



# Sun Update Connection – Enterprise 1.0 User's Guide



Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054  
U.S.A.

Part No: 819-6534-12  
September, 2006

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

# Contents

---

<b>Preface</b> .....	15
<b>1 Introduction to the Sun Update Connection – Enterprise Product</b> .....	19
Sun Update Connection – Enterprise Overview .....	19
Features .....	20
Applications .....	20
<b>2 Getting Started</b> .....	23
Overview of the Console User Interface .....	23
Main Window Control Area .....	23
Main Window Inventory Panel .....	31
Main Window Jobs Panel .....	33
Logging In and Starting Applications (Task Map) .....	35
▼ To Log In to the Console for the First Time .....	36
▼ To Log In to the Console .....	37
▼ To Access the uce_cli CLI .....	38
▼ To Restart the System Dependency Server .....	38
▼ To Restart the Agent .....	38
Providing Authentication Information (Task Map) .....	39
▼ To View Authentication Information .....	39
▼ To Edit Authentication Information .....	40
Managing Hosts (Task Map) .....	40
▼ To View Managed Hosts .....	41
▼ To Save the Inventory of a Host .....	42
▼ To Change the Inventory of a Host .....	42
<b>3 User Accounts</b> .....	45
Managing User Accounts (Task Map) .....	45

▼ To Create a Full-Permission User Account .....	47
▼ To Create a User Account Restricted to Simulations Only .....	49
▼ To Create a User Account with Group Restrictions .....	51
▼ To Copy a User Account .....	52
▼ To Edit a User Account .....	53
▼ To Delete a User Account .....	54
▼ To Delete Multiple User Accounts .....	54
Managing Your Own Account (Task Map) .....	55
▼ To Change Your Password On Demand .....	55
▼ To Change Your Email Address .....	56
▼ To Relogin with a Different User Name .....	57
<b>4 Hosts and Groups .....</b>	<b>59</b>
Terms .....	59
Groups .....	60
User-Defined Groups .....	60
Default Groups .....	60
Updated Groups in Jobs .....	60
Hosts and Groups in the Hosts List .....	61
Managing Groups (Task Map) .....	61
▼ To Create a Group .....	62
▼ To Create a Nested Group .....	63
▼ To Edit a Group .....	65
▼ To Delete a Group .....	66
▼ To Delete Multiple Groups .....	66
Managing Hosts (Task Map) .....	67
▼ To Enable Add Hosts Commands .....	68
▼ To Add a Host .....	69
▼ To Assign a Host to Groups .....	70
▼ To Edit a Managed Host .....	71
▼ To Delete a Managed Host from Sun Update Connection – Enterprise .....	72
▼ To Delete Multiple Managed Hosts from Sun Update Connection – Enterprise .....	72
Profile Compliance .....	73
▼ To Check Profile Compliance .....	74

<b>5 Local Inventory</b> .....	75
Terms .....	75
Local Inventories – NCOs and Files .....	76
Troubleshooting – Local Inventory Management Fails .....	77
Inventory Panel .....	77
Managing Local Categories .....	78
Default Local Categories .....	79
User-Defined Local Categories .....	79
Adding Categories .....	79
▼ To Add a Category .....	79
Editing Categories .....	81
▼ To Edit a Category .....	81
Deleting Categories .....	82
▼ To Delete a Category .....	82
Understanding Local Software .....	83
NCO Detection and Rule Generation .....	83
NCOs in Component Lists .....	84
NCO Privacy .....	84
Uploading Linux Software .....	84
Using Console on Windows .....	84
Adding Undetected Linux Software .....	85
▼ To Upload a New RPM .....	85
▼ To Upload from the Console Machine .....	86
▼ To Upload from a Managed Host .....	87
Attaching Linux Software to Detected Listings .....	88
▼ To Attach an RPM .....	88
▼ To Attach an RPM from the Console Machine .....	89
▼ To Attach an RPM from a Managed Host .....	89
Uploading Solaris Software .....	90
Using Console on Windows .....	90
Adding Undetected Solaris Software .....	90
▼ To Upload a Single PKG .....	91
Adding Multiple Solaris Packages .....	91
▼ To Upload Solaris CDs .....	92
Adding Solaris Software with a Script .....	92
▼ To Upload Solaris Software With pkg_loader .....	93
Attaching Solaris Software to Detected Listings .....	93

▼ To Upload Solaris Software .....	94
Editing NCO Listings in Components List .....	95
Editing Local Software Package Groups .....	95
▼ To Edit a Package Group .....	95
Editing Local Software Packages .....	96
▼ To Edit a Package .....	96
Moving a Local RPM to Another Package Group .....	97
▼ To Move a Local RPM to Another Package Group .....	97
Deleting NCOs .....	97
▼ To Delete an NCO .....	98
Managing Local Patches and Dependencies .....	98
Using Local Security Fixes .....	99
Fixing Local Dependencies .....	100
▼ To Fix Local Software Missing Dependencies .....	100
Troubleshooting NCOs .....	101
Managing Local Files .....	102
Actions .....	103
Writing Actions .....	104
Uploading Actions .....	104
▼ To Add an Action .....	104
▼ To Upload a Post-action or a Pre-action from the Console Machine .....	105
▼ To Upload a Post-action or a Pre-action from a Managed Host .....	105
Probes .....	107
Writing Probes .....	107
Uploading Probes .....	107
▼ To Add a Probe .....	108
▼ To Upload a Probe from the Console Machine .....	108
▼ To Upload a Probe from a Managed Host .....	109
Configuration Files .....	110
Creating File Declarations .....	111
▼ To Add a File Declaration .....	111
Uploading Local Configuration Files .....	113
▼ To Add a Local Configuration File .....	113
▼ To Upload a Configuration File from the Console Machine .....	114
▼ To Upload a Configuration File from a Managed Host .....	114
Macros .....	116
Writing Macros .....	116

Uploading Macros .....	117
▼ To Add a Macro .....	117
▼ To Upload a Macro from the Console Machine .....	118
▼ To Upload a Macro from a Managed Host .....	118
Editing Files .....	119
Editing Local File Properties .....	120
▼ To Edit Local File Properties .....	120
Editing Knowledge Base Files .....	120
▼ To Edit a Local File .....	121
Replacing Knowledge Base Files .....	121
▼ To Replace Knowledge Base Files .....	121
▼ To Attach a File from the Console Machine .....	122
▼ To Attach a File from a Managed Host .....	122
Deleting Knowledge Base Files .....	123
▼ To Delete a Local File .....	123
Opening Host Files .....	124
▼ To Access a File from a Remote Host .....	124
<b>6 Solaris Baselines .....</b>	<b>127</b>
Using Baselines to Update a Solaris Host With Patches (Task Map) .....	127
▼ To Create a Solaris Baseline White List .....	128
▼ To Create a Solaris Baseline Black List .....	130
▼ To Perform a Solaris Baseline Compliance Analysis .....	131
▼ To Install a Solaris Baseline .....	132
▼ To View a Summary of a Baseline Installation Job .....	133
<b>7 System Management Profiles .....</b>	<b>135</b>
Terms .....	136
Predefined Profiles .....	136
Policies for Predefined Profiles .....	137
Creating Policies for Predefined Profiles .....	138
▼ To Create a Policy for Predefined Profiles .....	138
Policy Recommendations for Predefined Profiles .....	139
Predefined Profiles in Jobs .....	140
Running Predefined Profiles .....	140
▼ To Create Job with a Predefined Profile .....	140

Confirming Actions .....	142
▼ To Confirm Actions .....	142
Running Restart Predefined Profiles .....	143
▼ To Create a Job with a Restart Predefined Profile .....	143
Handling Large Jobs .....	145
▼ To Handle Large Predefined Profile Jobs .....	145
<b>8 Inventories .....</b>	<b>147</b>
Terms .....	147
Understanding Inventories .....	148
Viewing Inventories .....	149
▼ To View the Inventory of the universal server .....	149
▼ To View the Installed Inventory of Selected Hosts .....	150
Saving Inventories .....	152
▼ To Save an Inventory .....	152
Inventory Jobs .....	154
Creating Inventory Jobs .....	154
▼ To Change the Inventory of a Host or Group .....	154
Comparing Inventories .....	155
▼ To Compare Inventories .....	155
Cloning Inventories .....	158
▼ To Clone Software Inventory .....	158
Patch Management in Solaris Comparisons .....	159
Restoring Managed Hosts .....	161
▼ To Roll Back an Inventory .....	161
Saving Inventory Settings as Profiles .....	163
▼ To Save Inventory Settings as a Profile .....	163
Inventory Jobs with Local Scripts and Files .....	166
Executing Scripts on Hosts .....	166
▼ To Execute a Local File on Multiple Hosts .....	166
Distributing Local Files .....	168
▼ To Install Configuration Files on Multiple Remote Hosts .....	168
<b>9 Profiles .....</b>	<b>171</b>
Terms .....	171
Working With Profiles .....	172



▼ To Create a Profile .....	173
▼ To Edit a Profile .....	175
▼ To Edit a Scheduled Profile .....	176
▼ To Copy a Profile .....	177
▼ To Copy an Active Profile .....	178
▼ To Delete a Profile .....	179
<b>10 Policies .....</b>	<b>181</b>
Terms .....	181
Working With Policies .....	182
▼ To Create a Policy .....	183
▼ To Edit a Policy .....	185
▼ To Edit a Scheduled Policy .....	186
▼ To Copy a Policy .....	187
▼ To Copy an Active Policy .....	188
▼ To Delete a Policy .....	189
<b>11 Complex Jobs .....</b>	<b>191</b>
Terms .....	191
Complex Job Processes .....	192
Post-Fix Actions .....	193
Agent Queuing .....	193
Complex Job Objects .....	194
Creating Complex Jobs .....	194
▼ To Set Up the Objects of a Job .....	195
▼ To Create the Tasks of a Job .....	195
▼ To Set Job Schedules .....	196
▼ To Set a Single Schedule .....	197
▼ To Set a Recurring Schedule .....	198
▼ To Set Job Options .....	198
Running a Job with the CLI .....	200
Saving Job Templates .....	201
▼ To Save a Job Template .....	201
Copying Jobs .....	201
▼ To Copy a Job .....	201
Creating Complex Jobs .....	202

▼ To Create a Simple Complex Job .....	202
▼ To Create a Feature-Rich Complex Job .....	203
<b>12 Common Job Operations .....</b>	<b>207</b>
Job Preparation .....	207
Settings for PKG Jobs .....	207
▼ To Set PKG Preferences .....	208
Multiple Distribution Host Lists .....	210
▼ To Align Component Settings for Multiple Distributions .....	210
Component Search .....	212
▼ To Find Components .....	212
To Use Regular Expressions .....	214
Job Management Features .....	214
▼ To Confirm Tasks .....	214
More Information About Confirmation .....	217
▼ To Monitor a Current Job .....	218
▼ To View Job Log .....	219
▼ To Rerun a Job .....	220
▼ To Filter the Jobs Panel .....	221
▼ To Delete Jobs .....	222
▼ To Refresh the Jobs List .....	223
▼ To Reschedule Recurring Jobs .....	223
▼ To Install Interactive Solaris Patches .....	224
Troubleshooting Jobs .....	225
Handling Resolve Failures .....	225
Handling Failures Due to Cost .....	226
Handling Missing Components .....	226
Handling Installation Issues .....	227
<b>13 Reports .....</b>	<b>229</b>
Terms .....	229
Report Explanations .....	230
Generating Reports .....	231
▼ To Access Reports .....	231
Filtering and Viewing Incident Reports .....	232
▼ To Filter an Incident Report .....	232

▼ To Filter a Report by Date .....	233
▼ To Filter a Report by Channel .....	234
▼ To Filter a Report by Specific Package, CVE ID, or Incident .....	234
Viewing Incident Reports .....	234
Incident Compliance Reports .....	236
▼ To Filter an Incident Compliance Report .....	237
Viewing Incident Compliance Reports .....	239
▼ To Create an Incident Compliance Job .....	240
Host Compliance Reports .....	240
▼ To Filter a Host Compliance Report .....	240
Viewing Host Compliance Reports .....	241
▼ To Create a Host Compliance Job .....	242
CVE Compliance Reports .....	242
▼ To Filter a CVE Compliance Report .....	242
Viewing CVE Compliance Reports .....	244
▼ To Create a CVE Compliance Job .....	244
Package Compliance Reports .....	244
▼ To Filter a Package Compliance Report .....	245
Viewing Package Compliance Reports .....	246
▼ To Create a Package Compliance Job .....	246
Service Pack Compliance Reports .....	247
▼ To Filter a Service Pack Compliance Report .....	247
Viewing Service Pack Compliance Reports .....	248
Running Service Pack Compliance Jobs .....	248
▼ To Create a Service Pack Compliance Job .....	248
Job History Reports .....	249
▼ To Filter a Job History Report .....	249
Viewing Job History Reports .....	250
Managing Reports .....	250
Managing Report Templates .....	250
Managing Report Results .....	251
<b>14 Command-Line Interface .....</b>	<b>253</b>
Syntax .....	253
Arguments .....	254
User Names and Passwords .....	254

Special Characters .....	254
Commands .....	255
List and Find Commands .....	255
Host and Group Commands .....	265
Local Component Commands .....	268
Policy Commands .....	271
Job Commands .....	274
Inventory Commands .....	275
Help Commands .....	279
<b>15 Sun Update Connection – Enterprise Scenarios .....</b>	<b>281</b>
Clusters .....	281
Creating an openMosix Cluster with Sun Update Connection – Enterprise .....	282
▼ To Create an openMosix Cluster with Sun Update Connection – Enterprise .....	282
▼ To Add a Node to the Cluster .....	283
Floating Servers and Loads .....	284
Creating Floating Server Environment .....	284
▼ To Create a Floating Server .....	284
Cloning Servers .....	286
Before You Begin .....	287
▼ To Clone a Single Server .....	287
▼ To Clone Multiple Servers .....	288
Sharing Directories .....	288
Mounting an NFS Directory .....	289
▼ To Mount an NFS Directory .....	289
Mounting a Windows File System from Linux .....	289
▼ To Mount a Windows Directory from a Linux Filesystem .....	289
DB2 .....	290
▼ To Deploy DB2 on Multiple Machines .....	290
WebSphere .....	293
▼ To Deploy WebSphere on Multiple Machines .....	293
<b>16 Customizing Preferences .....</b>	<b>297</b>
Accessing and Editing Preferences .....	297
Opening the Preferences Window .....	298
▼ To Open the Preferences Window .....	298

Console Preferences .....	298
▼ To Change Console Preferences .....	298
Console Preferences – Files .....	298
Console Preferences – Jobs .....	299
Console Preferences – Logs .....	299
Host Preferences .....	300
▼ To Change Host Preferences .....	300
▼ To Share Host Preferences .....	300
Host Preferences – General .....	301
Host Preferences – Logs .....	301
Host Preferences – PKGs .....	301
Dependency Manager Preferences .....	302
▼ To Change DM Preferences .....	303
DM Preferences – Clients .....	303
DM Preferences – Logs .....	303
Submit Edits .....	304
Submitting Preferences Customizations .....	304
▼ To Submit Changes .....	304
<b>Index .....</b>	<b>305</b>



# Preface

---

The *Sun Update Connection – Enterprise 1.0 User’s Guide* provides information to system administrators about how to use the Sun<sup>SM</sup> Update Connection – Enterprise software to manage software updates to systems that run the Solaris<sup>TM</sup> Operating System or Linux distributions.

