (with a Generate button)
- Re-Enter: (text input field)
- Low Band:

If you have chosen the iXp User and Password Authentication model, you have to create user names and passwords in this tab, define the user type, and assign group memberships and/or privileges to them.

If you have chosen the Single Sign-On Authentication model, you just have to define the user type, and assign group memberships and/or privileges.

**NOTE:** The user name must match the Active Directory or OS user name. The user names are not case-sensitive if the iXp Server is running on Windows. If the iXp server is running on UNIX/Linux, then the user names are case-sensitive. We recommend that you use lowercase for all usernames in iXp, irrespective of the OS platform.

To find an existing User, you can select it by using the drop-down list in the User name area, or click the Search button to open a wild-card based Search dialog.



To create a new User, click the **New User** button on the toolbar. Enter the name for the user as per the specifications. The names cannot include any spaces. The left-hand side shows multiple tabs.

### 5.4.2.1 General

This tab enables you to assign user type and some general information. The following table provides details about the fields in this tab:

User Field	Description
<b>Account Type</b>	An iXp user can be of the following types: Regular, Admin, or Temporary. Click the Edit button to set the Account type. An administrator will be able to access the iXp Admin Tool and perform all the functions available here. A Temporary user is a Regular user, except that the user ID will Expire after the account expiration date has been reached.
<b>Account Status</b>	Indicates whether the account is Active or Suspended. If an account is Suspended, it cannot be used for opening the iXp Client or the iXp Admin Tool. To Suspend an account, click Edit and set the status to Suspended. To re-activate a Suspended account, click Edit and set the status to Active.
<b>Account Expiration</b>	The number of days after which the selected Temporary user ID will Expire. Administrator can re-activate Expired accounts by changing the Expiration Date. This field is available only for Temporary accounts.
<b>Description</b>	A text description for the username.
<b>Email Address</b>	You can use this to store any characteristics of the user, for example, the email address.
<b>Password / Re-enter</b>	The password for the iXp username. <u>This is required only if the GUI authentication is set to iXp User/Password.</u> Passwords have to be at least 8 characters long and need to contain at least one numerical character and one special (non-alphanumeric) character. A password supplied here is temporary, and users have to change their password at the next login time.
<b>Generate</b>	Use this button if you want iXp to create a temporary password. The temporary password will be shown in a pop-up dialog. You can highlight the text and copy it

## Users and Groups

User Field	Description
	using standard copy-and-paste operation.
<b>Low Band</b>	You can assign this setting to users that will connect to the iXp Server over a slow network connection. When you enable this setting, the iXp Client receives lesser amount of data on startup and on every refresh.



To set the above fields, click the Save icon after creating or modifying each user account.

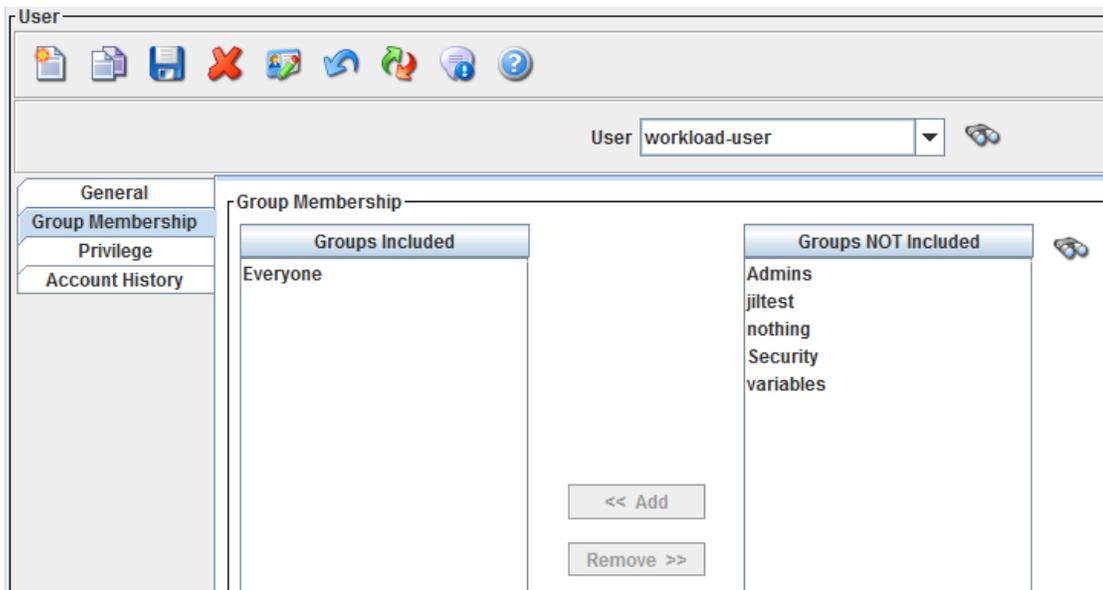
### 5.4.2.2 Group Membership

This tab enables you to assign group memberships to the selected user.

To add this user to a Group, select the Group from the “Groups NOT Included” area and click the “Add” button.

To remove this user from a Group, select the Group from the “Groups Included” area and click the “Remove” button.

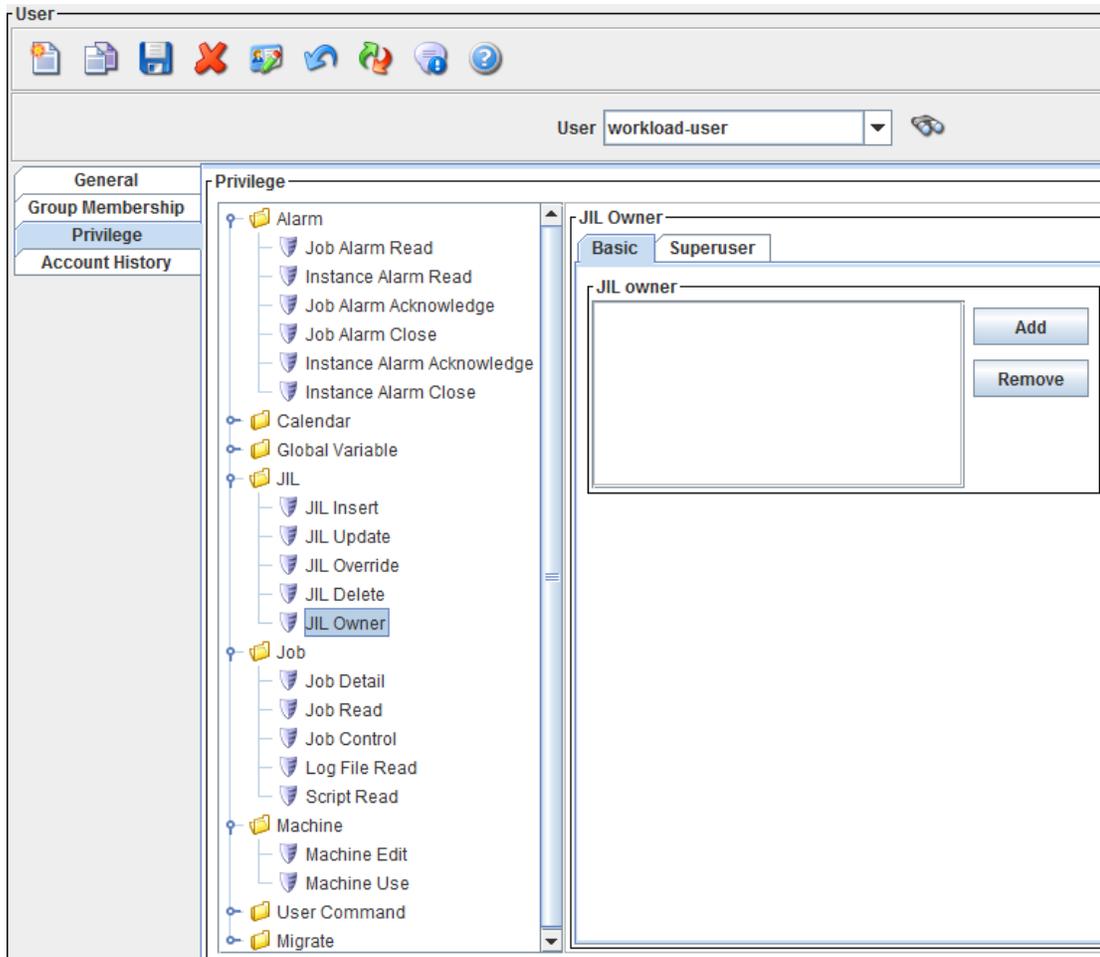
You can click the “Save” icon at any time to save the current User definition.



When a user is a member of multiple groups, the user inherits the combined privileges of all those groups.

### 5.4.2.3 Privilege

This tab enables you to assign specific privileges to users. These privileges will be given to the user, in addition to the privileges that the user inherits from its group membership. This is recommended if the user needs to be assigned some privileges temporarily, or if the user is fulfilling some unique responsibilities not assigned to the rest of the group members.



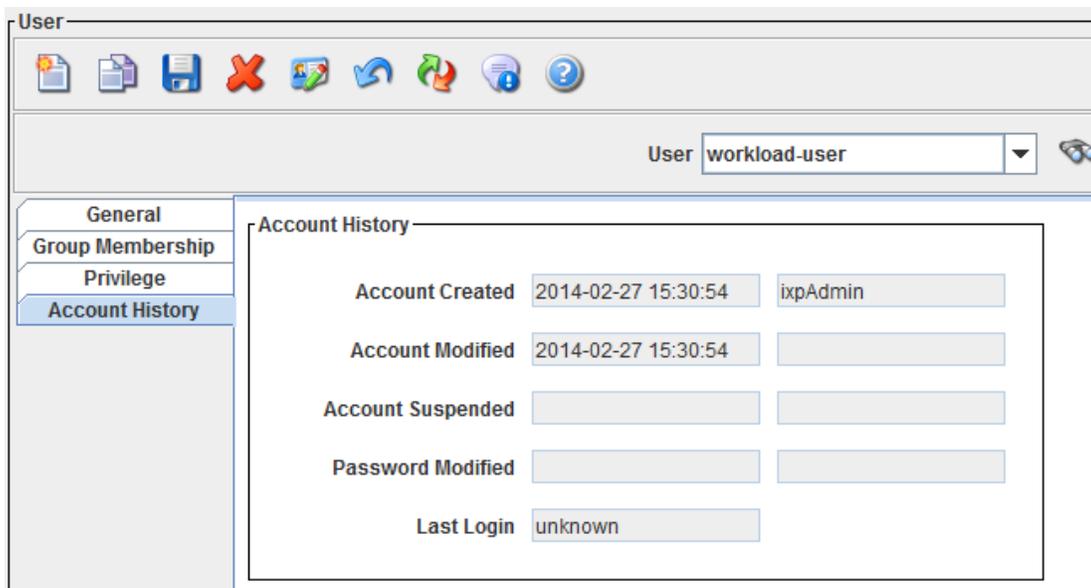
Note the search  icon beside the list of Filters NOT Included. This can be used to find a particular filter by name.

The privileges are identical to those at the group level. For more information about this tab, see Section 5.4.1.2 [Privilege](#).

### 5.4.2.4 Account History

The following table lists the informational fields shown in this tab for the selected user. This tab shows limited data when in SSO (Single Sign-On) mode.

Informational Field	Description
<b>Account Created</b>	The Date and time when an account was created.
<b>Account Modified</b>	The Date and time when an account was modified, either by an administrator or by the iXp Daemon.
<b>Account Suspended</b>	The Date and time when an account was Suspended, either by an administrator or by the iXp Daemon.
<b>Password Modified</b>	The Date and time when the password was last modified, either by an administrator or by the user.
<b>Last Login</b>	The Date and time of the last login by the user.



### 5.4.2.5 Create a New User

- 1) Click the New User icon on the toolbar.
- 2) Type the new **User Name** in the input box, and click **OK**.



- 3) If you are using iXp User/Password authentication, enter the new user **Password**, and re-enter for verification. This password will be temporary only. The user will be forced to change the password at the time of initial login. If you want iXp to create a temporary password, click the “**Auto PWD**” button next to the password field. The temporary password will be shown in a pop-up dialog. You can select the text of the password and copy it using standard OS text copy-and-paste buttons (e.g. Ctrl-C on Windows).
- 4) (Optional) Enter a **Description** for the user.
- 5) (Optional) Enter an **Email Address** for the user.
- 6) By default, the user type is set to “**Regular**”. If you want to assign iXp administrator privileges to this user, click the Edit button and select “**Admin**” as account type. If the user ID is a temporary ID, click the Edit button and select “**Temporary**” as account type.
- 7) If the User is of the type “**Temporary**”, then click the Edit button for **Account Expiration** and assign the number of days for which the user will be valid.
- 8) Assign the Group memberships for this user. Optionally, assign specific privileges to the user.
- 9) Click the **Save** icon to save the new user definition. Now, the saved user can log in to the iXp GUI.

#### 5.4.2.6 Copy User



Use the Copy User icon to create a clone of the selected user’s Group memberships and the properties defined in the ID box. Adjust the password and other identity and security properties as needed.

### 5.4.2.7 Edit User

- 1) Select the user from the User Name drill-down list.
- 2) Follow steps 3-9 of Section 5.4.2.5 [Create a New User](#).

### 5.4.2.8 Remove/Rename User



To remove a user, select the user from the User Name drill-down list and click the **Remove** icon.



To rename any user, except the “ixpAdmin” user, select the user from the User Name drop-down list and click the **Rename** icon.

After renaming a user, it is possible to edit the user definition as needed.

### 5.4.2.9 Undo Changes



While working with a user information, you can undo any changes you have made prior to a Save or Delete by clicking this icon.

### 5.4.2.10 User Message



This icon allows the administrator to send a message to the currently selected user. The message will display in a pop-up box and the user’s refresh will be paused until the message is acknowledged. A User Message expires after 20 minutes.

### 5.4.2.11 ixp Admin User

The security settings for the ixpAdmin user cannot be changed. This user ID represents the iXp “Administrator”. The password for this user can be changed from this screen.

## 5.4.3 Validate the Privileges

The following table shows the steps that users can perform to validate their privileges. The user must log in to the iXp client before performing these steps.

Category	Privilege	Validation Steps
<b>Alarm</b>	Job Alarm Read	✓ Click the “Alarm” button to open the Alarm dialog. If job alarms are not displayed, select “Show Closed Alarms” to fetch alarms that are in Closed State.
	Instance Alarm Read	✓ Click the “Alarm” button to open the Alarm dialog. If non-job alarms are not displayed, select “Show Closed Alarms” to fetch alarms that are in Closed state.
	Job Alarm Acknowledge	✓ Open the Alarm Dialog, and select a job alarm that is in Open or Acknowledged state. Click the Acknowledge button, enter a short response, and click OK. The alarm state will now be “Acknowledged”, and your username and response will be displayed in the Response field.
	Job Alarm Close	✓ Perform the same steps as above but, instead of clicking the “Acknowledge” button, click the “Close” button. The alarm state will change to “Closed” and it will disappear from the Alarm dialog if the “Show Closed Alarms” check box is cleared.
	Instance Alarm Acknowledge	✓ Perform the same steps as those for the “Job Alarm Acknowledge” privilege, but select a non-job alarm instead of an alarm related to a job.
	Instance Alarm Close	✓ Perform the same steps as those for the “Job Alarm Close”, but select a non-job alarm instead of an alarm related to a job.

Category	Privilege	Validation Steps
Calendar	Calendar Read	✓ Select the <b>Edit ► Edit Calendars</b> menu option, select the appropriate instance, and choose a Date or Extended calendar from the drop-down list.
	Calendar Update	✓ Select the <b>Edit ► Edit Calendars</b> menu option, and create a Date calendar with the current date. Click Save to create the calendar.
Global Variable	Global Variable Read	✓ Select the <b>View ► Global Variables</b> menu option to see your authorized global variables.
	Global Variable Update	✓ Select the appropriate instance in the Tree View, select the <b>File ► Sendevent</b> menu option, and click the Set Global tab. Enter the name of the new variable and value, and click Issue sendevent to create the variable.
	Global Variable Delete	✓ Delete the variable created in the validation test for “Global Variable Update” step by settings its value to “DELETE”.
JIL	JIL Insert	✓ Select the <b>Edit ► Edit Jobs</b> menu option, select the appropriate Instance, and create a new Command job. Define the attributes as appropriate, and click Save to create the job.
	JIL Update	✓ Select the appropriate job in any of the views, select the <b>Edit ► Edit Jobs</b> menu option to open the Job Editor, modify the description field for the job, and click Save to make the change.

Category	Privilege	Validation Steps
	JIL Override	✓ Select the appropriate job in any of the views, select the <b>Edit ► Edit Jobs</b> menu option, click the icon to “Add One-time Override”, specify the override, and click Save.
	JIL Delete	✓ Select the <b>File ► CLI ► JIL</b> menu option, select the appropriate instance, and enter “delete_job: JOB”, where JOB is the name of the job you want to delete. Click “Run” to process the delete jil sub-command.
	JIL Owner	✓ Select a job for which you have the Job Update privilege, select the <b>Edit ► Edit Jobs</b> menu option, modify the “owner” attribute to the appropriate value, and click Save to update the job with this new “owner” attribute.
<b>Job</b>	Job Detail	✓ Select the appropriate job, and select the <b>Edit ► Edit Jobs</b> menu option. The “owner” attribute of the job should be visible with the appropriate value.
	Job Read	✓ Select the <b>View ► Find Job By Name</b> menu option, and enter the name of the appropriate job. You can use “*” as a wildcard. Press “Enter” to find the job.
	Job Control	✓ Select the appropriate job, select the <b>File ► Sendevent</b> menu option to launch the sendevent dialog, click the “Comment” tab, enter a comment, and click “Issue Sendevent” to send the event.
	Log File Read	✓ Select a Command job, and select the <b>Job Information ► Log Files ► Standard Out</b> menu option to see the output file.

## Users and Groups

Category	Privilege	Validation Steps
	Script Read	✓ Select a Unicenter AutoSys JM 4.5 command job, and select the <b>Job Information ► Log Files ► Command Script</b> menu option to see the command script.
<b>Machine</b>	Machine Edit	✓ Select the <b>File ► CLI ► JIL</b> menu option, select the appropriate instance, and enter the JIL statements to create the machine definition. Click “Run” to process the JIL statements to create the machine.
	Machine Use	✓ Select a job for which you have the Job Update privilege, select the <b>Edit ► Edit Jobs</b> menu option, modify the “machine” attribute to the appropriate value, click Save to update the job to run on this machine.
<b>User Command</b>	Job Command	✓ Select the appropriate job, and select the <b>File ► User Command ► Job ► USERCOMMAND</b> menu option, where USERCOMMAND is the name of any user command shown in this menu option.
	Alarm Command	✓ Open the Alarm dialog, select an alarm, and select the <b>Alarm Command ► ALARMCOMMAND</b> menu option, where ALARMCOMMAND is the name of any user command shown in this menu option.
	Context Free Command	✓ With or without a job selected, select the <b>File ► User Command ► Context Free ► USERCOMMAND</b> menu option, where USERCOMMAND is the name of any user command shown in this menu option.

Category	Privilege	Validation Steps
Migrate	Create Migration package	✓ Select the <b>Migrate ► Edit Migrations</b> menu option to create a migration package.
	Perform Migration	✓ Select the <b>Migrate ► Edit Migrations</b> menu option, and create a new package or open an existing package. Perform all the steps until you reach the last panel. Verify that the Migrate Now button is enabled.

## 5.5 Migration

The **Migration** tab lets you configure settings related to the migration assistant. The following table provides details about the fields in this tab:

Setting	Description
<b>Migration Enabled</b>	Enables users to open the graphical migration assistant from this iXp server and create migration packages to copy their jobs and related objects from a Unicenter AutoSys JM 4.5.1 instance to a CA Workload Automation AE r11.3 or higher instance. By default, this is turned off.
<b>JIL Command</b>	The default command that will be used to upload the jobs from the migration package to the target CA Workload Automation AE instance.
<b>JIL Syntax Checker Command</b>	The default command that will be used to check the syntax of the JIL file generated by the migration assistant.
<b>Exclusion Rule Set</b>	The name of the rule set that will be applied, by default, to all migration packages created on this iXp server. The rule set can be created from the iXp user interface. Users creating the migration packages can elect not to apply the rule set. Users can also manually override the exclusion of one or more jobs.
<b>JIL Conversion Script</b>	The script or program to which the JIL file generated by the migration assistant will be passed as standard Input. The script can parse the JIL file and make modifications to meet the syntax requirements of the