## Before You Read This Book

To effectively use this book, you should be familiar with the following:

- Your client and host operating systems
- Basic Linux and Solaris commands
- Common X Windows actions

You should understand Solaris dependency issues and Linux dependency issues, and know how to use applications in X Windows. If you manage Solaris hosts, you should be familiar with basic Solaris commands. In general, you should be familiar with the hardware systems and network of your organization.

## How This Book Is Organized

This book includes 15 chapters.

[Chapter 1](#) describes the Sun Update Connection – Enterprise concepts.

[Chapter 2](#) gives a tour of the main window and basic usage of the GUI.

[Chapter 3](#) describes how to manage user accounts.

[Chapter 4](#) describes how to manage groups and how to view host properties.

[Chapter 5](#) describes how to upload and manage private software and files.

[Chapter 7](#) describes how to set up and execute complete machine tests.

[Chapter 8](#) describes how to set up and execute jobs to manage installed components.

[Chapter 9](#) describes how to create machine definition profiles.

[Chapter 10](#) describes how to create job policies to control and automate solutions.

[Chapter 11](#) describes how to set up and execute jobs to manage hosts with multiple profiles, policies, schedules, and options.

[Chapter 12](#) describes Solaris settings, jobs for multiple distributions, searching for components, confirming actions, troubleshooting jobs, and various other job-related functions.

[Chapter 13](#) describes how to set up incident queries and history queries, and how to manage the result reports.

[Chapter 14](#) describes the Sun Update Connection – Enterprise command-line interface (CLI).

[Chapter 15](#) includes advanced information for environment management.

[Chapter 16](#) describes how to view and change background parameters.

---

**Note** – Whenever possible, tasks include procedures for both the GUI and the CLI. You must be the admin user or a user with full permissions to use the CLI.

The CLI commands can be issued to the command line or can be included in shell scripts. The command syntax is shown, and when relevant, an example script is provided.

The CLI examples show how to authenticate the commands by providing the user name and the password on the command line. If you do not specify the user name and password, you will be prompted for the information. When you create a shell script with Sun Update Connection – Enterprise commands, specify the user name and password on each command line to avoid typing this authentication information each time the script runs a command. You can use variables to specify the user name and password.

---

## Related Books

In addition to this book, find more information in the following publications.

- *Sun Update Connection – Enterprise 1.0 Administration Guide*  
This book includes procedures for installation, customization, backup and restore, support of Shared Resources, and advanced configurations. This book also includes explanations of solutions for Linux and Solaris technology, servers in the solution, and security.
- Online Help  
This help is accessed in the GUI by pressing F1 and describes the user interface as well as other GUI explanations.
- Release Notes  
This book includes new features, platform support, problems and issues.



# What's New in This Sun Update Connection – Enterprise Release

Sun Update Connection – Enterprise included support for the Solaris Operating System, which makes Sun Update Connection – Enterprise the migration choice for enterprises that are looking for a more cost-effective solution.

This software include the following new features:

- Remote restart, both automated and on-demand
- Expansive incident reports for Solaris patch management
- Profile attachment to hosts and groups for compliance checks
- Complex jobs that use one or more profile deployments and system-wide scans
- Email notifications of host status and job status
- Improved and easy access to the graphical user interface (GUI)

## Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- [Documentation](http://www.sun.com/documentation/) (<http://www.sun.com/documentation/>)
- [Support](http://www.sun.com/support/) (<http://www.sun.com/support/>)
- [Training](http://www.sun.com/training/) (<http://www.sun.com/training/>)

Sun will provide a technical faq in a read only format at <http://forum.sun.com/jive/forum.jspa?forumID=334>. The URL is subject to change and may be removed at Sun's discretion.

## Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P-1 Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% you have mail.</code>
<b>AaBbCc123</b>	What you type, contrasted with onscreen computer output	<code>machine_name% su</code> <code>Password:</code>

TABLE P-1 Typographic Conventions (Continued)

Typeface	Meaning	Example
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <i>rm filename</i> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file. <b>Note:</b> Some emphasized items appear bold online.

## Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell	machine_name%
C shell for superuser	machine_name#
Bourne shell and Korn shell	\$
Bourne shell and Korn shell for superuser	#

# Introduction to the Sun Update Connection – Enterprise Product

---

Sun Update Connection – Enterprise provides lifecycle change management for Solaris environments or Linux environments.

This chapter explains how Sun Update Connection – Enterprise makes your network and system administration more efficient and more secure.

This chapter covers the following topics:

- “Sun Update Connection – Enterprise Overview” on page 19
- “Features” on page 20
- “Applications” on page 20

## Sun Update Connection – Enterprise Overview

Sun Update Connection – Enterprise is a software tool that manages the complete lifecycle deployment in an enterprise Linux environment and in an enterprise Solaris environment. The Sun Update Connection – Enterprise solution significantly reduces the time and expertise required to build and deploy an updated, secure, and reliable environment.

Sun Update Connection – Enterprise ensures the integrity of the environment, which includes the kernel, the operating system, open source components, middleware, third-party applications, and homegrown applications. Sun Update Connection – Enterprise uses a sophisticated patented technology that maps interdependencies between software components.

The Certification Lab generates real-world deployment rules, the most exact and up-to-date, for thousands of authenticated components. These rules are based on actual tests for every phase of the system lifecycle. You can use Sun Update Connection – Enterprise to manage development, test, and production machines with certified components and rules. You can also manage machines with rules you generate by using the local expansion technology to include third-part applications and homegrown applications. Every day the Certification Lab adds more components and deployment rules to the universal server.

The *system dependency server* is installed at your site. This server extracts and retains system logic from the underlying operating systems and hardware platforms of your managed hosts. Logic abstraction maximizes ongoing system investment and mitigates the risk of being locked into a single vendor, distribution, or hardware platform.

## Features

Sun Update Connection – Enterprise includes the following functions and features:

- Audit trail
- Auto-dependency handling
- Auto-discovery of installed components
- CLI and API for integration with IT processes and other management tools
- Graphical user interface (GUI) for centralized control of numerous remote machines
- Individual deployment resolutions for each managed host
- Job automation
- Machine comparisons and cloning
- Patch management
- Script repository
- Multiple host execution of pre-installation actions and post-installation actions
- Simultaneous support for multiple Solaris versions and Linux distributions and hardware
- Software inventory backups for rollback and disaster-recovery
- Software provisioning and file installation for multiple hosts
- Support for private and third-party components

## Applications

The Sun Update Connection – Enterprise solution is scalable, equally applicable to standalone servers, clusters, and mainframes. This flexibility is a result of the architecture: a collection of separate applications that interact to provide a synergistic environment for Linux and Solaris optimization.

---

The Sun Update Connection – Enterprise product includes the following applications:

- **System Dependency Server (SDS).** Acts as your local proxy to the universal server at Sun.  
The SDS includes the following:
  - **Server application.** Pulls certified updates from the universal server and pushes local packages and scripts to the local knowledge base.
  - **Dependency manager (DM).** Manages communications between applications, and performs job queuing and data storage.
  - **Knowledge base.** Caches both certified and generated deployment rules, as well as certified and local components.
  - **Local expansion technology.** Generates rules for local components.
- **Agent.** Is installed on each managed host. The agent runs the dependency resolver (DR) to find the best job solutions for the individual managed host.
- **Console.** Is the graphical user interface (GUI) from which users initiate tasks for the agents on the managed hosts. You can also use a command-line interface (CLI) or application programming interfaces (APIs) to create your own user interface.

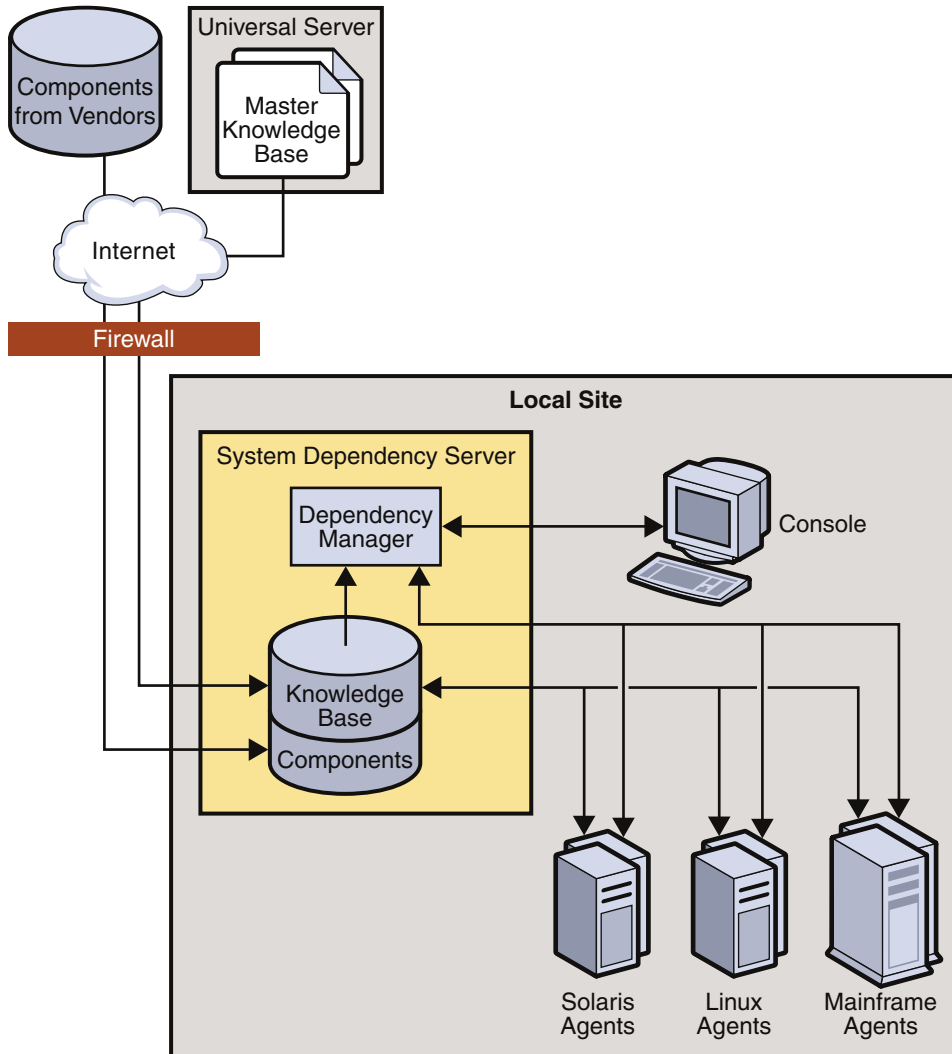


FIGURE 1-1 Sun Update Connection – Enterprise Architecture

# Getting Started

---

This chapter describes the main application window in the Console. This chapter also explains how to access the user interfaces, how to start the Sun Update Connection – Enterprise applications, and how to start managing a host.

This chapter covers the following topics:

- “Overview of the Console User Interface” on page 23
- “Logging In and Starting Applications (Task Map)” on page 35
- “Providing Authentication Information (Task Map)” on page 39
- “Managing Hosts (Task Map)” on page 40

## Overview of the Console User Interface

The following sections describe the following parts of the console user interface:

- “Main Window Control Area” on page 23
- “Main Window Inventory Panel” on page 31
- “Main Window Jobs Panel” on page 33

## Main Window Control Area

The control area of the main window is divided into the following tool bars:








- “Hosts Tool Bar” on page 24
- “Components Tool Bar” on page 24
- “Actions Tool Bar” on page 27
- “Jobs Tool Bar” on page 28
- “Tools Tool Bar” on page 30

You can customize which tool bars appear in the control area. Right-click anywhere in a tool bar or on the menu bar to select or deselect tool bar names.

## Hosts Tool Bar

Use the buttons of the Hosts tool to perform operations on managed hosts or groups.

TABLE 2-1 Hosts Buttons






Icon	Button	Description	Enabled
	Add Group	Create a new user-defined group of managed hosts.	Always
	Add Host	Predefine a managed host.	Start the console with the <code>manual_host_create</code> command.
	Edit Host/Group	Modify the properties of the selected managed host or group.	Host or group selected
	Delete Host/Group	Delete the selected host or group.	Host or group selected
	Save Inventory	Save a record of the installed components of the selected host or group with a name that you choose.	Host or group selected
	Compare Inventories	Compare current or saved inventories. You can either compare two different hosts or different inventories of a single host.	Always
	Profile Compliance Check	Check that the selected host is currently compliant with its associated profile.	Host selected

## Components Tool Bar

Use the buttons of the Components tool bar to manipulate the Components list, mark selected components for jobs, and manage local components.



TABLE 2-2 Components Buttons

Icon	Button	Description	Enabled
	Drop-down menu	List of activated distributions. Select a distribution to show its components in the Components list.	Always
	Find	Search for components.	Always
	Details	View detailed information about the selected component.	Component selected
	Show Installed	In the Components list, show only the components that are installed on the selected host or group. All hosts are shown if none are selected.	Always
	Required	Add the selected component to the Actions list and mark it as required, which means that it should be installed.	Component selected
	Not Allowed	Add the selected component to the Actions list and mark it as not allowed, which means that it should be uninstalled.	Component selected

**TABLE 2-2** Components Buttons *(Continued)*










Icon	Button	Description	Enabled
	Upgrade	Add the selected component to the Actions list and mark it as upgrade, which means that it should be upgraded to a later version, if possible.	Component selected
	Add Category	Add a category to the Local Components list	Local category selected
	Add Local	Add a local component to the Local Components list, which is a private software package or your own file.	Local category selected
	Upload Local	Upload software or file to an empty listing. Or, replace an upload with one of the same name.	Package selected
	Edit Local	Modify the properties of the selected item from the Local Components list.	Component selected
	Move Local Component	Move the selected item to another category in the Local Components list.	Component selected




TABLE 2-2 Components Buttons *(Continued)*

Icon	Button	Description	Enabled
	Open Host File	Open a file from a remote managed host for viewing and editing.	Host and local file selected
	Open Knowledge Base File	Open a file from the knowledge base server for viewing and editing.	Host and local file selected
	Delete Local	Delete the selected item from the Local Components list.	Component selected


## Actions Tool Bar

Use the buttons of the Actions tool bar to manage the Actions list of the Inventory panel. Actions buttons offer advanced features both for inventory-based jobs and for complex jobs.

TABLE 2-3 Actions Buttons

Icon	Button	Description	Enabled
	Save a Profile	Save the Actions list as a reusable profile.	Actions are in the Actions list
	Multi Distributions	Expand the Actions list to include actions on components of other active distributions.	Actions are in the Actions list
	Run on Selected Hosts	Execute actions of Actions list on selected hosts.	Host or group selected and there are actions

**TABLE 2-3** Actions Buttons *(Continued)*

Icon	Button	Description	Enabled
	Delete Selected Action	Delete selected action from Actions list.	Action selected

## Jobs Tool Bar

Use the buttons of the Jobs tool bar to manage jobs. Most buttons are for complex jobs, while some are also for inventory-based jobs.