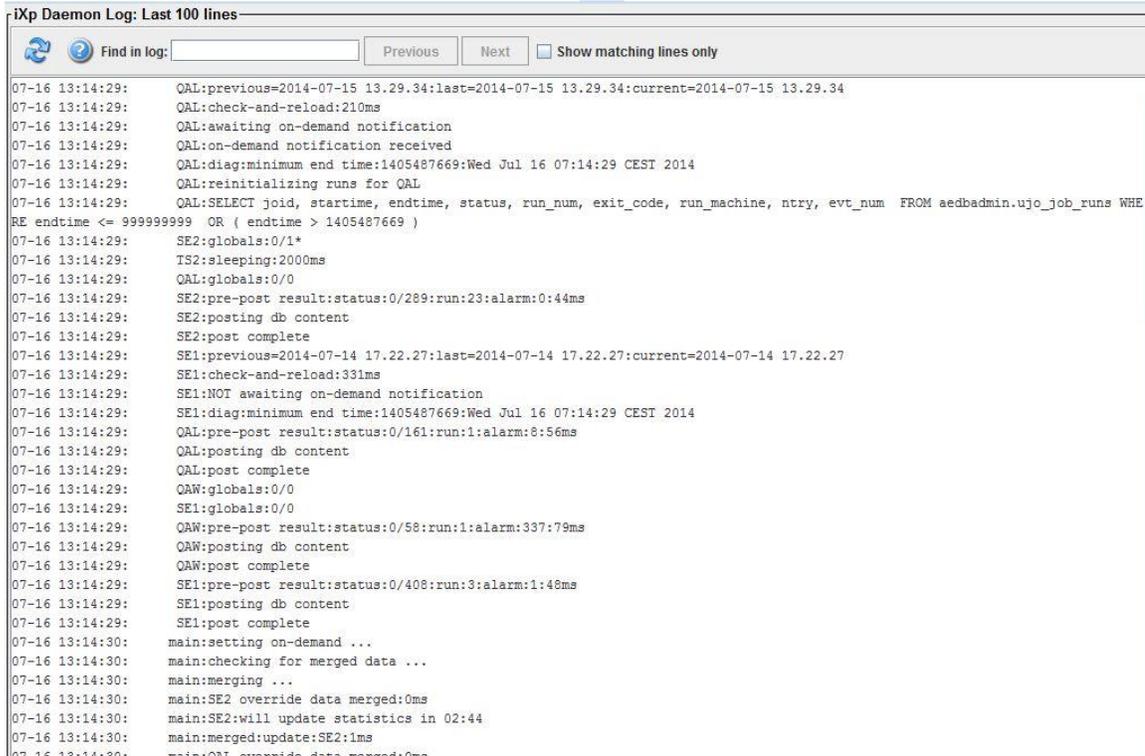
## Migration

Setting	Description
	target instance and the internal corporate standards. The migration assistant will capture the standard output and use that as the new JIL file. A sample PERL script (ixpParseJobs.pl) is provided in the “contrib” directory.
<b>Global Conversion Script</b>	The script or program to which the sendevent script generated by the migration assistant to create the related global variables will be passed as standard input. The script can parse that sendevent script and make modifications to meet the syntax requirements of the target instance and the internal corporate standards. The migration assistant will capture the standard output and use that as the new sendevent script. A sample PERL script (ixpParseGlobals.pl) is provided in the “contrib” directory.
<b>Calendar Conversion Script</b>	The script or program to which the file generated by the migration assistant to create all related calendars in the target instance, which is compatible with the “autocal_asc” command, will be passed as standard input. The script can parse that file and make modifications to meet the syntax requirements of the target instance and the internal corporate standards. The migration assistant will capture the standard output and use that as the new calendar file. A sample PERL script (ixpParseCalendars.pl) is provided in the “contrib” directory.
<b>Remove Migration Packages after X days</b>	Specifies that any package that has been successfully migrated to the target instance will be removed from the iXp server after this number of days.

**NOTE:** For more information about migration, see Chapter 7: [Managing Workload Migration](#).

## 5.6 Administration Log

Select the **Log** tab in the iXp Admin Tool to view the iXp Daemon log.



The screenshot shows the 'iXp Daemon Log: Last 100 lines' window. It features a search bar labeled 'Find in log:', 'Previous' and 'Next' buttons, and a checkbox for 'Show matching lines only'. The log content is as follows:

```
07-16 13:14:29: QAL:previous=2014-07-15 13.29.34:last=2014-07-15 13.29.34:current=2014-07-15 13.29.34
07-16 13:14:29: QAL:check-and-reload:210ms
07-16 13:14:29: QAL:awaiting on-demand notification
07-16 13:14:29: QAL:on-demand notification received
07-16 13:14:29: QAL:diag:minimum end time:1405487669:Wed Jul 16 07:14:29 CEST 2014
07-16 13:14:29: QAL:reinitializing runs for QAL
07-16 13:14:29: QAL:SELECT joid, starttime, endtime, status, run_num, exit_code, run_machine, ntry, evt_num FROM aedbadmin.ujo_job_runs WHE
RE endtime <= 999999999 OR ( endtime > 1405487669 )
07-16 13:14:29: SE2:globals:0/1*
07-16 13:14:29: TS2:sleeping:2000ms
07-16 13:14:29: QAL:globals:0/0
07-16 13:14:29: SE2:pre-post result:status:0/289:run:23:alarm:0:44ms
07-16 13:14:29: SE2:posting db content
07-16 13:14:29: SE2:post complete
07-16 13:14:29: SEL:previous=2014-07-14 17.22.27:last=2014-07-14 17.22.27:current=2014-07-14 17.22.27
07-16 13:14:29: SEL:check-and-reload:331ms
07-16 13:14:29: SEL:NOT awaiting on-demand notification
07-16 13:14:29: SEL:diag:minimum end time:1405487669:Wed Jul 16 07:14:29 CEST 2014
07-16 13:14:29: QAL:pre-post result:status:0/161:run:1:alarm:8:56ms
07-16 13:14:29: QAL:posting db content
07-16 13:14:29: QAL:post complete
07-16 13:14:29: QAW:globals:0/0
07-16 13:14:29: SEL:globals:0/0
07-16 13:14:29: QAW:pre-post result:status:0/58:run:1:alarm:337:79ms
07-16 13:14:29: QAW:posting db content
07-16 13:14:29: QAW:post complete
07-16 13:14:29: SEL:pre-post result:status:0/408:run:3:alarm:1:48ms
07-16 13:14:29: SEL:posting db content
07-16 13:14:29: SEL:post complete
07-16 13:14:30: main:setting on-demand ...
07-16 13:14:30: main:checking for merged data ...
07-16 13:14:30: main:merging ...
07-16 13:14:30: main:SE2 override data merged:0ms
07-16 13:14:30: main:SE2:will update statistics in 02:44
07-16 13:14:30: main:merged:update:SE2:1ms
07-16 13:14:30: main:QAL override data merged:0ms
```



Click the Refresh icon to fetch the latest log, and select the number of lines, counted from the end of the log, that you want to view.

The iXp Daemon log stores all the messages, warnings and errors generated by the daemon. This log is very useful in tracking the status of the daemon and its threads, and also in troubleshooting the problems. The log is particularly useful for:

- 1) Changing or adding an Instance configuration. The effect of instance modifications on the daemon can be seen.
- 2) Monitoring client access.

## 5.7 User Commands

User Commands are a way for iXp to pass job data to an existing UNIX, Linux or Windows script, command, or program. If a user selects one job and executes a User Command, it is processed as follows:

- 1) The command is authorized for the user.
- 2) The proper environment variables are set.
- 3) The command is executed.
- 4) The results are returned.

User commands can be executed for a single or multiple jobs / alarms. If the command fails, or is unauthorized, the server captures the resulting text, and returns the results to the client.

There are three types of User Commands in iXp – Job, Alarm, and Context-Free commands.

Job and Alarm commands are available only when the user has selected a job or an alarm in the iXp client. Context-free commands can be executed without selecting any job or alarm. A job command may be set up to return Operator Instructions for any job selected by the user on the client. An alarm command may be set up to page the on-call person with details about the alarm generated. A context-free command may be used to get system details of the iXp Server.

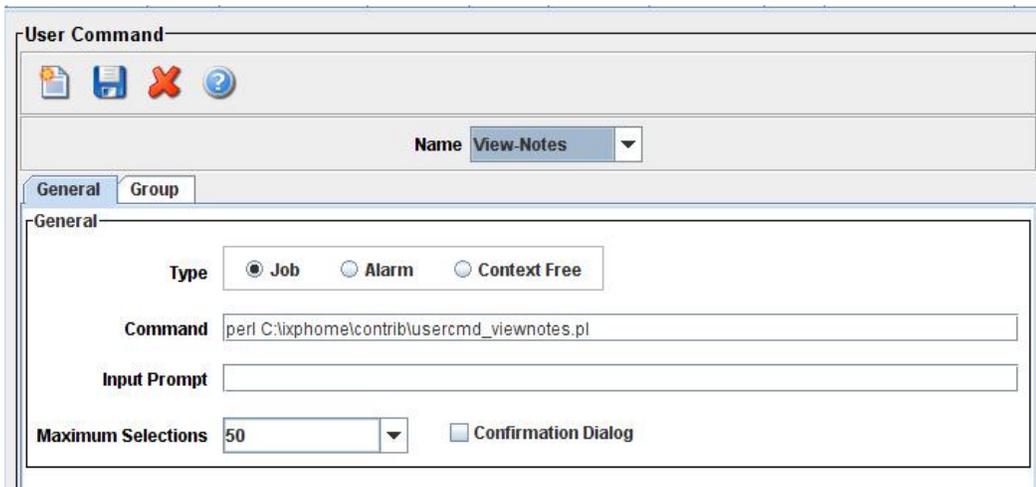
### 5.7.1 Create or Edit User Commands



To create a new User Command:

- 1) Click the New User Command icon and assign a name.
- 2) Type or edit the command in the **Command** text box. Enter the full path to any command or executable that is not included in the PATH set on the iXp Server for the user running the iXp Daemon.
- 3) Enter the **Input Prompt** text if applicable. (See the email address example in the Section 5.7.2 [Interactive User Commands](#) of this document.)
- 4) Select the **Type**: Job, Alarm, or Context Free.

- 5) Click the Save icon to save the new User Command to the iXp Daemon. This will make the User Command available to iXp users with the proper permissions. After defining a new User command, users with active sessions will have to exit and log back in to the GUI to access the new commands.
- 6) By default, when users execute any user command, they need to confirm the execution. If required, the additional step of confirmation can be eliminated for certain user commands by clearing the **Confirmation Dialog** check box.
- 7) If you are creating a Job or Alarm User Command, you can run the User Command on multiple jobs. In order to do so, you have to specify the maximum number of jobs/alarms that a user can select when executing this User Command. Use the **Maximum Selections** field to specify that limit. The default value for this setting is 50 (fifty). If the user command is returning a URL, then we recommend that you should set the value for this field to 1.
- 8) Click the Remove icon to remove the User Command from the iXp Daemon.



For User Commands of **Type Job**, the following environment variables are set on the iXp Server before the command is executed:

User Command Variable	Description
IXP_USERCOMMAND_JOB_NAME	The selected job's name.
IXP_USERCOMMAND_JOB_LAST_START	The selected job's last start time.

## User Commands

User Command Variable	Description
IXP_USERCOMMAND_JOB_LAST_END	The selected job's last end time.
IXP_USERCOMMAND_JOB_LAST_RUN_MACHINE	The selected job's last run machine.
IXP_USERCOMMAND_JOB_JOID	The selected job's joid value.
IXP_USERCOMMAND_JOB_STATUS	The selected job's current status, e.g. "SUCCESS".
IXP_USERCOMMAND_USER_NAME	The name of the iXp user executing the command.
IXP_USERCOMMAND_INPUT	The text input by a user during execution of an <i>Interactive User Command</i> .
IXP_USERCOMMAND_INPUT_PROMPT	The text prompted to a user during execution of an <i>Interactive User Command</i> .
IXP_USERCOMMAND_USER_HOSTNAME	Set value to the user's host name where the iXp client runs.