**TABLE 2-4** Jobs Buttons

















Icon	Button	Description	Enabled
	New Job	Create a new complex job.	Always
	Copy Job	Copy the job with its profile based on the original job.	Job selected
	Stop Job	Stop the selected job.	Job in progress selected
	Reschedule Job	Modify the schedule of a complex job. You can only reschedule a job if the job had a schedule when it was first created.	Job with schedule selected
	Rerun Job	Rerun the selected job.	Completed job selected
	Delete Job	Delete the job from the Jobs list.	Job selected

TABLE 2-4 Jobs Buttons (Continued)

Icon	Button	Description	Enabled
	Job Summary Report	View the summary information of a selected job.	Job selected
	Confirm Task Actions	Confirm or deny the actions of a task.	Task with questions selected
	Copy Profile	Copy the profile of a task and save it with a new name.	Task selected
	Edit Scheduled Profile	Modify the profile of a task. You can only modify a profile if it is yours and is scheduled to be used in a future job.	Task with such a profile selected
	Copy Policy	Copy the policy of a task and save it with a new name.	Task selected
	Edit Scheduled Policy	Modify the policy of a task. You can only modify a policy if it is yours and is scheduled to be used in a future job.	Task with such a policy selected

**TABLE 2-4 Jobs Buttons** (Continued)

Icon	Button	Description	Enabled
	Show Progress	Display the progress of a host running a job.	Host in the Jobs panel is selected
	Show Log	Display the log of actions taken on a host for a job.	Host in the Jobs panel is selected
	Filter	Display only job listings that meet the specified criteria.	Always
	Refresh	Refresh the job status information. This list is refreshed periodically.	Always

## Tools Tool Bar

Use the buttons of the Tools tool bar to manage user accounts, profiles, policies, reports, and Sun Update Connection – Enterprise preferences.

**TABLE 2-5 Tools Buttons**






Icon	Button	Description	Enabled
	Users	Access the user account list and features.	Always
	Profiles	Access the profile list and features.	Always
	Policies	Access the policy list and features.	Always

TABLE 2-5 Tools Buttons (Continued)

Icon	Button	Description	Enabled
	Reports	Access the report list and features.	Always
	Preferences	View and edit the behavior parameters of the console, the agents, or the dependency manager applications.	Always

## Main Window Inventory Panel

From the Inventory panel, you can see hosts and groups, components of the knowledge base for the selected distribution, components installed on selected hosts and groups, and component-action settings.

If you do not see the Inventory panel on the main window, choose Inventory from the View menu.

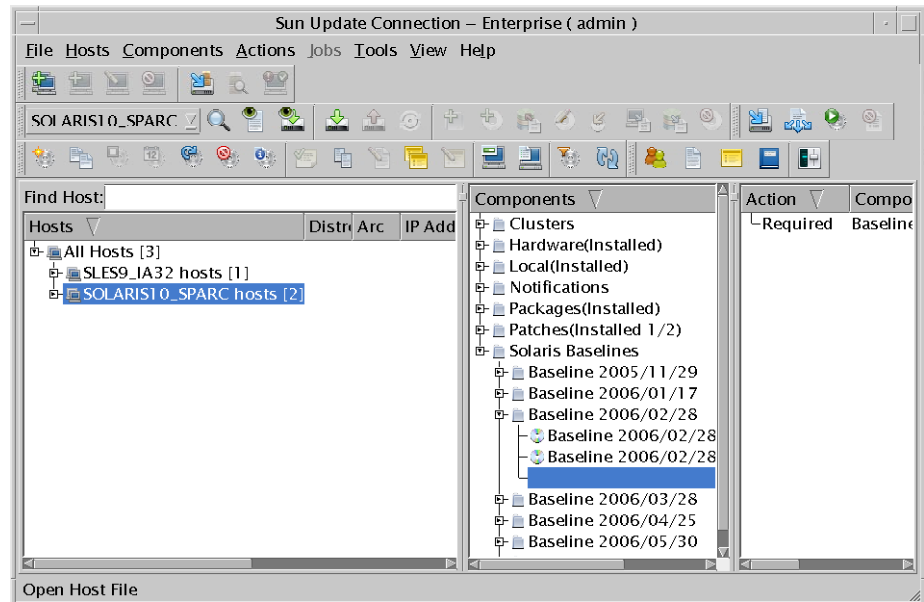


FIGURE 2-1 Main Window – Inventory Panel







## Hosts List

The Hosts frame shows information about hosts and groups. Right-click to open the Hosts menu in a pop-up window.

This frame includes the following fields:

- **Hosts** – Group names, with number of hosts in group, host names, and the status icon of the host
- **Distro** – Distribution installed on the managed host
- **Arch** – Hardware architecture of the managed host
- **IP Address** – IP address of the managed host
- **Register Time** – Date and time at which the agent was registered with the dependency manager
- **Last Inventory update** – Date and time that the host inventory was last updated to the console
- **Find Host** – Search feature for host names

TABLE 2-6 Hosts List Status Icons

Icons	Description
	Default group – All Hosts group and distribution groups
	User-defined group
	Managed host
	Disconnected host. The agent is not reaching the dependency manager
	Unrecognized group
	Unrecognized host. Errors with the machine or with the agent

## Components List

The Components frame shows hardware drivers for distributions, local components, and software packages of the selected distribution. Right-click to open the Components menu in a pop-up window.



## Actions List

The Actions frame shows actions that you set on specific components. Right-click to open the Actions menu in a pop-up window.

This frame includes the following fields:

- **Action** – One of these values: Required, Not Allowed, or Upgrade.
- **Component** – Any item from the Components list of any active distribution
- **Arch** – Hardware architecture of a component
- **Distro** – Distribution of a component

## Main Window Jobs Panel

The Jobs panel shows the status of jobs, both complex jobs and inventory-based jobs. Select a job to view its tasks and the hosts that are running the task.

If the Jobs panel does not appear on the main window, choose Jobs from the View menu.

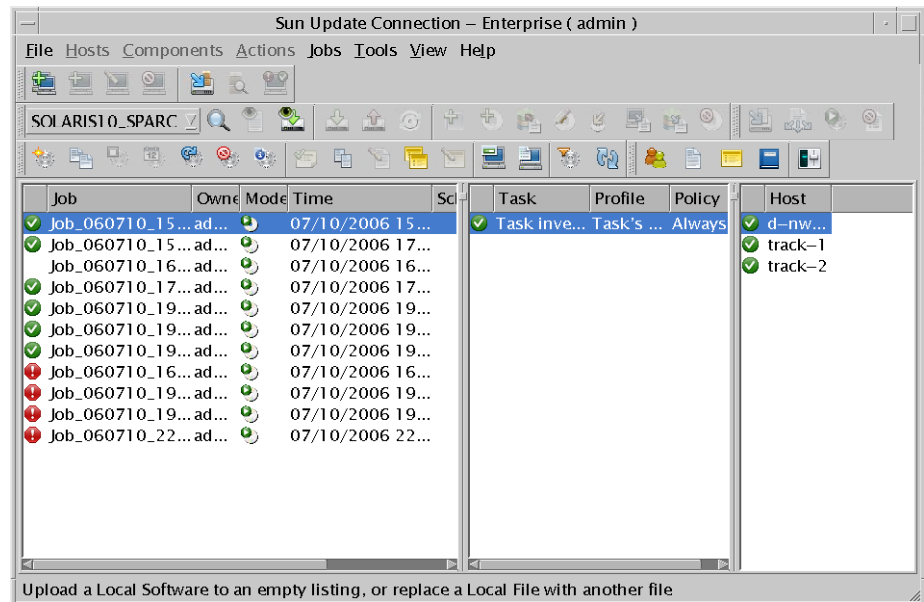


FIGURE 2-2 Main Window – Jobs Panel

## Jobs List

The Jobs panel shows completed, active, and scheduled jobs. Job information includes the following:

- Job name
- Name of the user who created the job

- Date and time at which the job was received by the dependency manager
- Mode and status icons

Right-click the Jobs list to open the Jobs menu in a pop-up window.

TABLE 2-7 Jobs List Mode Icons










Icons	Description
	Perform an action (deploy) on a managed host.
	Simulate the action, but do not actually do anything on the managed hosts.

TABLE 2-8 Jobs Panel Status Icons

Icons	Description
	At least one managed host is waiting to receive the job or is in process
	All selected managed hosts have successfully completed the job
	At least one managed host is disconnected from the dependency manager
	At least one managed host failed to complete the job
	The job is scheduled to run on a recurring basis, or it is a job template without a schedule
	The job is scheduled for single future run
	The job is paused until you confirm the actions for one of the tasks

## Tasks List

The Tasks panel shows the job tasks. Right-click to open the Tasks submenu of the Jobs menu in a pop-up window.

- Task status
- Task name
- Name of the profile associated with the task
- Name of the policy associated with the task

## Hosts in Jobs List

The Hosts in Jobs panel lists selected hosts receiving the task selected in the Tasks list. Right-click to open the Hosts submenu of the Jobs menu in a pop-up window.

- Host status in the job
- Host name

# Logging In and Starting Applications (Task Map)

The following table identifies the tasks that you might perform when you need to log in to the console and to start or restart Sun Update Connection – Enterprise applications.

Task	Description	For Instructions
Log in to the console for the first time.	You must log in as the <code>admin</code> user the first time you log in to the Sun Update Connection – Enterprise Console. As the <code>admin</code> user, you can create other user accounts to be used for managing systems.	<a href="#">“To Log In to the Console for the First Time” on page 36</a>
Log in to the console.	You do not need to be superuser to run the console, but you must be a user with full permissions or use the <code>admin</code> user’s password to log in.	<a href="#">“To Log In to the Console” on page 37</a>
Access the command-line interface (CLI).	You do not need to be superuser to use the CLI, but you must be a user with full permissions or use the <code>admin</code> user’s password to log in.	<a href="#">“To Access the <code>uce_cli</code> CLI” on page 38</a>

Task	Description	For Instructions
(Optional) Restart the system dependency server.	The system dependency server starts automatically after installation. If you need to restart it, you must restart both the server application, which includes the knowledge base, and the dependency manager application.	<a href="#">“To Restart the System Dependency Server” on page 38</a>
(Optional) Restart the agent on a managed host.	The agent starts automatically after installation. The agent software must be installed on each machine you want to manage.	<a href="#">“To Restart the Agent” on page 38</a>

## ▼ To Log In to the Console for the First Time

Sun Update Connection – Enterprise provides a default user, the `admin` user. Log in as `admin` the first time you access the console. You must be the `admin` user to create other user accounts.

You can also use the `uce_cli` command. For more information, see [Chapter 14](#).

### 1 Start the console.

```
$ uce_console
```

A dialog box appears.

Click Exit to prevent the console from starting.

Wait for your locally active distributions to be updated from the universal server.

The Login window appears.

### 2 Log in as the `admin` user.

### 3 Specify the password.

The default password is 123.

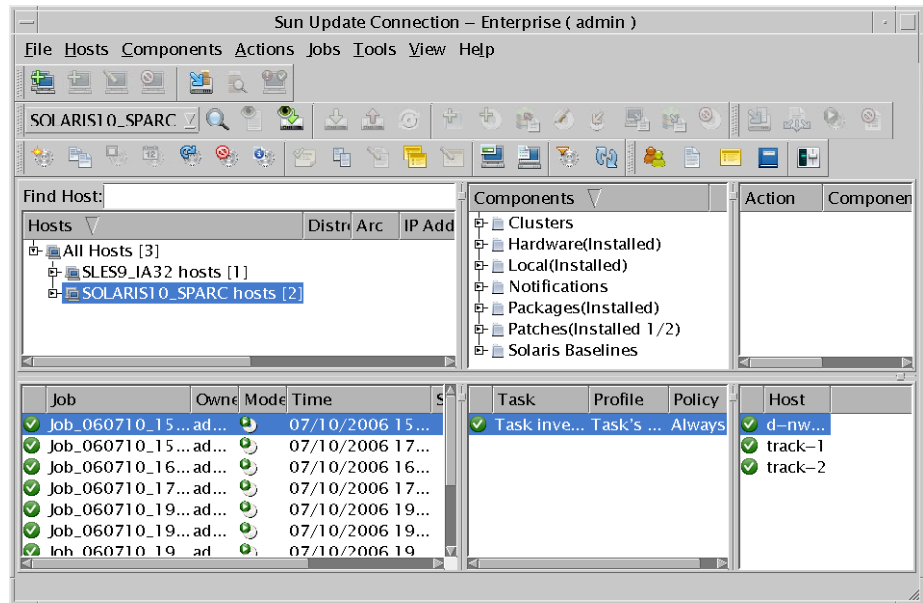
### 4 Click OK.

After the first login of any user, including the `admin` user, the Change Password window appears. Change default passwords immediately.

### 5 Type the new password, verify it, and click OK.

The password is changed.

The console opens, and shows the main window.



## ▼ To Log In to the Console

You do not need to be superuser to access the console.

You can also use the `uce_cli` command. For more information, see [Chapter 14](#).

### 1 Start the console.

```
$ uce_console
```

The Login window appears.

### 2 Type your user name in the User Name field.

### 3 Type your password in the Password field.

### 4 Click OK.

The console initializes and the main window appears.

If you do not want to log in, click Cancel.

## ▼ To Access the `uce_cli` CLI

You do not need to be superuser to use the CLI, but you must be a user with full permissions or use the `admin` user password.

### ► Type a CLI command.

```
$ uce_cli -command -param value [...] [-flag][...] -u username -p password
```

For more information about the `uce_cli` command, see [Chapter 14](#).

## ▼ To Restart the System Dependency Server

1 Log in to the system dependency server as superuser.

2 Restart the server.

```
# /etc/init.d/uce_server restart
```

3 Restart the DM:

```
# /etc/init.d/uce_engine restart
```

4 (Optional) If you have a proxy SDS, restart the proxy.

a. Log in to the system dependency server proxy system as superuser.

b. Restart the main server.

c. Restart the proxy:

```
# /etc/init.d/uce_proxy restart
```

5 Restart the DM of both the server and the proxy server.

## ▼ To Restart the Agent

1 Log in to the managed host as superuser.

2 Restart the agent.

```
# /etc/init.d/uce_agent restart
```

## Providing Authentication Information (Task Map)

The following table identifies the tasks that you might perform when you need to provide authentication information to the console application.

Task	Description	For Instructions
View authentication information.	Some of your Linux and Solaris managed hosts might need to download content from an external vendor source. These vendor sources require that you specify a user name and a password to access and download content.	<a href="#">“To View Authentication Information” on page 39</a>
Edit authentication information.	You must be the <code>admin</code> user to edit the authentication information for an external vendor source.  The user name and password you specify are not verified with the external vendor source. So, ensure that you supply the correct information or jobs that attempt to access an external vendor source will fail.	<a href="#">“To Edit Authentication Information” on page 40</a>

### ▼ To View Authentication Information

Some of your Linux and Solaris managed hosts might need to download content from an external vendor source. These vendor sources require that you specify a user name and a password to access and download content.

#### 1 Choose Authentication from the Tools menu.

The Authentication window opens.

---

**Note** – The Authentication window might open when you start the console. This window opens when the authentication information for a vendor source is incomplete.

---

#### 2 View the authentication information for each vendor source that is appropriate for your environment.

A complete vendor source entry includes the following information:

- Name of the vendor source
- User name you use to access content
- Password shown as asterisks

## ▼ To Edit Authentication Information

You must be the admin user to edit the authentication information for an external vendor source.

---

**Note** – The user name and password you specify are not verified with the external vendor source. So, ensure that you supply the correct information or jobs that attempt to access the external vendor source will fail.

---

**1 Choose Authentication from the Tools menu.**

The Authentication window opens.

**2 Select the vendor source that needs its information updated, and click Edit.**

The Authentication Editor window opens.

**3 Type the user name associated with the selected vendor source in the Username field.**

**4 Type the password in the Password field.**

**5 Type the password again in the Verify Password field.**

**6 Click OK.**

The Authentication Editor window closes.

The updated authentication information appears in the Authentication window.

## Managing Hosts (Task Map)

The following table identifies the tasks that you might perform to get started with basic host-management features.

Task	Description	For Instructions
View managed hosts.	The console shows a hierarchical view of the inventory of each of the managed hosts. You can also customize your view of the information.	<a href="#">“To View Managed Hosts” on page 41</a>



Task	Description	For Instructions
Save the inventory of a managed host.	An inventory is saved for each managed host prior to running a job. By creating an inventory, you can roll back to a previous inventory if you have problems with the current inventory.  You can also use this procedure to save an inventory manually. When you assign it a name, the name should be used to help you identify a particular configuration.	<a href="#">“To Save the Inventory of a Host” on page 42</a>
Change the inventory of a managed host.	You can create and execute a simple job on a managed host. This procedure can be used as a starting point for running simple jobs.	<a href="#">“To Change the Inventory of a Host” on page 42</a>

## ▼ To View Managed Hosts

Sun Update Connection – Enterprise provides a hierarchical view of the inventory of all managed hosts. An *inventory* is a list of components that are installed on a managed host.

This view includes a brief description of the information shown for each host. You can also perform a procedure to manipulate the views.

- 1 Choose Inventory from the View menu to open the Inventory panel.**
- 2 In the Hosts list, view the data of the managed hosts whose agents have registered with the system dependency server.**

Expand the All Hosts group and a distribution subgroup to view the list of managed hosts.

Information about each managed host appears in the following columns:

- **Distro** – Linux distribution version or Solaris release that is installed on the managed host
- **Arch** – Hardware architecture of the managed host
- **IP Address** – IP address of the managed host
- **Register Time** – Date and time at which the agent registered with the dependency manager
- **Last Inventory update** – Date and time that the host inventory was last updated to the console

- 3 Select a managed host from the list to view information about it.**

When no host is selected, you can browse the Components list to see what is available in the knowledge base for installation. This information pertains only to the distribution selected in the drop-down list in the tool bar.

- To see the Components list of a different distribution, change the selection of the tool bar drop-down list.
- To see which of the knowledge base components are installed on a specific host or hosts, select one or more hosts or groups from the Hosts list. The components installed on the selected hosts are marked as Installed on the Components list.
- To see only the installed inventory of hosts, select the hosts. Then, choose Show Installed from the Components menu.

The Components list displays only the inventory of the selected hosts.

## ▼ To Save the Inventory of a Host

Sun Update Connection – Enterprise provides a rollback feature. You can restore a managed host to a previous inventory, either full or filtered, as needed. The software automatically saves host inventories before executing a job to ensure that rollback is possible. You can also save inventories manually and give them meaningful names. Using such names makes it easier for you to choose the particular configuration to use.

### 1 From the Hosts list, right-click a host or a group and choose Save Inventory.

The Save Inventory window opens.

### 2 (Optional) Specify the name of the saved inventory.

The default file name uses this format *name\_yymmdd\_hhmmss*.

*name* is either the name of a managed host or a group. *yymmdd* represents the date as a two-digit year, two-digit month, and two-digit day. *hhmmss* represents the time as a two-digit hour, two-digit minute, and two-digit second.

### 3 Click OK.

The host inventory is saved and the Save Inventory window closes.

If you selected a group, an inventory is saved for each managed host in the group.

### 4 View a list of saved inventories in the Inventory Comparison window.

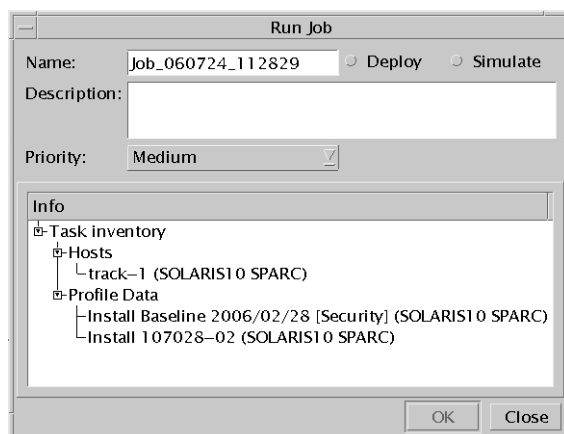
Right-click a managed host or group in the Hosts list, and then choose Compare Inventories.

### 5 Expand one of the Inventory drop-down lists to see the list of saved inventories for the selected host or group.

## ▼ To Change the Inventory of a Host

This procedure creates and executes a simple job. Besides offering a starting point, you should run a task-driven job the first time you use Sun Update Connection – Enterprise to deploy software.

- 1 From the View menu, choose Inventory.**
- 2 From the drop-down list on the tool bar, select a distribution for a particular architecture.**  
The Components list changes to display components of the selected distribution.
- 3 From the Hosts list, select a host.**
- 4 From the Components list, right-click a component, and then select Required.**  
The action-component setting appears in the Actions list.
- 5 From the tool bar, click Run Job.**  
The Run Job window opens.



- 6 Specify a job name, a description, and select Deploy.**
- 7 Click OK.**  
The job starts and the Run Job window closes.



◆ ◆ ◆    3  
CHAPTER 3

# User Accounts

---

This chapter explains how to access, create, edit, and delete user accounts.

Most of the procedures described in this chapter are applicable only to users with `admin` user permissions. Users of other permissions can change their passwords, email addresses, and notification events.

The following topics are covered:

- [“Managing User Accounts \(Task Map\)” on page 45](#)
- [“Managing Your Own Account \(Task Map\)” on page 55](#)

## Managing User Accounts (Task Map)

The `admin` user can create, edit, and delete user accounts. You cannot create another user account with the `admin` user name.

User names are case insensitive. All user names must be unique, so you cannot create a new account with the `Admin` user name.

Users can be granted full permissions to create deployment jobs over all managed hosts.

You can also restrict user permissions.

User restrictions include the following:

- **Simulations** – Restrict a user to create jobs that only simulate deployment on managed hosts. This restriction would be useful for a team manager, who could use the simulation results in time estimates and prioritization of administration tasks; or use the restriction for new team members to safely become familiar with the environment.
- **Permitted Groups** – Restrict a user to have permissions only on specified groups. If you have a large IT team, this restriction could help you manage and audit the work of team members.  
You can restrict a user to either simulations or to permitted groups, or to both. User accounts that are restricted, either for jobs or for groups, are also automatically restricted with Local components. Restricted users may select Local components for their jobs, but they do not have permission to add, edit, or delete components to the Local inventory.

The following table identifies the tasks that you might perform when you want to manage users as the admin user.

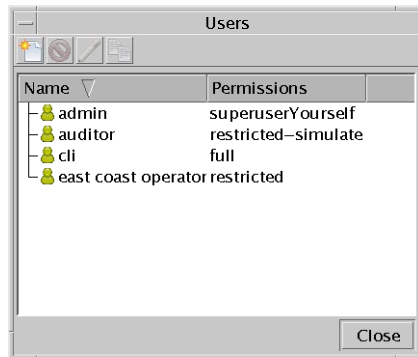
Task	Description	For Instructions
Create a user account that has full permissions.	An account with these permissions can run deployments jobs on any hosts.	<a href="#">“To Create a Full-Permission User Account” on page 47</a>
Create a user account that can only run simulation jobs.	Use this procedure to create a user that can only run simulation jobs. If this user needs to be able to run deployment jobs, the user needs full permissions.	<a href="#">“To Create a User Account Restricted to Simulations Only” on page 49</a>
Create a user account that can run jobs only on selected groups.	You create a user account that is only permitted to run jobs on particular groups. If this user needs to be able to run jobs on all groups, the user needs full permissions.	<a href="#">“To Create a User Account with Group Restrictions” on page 51</a>
Create a copy of a user account.	Copy a user account to create a new one with similar preferences.	<a href="#">“To Copy a User Account” on page 52</a>
Edit a user account.	In this procedure you edit user accounts. Use it to change the name, password, notifications, email, or list of permitted groups.	<a href="#">“To Edit a User Account” on page 53</a>
Delete a user account.	You can use this procedure to delete a user account that you no longer need.	<a href="#">“To Delete a User Account” on page 54</a>
Delete more than one user account at the same time.	You can use this procedure to delete more than one user account at a time.	<a href="#">“To Delete Multiple User Accounts” on page 54</a>

## ▼ To Create a Full-Permission User Account

In this procedure you create new user accounts with full permissions over all jobs, hosts, groups, and components (including Local component management).

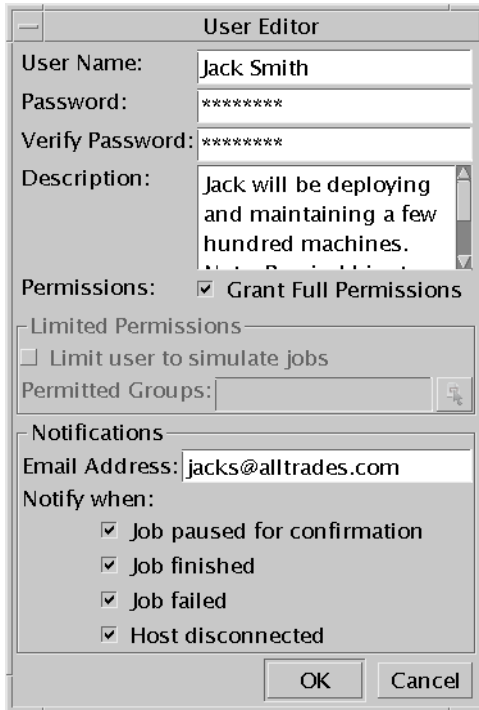
- 1 **Log in as the admin user.**
- 2 **Do one of the following:**
  - From the tool bar, click the Users button.
  - From the Tools menu, choose Users.

The Users window opens.



- 3 **Do one of the following:**
  - From the tool bar of the Users window, click the New button.
  - Right-click in a blank space in the Users window and choose New.

The User Editor window opens.



- 4 Type a name for the user account.
- 5 Type a password for the user and then verify it.
- 6 Type a description of the account.
- 7 Check the Grant Full Permissions checkbox.
- 8 In the Notifications section, type an email address to which the user of this account will receive Sun Update Connection – Enterprise notification emails.
- 9 Check the Notify when options that are relevant for this user.
- 10 Click OK.

The User Editor window closes. The new user name, with full permissions, is added to the Users window.



## ▼ To Create a User Account Restricted to Simulations Only

In this procedure you create new user accounts that are restricted for simulations only. These users cannot touch hosts. Restricted users cannot manage Local inventory, though they can select Local components for to include in simulation jobs.

**1 Log in as the admin user.**

**2 Do one of the following:**

- From the tool bar, click the Users button.
- From the Tools menu, choose Users.

The Users window opens.

**3 Do one of the following:**

- From the tool bar of the Users window, click the New button.
- Right-click in a blank space in the Users window and choose New.

The User Editor window opens.

- 4 **Type a name for the user account.**
- 5 **Type a password for the user and then verify it.**
- 6 **Type a description of the account.**
- 7 **Uncheck the Grant Full Permissions checkbox.**  
The Limited Permissions options are enabled.
- 8 **Check the Limit user to simulate jobs checkbox.**
- 9 **Click the Groups button to the right of the Permitted Groups field.**  
The Select Hosts window opens.
- 10 **Select the groups over which this user is to have permissions and click the Add button.**  
You must select permitted groups for restricted users, which are listed in the right-hand list of the Groups window. Groups that you do not add are invisible to this user
- 11 **Click OK to close the Select Hosts window and return to the User Editor.**

**12 In the Notifications section, type the email address to which to send notification emails.**

**13 Check the Notify when options that are relevant for this user.**

**14 Click OK.**

The User Editor window closes and the new user name appears in the Users window.

## ▼ **To Create a User Account with Group Restrictions**

In this procedure you create new user accounts with management permissions over permitted groups only. Restricted users cannot manage Local inventory, though they can use Local components in jobs.

**1 Log in as the admin user.**

**2 Do one of the following:**

- From the tool bar, click the Users button.
- From the Tools menu, choose Users.

The Users window opens.

**3 Do one of the following:**

- From the tool bar of the Users window, click the New button.
- Right-click in a blank space in the Users window and choose New.

The User Editor window opens.

**4 Type a name for the user account.**

**5 Type a password for the user and then verify it.**

**6 Type a description of the account.**

**7 Uncheck the Grant Full Permissions checkbox.**

The Limited Permissions options are enabled.

**8 Decide if you want this user to be able to execute deployment jobs.**

- Check Limit user to simulate jobs to restrict this user to simulations.
- Uncheck this option to allow this user to execute deployments on the permitted groups.

**9 Click the Groups button to the right of the Permitted Groups field.**

The Select Hosts window opens.

- 10 Select the groups over which this user is to have permissions and click the Add button.**  
Groups that you do not add will be invisible to this user.
- 11 Click OK.**  
The Select Hosts window closes. The permitted groups are listed in the User Editor window, in the Permitted Groups field.
- 12 In the Notifications section, type an email address to which the user of this account will receive Sun Update Connection – Enterprise notification emails.**
- 13 Check the Notify when options that are relevant for this user.**
- 14 Click OK.**  
The User Editor window closes and the new user name appears in the Users window.

## ▼ To Copy a User Account

In this procedure you create new user accounts based on existing ones. Use it to create multiple user accounts with similar permissions.

- 1 Log in as the admin user.**
- 2 Do one of the following:**
  - From the tool bar, click the Users button.
  - From the Tools menu, choose Users.

The Users window opens.
- 3 Select a user name and then do one of the following:**
  - From the tool bar of the Users window, click the Copy button.
  - Right-click the selected user name and choose Copy.

The User Editor window opens with the permissions and notification options of the selected user name.
- 4 Type a new user name and password, and verify the new password.**  
The permissions options are not available for editing.
- 5 Check the email address and notification options, and change these as needed.**
- 6 Click OK.**  
The User Editor window closes and the new user name is added to the Users window.

## ▼ To Edit a User Account

In this procedure you edit user accounts. Use it to change the name, password, notifications, email, or list of permitted groups.

You cannot edit the following options of user accounts:

- You cannot change the selection of Full Permissions.
- You cannot change the selection of Restrict user to simulate jobs.
- You cannot edit the Permitted Groups list.

### 1 Log in as the admin user.

### 2 Do one of the following:

- From the tool bar, click the Users button.
- From the Tools menu, choose Users.

The Users window opens.

### 3 Select a user name and then do one of the following:

- From the tool bar of the Users window, click the Edit button.
- Right-click the selected user name and choose Edit.

The User Editor window opens, with the properties of the selected user name displayed.

### 4 You can change any of the account details:

- User Name
- Password (and Verify Password)
- Description

### 5 You can change your email address and the Notify When options (events for which you want Sun Update Connection – Enterprise to send you an email):

- Job paused for confirmation
- Job finished
- Job failed
- Host disconnected

### 6 Click OK.

The User Editor window closes.

If you changed the user name, the new name appears in the Users window, in place of the old name.

## ▼ To Delete a User Account

In this procedure you delete user accounts.

You cannot delete user accounts in the following circumstances:

- The user is logged in.
- The user has an active job.
- The user has scheduled jobs.

**1 Log in as the admin user.**

**2 Do one of the following:**

- From the tool bar, click the Users button.
- From the Tools menu, choose Users.

The Users window opens.

**3 Select the user name that you want to delete.**

**4 Do one of the following:**

- From the tool bar of the Users window, click the Delete button.
- Right-click the selected user name and choose Delete.

**5 In the confirmation dialog box that opens, click Delete.**

The user name is removed from the list.

## ▼ To Delete Multiple User Accounts

**1 Log in as the admin user.**

**2 Do one of the following:**

- From the tool bar, click the Users button.
- From the Tools menu, choose Users.