For User Commands of **Type Alarm**, the following variables are set on the iXp Server before the command is executed:

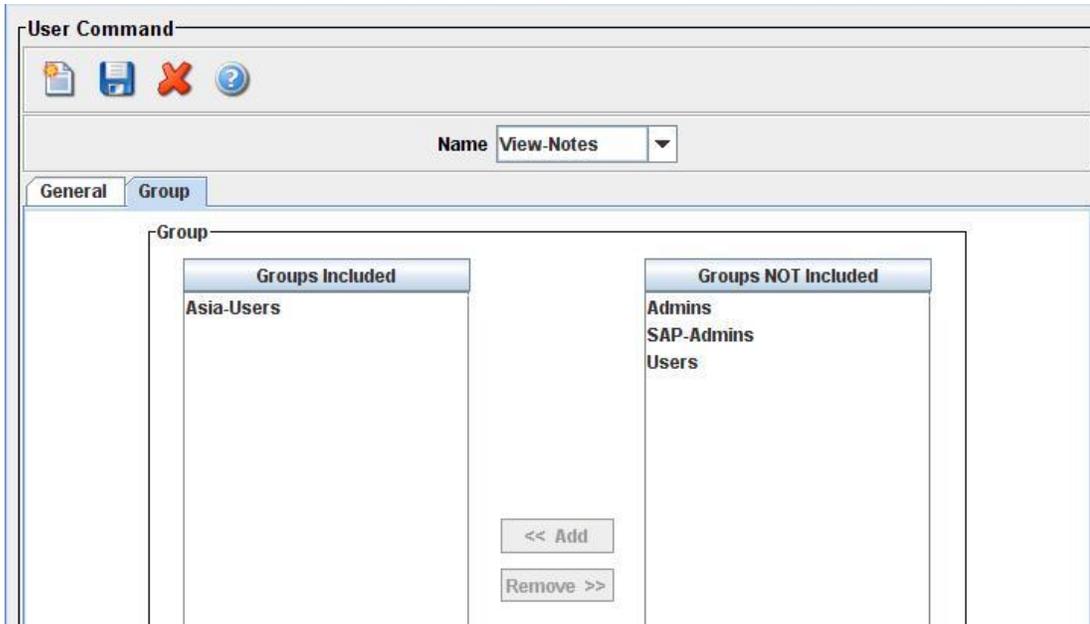
IXP\_USERCOMMAND\_ALARM\_NAME, (e.g. JOB\_FAILURE)  
 IXP\_USERCOMMAND\_ALARM\_TIME  
 IXP\_USERCOMMAND\_ALARM\_COMMENT  
 IXP\_USERCOMMAND\_USER\_NAME  
 IXP\_USERCOMMAND\_ALARM\_RESPONSE  
 IXP\_USERCOMMAND\_ALARM\_JOB\_NAME  
 IXP\_USERCOMMAND\_INPUT  
 IXP\_USERCOMMAND\_INPUT\_PROMPT

The following CA Workload Automation AE environment variables are set for both Job and Alarm User Commands:

AUTOSERV, AUTOUSER, AUTOSYS, DSQUERY, IXP\_SERVER\_URL,  
 PATH, prepended with the proper \$autosys¥bin directory.

For **Context Free** User Commands, no variables are set, except for IXP\_USERCOMMAND\_INPUT, IXP\_SERVER\_URL, and the PATH variable of the Web Server.

Similar to filters, you can assign groups to User Commands. When you do that, only the members of the included groups, and iXp administrators, will be able to execute the user commands.



## 5.7.2 Interactive User Commands

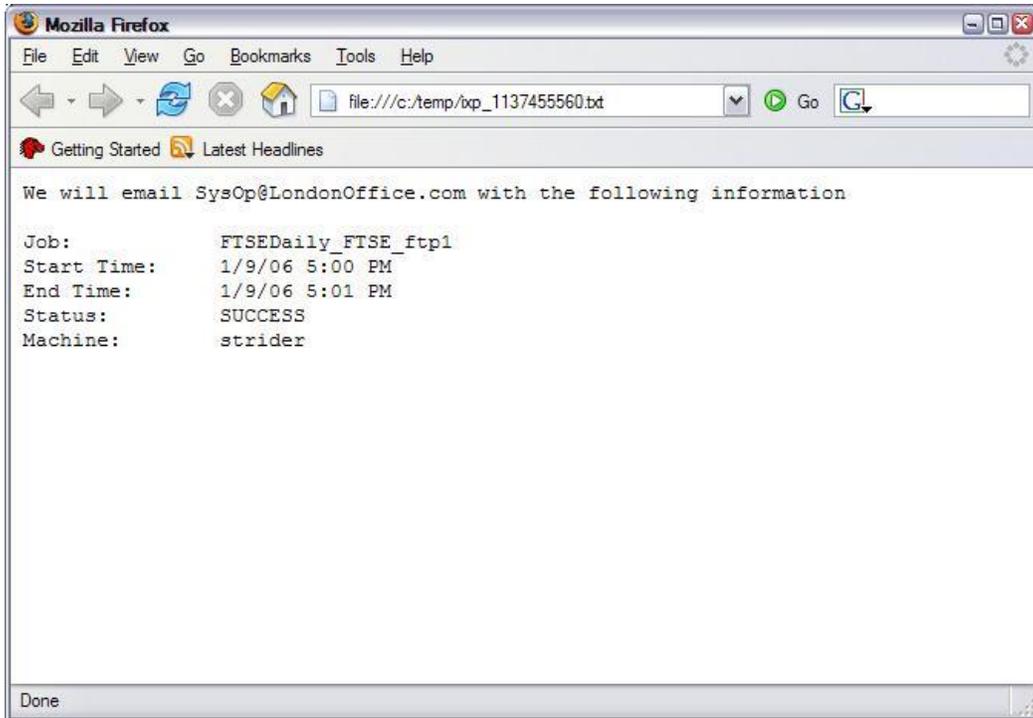
During user execution, a User Command may prompt for input, for example, the email address to which to send job run data.

In the iXp GUI, select a job, and select the **File►User Command►Job►Email** menu option. Since the User Command was set up with a non-empty Input Prompt, the iXp GUI will open a dialog with an input prompt. Enter the appropriate information, and click OK.



## User Commands

iXp shows any output generated by the User Command in a web browser window. Since iXp sets the above listed environment variables before executing the script associated with the User Command, the script can leverage the same variables and perform the required action.



## 5.8 Forecast

Select the **Forecast** tab to access iXp Forecast Properties.

The screenshot shows the 'CLI Forecast Properties' dialog box with the following fields and values:

Property	Value
Forecast Duration (Hours)	0
Set Status Time (Milliseconds)	50
Set STARTING Time (Milliseconds)	50
Set RUNNING Time (Milliseconds)	50
Set DONE Time (Milliseconds)	50
Status Read Time (Milliseconds)	50
Event Read Time (Milliseconds)	50
Start Job Time (Milliseconds)	20
VMStat Time (Milliseconds)	50
Cross Instance Sendevent Time (Milliseconds)	50

Edit and save these values to change the forecast properties, held in the `IXP_HOME/etc/forecast.props` file. These parameters delineate the output of the command line *forecast utility*, and the job run forecasts that will be viewable in the *Time View Chart*. These parameters also affect the iXp application *Interactive Forecasting tool*.

Forecast Property	Description
Forecast Duration	This setting is deprecated. Only the iXp forecasting command line interface uses it. This field specifies a time window for the forecasting engine, in hours. Example: setting this to "4" will generate a 4 hour forecast when processed via the command line.
Set Status Time	The estimated time in milliseconds that the scheduler

## Forecast

Forecast Property	Description
	requires to update a status in the Event Server database.
Set STARTING Time	The time in milliseconds the scheduler requires to update a status with the value of STARTING in the Event Server database. Its value may differ from the default (Set Status Time).
Set RUNNING Time	The time in milliseconds the scheduler requires to update a status with the value of RUNNING in the Event Server database. Its value may differ from the default (Set Status Time) because the value should also capture the contention that may arise from a remote agent simultaneously performing a roughly identical task.
Set DONE Time	The time in milliseconds the scheduler requires to update a status with the value of SUCCESS, TERMINATED, or FAILURE in the Event Server database. Its value may differ from the default (Set Status Time) because the value should also capture the contention that may arise from a remote agent simultaneously performing a roughly identical task.
Status Read Time	The time in milliseconds the scheduler requires to read a job's status (such as when evaluating a job's "condition:" field) from the Event Server database.
Event Read Time	The time in milliseconds the scheduler requires to read an event from the event server database. This value may reflect the presence of a backup server and the attendant event synchronization required.
Start Job Time	The time in milliseconds the scheduler requires to perform the calculations to determine if a job can be started.
VMStat Time	The time in milliseconds the scheduler requires to perform vmstat on each machine in the "machine:" field of a command job or file watcher.
Cross Instance Sendevent Time	The time in milliseconds the scheduler requires performing a sendevent to an external instance when processing the job completion of a job that has an external successor.

## 5.9 Message of the Day (MOTD)

Select the MOTD tab to view or change the Message of the Day. The MOTD format supports HTML 3 and pictures saved on your local Tomcat server.

Click the Save icon to save the message.

The Message of the Day appears in the iXp Login screen. If the Message of the Day is changed, then all active iXp Clients will display the new message. Users have to acknowledge the message before continuing with the client.

## 5.10 Clients

Select the Clients tab to access the active Client Connections list.

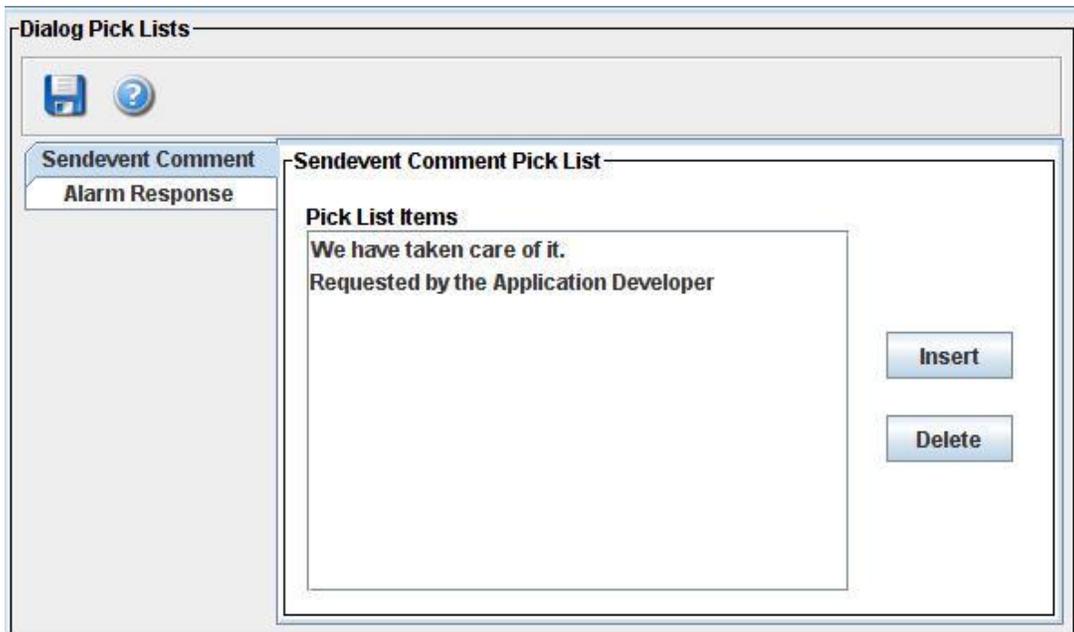
Audit	Authentication	Clients	Forecast	Group	Instance	iXp Server	Log	Migration	MOTD	Pick Lists	Run Log Files	User	User Command
Client Connections: 12/10/12 23:35    3 active user(s)													
 													
ID	Description	Filter	On Since	Email	Low Band								
Mark.Rypien		WLR	12/10/12 23:30	Mark.Rypien@ourdomain.com	<input type="checkbox"/>								
Steve.Anderson		Level Zero Filter	12/10/12 23:31	Steve.Anderson@ourdomai...	<input type="checkbox"/>								
Roger.Vesty		Instance Filter	12/10/12 23:34		<input type="checkbox"/>								

Client Attribute	Description
<b>ID</b>	User Name.
<b>Description</b>	Description as entered in the <a href="#">Users</a> tab.
<b>Filter</b>	Current active user filter.
<b>On Since</b>	Time elapsed since user logged on.
<b>Email</b>	Email address of user, as specified in the user definition.
<b>Low Band</b>	If a logged on user has been assigned the “Low Band” setting, then this check box will be selected.

Click the Refresh icon to update the list. The number of active client sessions (users) is displayed on the top line.