The Users window opens.

**3 Select the user names you want to delete with the Shift or Control keys, or use the mouse to select an area in the list, and then click the Delete button in the tool bar.**

**4 In the dialog box that opens, choose one of the following.**

- **Delete All** – Delete all selected user accounts at once.
- **Delete** – Confirm the delete command for each account separately.

## Managing Your Own Account (Task Map)

When you log into the console with a user name other than `admin`, you can manage your own user account. You do not have access to other user account features.

This section includes the procedure to change your password. After logging in, you can open the User Editor of your own account and change the password.

The first time that any user logs into the console, Sun Update Connection – Enterprise automatically opens the Change Password window, enabling you to give your account a password that is private even from the `admin` user who created the account.

Type and verify a new password for this user account and then click OK. The change takes effect immediately.

---

**Note** – If the Change Password window does not open automatically on the first login, the default behavior of Sun Update Connection – Enterprise has been changed. See [“DM Preferences – Clients” on page 303](#).

---

The following table identifies the tasks that you might perform when you want to manage your own account.

Task	Description	For Instructions
Change your password.	You do not have to be the <code>admin</code> user to change the password of your own account.	<a href="#">“To Change Your Password On Demand” on page 55</a>
Change your email address.	Use this procedure to change the email address to which notification emails are sent.	<a href="#">“To Change Your Email Address” on page 56</a>
Relogin as a different user.	You can log in as another user when you are logged in.	<a href="#">“To Relogin with a Different User Name” on page 57</a>

### ▼ To Change Your Password On Demand

In this procedure you change the password of your user account at any time.

- 1 **Log in as any user.**
- 2 **Do one of the following:**
  - From the tool bar, click the Users button.
  - From the Tools menu, choose Users.

The Users window opens.

**3 Select your currently logged in user name from the list.**

**4 Do one of the following:**

- From the tool bar of the Users window, click the Edit button.
- Right-click the selected user name and choose Edit.

The User Editor window opens.

**5 Change your password and then verify it.**

**6 Click OK.**

The change takes effect immediately.

## ▼ **To Change Your Email Address**

You can receive emails from Sun Update Connection – Enterprise when specific events occur. In this procedure you change the email address to which you receive event notifications.

**1 Log in as any user.**

**2 Do one of the following:**

- From the tool bar, click the Users button.
- From the Tools menu, choose Users.

The Users window opens.

**3 Select your currently logged in user name from the list.**

**4 Do one of the following:**

- From the tool bar of the Users window, click the Edit button.
- Right-click the selected user name and choose Edit.

The User Editor window opens.

**5 Change your email address.**

You can also change the selections of events for which you will receive notification; change the checkbox selections under Notify When:

- Job paused for confirmation
- Job finished
- Job failed
- Host disconnected



**6 Click OK.**

The change takes effect immediately.

**▼ To Relogin with a Different User Name**

In this procedure you log out of the console and automatically re-login, without having to type the shell command line to start the console, with a different user name and password.

---

**Note** – This feature is not available in the console on Microsoft Windows.

---

**1 Log in as any user.****2 From the File menu, choose Login as different user.****3 In the confirmation dialog box that opens, click Relogin.**

The console goes down and then closes. The startup windows open; then the Login window opens.

**4 Type the alternate user name and password, and then click OK.**



# Hosts and Groups

---

This chapter explains how to create, edit, and delete user-defined groups. Creating groups allows you to manage hosts in a consistent and efficient manner. This chapter also explains the purpose of the default groups; and it explains how to test single hosts for compliance with your company requirements.

The procedures of this section are relevant to the `admin` user and to users with full permissions. Users with restricted permissions do not have access to group management features.

The following topics are covered:

- “Terms” on page 59
- “Groups” on page 60
- “Managing Groups (Task Map)” on page 61
- “Managing Hosts (Task Map)” on page 67
- “Profile Compliance” on page 73

## Terms

This chapter uses the following terms:

Group	Logical set of managed hosts.
Managed Host	Linux or Solaris environment that is managed by Sun Update Connection – Enterprise through an agent.
Default Group	Group created by Sun Update Connection – Enterprise according to local configurations. Includes the All Hosts group and distribution groups.
Distribution Group	Default group containing all managed hosts with the same distribution and hardware platform.
Profile	Machine type definition. Associate a group or managed host with a profile to run compliance checks, which test whether a group or

host complies with all requirements of the associated profile.

## Groups

Managed hosts are assigned to and identified with groups. If you send a job to a group, all hosts in the group receive the job simultaneously. Sun Update Connection – Enterprise has two types of groups: user-defined groups and default groups.

### User-Defined Groups

Create groups to make a large Sun Update Connection – Enterprise system more efficient. Groups enable you to simultaneously and consistently control managed hosts of similar functions and to prevent inappropriate configurations.

A *User-defined group* can hold as many hosts as you choose. Such a group can be comprised of mixed or homogeneous operating systems and can be nested within other groups.

### Default Groups

A *default group* is system-defined collection of hosts and cannot be deleted or edited.

- **All Hosts group.** Contains all managed hosts. Every machine with an installed agent automatically belongs to this group.
- **Distribution groups.** Contains all hosts of a particular distribution and hardware platform. When an Agent registers with the SDS, it is identified by its operating system (specific Linux or Solaris distribution) and assigned to the group of agents with the same distribution and hardware platform.

For example, you install the agent on five Red Hat 8.0 Intel 32-bit machines. The agents rise. In the console you see a group called `RH8_IA32 Hosts`, and the five machines are listed under it. You install the agent on another five machines with SLES 9 on Power 64-bit. When the agents rise, you see a new group, `SLES9_PPC64 Hosts`, and it contains the five machines.

### Updated Groups in Jobs

If you set a job to start at a single future date, any change in the host list of the group is reflected in the list of hosts that run the job.

For example, you select a group of five hosts to receive a job scheduled for the first of the next month. Before the job runs, you add two hosts to the group. When the first of the month comes, the job is sent to the seven hosts in the selected group.

If you set a job to a recurring schedule, you can add hosts to the group, and the next run of the job will be sent to the new host list. You cannot remove hosts from the group.

Say you reschedule the job of the previous example to be a recurring job for the first of each month. Before the next month, you want to remove four hosts from the group. When you attempt to do so, you receive an error message. You must delete the recurring job before you can edit the group.

## Hosts and Groups in the Hosts List

To view the Hosts list, make sure the Inventory panel is open in the main window. From the View menu, choose Inventory.

The Hosts list displays default and user-defined groups, and their hosts. The distribution groups appear under the All Hosts group and contain only those distributions that are represented by managed hosts whose agents have risen and automatically registered their hosts with the system dependency server. Every group has a number next to it, which indicates how many hosts are in that group.

See [“Hosts List” on page 32](#) for explanations of the Hosts List columns and status icons.

## Managing Groups (Task Map)

The following table identifies the tasks that you might perform when you want to manage groups.

Task	Description	For Instructions
Create a group.	You might want to create a group of managed hosts so that you can manage them by function rather than by operating system and platform architecture type. For example, you can create a group of web servers and manage them as a group rather than individually.	<a href="#">“To Create a Group” on page 62</a>
Create a nested group.	You might want to create a nested group of managed hosts to clearly delineate differences between different kinds of systems that perform similar functions. Or, you might use nested group to show how different hosts are related to each other.	<a href="#">“To Create a Nested Group” on page 63</a>

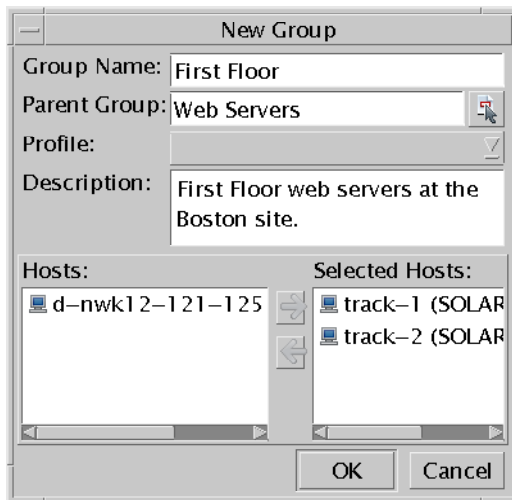
Task	Description	For Instructions
Edit a group.	When you edit a group, you can change its name or change the list of hosts that is assigned to it.	<a href="#">“To Edit a Group” on page 65</a>
Delete a group.	You can delete a group that you no longer want.	<a href="#">“To Delete a Group” on page 66</a>
Delete more than one group at a time.	You can use this procedure to delete more than one group at a time.	<a href="#">“To Delete Multiple Groups” on page 66</a>

## ▼ To Create a Group

In this procedure, you create groups of managed hosts. Your groups can be on the same level as the default groups, or you can create a hierarchy of groups. The first procedure explains how to create a group in general. Then there is a procedure for creating nested groups.

- 1 **Login as a user with full permissions or as the admin user.**
- 2 **Do one of the following:**
  - From the tool bar, click the Add Group button.
  - In the Host list, right-click and choose Add Group.
  - From the Hosts menu, choose Add Group.

The New Group window opens.



- 3 **Type a name for the group.**

**4 If you want all hosts in this group to comply to a profile, select one from the Profile drop-down list.**

This does not lock the hosts to the profile; you can still run any job on the group. It does provide information, letting you know whenever one of the hosts in the group does not comply with the profile requirements.

**5 Type an optional, free-text description of the group.****6 Select the hosts that you want to put into this group and then click the Add button.**

The Selected Hosts list shows the hosts that are to be assigned to this group.

**7 Click OK.**

The New Group window closes. The new group appears in the Hosts list of the main window.

## ▼ To Create a Nested Group

**1 Do one of the following:**

- In the Hosts list, select an existing group. The new group will be a nested group of the selected group. Right-click the selected group and choose Add Group.
- Do not select a group yet. You can choose the parent group when you create the new group. Click the Add Group button.

The New Group window opens.

**2 Check the Parent Group field:**

- If you selected a group before opening the New Group window, notice that the name of the selected group appears in the Parent Group field.
- If you want to assign the new group to a different parent group, including if you did not select a group beforehand, click the Group Select button.

The Group Selection window opens.

**3 Select one group to be the parent of the new group and then click OK.****4 Finish creating the new group as in the previous procedure.**

### Example 4–1 Creating a Group with the CLI

The Add Group command in the CLI can create a top-level group. It has an optional parameter to create a nested group. To add hosts to the created group, use the Add Host to Group command. See “Add Group (-ag) Command” on page 266 and “Add Host to Group (-ahg) Command” on page 266.

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}

function groupBasics {
    echo -n "Type a name for the new group:"
    read newGroup
    echo -n "Should the new group be nested? (y | n):"
    read pGyes
}

function createGroupWParent {
    echo "Existing groups are:"
    uce_cli -lg -u "$user" -p "$password"
    echo "Copy the name of the group to be the parent."
    echo -n "It cannot be a default group:"
    read parentGroup
    echo "Creating $newGroup under $parentGroup"
    uce_cli -ag -g "$newGroup" -pG "$parentGroup" -u "$user" -p "$password"
}

function createGroupNoParent {
    echo "Creating group without parent"
    uce_cli -ag -g "$newGroup" -u "$user" -p "$password"
}

function addHost {
    echo "Add a host to $newGroup..."
    echo "Hosts are:"
    uce_cli -lah -u "$user" -p "$password"
    echo -n "Copy the host name that you want to add:"
    read hostname
    uce_cli -ahg -h "$hostname" -g "$newGroup" -u "$user" -p "$password"
}

login
groupBasics
if [ "$pGyes" = "y" ]; then
    createGroupWParent
else
    createGroupNoParent
fi
addHost
```



## ▼ To Edit a Group

In this procedure you edit groups of managed hosts. Use this procedure to change the name of a group, or the list of managed hosts assigned to it. If the group is scheduled for future jobs, the host list of the job is updated for the added hosts.

You cannot edit a group in the following circumstances:

- You cannot edit a group that is currently in an active job.
- You cannot remove hosts from a group that is scheduled for a future job.

**1 Login as a user with full permissions or as the admin user.**

**2 In the Hosts list, select the group that you want to edit.**

**3 Do one of the following:**

- From the tool bar, click the Edit Group button.
- Right-click the selected group in the Hosts list and choose Edit.
- From the Hosts menu, choose Edit.

The Group Properties window opens.

**4 Change any of the following:**

- Name
- Parent Group
- Profile
- Description
- Add more hosts
- Remove hosts, if not in scheduled jobs

### Example 4-2 Editing a Group with the CLI

A group can be edited with the CLI command to rename a group. See [“Rename Group \(-rg\) Command” on page 267](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of existing groups is:"
uce_cli -lg -u "$user" -p "$password"
echo -n "Copy the full path and name of the group you want to rename:"
read origName
```

```
echo -n "Type a name for the new group:"
read newName

uclcli -rg -sG "$origName" -tG "$newName" -u "$user" -p "$password"
```

## ▼ To Delete a Group

In this procedure you delete user-defined groups. The hosts are not deleted, but nested groups are. Though you cannot delete default distribution groups, if you uninstall the Sun Update Connection – Enterprise Agent from the last managed host of a distribution group, that group is deleted automatically.

You cannot delete groups in the following circumstances:

- The group is a default group: All Hosts or a distribution group.
- The group is in a currently active job.
- The group is selected for a scheduled job.

**1 Login as a user with full permissions or as the `admin` user.**

**2 In the Hosts list, select the group that you want to delete.**

**3 Do one of the following:**

- From the tool bar, click the Delete Group button.
- Right-click the selected group and choose Delete.
- From the Hosts menu, choose Delete.

**4 In the dialog box that opens, click Delete again.**

The group and its child groups are deleted.

## ▼ To Delete Multiple Groups

**1 Login as a user with full permissions or as the `admin` user.**

**2 In the Hosts list, hold Shift or Control while selecting groups.**

**3 Do one of the following:**

- From the tool bar, click the Delete Group button.
- Right-click the selection and choose Delete.
- From the Hosts menu, choose Delete.

**4 In the dialog box that opens, click one of the following:**

- **Delete All** – Delete all selected groups at the same time.

- **Delete** – Delete each selected group one at a time.