## 5.11 Pick Lists

Select the **Pick Lists** tab to access the Dialog Pick Lists functions.



**Sendevent Comment** and **Alarm Response** pick lists may be populated to be available in the iXp application. The pick lists can be used to pre-define standard comments and responses that can be selected by users when executing sendevents or responding to alarms.

The Sendevent Comment pick lists appear in the *Job Control Popup* functionality sendevent comment input boxes. The Alarm Response pick lists appear in the *Alarm Manager* functions Acknowledge and Close alarm response input boxes.

To insert pick list items, click **Insert**, enter the pick list text, click OK, then click the **Save** icon.

To delete pick list items, highlight them, click **Delete** to remove them from the list, then click the **Save** icon.

## 5.12 Audit Trail

iXp keeps track of certain activities performed within the iXp GUI or the iXp Admin Tool. The audit trail of such activities is displayed in this tab of the iXp Admin Tool.

Audit Information						
						Selected User   All Users
Time	User	Host	Type	Action	Instance	Detail
2008-10-24 18:41:50	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-24 18:41:46	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-24 17:41:41	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-24 17:11:37	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-24 16:47:48	John.Doe	192.168.1.8		LOGIN		
2008-10-24 16:47:10	ixpAdmin		USER	UPDATE		/install/PGT/ixphome/etc/user/John.Doe.conf
2008-10-24 16:46:02	ixpAdmin		USER	UPDATE		/install/PGT/ixphome/etc/user/ixpAdmin.conf
2008-10-24 16:46:02	ixpAdmin			LOGIN		
2008-10-24 16:45:51	John.Doe	192.168.1.8		LOGIN		
2008-10-24 16:45:19	John.Doe	192.168.1.8		LOGIN		
2008-10-24 16:44:32	ixpAdmin		USER	UPDATE		/install/PGT/ixphome/etc/user/ixpAdmin.conf
2008-10-24 16:44:32	ixpAdmin			LOGIN		
2008-10-24 16:42:43	John.Doe	192.168.1.8		LOGIN		
2008-10-24 16:41:31	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-23 21:53:23	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-23 21:48:54	John.Doe	192.168.1.8	PREFERENCES	UPDATE		/install/PGT/ixphome/dati/user/John.Doe/props
2008-10-23 21:47:57	John.Doe	192.168.1.8		LOGIN		
2008-10-23 21:23:15	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-23 21:17:57	John.Doe	192.168.1.8		LOGIN		
2008-10-23 21:02:14	John.Doe	192.168.1.8	FILTER	CREATE		/install/PGT/ixphome/dati/user/John.Doe/hacssap51.ftr
2008-10-23 21:00:48	John.Doe	192.168.1.8		LOGIN		
2008-10-23 20:56:53	John.Doe	192.168.1.8		LOGIN		
2008-10-23 20:53:09	ixpAdmin			COMMAND	PL1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN
2008-10-22 20:45:37	ixpAdmin			COMMAND	IAS1	java -Dixp.home=/install/PGT/ixphome-DIXP_STATS_IN

Toolbar Field	Description
<b>Duration</b>	Choose to display all the audited activities for the last X days
	Refresh the displayed audit trail to show the latest information.
	Click this button to create a CSV file of the displayed audit trail.
	Click this button to create an HTML file of the displayed audit trail.

If a user performs any of the following activities in the **iXp Admin Tool**, the audit trail will include them:

- Logs on to the iXp Admin Tool
- Creates, Updates, or Deletes an iXp user definition.
- Updates the iXp Server information
- Creates, Updates, or Deletes an CA Workload Automation AE Instance information
- Creates, Updates, or Deletes an iXp User Command
- Creates, or Updates the Message of the Day.
- Creates, Updates, or Deletes any of the Pick list lines
- Creates, Updates, or Deletes a Filter definition.

If a user performs any of the following activities in the **iXp GUI**, the audit trail will include them:

- Logs on to the iXp GUI.
- Creates, Updates, or Deletes a Filter definition.
- Issues any sendevent successfully.
- Updates a job definition successfully.
- Creates, Updates, or Deletes a job override successfully.
- Updates the user preferences

## Run Log Files

- Saves the Session settings.
- Executes a User command successfully.
- Acknowledges or Closes an Alarm successfully.
- Changes the Password.
- Creates, Updates, or Deletes a Report definition.

If a user performs any of the following activities in the **iXp CLI**, the audit trail will include them:

- Views job summary, detail, or definition using *ixautorep*
- Creates, Updates Job definitions using *ixjil*
- Issues sendevents using *ixsendevent*
- Creates one-time job overrides using *ixjil*

<b>Audit Attribute</b>	<b>Description</b>
<b>Time</b>	The time of the activity.
<b>User</b>	The User that performed the activity.
<b>Host</b>	The name of the client machine from which the user performed the audited action. This field is used only in Single Sign-On mode.
<b>Type</b>	The Type of activity performed. This is an internal iXp classification mechanism.
<b>Action</b>	The performed activity.
<b>Instance</b>	The name of the CA Workload Automation AE Instance on which the action was performed.
<b>Detail</b>	The details of the actual activity performed.

You can sort by any of the above columns by clicking the column header.

You can also view the Audit Trails for a single user by selecting the user from the **View ► View By User** menu option.

## 5.13 Run Log Files

Select the **Run Log Files** tab to configure the Log File Retrieval from iXp Client.

**NOTE:** This tab is applicable for environments running Unicenter AutoSys JM r11 or older only.

### 5.13.1 Functional Overview

From the iXp Client, users can request access to the log files created by any job when it runs on its Remote Agent machine. These files include the STDOUT, STDERR, STDIN, Remote Agent log file, and Job Profile file. Since these files reside on the Remote Agent machine, the iXp Server communicates with the iXp Agent, which must be running on the Remote Agent machine, to retrieve the files.

For more information about the iXp Agent, see Chapter 3: *Architecture and Section 4.5.4 Installing the iXp Agents*.

### 5.13.2 Configuration Settings

If “Run Log Retrieval Enabled” check box is selected, (and the iXp Agent is running) users will be able to view log files (std\_in, std\_out, std\_err, profile, auto\_remote log, script) depending on security permissions. If it is NOT selected, no access to logs is available through iXp.

### 5.13.3 Resolving File Names

The file name for each of the log files is resolved by the iXp Daemon and the iXp Agent by extracting the name of the file from the job definitions and then resolving Environment variables and Global Variables. If the file name includes standard CA Workload Automation AE variables such as AUTO\_JOB\_NAME, AUTORUN, AUTOROOT, AUTOUSER, AUTOSERV, AUTOSYS, then the applicable substitution is made depending on the name of the selected job, and the values for the variables in either the iXp Agent's execution environment, or in the Instance's configuration file in the \$IXP\_HOME/agent/conf sub-directory on the Agent machine. If the file name includes any Global variables, then the appropriate value is substituted in the file name.

If the file name includes any non-standard variable or a variable whose value is dynamic, then you can specify the definition of such variables to iXp.

The iXp Daemon substitutes values for Global variables and substitution parameters defined to iXp. It then passes the resulting file name to the iXp Agent. The iXp Agent will substitute any remaining environment variables with the values found in the current environment. The file name that results from these substitutions will be then retrieved.

If the file name includes the following CA Workload Automation AE variables, then the substitution will occur as follows:

## Run Log Files

Variable Name	Substituted Value
<b>AUTO_JOB_NAME</b>	The name of the selected job.
<b>AUTORUN</b>	RUN_NUM-NTRY where RUN_NUM and NTRY are the highest run number and ntry values for the selected job.
<b>AUTOSERV</b>	The 3-letter AUTOSERV value of the selected job.
<b>Base_Time</b>	The UTC time of the last start time of the selected job.
<b>__box_joid</b>	The JOID of the box job that contains the selected job.
<b>__box_name</b>	The name of the box job that contains the selected job.
<b>__job_name</b>	The name of the selected job.
<b>__joid</b>	The JOID of the selected job.
<b>__ntry</b>	The highest NTRY for the latest run number of the selected job.
<b>__run_num</b>	The highest RUN_NUM of the selected job.
<b>__run_machine</b>	The name of the Remote Agent machine.

For example, if the selected job has the following JIL definition:

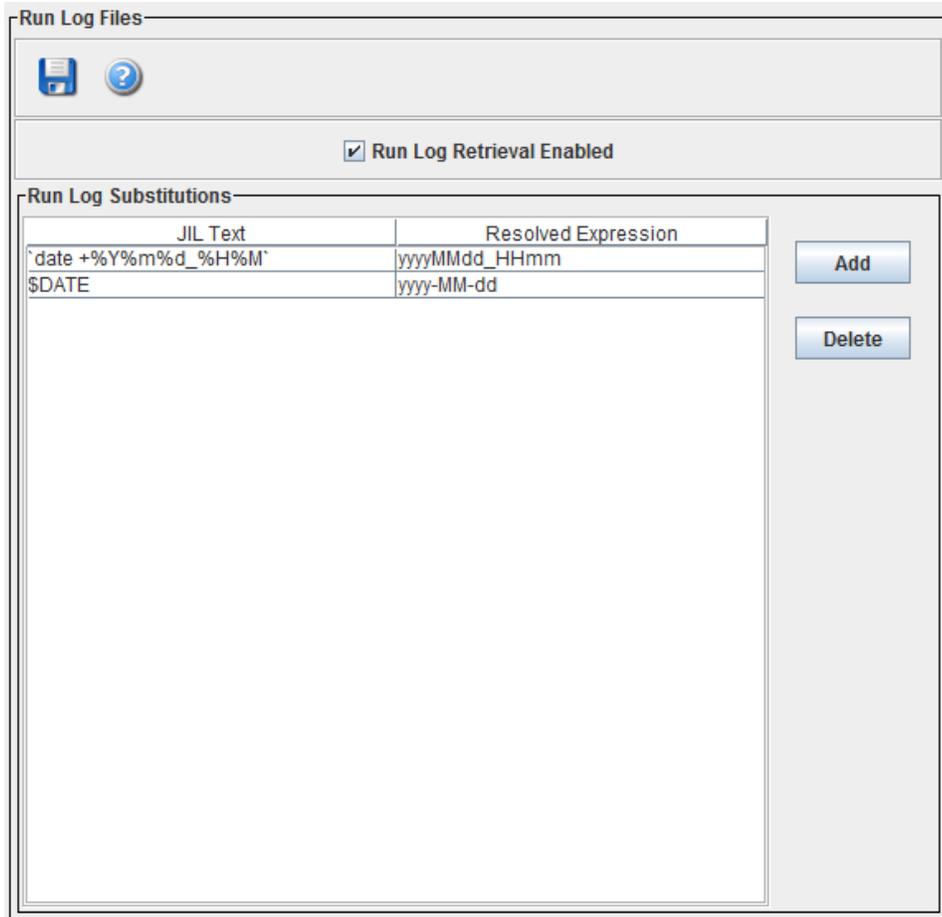
```
insert_job: FTSEDaily_FTSE_upld
job_type: c
box_name: FTSEDaily
machine: venus
command: sleep 5
std_out_file: /tmp/$AUTO_JOB_NAME.$AUTORUN.txt
std_err_file: /tmp/$AUTO_JOB_NAME.$AUTORUN.txt
```

And, if the job last ran with the run number 114 and ntry 1, then the file name for STDOUT and STDERR will be /tmp/FTSEDaily\_FTSE\_upld.114-1.txt

If there is a global variable called LOGDIR defined to CA Workload Automation AE that has the value set to “/opt/CA/logs” and is used as follows in the JIL definition of a job:

```
std_out_file: $$LOGDIR/$AUTO_JOB_NAME.$AUTORUN.txt
std_err_file: $$LOGDIR/$AUTO_JOB_NAME.$AUTORUN.txt
```

Then, the file name for STDOUT and STDERR will be resolved to /opt/CA/logs/FTSEDaily\_FTSE\_Daily\_upld.114-1.txt



If the file name uses variables that cannot be determined from the current environment on the Remote Agent, or if it uses variables that have their values set depending on the date and time of the execution of the job, then you can specify the resolution format of those variables to iXp.

During substitution, the iXp Daemon will calculate the values of these variables as specified and then substitute in the file names. If the variable value includes date or time substitutions, then the iXp Daemon will calculate the value of those variables using the latest start time of the selected job.

## Run Log Files

As shown above, two (2) variables are defined to CA Workload Automation iXp. The “\$DATE” variable needs date and time values to be substituted in a “yyyy-MM-dd” format. The iXp Daemon will use the latest start time of the selected job to determine the value of this variable.

For example, if the selected job last ran on 12<sup>th</sup> of January, 2006 and has the following JIL definition:

```
std_out_file: /tmp/$AUTO_JOB_NAME.$DATE.txt
std_err_file: /tmp/$AUTO_JOB_NAME.$DATE.txt
```

Then, the file name for `STDOUT` and `STDERR` will be resolved to  
`/tmp/FTSEDaily_FTSE_Daily_upld.2006-01-12.txt`

For more information on how to specify date and time format substitutions, refer to the following table:

Letter	Description	Format	Example
yy/yyyy	Year	Numeric	05 / 2005
M/MM	Month	Numeric	2 / 02
MMM/MMMM	Month	Text	Jan / January
d / dd	Day	Numeric	8 / 08
EEE/EEEE	Day	Text	Tue / Tuesday
H/HH	Hour	Numeric	1 / 01
m/mm	Minute	Numeric	9 / 09
s/ss	Second	Numeric	8 / 08

**Tip:** For substitution variables, remember to put single-quotes around any letters/words in the values that need to be substituted “as-is”.

# 6 OTHER CLI UTILITIES

Command line utilities may be run at a Windows command line, or UNIX shell prompt, on the iXp Server machine.

## 6.1 Server statistics

The `ixserverstats` utility in the `IXP_HOME/contr ib` directory allows users to get the iXp generated statistics for any CA Workload Automation AE instance. For information on how to run `ixserverstats.pl`, type:

```
%perl ixserverstats.pl
```

The output must be as follows:

```
perl ixserverstats.pl -i instance -k [s|c|e|l] \  
-t [6|12|24|48|72|168] -f outputFile
```

`-i` (instance) should be the AUTOSERV variable (e.g. "ACE").  
`-k` (kind) can be `s` (starts), `c` (completions), `e` (events), or `l` (latency).  
`-t` (time in hours) can be one of the following: 6, 12, 24, 48, 72, 168.  
`-f` (file) to contain report output.  
`IXP_HOME` must be set.

The `serverstats` script prints to the output file, in three columns. The first column contains sequential UNIX timestamps, the second column has the standard date/time stamp, and the third column has the number of events.

Example: `%perl ixserverstats.pl -i PA1 -ks -t6 -f outputfile` will create the output file with rows showing the number of events over the last 6 hours in the PA1 CA Workload Automation AE instance.

```
1207655707|4/8/08 5:55 AM|190  
1207655857|4/8/08 5:57 AM|435  
1207656007|4/8/08 6:00 AM|432  
1207656157|4/8/08 6:02 AM|389  
1207656307|4/8/08 6:05 AM|268  
1207656457|4/8/08 6:07 AM|296  
1207656607|4/8/08 6:10 AM|301  
1207656757|4/8/08 6:12 AM|210
```

## 6.2 Forecast

For information on how to run `ixforecast.pl` in the `IXP_HOME/contrib` directory, type

```
%perl ixforecast.pl.
```

The output must be as follows:

```
perl ixforecast.pl [-p propertyFile] [-r runReportFile] \
  [-e eventReportFile] [-f filter]
```

Must have either `-r` or `-e` (or both).

`IXP_HOME` must be set.

`IXP_SERVER_URL` must be set.

The default `propertyFile` is `$IXP_HOME/etc/forecast.props`

The default filter is "No Filter"

### 6.2.1 Forecasting Job Runs

For example, `%perl ixforecast.pl -r` prints ten columns to output file. Each row of output corresponds to one job run, similar to the Time View, as shown below:

```
JU2|job_0_0_0|EveryHour_15|963878909|7/17/00 6:08
PM|963879209000|7/17/00 6:13 PM|05m00s||SUCCESS|Run was
Scheduled based on Job Definition.
```

The columns are as follows:

- Instance
- Jobname
- Box name of parent job
- UNIX time stamp in seconds of start of run
- Normal time stamp of start of run
- UNIX time stamp in seconds of end of run of job
- Normal time stamp of end time
- Duration
- Machine
- Forecasted status of run
- Reason for the job run

If a column entry is not available, it is blank as in `||`.

## 6.2.2 Forecasting Events

For example, `%perl ixforecast.pl -e` prints eight columns to the output file. Each row of output corresponds to one event in the CA Workload Automation AE database, as shown below:

```
964114081955|7/20/00 11:28  
AM|JU2|oftenMins||STARTJOB|<eventQualifier>|Event was  
Scheduled based on Job Definition.
```

```
964114084055|7/20/00 11:28  
AM|JU2|oftenMins||CHANGE_STATUS|STARTING|<reason>
```

The columns are as follows:

- UNIX time stamp in milliseconds
- human readable time
- instance of the job,
- jobname,
- box name,
- type of event,
- event qualifier,
- reason for the event.

## 6.3 Currently Active Users

**ixusers.pl** is an iXp command, located in the `IXP_HOME/contrib` directory, which provides information about currently active users. It returns the user IDs, their current filters, the size of the users' caches, and the time each user logged onto iXp.

For example,

```
total users=4  
John.Doe, Level Zero Filter,6k,04/01/08 22:49  
Jane.Doe,AsiaJobs,3k,03/25/08 19:18  
Rob.Smith,EuropeJobs,3k,03/28/08 15:34  
Mary.Jackson, Exception Filter,1k,04/03/08 22:01
```

## 6.4 Job Information and Restart Instructions

A **Job Information and Restart Instructions** browser pop-up function is available. Select on a job name in iXp (the following example uses “EuropeHourlyBox”) then open a new browser to view the Job Information and Restart Instructions pop-up as shown below:

**Job Restart Instructions**  
**How to recover from failure of AutoSys job `Payroll_CalcPaysheet`**

Purpose	This document describes what actions to take in the event that any of the AutoSys job <code>Payroll_CalcPaysheet</code> fails.
Business Impact	These are SAP jobs that are used to calculate the Paysheets for employees.
What You Will Need	Operations Group will need the following: <ul style="list-style-type: none"> <li>· <i>Administrator</i> access to server HRTS  \\HR\shareddata\sap\logs</li> </ul>
What You Should Know	<ul style="list-style-type: none"> <li>· This job will load table <code>hr_psx_empl</code> in HRDB using ABAP Program <code>calcpsx</code>. This is the foundation for all other proceeding jobs.</li> </ul>
RULE/CAUTION	If <u>any</u> problems arise that prohibit completion of this program, escalate to <a href="#">SAP HRIS Technical Support</a> immediately.
<b>Step 1</b>	<p>Make sure program is in Failed State in the CCMS Manager.</p> <p>View SAP log and look for one the following messages and respond accordingly:</p> <p>A. If SAP Program log reads "<i>Your transaction (process id # N) was <b>deadlocked</b> with another process and has been chosen as the deadlock victim. Rerun your transaction.</i>"</p> <ol style="list-style-type: none"> <li>1. Wait 30 minutes and restart the job.</li> <li>2. Wait 30 minutes and restart the job.</li> <li>3. If it fails with the same error, escalate to <a href="#">SAP HRIS Technical Support</a>.</li> </ol> <p>B. <code>calcpsx</code> program has failed and has "<i>No Completion Time</i>"</p>

## 6.5 Audit Report

**ixauditreport.pl** is an iXp command, located in the `IXP_HOME/contrib` directory, which generates an Audit Report in HTML or CSV format. You can generate a report for either a specific user or all the “Admin” users.

For information on how to generate the Audit Report, run the command “**perl ixauditreport.pl**”

```
perl ixauditreport.pl -d auditDays -f outputFileName [-h || -c] [-u
user || -i]
-d is required and should contain the number of days
-f is required and should contain the full Path for the output
fileName.
-h OR -c is required and indicates file extension html OR csv
-u OR -i is required and -u should contain the valid user name. -i
indicates all the users with ixpAdmin Privilege
IXP_HOME and CATALINA_HOME must be set
```

# 7 MANAGING WORKLOAD MIGRATION

## 7.1 Scenario: How to Manage Workload Migration in CA Workload Automation iXp

CA Workload Automation iXp migration assistant lets users migrate jobs and other related objects, such as calendars and global variables, from a Unicenter AutoSys JM 4.5.1 instance to a CA Workload Automation AE r11.3 or higher instance.

**NOTE:** To migrate workload objects from an older Unicenter AutoSys JM release instance to a newer release instance, you can also use [CA Workload Automation AutoSys Upgrade Assistant \(AUA\)](#).

As an administrator, you are responsible for managing migration, including setting up security, enabling the migration feature, and controlling what is available during migration.

You can also perform any of the following migration management tasks:

- Configure the parameters of the CA Workload Automation AE r11.3 or higher instance to which the CA Workload Automation iXp server connects.
- Manage authorization policies for migration.
- Create exclusion rule sets that, when applied, filter the workload objects retained in the package during migration.
- Create conversion scripts that, when applied, eliminate syntax errors that can be potentially encountered during the migration of workload objects.

**NOTE:** You may also be tasked with creating migration packages and performing the actual migration of packages created by users without the migration privileges. For more information about migrating workload, see Chapter 10: *Migrating Workload Objects* in the [CA Workload Automation iXp User Guide](#).

As prerequisites, configure the parameters of the CA Workload Automation iXp server to let users create and perform migrations from the CA Workload Automation iXp server. Also define authentication policies for users.