### Example 4–3 Deleting a Group with the CLI

The Delete Group command in the CLI deletes a given user-defined group and its nested groups. It does not delete hosts and cannot be used to delete default groups. See [“Delete Group \(-dg\) Command” on page 267](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of existing groups is:"
uce_cli -lg -u "$user" -p "$password"
echo -n "Copy the full path and name of the group you want to delete:"
read delGroup
uce_cli -dg -g "$delGroup" -u "$user" -p "$password"
```

## Managing Hosts (Task Map)

A managed host is any computer or virtual machine:

- running a supported Linux distribution or Solaris on SPARC
- that has the Sun Update Connection – Enterprise Agent installed and
- is connected through TCP/IP to the system dependency server (SDS).

A machine becomes an Sun Update Connection – Enterprise managed host when the agent starts up and registers its machine with the SDS.

Users with full permissions and the admin user can perform the procedures in this section.

The following table identifies the tasks that you might perform when you want to manage hosts.

Task	Description	For Instructions
Enable Add Host creation in the console.	The Add Host commands on the console are disabled by default. Use the flag that permits you to add hosts manually before starting or restarting the console.	<a href="#">“To Enable Add Hosts Commands” on page 68</a>

Task	Description	For Instructions
Create a host.	Use this procedure to manually add a host to Sun Update Connection – Enterprise. Usually, Sun Update Connection – Enterprise recognizes and automatically adds hosts when their agents rise.	<a href="#">“To Add a Host” on page 69</a>
Assign a host to one or more groups.	You assign a managed host to user-defined groups. This does the same as adding hosts to groups, but from the perspective of each host and the groups it should belong to, rather than adding hosts to a single group.	<a href="#">“To Assign a Host to Groups” on page 70</a>
Edit a managed host.	View and edit the properties of a managed host.	<a href="#">“To Edit a Managed Host” on page 71</a>
Delete a managed host.	You can delete a managed host that you no longer want.	<a href="#">“To Delete a Managed Host from Sun Update Connection – Enterprise” on page 72</a>
Delete more than one managed host at a time.	You can use this procedure to delete more than one managed host at a time.	<a href="#">“To Delete Multiple Managed Hosts from Sun Update Connection – Enterprise” on page 72</a>

## ▼ To Enable Add Hosts Commands

The Add Host commands on the console are disabled by default. Turn on the flag that permits you to add hosts manually before starting or restarting the console.

- 1 Copy the following line from `/usr/local/uce/console/bin/uce.rc` to `.uce.rc` and change its value to `true`.**

```
( all ) ( invisible.gui.__general.manual_host_create, false );
```

- 2 Start the console with the parameter and value.**

- **Linux:** `uce_console -manual_host_create true`
- **Windows:** `uce_console.exe -manual_host_create true`

## ▼ To Add a Host

In this procedure, you manually add a host to Sun Update Connection – Enterprise. As Sun Update Connection – Enterprise will recognize and automatically add hosts when their agents rise, you will not use this procedure in general. Use the Add Host feature to predefine hosts.

**1 Login as a user with full permissions or as the admin user.**

**2 Do one of the following:**

- From the tool bar, click the Add Host button.
- In the Hosts list, right-click and choose Add Host.
- From the Hosts menu, choose Add Host.

The New Host window opens.

**3 In the Host Name text box, create an Sun Update Connection – Enterprise name for the host.**

**4 In the Unique String text box, type the unique string of the machine.**

**5 From the Distro list, click one of the locally activated distributions.**

**6 From the Profile list, optionally click a user-defined profile to attach to this host.**

**7 Type an optional description of the host.**

**8 In the Groups list, select a user-defined group and click the Add button.**

**9 Click OK.**

The New Host window closes.

### Example 4–4 Adding a Host with the CLI

The Add Host to Group command allows you to predefine a host, before it has an installed agent. In this command, the `-D` parameter is mandatory. See [“Add Host to Group \(-ahg\) Command” on page 266](#).

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}
```

```
function addHost {
    echo "Add a host"
    echo "Existing hosts are:"
    uce_cli -lah -u "$user" -p "$password"
    echo -n "Create a new name, one not already used:"
    read hostname
    echo "Active distros are:"
    uce_cli -ld -u "$user" -p "$password"
    echo -n "What is the distribution of the host?"
    read distro
    uce_cli -ah -h "$hostname" -D "$distro" -u "$user" -p "$password"
}
login addHost
```

## ▼ To Assign a Host to Groups

You assign a managed host to user-defined groups. This does the same as adding hosts to groups, but from the perspective of each host and the groups it should belong to, rather than adding hosts to a single group.

- 1 Login as a user with full permissions or as the admin user.**
- 2 In the Hosts list, expand a group and select a single managed host.**
- 3 Do one of the following:**
  - From the tool bar, click the Edit Host button.
  - Right-click the managed host and choose Edit.
  - From the Hosts menu, choose Edit.

The Host Properties window opens.

- 4 In the Groups list, select a group and click the Add button.**

The host is added to the selected group. You can assign a managed host to multiple user-defined groups of any hierarchy.
- 5 Click OK.**

The Host Properties window closes.

### Example 4–5 Assigning a Host to a Group with the CLI

The Add Host to Group command allows you to add a single host to a single group. See [“Add Host to Group \(-ahg\) Command” on page 266](#).

See [Example 4–1](#) for an example script.

## ▼ To Edit a Managed Host

In this procedure you will view and edit properties of a managed host.

You cannot edit managed hosts in the following circumstances:

- The host is currently in an active job.
- The host is selected for a scheduled job.
- The host belongs to a group that is currently in an active job.
- If the host belongs to a permitted group of a user with restricted permissions, which group is selected for a scheduled job, you cannot remove a group from the Selected Groups list of the host.

**1 Login as a user with full permissions or as the admin user.**

**2 In the Hosts list, expand a group and select a single managed host.**

**3 Do one of the following:**

- From the tool bar, click the Edit Host button.
- Right-click the managed host and choose Edit.
- From the Hosts menu, choose Edit.

The Host Properties window opens.

**4 (Optional) Change the Host Name.**

The name is for Sun Update Connection – Enterprise display only and the name does not affect the host. You cannot change the Unique String, IP Address, or Distribution.

**5 (Optional) Change the Profile of the host.**

This step does not lock the host to the profile. You can still run any job on the managed host. This step does provide information, letting you know whenever the host does not comply with the profile requirements.

**6 (Optional) Change the free-text description.**

**7 (Optional) Add more groups to the Selected Groups list of this host.**

**8 (Optional) Remove groups from the Selected Groups list, but only if the groups are not selected for active or scheduled jobs.**

**9 Click OK.**

The Host Properties window closes.

## ▼ To Delete a Managed Host from Sun Update Connection – Enterprise

You cannot delete managed hosts in the following circumstances:

- The agent of the host is still running.
- The host is in a currently active job.
- The host is selected for a scheduled job.

If you delete a host and then restart its agent, it is re-registered as an Sun Update Connection – Enterprise managed host, but it is not assigned to user-defined groups.

- 1 **Log into a terminal with root permissions and stop the agent application.**

```
# /etc/init.d/uce_agent stop
```

- 2 **Log in to Sun Update Connection – Enterprise as a user with full permissions or as the `admin` user.**

- 3 **In the Hosts list, select the host from within any group.**

- 4 **Do one of the following:**

- From the tool bar, click the Delete Host button.
- Right-click the selected host and choose Delete.
- From the Hosts menu, choose Delete.

- 5 **In the confirmation dialog box that opens, click Delete.**

The host name is removed from all groups and the host is deleted from Sun Update Connection – Enterprise.

## ▼ To Delete Multiple Managed Hosts from Sun Update Connection – Enterprise

You cannot delete managed hosts in the following circumstances:

- The agent of the host is still running.
- The host is in a currently active job.
- The host is selected for a scheduled job.

If you delete a host and then restart its agent, it is re-registered as an Sun Update Connection – Enterprise managed host, but it is not assigned to user-defined groups.

- 1 **Log into a terminal with root permissions and stop the agent application on each managed host.**

```
# /etc/init.d/uce_agent stop
```



- 2 **Log into Sun Update Connection – Enterprise as a user with full permissions or as the admin user.**
- 3 **In the Hosts list, hold Shift or Control while selecting hosts.**
- 4 **Do one of the following:**
  - From the tool bar, click the Delete Host button.
  - Right-click the selection and choose Delete.
  - From the Hosts menu, choose Delete.
- 5 **In the dialog box that opens, click one of the following:**
  - **Delete All** – Delete all selected hosts at once.
  - **Delete** – Delete selected hosts separately.

#### Example 4–6 Deleting a Managed Host with the CLI

The Delete Host command functions only if the agent is already stopped. The following script example stops the agent, so the user would need root permissions to run it. See [“Delete Host \(-dh\) Command” on page 265](#).

```
#!/bin/bash

echo "To run this script, you need root permissions."
echo "If you are not root, exit this script and re-login."
echo -n "Enter your Sun Update Connection – Enterprise user name:"
read user
echo -n "Enter your password:"
read password

echo -n "Enter the name of the host you want to delete:"
read host
echo "Stopping the agent..."
/etc/init.d/uce_agent stop
echo "Deleting the host..."
uce_cli -dh -h "$host" -u "$user" -p "$password"
```

## Profile Compliance

You can assign a profile to a managed host. You can also assign a profile to a group. Profile assignment does not limit the jobs you can run on hosts or groups. However, it does allow you to run a profile compliance check.

A profile compliance check tests whether a host complies with the requirements of its assigned profile, and to the profiles assigned to the groups to which the host belongs.

**EXAMPLE 4-7** Checking a Host for Profile Compliance

This example uses predefined profiles, which run tests on a complete system. Once you have created your own profiles (see [Chapter 9](#)), that specifically define the requirements of your different machines, you can assign the appropriate profile to each host or group. In the example, you would probably change the assigned profile of the host from Check System to Web Server.

You have a host that will be a web server. You assign the Check System profile to this host. The Check System profile tests for missing or conflicting dependencies.

You assign the web server host to the test group. This group tests the integrity and stability of upgraded software. Its assigned profile is the Upgrade All Components check.

When the web server host has passed all tests, you move it to the web server production group. This group has an assigned profile of Check Security, which tests for known security holes.

At any time, you can run the profile compliance test and make sure that the web server host does not have dependency issues. While it is in the test group, you can also check, simultaneously, that all its software is upgraded. While it is in the production group, you can check (again, at the same time as you check for dependencies) that the server is secured.

## ▼ To Check Profile Compliance

In this procedure, you will run a profile compliance check on a host that belongs to a group. Both the host and the group have assigned profiles. This procedure may be run by any user, of any level permissions.

- 1 In the Hosts list, expand a group and select a single managed host or group.**
- 2 Do one of the following:**
  - From the tool bar, click the Profile Compliance Check button.
  - Right-click the selected host and choose Profile Compliance.
  - From the Hosts menu, choose Profile Compliance Check.

The Profile Compliance window opens.

The Profile Compliance Check executes within seconds, resulting in compliance status for the profile attached to the host, and for the profiles attached to groups to which the host belongs.

Select a profile in the list. Its details appear in the bottom panel.

If the icon of a profile is marked with an exclamation mark in a red circle, the host is not compliant with that profile. Create a Complex Job to fix the issues (see [Chapter 11](#)).

# Local Inventory

---

This chapter explains how to set up the Sun Update Connection – Enterprise knowledge base to recognize your local components, both software packages and private files; and how the Local Expansion technology, which generates deployment rules for your local software, is initiated.

Local inventory components are available for *use* in any job, by any user. Even users with restricted permission can create jobs with local software and local files. However, you will see in this chapter’s procedures that management features of local components are available only to users with full permissions and to the admin user. This is to avoid change conflicts in the Local Inventory.

This chapter covers the following topics:

- “Terms” on page 75
- “Local Inventories – NCOs and Files” on page 76
- “Managing Local Categories” on page 78
- “Understanding Local Software” on page 83
- “Uploading Linux Software” on page 84
- “Uploading Solaris Software” on page 90
- “Editing NCO Listings in Components List” on page 95
- “Managing Local Files” on page 102

## Terms

This chapter uses the following terms:

Certified Object (CO)	Component that has passed the certification process of the Certification Lab and is available for download and management.
Component	Any logical unit that is, or can be, part of a machine. Such a unit is not only a software component itself, but also any logical construct of the component hierarchy.

Components list	Organizational structure of software in Sun Update Connection – Enterprise, using a hierarchy of logical holders for actual software packages.
Inventory	(1) List of components installed on a managed host. (2) List of components on the universal server.
Knowledge Base	A local knowledge base is a private, on-site only, collection of NCO listings and their deployment rules as generated by the Local Expansion technology.
Local Expansion technology	Application that generates knowledge for local components unknown to the universal server.
Local Files	Files that you add to the local knowledge base. Categorized as the following: <ul style="list-style-type: none"><li>▪ <b>Action</b> – Script or binary that directly causes a change in a host. Defined as a pre-action or a post-action according to its order in a job.</li><li>▪ <b>Configuration File</b> – Non-action file that can contain user-defined macros.</li><li>▪ <b>Macro</b> – Script or binary that overwrites a variable with a value, usually taken from a host to localize a file.</li><li>▪ <b>Probe</b> – Script or binary that runs a test on a host as a job prerequisite.</li></ul>
Local Software (NCO)	Component from a local environment, a third party, or Solaris that has not passed certification and is not permitted to be distributed without a specific license.  Also known as a Non Certified Object (NCO).

## Local Inventories – NCOs and Files

For each supported distribution, there is a component *inventory*.

Inventories include default categories:

- **Hardware** – Contains local hardware information.
- **Software** – Contains COs, indicated by the certified component icon:
- **Running Kernel** – Lists the active KernelBase. Search under Software for other installable kernel components
- **Notifications** – Lists actions to be done, such as restart, on specific hosts

- **Local** – This chapter deals with the Local category and the components it may contain, indicated by the Local component icon:

Non Certified Object (NCO)	Software packages that are not in the knowledge base of the universal server (such as private, proprietary, and third-party software packages), but are installed on a local machine or for which you have a source, such as a third-party CD.
Local Files	Private scripts, binaries, executables, and configuration files available for environment management.

Your local components, NCOs and Local Files, are added to the knowledge base on your site. They are never pushed outside of your enterprise.

Only users with full permissions or the admin user can set up local inventories. All users can use them in jobs.

## Troubleshooting – Local Inventory Management Fails

<b>Description:</b>	An Sun Update Connection – Enterprise command fails with the following error:
	Cannot process comand. Reason: another command running.
<b>Cause:</b>	Sun Update Connection – Enterprise is busy handling back-end processes and your new command timed out. This error is most commonly seen while you manage Local Inventories.
<b>Workaround:</b>	Execute the command again, or wait a few minutes before running the command again.

## Inventory Panel

The main window is comprised of the Inventory panel and the Jobs panel. To manage Local Inventory, the Inventory panel must be visible.

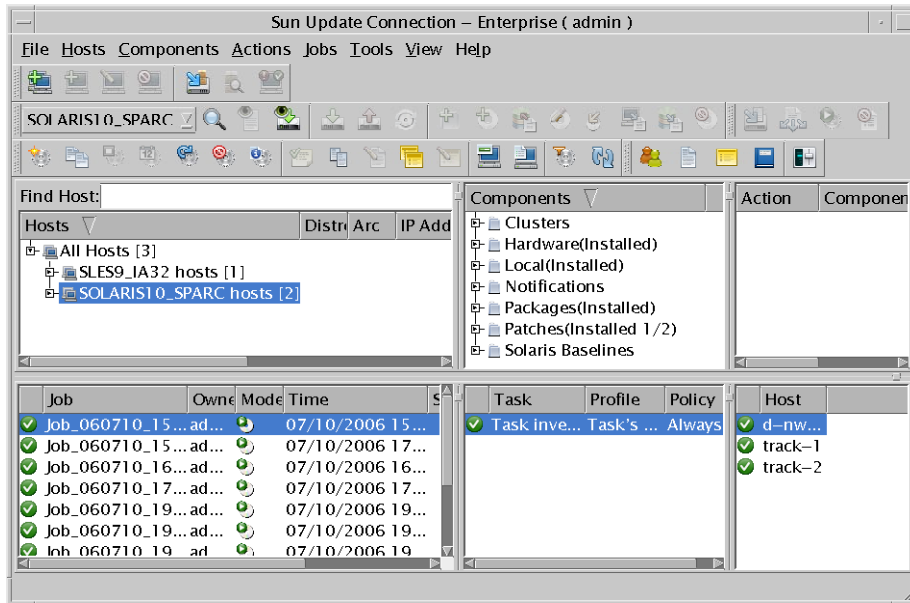


FIGURE 5-1 Main Window

If the Inventory view is not open when you log into Sun Update Connection – Enterprise, from the View menu, choose Inventory. In the Components list of the Inventory view, find the Local category.