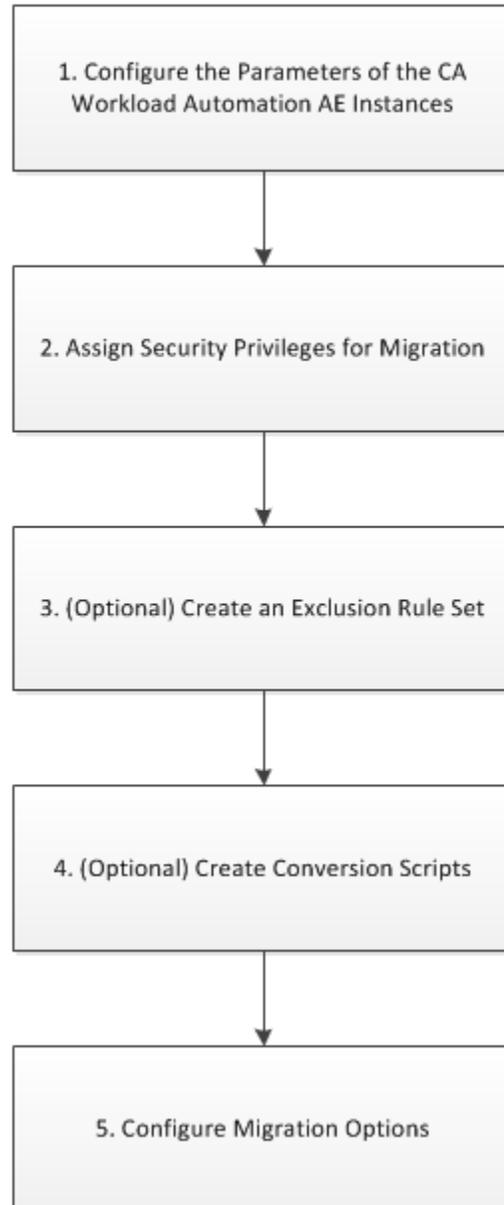
## Scenario: How to Manage Workload Migration in CA Workload Automation iXp

The following scenario walks you through the process of managing the workload migration in CA Workload Automation iXp:

### How to Manage Workload Migration in CA Workload Automation iXp



Administrator



To manage workload migration in CA Workload Automation iXp, follow these steps:

- 1) [Configure the parameters of the CA Workload Automation AE instances](#) (see page 108)
- 2) [Assign security privileges for migration](#) (see page 111)
- 3) (Optional) [Create exclusion rule set](#) (see page 113)
- 4) (Optional) [Create conversion scripts](#) (see page 115)
- 5) [Configure migration options](#) (see page 118)

## 7.1.1 Configure the Parameters of the CA Workload Automation AE Instances

You must configure the parameters, such as environment variables and database connection information, of the CA Workload Automation AE instances to which you want to migrate workload. The configuration of the CA Workload Automation AE instances lets the CA Workload Automation iXp server access the CA Workload Automation AE data.

**NOTE:** You can select a predefined CA Workload Automation AE instance to edit it or create a new CA Workload Automation AE instance.

### 7.1.1.1 Configure Two Instances with Identical Names on a UNIX/Linux iXp Server

If the name of the new CA Workload Automation AE instance is the same as that of an existing Unicenter AutoSys JM 4.5.1 instance, and you want to connect CA Workload Automation iXp to both instances, we recommend that you install the CA Workload Automation iXp server on a UNIX/Linux machine.

**Follow these steps:**

- 1) Log in to the iXp server.
- 2) Install and configure the Unicenter AutoSys JM 4.5.1 client and the CA Workload Automation AE r11.3 or higher Client.

**IMPORTANT!** Both clients can be installed with the same name, but the software files have to be located in two separate directories.

- 3) Configure the relevant database client files with the proper connection information for the Unicenter AutoSys JM 4.5.1 instance.
- 4) Open the iXp Admin tool and then click the **Instance** tab.

**NOTE:** We recommend that you configure the Unicenter AutoSys JM 4.5.1 instance first.

- 5) Click New, and define a 3-letter designation that is different from the original instance name for the new Unicenter AutoSys JM 4.5.1 instance.

For example, if the Unicenter AutoSys JM 4.5.1 instance is called “ACE”, you can name it as “A45” in CA Workload Automation iXp.

- 6) Define proper values for the other instance parameters as per the location of the software files on the iXp server, the Unicenter AutoSys JM 4.5.1 database connection properties, and other CA Workload Automation iXp related settings. For more information about setting up an instance definition, see Section 5.2 [CA Workload Automation AE Instance Configuration](#).

- 7) Click Save to save the configuration of the first instance.

- 8) Click New, and define a 3-letter designation that is the original instance name for the new CA Workload Automation AE r11.3 or higher instance, for example, “ACE”.

- 9) Define proper values for the other instance parameters, and click Save.

The configuration of the second instance is saved.

- 10) Set the environment for the Unicenter AutoSys JM 4.5.1 instance and the iXp installation.

- 11) Open the \$IXP\_HOME/etc/instance directory, and run the following command:

```
env |sort > $AUTOSERV.env
```

A file with the original name of the Unicenter AutoSys JM 4.5.1 instance is created.

- 12) Rename the file with the name of the Unicenter AutoSys JM 4.5.1 instance as configured in CA Workload Automation iXp, for example, “A45.env”.

The “env” file is created.

Two instances with identical names are successfully created on a UNIX/Linux iXp server.

## NOTES:

- Every time the Unicenter AutoSys JM 4.5.1 command runs, CA Workload Automation iXp sets its environment based on the “env” file that is created. Although the instance is identified with a different name, the environment is set with the original name and the command work properly.
- When you configure the filters and user/group security policies in CA Workload Automation iXp, use the name designated for the Unicenter AutoSys JM 4.5.1 instance and not its original name. For example, the filters and security policies must refer to the Unicenter AutoSys JM 4.5.1 instance as “A45” and not “ACE”. The name “ACE” must be used for the new CA Workload Automation AE instance.
- You must let the users know the meaning of the names designated in CA Workload Automation iXp.

### 7.1.1.2 Configure Two Instances with Identical Names on a Windows iXp Server

You can configure two instances with identical names on a Windows platform only if the Unicenter AutoSys JM 4.5.1 instance is not eTrust-enabled. If the Unicenter AutoSys JM 4.5.1 instance is eTrust-enabled, you must install CA Workload Automation iXp on a UNIX/Linux machine to connect it to two identically named instances.

#### Follow these steps:

- 1) Log in to the iXp server.
- 2) Install and configure the Unicenter AutoSys JM 4.5.1 client.
- 3) Define a 3-letter designation that is different from the original name of the instance.

For example, if the Unicenter AutoSys JM 4.5.1 instance is named “ACE”, you can name it “A45” during the client installation.

- 4) Define proper values for the other instance parameters.

**NOTE:** The parameter values must match their values in the original instance.

- 5) Configure the relevant database client files with the proper connection information for the Unicenter AutoSys JM 4.5.1 instance.

- 6) Install the CA Workload Automation AE r11.3 or higher instance with its original name and settings.
- 7) Open the iXp Admin tool and then click the **Instance** tab.

**NOTE:** We recommend that you configure the Unicenter AutoSys JM 4.5.1 instance first.

- 8) Click New, and define a 3-letter designation that is used during the installation of the Unicenter AutoSys JM 4.5.1 client, for example, "A45".
- 9) Define the values for the other instance parameters based on the location of the software files on the iXp server, the Unicenter AutoSys JM 4.5.1 database connection properties, and other iXp related settings. For more information about setting up an instance definition, see Section 5.2 [CA Workload Automation AE Instance Configuration](#).
- 10) Click Save to save the configuration of first instance.
- 11) Click New, and define a 3-letter designation that is the original instance name for the new CA Workload Automation AE r11.3 or higher instance, for example, "ACE".
- 12) Define the proper values for the other instance parameters, and click Save to save the configuration of second instance.

Two instances with identical names are successfully created on a Windows iXp server.

**NOTES:**

- When you configure the filters and user/group security policies in CA Workload Automation iXp, you must use the name designated for the Unicenter AutoSys JM 4.5.1 instance and not its original name. For example, the filters and security policies must refer to the Unicenter AutoSys JM 4.5.1 instance as "A45" and not "ACE". The name "ACE" must be used for the new CA Workload Automation AE instance.
- You must let the users know the meaning of the names designated in iXp.

## 7.1.2 Assign Security Privileges for Migration

You can assign migration-related privileges to the existing users and groups. The Migrate privilege determines whether a user or a group can open the migration assistant to create a migration package or perform migration.

You must have the following iXp privileges to create migration packages:

- Users can create migration packages with only the jobs that are included in their individual- or group-inherited Job Read and Job Detail privileges.
- Additionally, users will need the read privilege for global variables (Global Variables Read) and calendars (Calendars Read) that are related to the jobs included in the migration package.

For more information about how users validate specific privileges, see Section 5.4.3 [Validate the Privileges](#).

**Follow these steps:**

1) Log in to the iXp Admin tool.

2) Do one of the following:

- Assign the migration privilege to a group, as follows:

a) Click the **Group** tab.

The Group dialog is displayed.

b) Select a group from the Group drop-down list.

- Assign the migration privilege to a user, as follows:

a) Click the **User** tab.

The User dialog is displayed.

b) Select a user from the User drop-down list.

3) Click the **Privilege** tab to view the list of security privileges.

4) Double-click Migrate.

The migration privileges are displayed under the Migrate category.

5) Select the Create Migration Package privilege, and set the **User can create migration packages for job streams** check box as appropriate.

6) Select the Perform Migration privilege, and set the **User can perform migrations of job stream** check box as appropriate.

**NOTE:** You can migrate the packages created by other users if you have been set up as an “Admin” user and the “Perform Migration” privilege has been assigned to you.

7) Click the Save icon to save the settings for migration privileges.

**Important!** When you are assigned the “Perform Migration” privilege, you also need the following privileges to successfully migrate the objects to the target instance:

- Job Read, Job Detail, JIL Insert, JIL Update, and Job Control privileges on all the jobs included in the package.
- Machine Use privilege should include all the names shown in the “Machines” tab of the Migration Assistant.
- JIL Owner privilege should include all the names shown in the “Owners” tab of the Migration Assistant.
- Global Variable Read, Global Variable Update, and Global Variable Delete privileges should include all the names shown in the “Globals” tab of the Migration Assistant.
- Calendar Read and Calendar Update privileges should include all the names shown in the “Calendars” tab of the Migration Assistant

**NOTE:** Refer to Section 5.4 [Users and Groups](#) for further details about the security privileges. Also, refer to Section 5.4.3 [Validate the Privileges](#) for further details about how users can validate specific privileges.

### 7.1.3 Create an Exclusion Rule Set

You can create an exclusion rule set, so users can apply the rule set to their migration packages. An exclusion rule set is a set of rules that specifies the criteria to exclude jobs from the migration package before the package is migrated. The criteria can be based on the status of the jobs (for example, jobs with statuses that have not changed in over 500 days, jobs that are in ON\_ICE for more than 365 days, and so on) and other attributes. Once you assign the rule set in the migration configuration, the migration assistant automatically applies the rule set every time a package is created or opened.

## NOTES:

- Users creating migration packages can choose not to apply the rule set.
- Users can also manually override the exclusion of one or more jobs.

### Follow these steps:

- 1) Log in to the iXp user interface client.
- 2) Click the **View** tab, and select Hide Selected Jobs to create an exclusion rule set.

The Hide Selected Jobs window is displayed.

- 3) Click the Create New Rule Set icon at the top left.

The Input dialog is displayed.

- 4) Enter the name of the exclusion rule set, and click OK.

**NOTE:** Do not include spaces in the name of the exclusion rule set.

- 5) (Optional) Select the newly-created rule set from the Rule Set drop-down list to apply the job exclusion rules based on the job status, machine, and owner.
- 6) Click the **Status** tab to add exclusion rules based on job status.
- 7) Select the corresponding **Apply** check box, and specify the options as appropriate.
- 8) Click the Machine tab to exclude jobs based on machine, and specify the following as appropriate:

#### **Insert**

Lets you add the name of the machine in the exclusion list.

#### **Delete**

Lets you remove the name of the machine from the exclusion list.

- 9) Click the **Owner** tab to exclude jobs based on owner, and specify the following as appropriate:

**Insert**

Lets you add the name of the owner in the exclusion list.

**Delete**

Lets you remove the name of the owner from the exclusion list.