If the Local category is empty, or not visible, check whether Show Installed is selected. If it is, only components installed on selected hosts are shown in the Components list; if none are selected, the Components list shows only COs. Deselect this option to see all Local categories.

## Managing Local Categories

In this section, you will learn how to add, edit, and delete categories in the Components list under Local.

Each category can hold package groups and packages, which may be either software or files, depending on the top-level default category under which you create your own categories.

These features are available only to users with full permissions and to the admin user.

## Default Local Categories

Expand the Local category to see the default categories. You cannot edit or delete these categories.

- **Local RPMs or Local PKGs** – Your local software components (NCOs)
- **Configuration files** – Local versions of configuration files
- **Macros** – Scripts that pull data from hosts to replace macro signs in local Configuration files
- **Pre-actions** – Executables that do something to a host before the tasks of a job begin
- **Post-actions** – Executables that do something to a host after the tasks of a job finish
- **Probes** – Executables that test a pre-requisite condition of a host, to see whether a job should begin

## User-Defined Local Categories

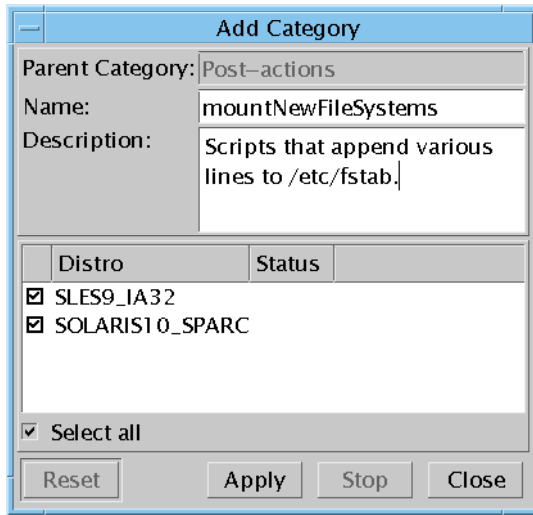
Under a default category, you create, edit, or delete your own categories. Choose the default category that best describes the software or files that you will be adding to the knowledge base.

## Adding Categories

You customize the Local components list by adding your own categories to the default ones under Local.

### ▼ To Add a Category

- 1 In the Components list, under Local, select a default category.
- 2 Do one of the following:
  - From the tool bar, click the Add Category button.
  - From the Components menu, choose Local -> Add Category.
  - In the Components list, right-click the selected category and choose Local -> Add Category.  
The Add Category window opens.



- 3 Type a name and description for the new category.
- 4 Check distributions to which you want this category to be assigned.
- 5 Click Apply.

The status column indicates when the category is uploaded to the knowledge base.

- 6 Click Close.

The Add Category window closes. You might have to wait until the Components list is updated with the new category; time depends on your local environment configuration.

### Example 5-1 Adding a Category with the CLI

The create a new category CLI command puts the category into all distributions (default) if you do not use the `-D` parameter. To add the category to one specific distribution, use the `-D` parameter and the name of the distribution. (The `-ld` command outputs the names of distributions.) See [“Add Local Category \(-alc\) Command” on page 268](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo -n "Type a name for the new category:"
read newCatName
```



```
echo -n "Enter a description for the new category:"
read newCatDesc
echo "Under which category should this one be added?"
echo "Valid answers: Local RPMs, Local PKGs, Probes, Pre-actions,"
echo "Post-actions, Macros, Configuration files,"
echo "or an existing user category under one of these: /existing_subcategory"
read parent

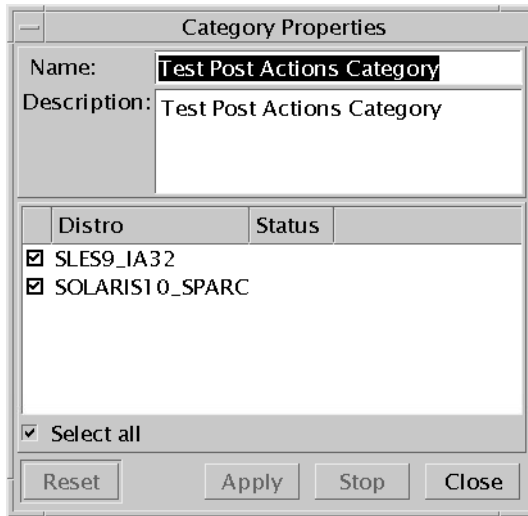
uce_cli -alc -T "$newCatName" -ds "$newCatDesc" -pT "$parent" -u "$user" -p "$password"
```

## Editing Categories

In this procedure, you edit Local categories. You can change the name, description, and list of distribution assignments of any category that you or another user created. You cannot change the default categories.

### ▼ To Edit a Category

- 1 From the Distro drop-down list, select the distribution-architecture holding the component that you want to change.
- 2 In the Components list, select the category that you want to change.
- 3 Do one of the following:
  - From the tool bar, click the Edit Local Component button.
  - Right-click the selected category and choose Edit.
  - From the Components menu, choose Edit.  
The Category Properties window opens.



**4 Edit as needed: Name, Description, selected Distributions.**

**5 Click Apply.**

The status column indicates when the category has been changed for each distribution.

**6 Click Close.**

The Category Properties window closes. You might have to wait until the console is updated with the changes. The time depends on your local environment configuration.

## Deleting Categories

In this procedure, you delete a user-defined Local categories. Everything inside of the category will be deleted as well. However, if there are many components in the category, the delete function might fail with the another process running error. To ensure this does not occur, delete the contained components before deleting the category.

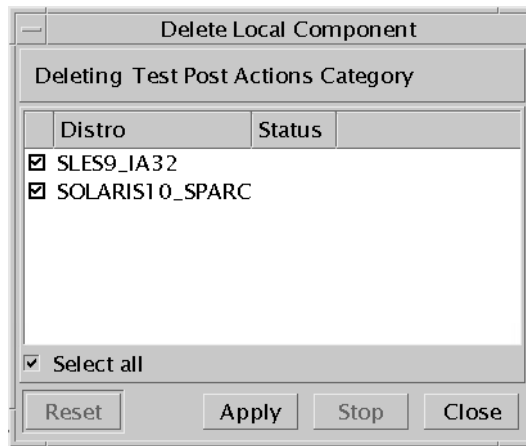
### ▼ To Delete a Category

**1 In the Components list, select the category that you want to delete.**

**2 Do one of the following:**

- From the tool bar, click the Delete Local Component button.
- Right-click the selected category and choose Delete.

- From the Components menu, choose Delete.  
The Delete Local Component window opens.



**3 Check the distributions from which you want to delete the category.**

**4 Click Apply.**

The status column indicates when the category has been deleted from each distribution.

**5 Click Close.**

The Delete Local Component window closes. You might have to wait until the console is updated with the changes. The time depends on your local environment configuration.

## Understanding Local Software

In this section, you will learn how to add, edit, and delete local software components that are Non-Certified by the Lab (NCOs). These procedures are available only to users with full permissions or the admin user.

### NCO Detection and Rule Generation

If an NCO is installed on a managed host, Sun Update Connection – Enterprise automatically detects it and adds it to your local knowledge base. If the NCO is not yet installed (it is on a CD or other source), you can add it to the knowledge base on demand.

When an NCO is added to the local knowledge base, the Local Expansion technology generates rules for NCO deployment. (Be aware that rules generated on-site are not as rigorous as those created by Sun.)

## NCOs in Component Lists

The NCO is placed in the Components list. If it is a new package, it is placed under Local RPMs or Local PKGs. If it is an unknown version of a known package (for example, if your organization creates a proprietary patch for an application), the NCO is placed under Software. You can use the Find feature (see [“To Find Components” on page 212](#)) to find it under a Software listing.

## NCO Privacy

Your local knowledge base data (the package, its listing, its rules) are never pushed back to the universal server, nor are they overwritten by downloaded updates. The local knowledge base is secured for your private site.

# Uploading Linux Software

Though Sun Update Connection – Enterprise should automatically detect NCOs that are already installed on a host in the solution, sometimes you want to manually add your NCOs to your local knowledge base. Procedures for adding RPMs that belong to Linux distributions are slightly different than those for adding Solaris PKGs.

The procedures in this section include the following:

- [“Using Console on Windows” on page 84](#)
- [“Adding Undetected Linux Software” on page 85](#)
- [“Attaching Linux Software to Detected Listings” on page 88](#)

## Using Console on Windows

You cannot upload RPMs with a console on Microsoft Windows. Use the Sun Update Connection – Enterprise CLI on a Linux machine to upload RPMs. See [Example 5–2](#).

## Adding Undetected Linux Software

In this procedure, you add a local RPM to the knowledge base, when it has not been detected automatically. For example, you would use this procedure for uploading a third-party bundle of components from a CD.

You cannot upload RPMs with a console on Microsoft Windows. Use the Sun Update Connection – Enterprise CLI on a Linux machine to upload RPMs. See [Example 5–2](#).

### ▼ To Upload a New RPM

**1 Log in with full permissions or as the `admin` user.**

**2 From the drop-down list in the tool bar, select a Linux distribution-architecture.**

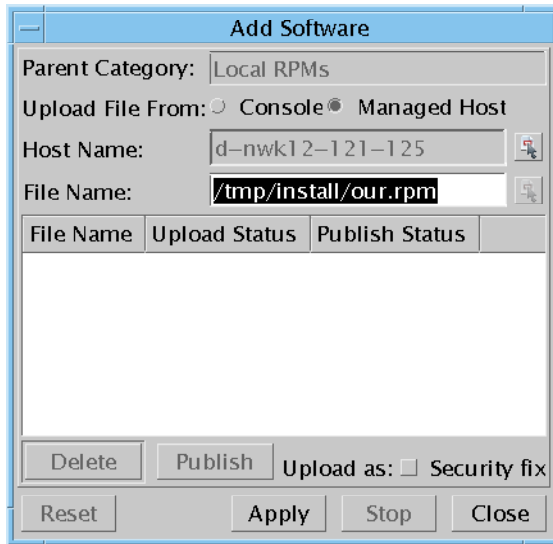
The Components list shows the components relevant to your selection. The NCOs that you add with this procedure will be added to the inventory of the displayed distribution.

**3 Select `Local/Local RPMs/[category]`.**

**4 Do one of the following:**

- From the tool bar, click the Add Component button.
- Right-click the selected category and choose Local -> Add.
- From the Components menu, choose Local -> Add.

The Add Software window opens.



**5 Select a source machine:**

- If the console has access to the RPM, select Console.
- If a remote managed host has access to the RPM, select Managed Host.

---

**Note** – Remote upload is limited to 5 Mbytes. Console upload is unlimited. You should upload from the console whenever possible.

---

**▼ To Upload from the Console Machine**

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Upload from a Managed Host” on page 87](#).

**1 Click the Select File button of the File Name field.**

The Choose RPM window opens.

**2 Browse to and select packages you want to add. Use the Control or Shift keys to make a multiple selection from one directory.**

**3 Click Open.**

The Choose RPM window closes, and the path names appear in the File Name list of the Add Software window. Add as many packages as you want.

**4 Click Apply.**

The Status column indicates when the upload is done. You might have to wait until the console is updated with the changes. The time depends on your local environment configuration.

**▼ To Upload from a Managed Host**

If you selected Managed Host, follow this procedure. Note that this procedure upload only one RPM at a time.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the software, and click OK.**

The Host Selection window closes and the host name appears in the Host Name field of the Add Software window.

**3 In the File Name field, type the full path name of the package.****4 Click Apply.**

The Status column indicates when the upload is done. You might have to wait until the console is updated with the changes; time depends on your local environment configuration.

**Example 5-2 To Upload NCOs with the CLI**

The Add Software Package command allows you to give a path name of a package for upload. The package should be on the local machine or on a mount point. The Distribution parameter is required in this command (the `-ld` command outputs a list), and you add the package to a single distribution at a time. See [“Add Software Package \(-asp\) Command” on page 268](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of active distributions is:"
uce_cli -ld -u $user -p $password
echo -n "Type the exact name of the distribution for this software:"
read distro
echo -n "Type the source path name of the file:"
read pathname
echo -n "Is this software a secured version of a previous one? (y | n)"
read secure
```

```
if [ "$secure" = "y" ]; then
    uce_cli -asp -f "$pathname" -secure -D $distro -u "$user" -p "$password"
else
    uce_cli -asp -f "$pathname" -D $distro -u "$user" -p "$password"
fi
```

## Attaching Linux Software to Detected Listings

In this procedure, you learn how to attach a local RPM to an NCO name in the Components list. The name must already be in the Components list.

TABLE 5-1 Reasons for Performing the Attach Procedure

Environment	Indicator
Sometimes a package may be uploaded and automatically attached to the NCO listing, but you want to <i>replace</i> the package with one of your own choosing.	A local component listing that has a package already associated with it, is indicated by the full icon.
Sometimes the system dependency server may be <i>unable to upload</i> the package itself. Use this procedure to manually attach the correct software with the listing.	A software component listing without an attached software, is indicated by the empty icon.
Sometimes, after a package was uploaded, the Local Expansion technology may discover that this software has missing local dependencies; its rules require components that are not yet in the knowledge base. Until you fix this issue, the component can not be managed by Sun Update Connection – Enterprise.	An exclamation point in a red circle, on either a full (has software attached) or an empty (does not have software attached) listing, indicates that there are missing local dependencies.

### Console on Windows

You cannot upload or attach RPMs with a console on Microsoft Windows. Use the Sun Update Connection – Enterprise CLI on a Linux machine to upload RPMs. See [Example 5-2](#).

#### ▼ To Attach an RPM

- 1 **Log in with full permissions or as the admin user.**
- 2 **From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows the components relevant to your selection.
- 3 **Select Local/Local RPMs/[category]/package group/<package>.**
- 4 **Do one of the following:**
  - From the tool bar, click the Upload knowledge base File button.



- Right-click the selected component and choose Local -> Upload.
- From the Components menu, choose Local -> Upload.  
The Attach Target File window opens.

**5 Check each distribution to which this NCO is applicable.**

**6 Select a source machine:**

- If the console has access to the NCO, select Console.
- If a remote managed host has access to the NCO, select Managed Host.

---

**Note** – Remote upload is limited to 5Mb; console upload is unlimited. It is recommended that you upload from the console whenever possible.

---

## ▼ **To Attach an RPM from the Console Machine**

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Attach an RPM from a Managed Host” on page 89](#).

**1 Click the Select File button of the File Name field.**

The Choose RPM window opens.

**2 Browse to and select the relevant package.**

**3 Click Open.**

The Choose RPM window closes, and the path name appears in the File Name field of the Attach Target File window.

## ▼ **To Attach an RPM from a Managed Host**

If you selected Managed Host, follow this procedure.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the software, and click OK.**

The Host Selection window closes, and the host name appears in the Host Name field of the Attach Target File window.

**3 In the File Name field, type the full path name of the package.**

**4 Click Apply.**

The Status column indicates when the upload is done. The Local Expansion technology generates deployment rules for the new package.

# Uploading Solaris Software

Solaris software and file formats are not known by Linux. Therefore, the procedures for adding Solaris software to your local knowledge base include creating a tar file of Solaris packages:

Expand the PKG, to create a directory of files; then tar the directory.

Using Sun Update Connection – Enterprise, you will upload the tar file. Sun Update Connection – Enterprise will recognize it as a Solaris software and make the PKG accessible for deployment in jobs.