- 10) Click the **Miscellaneous** tab to view the remaining exclusion settings, and specify the following as appropriate:

**Exclude empty boxes**

Lets you exclude the empty box jobs.

**Exclude sleep, dir, env, and ls jobs**

Lets you exclude jobs whose command attributes begin with “sleep”, “dir”, “env”, and “ls”.

- 11) Click the Save icon to save all the specified rules.
- 12) Click OK to apply the rule set to the current view and close the dialog.

All the specified rules are applied to the rule set.

## 7.1.4 Create Conversion Scripts

CA Workload Automation AE r11.3 or higher has stringent syntax requirements, compared to Unicenter AutoSys JM 4.5.1. Therefore, some existing object definitions or attribute values may not meet the new requirements. You can create scripts or programs to parse job, calendar, and global variable files and modify their definitions and attribute values to meet the new syntax requirements. The scripts can also be used to make changes to meet internal standards.

Once applied, the migration assistant automatically runs the scripts specified for each object type on the respective files generated from the Unicenter AutoSys JM 4.5.1 data.

### 7.1.4.1 JIL Conversion Script

The JIL conversion script receives the JIL file generated by the migration assistant as standard input. The script then parses the JIL file and modifies the file to meet the syntax requirements of the target CA Workload Automation AE instance and the internal corporate standards. The migration assistant captures the standard output and uses the modified JIL file as the new JIL file.

**NOTE:** A sample PERL script (ixpParseJobs.pl) is provided in the “contrib” sub-directory under the iXp home directory.

#### 7.1.4.1.1 Run the Syntax Checker on the Generated JIL File

You can run the syntax checker on the generated JIL file to identify the syntax-related errors and verify that the JIL file meets the syntax requirements of the target instance.

#### To run the syntax checker on the generated JIL file

- 1) Extract your current Unicenter AutoSys JM 4.5.1 job definitions to a JIL file by running the command:

```
autorep -J ALL -q
```

- 2) Run the following command to verify any missing dependencies in the Unicenter AutoSys JM 4.5.1 instance. The output from this command shows the names of the jobs and any of their predecessor jobs that do not exist. Missing dependencies generate warnings during migration and prevent the jobs from running properly in the new CA Workload Automation AE environment:

```
echo exit 0 |jil -V batch >OUTPUT_FILE 2>&1
```

**OUTPUT\_FILE** = Defines the name of the JIL file where the output must be stored.

- 3) Copy the JIL file to a machine in which the new CA Workload Automation AE r11.3 or higher Client is installed.
- 4) Run the following command to perform a syntax check on the entire JIL file. The output from this command shows the potential errors and warnings that are encountered during migration if no changes are made to the job definitions or the JIL file:

```
jil -V syntax <INPUT_FILE>OUTPUT_FILE 2>&1
```

**INPUT\_FILE** = Defines the name of the JIL file that contains the Unicenter AutoSys JM 4.5.1 job definitions.

**OUTPUT\_FILE** = Defines the name of the JIL file where the output from the syntax check command must be stored.

**NOTE:** If you want to create a conversion script for calendars, you must identify the names of the calendars that generate error messages about invalid characters or symbols when you run the syntax checker on the JIL file.

The two output files let users identify possible syntax-related issues that are encountered when the jobs are migrated to the new CA Workload Automation AE r11.3 or higher instance. You can view the error messages that begin with “CAUAJM\_E”, from the output file generated by the syntax checker.

### 7.1.4.2 Global Variables Script

The global variables script receives the sendevent script generated by the migration assistant as standard input. The sendevent script is used to create the related global variables. The global variables script parses and modifies the sendevent script to meet the syntax requirements of the target instance and the internal corporate standards. The migration assistant captures the standard output and uses that as the new sendevent script.

**NOTE:** A sample PERL script (`ixpParseGlobals.pl`) is provided in the “contrib” sub-directory under the iXp home directory.

#### 7.1.4.2.1 Extract Global Variable Names and Values to a JIL File

You can extract the existing global variable names and values to a file and parse the contents to verify that the names of the global variables match the syntax requirements as listed in the [CA Workload Automation AE Reference Guide](#).

#### To extract global variable names and values to a JIL file

- 1) Extract your current Unicenter AutoSys JM 4.5.1 global variable names and values to a file by running the following command:

```
autorep -G ALL > OUTPUT_FILE 2>&1
```

**OUTPUT\_FILE** = Defines the name of the file where the output must be stored.

- 2) Identify the global variables whose names or values do not match the syntax requirements as listed in the **CA Workload Automation AE Reference Guide**.

For example, the following global variable does not pass the syntax requirements of CA Workload Automation AE r11.3 or higher:

```
VAR%1          FAIL          10/31/2012  00:00:01
```

The conversion script must find such variable names and replace "%" with a valid character.

### 7.1.4.3 Calendars Script

The migration assistant creates a file to create all related calendars in the target instance. This file is compatible with the "autocal\_asc" command. The calendars script parses and modifies this file to meet the syntax requirements of the target instance and the internal corporate standards. The migration assistant captures the standard output and uses that as the new calendar file.

**NOTE:** A sample PERL script (`ixpParseCalendars.pl`) is provided in the "contrib" sub-directory under the iXp home directory.

### 7.1.5 Configure Migration Options

You must enable migration at your site if you want users to be able to open the migration assistant from the iXp user interface.

#### **Follow these steps:**

- 1) Log in to the iXp Admin tool.
- 2) Click the **Migration** tab.

The General migration settings are displayed by default.

- 3) Select the **Migration enabled** check box to enable the migration feature in the iXp user interface.

**NOTE:** By default, this option is turned off.

- 4) Specify the following instructions on the **General** tab:

#### **JIL Command**

Defines the default command that is executed to upload the jobs from the migration package to the target CA Workload Automation AE instance.

#### **JIL Syntax Checker Command**

Defines the default command that is executed to check the syntax of the JIL file generated by the migration assistant.

#### **Exclusion Rule Set**

Specifies the exclusion rule set that you want to apply to each migration to skip certain jobs when migration packages are being created.

**NOTE:** You can use the iXp user interface to create a new exclusion rule set. For more information about the exclusion rule set, see Section 7.1.3 [Create an Exclusion Rule Set](#).

#### **JIL Conversion Script**

(Optional) Defines the conversion script that runs against the JIL file.

#### **Global Conversion Script**

(Optional) Defines the conversion script that runs against the global variables definition file.

#### **Calendar Conversion Script**

(Optional) Defines the conversion script that runs against the calendar definition file.

#### **Remove Migration Packages after X days**

Specifies the number of days after which any packages that are successfully migrated to the target instance are removed from the CA Workload Automation iXp server.

5) Click Save to save the migration options.

You configured complete settings for the migration of workload object using CA Workload Automation iXp. Users with the necessary privileges can now open the migration assistant, create migration packages, and migrate workload objects from Unicenter AutoSys JM 4.5.1 instance to a newer release of CA Workload Automation AE.

# 8 GLOSSARY

## 8.1 CA Workload Automation iXp Related Terms

**Console View:** Tabular listing of jobs and their vital data in the upper right portion of the iXp window.

**Critical Path Filter:** Focuses on a job and then follows predecessor and successor relationships (dependency relationships) from that job.

**Exception Filter:** A Job Attribute Filter that Displays only jobs that have failed or been terminated.

**HTTPD:** Hypertext Transfer Protocol Daemon.

**Instance Filter:** A Job Attribute Filter that displays only the Site and its Instances.

**Job Attribute Filters:** Filters that use each CA Workload Automation AE job attribute to further define or limit the views in iXp.

**Job Dependency Filters:** Filters that limit the iXp views according to specified job dependencies.

**Job Detail View:** View in the upper center of the iXp window that shows details of the selected job.

**Job Flow View:** View in the lower right portion of the iXp window that shows the predecessor and successor job relationships for each job.

**Level Zero Filter:** A Job Attribute Filter that displays the Site, the Instances, and Level 0 boxes.

**Recursive Critical Path Filter:** Applies an ancestor-progeny filter that passes all the parents and children of the selected job, all their parents and children, and so forth through the job stream. Then a Critical Path filter is applied to each of those jobs.

**Running Filter:** A Job Attribute Filter that displays only running jobs.

**Server Invocation:** A call from a client (web browser) to the server, which in turn makes a call to refresh or request data from a CA Workload Automation AE Instance.

**SHTTP:** Secure Hypertext Transfer Protocol

**Site:** A group of one or more CA Workload Automation AE instances.

**Site Filter:** A Job Attribute Filter that displays only the Site icon.

**Transitive Closure Filter:** Follows all Box and dependency relationships in both directions, throughout the CA Workload Automation AE Job structure. First a Recursive Critical Path filter is applied to the selected job, and then a Recursive Critical Path filter is applied to the resulting jobs, and so forth through the job stream.

**Tree View:** View on the left of the iXp window that depicts the hierarchical box structure of the jobs.

## 8.2 CA Workload Automation AE Terms

See also [CA Workload Automation AE User Guide](#)

**Alarm:** Alarms are special events that notify operations personnel of situations requiring attention.

**Box Job:** A CA Workload Automation AE job that spawns other jobs that are “contained” in the Box Job.

**Global Variable:** Set by the sendevent SET\_GLOBAL commands, Global Variables are used to create dependency relationships.

**JIL:** Job Information Language. Refer to the [CA Workload Automation AE User Guide](#).

**Job:** A job is the basic building block on which an operations cycle is built. A CA Workload Automation AE job is any single command or executable, UNIX shell script, or NT batch file. Each CA Workload Automation AE job definition contains qualifying attributes, including conditions for when and where a job should be run. Command Jobs execute commands, Box Jobs are containers, which hold other jobs, and File Watcher Jobs watch for the arrival of a specified file.

**Job Name:** The job name is used to identify the job to CA Workload Automation AE, and must be unique within CA Workload Automation AE. It can be from 1 to 30 alphanumeric characters, and is terminated with white space. Embedded blanks and tabs are illegal.

**JOID:** Job ID (see [CA Workload Automation AE Reference Guide](#)).

**sendevent:** A CA Workload Automation AE command to activate the scheduler.

## 8.3 Symbols in this Guide

Symbol or type style	Represents	Example
<b>Bold</b>	A new term.	The <b>console</b> is the upper right window in iXp.
<b>8.3.1.1.1 Alternate color</b>	Hyperlinks to other sections, or to the internet.	See <a href="http://www.ca.com">http://www.ca.com</a> for further information.
<b>8.3.1.1.1 Italic</b>	Words that are emphasized and <i>blue italic</i> for hyperlinks. <u><i>Underlined Italic</i></u> for titles of other documents.	Dismiss the window <i>after</i> finalizing your changes.  <u><i>CA Workload Automation AE User Guide</i></u>
Monospace	Syntax variables. Directories, file names, command names, computer code.	<code>COPY filename</code> <code>&amp;HIGHLVL. SRCLIB</code>
Monospace bold	Computer screen text, system responses, command line commands. What a user types.	Copy file? Y/N  ...enter <b>RUN APP. EXE</b> in the Application field.
<>	The name of a key on the Keyboard.	Press <Enter>.
▶	Choosing a command from a menu.	<b>Edit ▶ Preferences.</b>

## 8.4 Related Documents

***CA Workload Automation AE Windows Implementation Guide***

***CA Workload Automation AE UNIX Implementation Guide***

***CA Workload Automation AE Reference Guide***

***CA Workload Automation AE User Guide***

***CA Workload Automation iXp Release Notes***

***CA Workload Automation iXp User Guide***