The procedures in this section include the following:

- “Using Console on Windows” on page 90
- “Adding Undetected Solaris Software” on page 90
- “Adding Multiple Solaris Packages” on page 91
- “Adding Solaris Software with a Script” on page 92
- “Attaching Solaris Software to Detected Listings” on page 93

## Using Console on Windows

You cannot upload PKGs with a console on Microsoft Windows. To upload single PKGs, on the SDS machine, use the script created for external upload. See [“Adding Solaris Software with a Script” on page 92](#).

## Adding Undetected Solaris Software

In this procedure, you add a Solaris PKG to the knowledge base, when it has not been detected automatically. This procedure is best used for single packages, when you feel more comfortable using the console rather than a command-line.

### Before You Begin

When you upload Solaris software, it must be in the form of a tarball, not a PKG.

1. Make sure the software is a directory of files, not a PKG.
2. Tar the directory: `tar -cf name.tar /path/*`
3. Copy the tarball to the console machine.

If you are using a console on Microsoft Windows, this procedure is not applicable. See [“Adding Solaris Software with a Script” on page 92](#).

## ▼ To Upload a Single PKG

- 1 Log in with full permissions or as the `admin` user.
- 2 From the drop-down list in the tool bar, select the Solaris distribution-architecture.
- 3 Select Local/Local PKGs/[<category>].
- 4 Do one of the following:
  - From the tool bar, click the Add Component button.
  - Right-click the selected category and choose Local -> Add.
  - From the Components menu, choose Local -> Add.  
The Add Software window opens.
- 5 In Upload File From, select Console.
- 6 Click the Select File button of the File Name field.  
The Choose RPM window opens. This window has the same name for both Linux (RPM) and Solaris (tarball).
- 7 Browse to and select the package you want to add. Use the Control or Shift keys to make a multiple selection from one directory.
- 8 Click Open.  
The choose RPM window closes, and the path name appears in the File Name List of the Add Software window.
- 9 Click Apply.  
The Status column indicates when the upload is done. You might have to wait until the console is updated with the changes; time depends on your local environment configuration.
- 10 If a software component is a security fix for an earlier version (see [“To Fix Local Software Missing Dependencies” on page 100](#)), check the Security Fix option.

## Adding Multiple Solaris Packages

In this procedure, you add a large amount of Solaris software to your local knowledge base. Use this procedure for upload of Solaris software CDs. This procedure does not use the console; it uses a web application created specifically to make Sun Update Connection – Enterprise support and management of Solaris more efficient. Notice that this procedure is also found in the Administrator’s Guide; it must be done after installation of the Sun Update Connection – Enterprise Agent on a Solaris machine, to enable the system dependency server to recognize Solaris software.

## Before You Begin

Make sure of the following:

- You have standard NFS or direct access to the PKGs from the system dependency server machine. The CD is in the CD-ROM of the SDS machine; or the SDS has direct access to Solaris files. This procedure does not support FTP or HTTP.
- Directories and files to be uploaded are readable by the nobody user.
- If the software is in PKG format, expand the PKGs. Each creates a directory (and possible sub-directories) and places there the files of the package.

## ▼ To Upload Solaris CDs

- 1 **Open a web browser and in the URL address field, type:**

`https://SDS-hostname-or-IP-address:8002/upload.html`

- 2 **In the Package path text box, type the full path to the directory that contains the Solaris software.**

For example, if you specify the `/tmp/tmpdso1` directory, it should contain all the subdirectories and contents copied from the Products directory on the CD ISO image.

---

**Note** – There is no recursive search, so the upload path must be only one level above the software directories.

---

- 3 **Click Upload.**

The packages are added to the Solaris knowledge base of the Sun Update Connection – Enterprise system dependency server. The browser window shows the automated actions: reading packages, adding packages, and searching for missing packages.

## Adding Solaris Software with a Script

In this procedure, you will use a script from the Sun Update Connection – Enterprise CLI application to upload Solaris software. Use this procedure if you are unfamiliar with Solaris commands and having trouble unpacking the PKGs or tarring the directories.

## Before You Begin

Install the latest Sun Update Connection – Enterprise CLI.

The script is `/usr/local/uce/cli/bin/pkg_loader.sh`

## ▼ To Upload Solaris Software With `pkg_loader`

- 1 Change to the following directory by typing:

```
cd /usr/local/uce/cli/bin/
```

- 2 Type the following command:

---

**Note** – `-p` is required and its value is the path of the packages to be uploaded.

`-r` is optional and provides a recursive search through the given path.

`-d` is optional and provides debugging information.

---

```
./pkg_loader.sh -p path [ -r ] [ -d ]
```

- 3 Type a Sun Update Connection – Enterprise user name with full permissions.
- 4 Type a password for the Sun Update Connection – Enterprise user.
- 5 For the channel, type the number of the distribution-architecture, according to the displayed list of Available Channels, to which the packages you want to upload belong.
- 6 At the prompt `Would you like all found components to be added under specific category?`, type `y` to put the packages in a user-defined category, and then at the `Category name` prompt, type the name of the category.

If the category does not yet exist in the Sun Update Connection – Enterprise components list, it will be created. If you type `n`, the packages are added under a default category in the components list.

`pkg_loader.sh` will tar the Solaris package directories. Then it uploads the tarballs to the knowledge base. Sun Update Connection – Enterprise recognizes them as Solaris packages and enables you to deploy them as PKGs.

## Attaching Solaris Software to Detected Listings

In this procedure, you learn how to attach a Solaris software to a name in the Components list under Local/Local PKGs. The name must already be in the Components list. Use this procedure to: replace a package with another one; manually upload a package; fix missing dependencies. See [Table 5–1](#) for more explanations of when to use an attach procedure.

### Console on Windows

If you are using a console on Microsoft Windows, this procedure is not applicable. See [“Adding Solaris Software with a Script” on page 92](#), or delete an existing component (that you want to replace or fill), and use the script to upload the new PKG.

## Before You Begin

When you upload Solaris software, it must be in the form of a tar file, not a PKG.

1. Make sure the software is a directory of files, not a PKG.
2. Tar the directory:

```
tar -cf name.tar /path/*
```

3. Copy the tarball to the console machine.

## ▼ To Upload Solaris Software

- 1 **Log in with full permissions or as the admin user.**

- 2 **From the drop-down list in the tool bar, select a distribution-architecture.**

The Components list shows the components relevant to your selection.

- 3 **Select Local/Local PKGs/[category]/package group/package.**

- 4 **Do one of the following:**

- From the tool bar, click the Upload knowledge base File button.
- Right-click the selected component and choose Local -> Upload.
- From the Components menu, choose Local -> Upload.

The Attach Target File window opens.

- 5 **Check the relevant Solaris architecture-distribution.**

- 6 **In the Upload File From options, select Console.**

- 7 **Click the Select File button of the File Name field.**

The Choose RPM window opens.

This window has the same name for both Linux (RPM) and Solaris (tarball).

- 8 **Browse to and select the relevant package.**

- 9 **Click Open.**

The Choose RPM window closes, and the path name appears in the File Name field of the Attach Target File window.

- 10 **Click Apply.**

The Status column indicates when the upload is done. The Local Expansion technology generates deployment rules for the new package.

# Editing NCO Listings in Components List

After you have added your local components to the Sun Update Connection – Enterprise knowledge base, remaining management procedures are the same, whether for Local RPMs or for Local PKGs, and on a console of any platform.

This section includes the following procedures:

- “Editing Local Software Package Groups” on page 95
- “Editing Local Software Packages” on page 96
- “Deleting NCOs” on page 97
- “Managing Local Patches and Dependencies” on page 98
- “Using Local Security Fixes” on page 99
- “Fixing Local Dependencies” on page 100
- “Troubleshooting NCOs” on page 101

## Editing Local Software Package Groups

In this procedure you edit a package group that Sun Update Connection – Enterprise creates when you add a local component to the knowledge base. Use this procedure to apply a package group to additional distributions.

### ▼ To Edit a Package Group

- 1 **Log in with full permissions or as the admin user.**
- 2 **From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows the components relevant to your selection.
- 3 **Select Local/Local RPMs | Local PKGs/[category]/package group.**
- 4 **Do one of the following:**
  - From the tool bar, click the Edit Local Component button.
  - Right-click the selected component and choose Local -> Edit.
  - From the Components menu, choose Local -> Edit.  
The Package Group Properties window opens.
- 5 **Change the description or the list of applicable distributions.**
- 6 **Click Apply.**  
The Status column displays icons to indicate the success or error.

**7 Click Close.**

The Package Group Properties window closes. Wait for the console to be updated.

## Editing Local Software Packages

In this procedure you edit the properties of a local package. Use this procedure to add the software to the knowledge bases of more distributions or to mark a package as a security fix for a previous version.

### ▼ To Edit a Package

**1 Log in with full permissions or as the admin user.**

**2 From the drop-down list in the tool bar, select a distribution-architecture.**

The Components list shows the components relevant to your selection.

**3 Select Local/Local RPMs | Local PKGs/[category]/package group/package.**

**4 Do one of the following:**

- From the tool bar, click the Edit Local Component button.
- Right-click the selected component and choose Local -> Edit.
- From the Components menu, choose Local -> Edit.

The Package Properties window opens.

**5 If this package is a fix for a previous package, select Security fix (see [“To Mark Local Software as a Security Fix” on page 99](#)).**

**6 Change the description or the list of applicable distributions.**

**7 Click Apply.**

The Status column displays icons to indicate the result of the change.

**8 Click Close.**

The Package Group Properties window closes. Wait until the console is updated with the changes; time depends on your local environment configuration.



## Moving a Local RPM to Another Package Group

### ▼ To Move a Local RPM to Another Package Group

Use the Move Package Group window to reorganize the Local RPMs hierarchy for one or more distributions on your system dependency server.

This procedure applies to local RPMs only. You can only move a local RPM to a different category under the Local RPMs category.

- 1 From the Hosts list, select a host or a host group to specify the distribution type.
- 2 From the Components list, expand the Local folder and then expand the Local RPMs folder to see the local RPM categories for this distribution.
- 3 Expand the local RPM category that contains the RPM that you want to move.
- 4 Select the RPM element to move.  
If you select one of the components under the RPM element, the Move option is disabled.
- 5 Open the Move Package Group window in one of these ways:
  - From the tool bar, click the Move the Selected Local Component button.
  - From the Components menu, choose Local->Move.
  - In the Components list, right-click the selected package and choose Local->Move.The Move Package Group window opens.
- 6 Specify the distributions you want affected by this change.  
By default, all distributions are affected by the change.  
To select a subset of the distributions, deselect Select All, and then select one or more distributions.
- 7 Select the category to which you want to move the RPM.  
To create a new category under Local RPMs, see [“To Add a Category”](#) on page 79.
- 8 Click Apply.
- 9 Verify that the RPM was moved correctly.
- 10 Click Close to close the window.

## Deleting NCOs

In this procedure, you remove NCOs from your Local components list or from specific distributions.

## Before You Begin

Make sure that the NCO is uninstalled from every host before attempting to remove it from the knowledge base. If it is installed on a managed host, it will be automatically detected and added again to your local knowledge base.

### ▼ To Delete an NCO

- 1 Log in with full permissions or as the admin user.**
- 2 From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows the components relevant to your selection.
- 3 Under Local/Local RPMs | Local PKGs/, select the component that you want to delete.**  
It may be a user-defined category, a package-group, or a package.
- 4 Do one of the following:**
  - From the tool bar, click the Delete Local Component button.
  - Right-click the selected component and choose Delete.
  - From the Components menu, choose Delete.  
The Delete Local Component window opens.
- 5 Check the distributions from which you want to delete the NCO.**  
You may check any or all distributions, even those that did not have the NCO.
- 6 Click Apply.**  
The Status column displays icons to indicate the result of the delete.
- 7 Click Close.**  
The Delete Local Component window closes. Wait until the console is updated.

## Managing Local Patches and Dependencies

If you create a homegrown patch for either a CO or an NCO, you can upload your component and mark it as a patch.

For example, your organization has a software developed in-house. Some time later, it is discovered that this software has a security issue. The component is patched to fix the security issue and is packed again.

Without Sun Update Connection – Enterprise, you would have to uninstall every instance of the software and install the new one. With Sun Update Connection – Enterprise, everything is handled automatically. You upload the new version to the knowledge base, and in the Add Software window, you mark the upload as a Security Fix.

You run a Security Check ([“Running Predefined Profiles” on page 140](#)). Wherever the earlier version was installed, the agents upgrade it to the secured version.

## Using Local Security Fixes

In this procedure you mark a local component as being a security fix for an earlier version.

### To Mark Local Software as a Security Fix

In the Add Software window, select Upload as: Security Fix.

If you are using a console on Windows, use the CLI command.

#### Marking as a Fix in CLI

Execute the CLI `-asp` command with the `-secure` option. See [“Add Software Package \(-asp\) Command” on page 268](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
echo "The list of active distributions is:"
uce_cli -ld -u $user -p $password
echo -n "Type the exact name of the distribution for this software:"
read distro
echo -n "Type the source path name of the file:"
read pathname
echo -n "Is this software a secured version of a previous one? (y | n)"
read secure
if [ "$secure" = "y" ]; then
    uce_cli -asp -f "$pathname" -secure -D $distro -u "$user" -p "$password"
else
    uce_cli -asp -f "$pathname" -D $distro -u "$user" -p "$password"
fi
```

### To Handle a Series of Fixes

If you upload a package and mark it as Security Fix, consider earlier versions:

- Maintain a series of Security Fixes by keeping all versions marked as Security Fix. All packages are considered secure.
- Edit properties of previous packages by unmarking the earlier versions. Sun Update Connection – Enterprise considers only the latest marked package as secure.

## Fixing Local Dependencies

A dependency is a component that is needed by a package for deployment. This dependent component may be another software component, a file, a symbol, and so on. When you upload packages to your local knowledge base, the Local Expansion technology finds the list of dependencies for each package. If the knowledge base is missing dependencies, use the information given by Sun Update Connection – Enterprise to fix them.

NCOs with missing dependencies are marked with an exclamation point in a red circle icon:

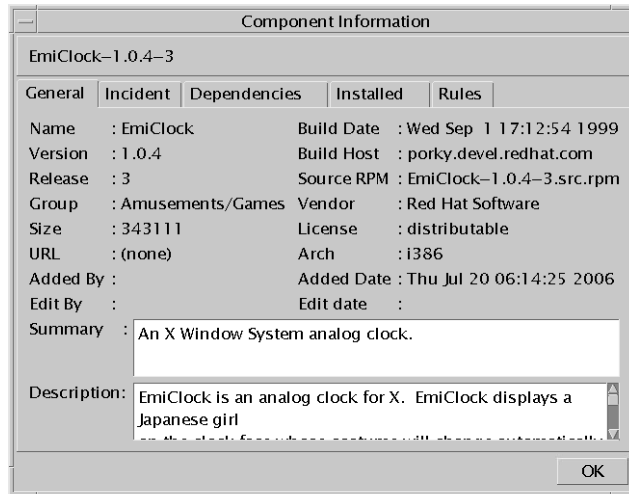
### Before You Begin

Before you fix missing dependencies of a marked NCO, you should wait at least two minutes from the time that uploaded succeeded. The Local Expansion technology generates rules for local components on a scheduled basis; if you wait, some of the missing dependencies may be handled automatically.

If the NCO is Solaris software, make sure the dependent components to be uploaded are tarballs and have been copied to the console machine.

## ▼ To Fix Local Software Missing Dependencies

- 1 Log in with full permissions or as the `admin` user.
- 2 From the Components list, select the component marked with an exclamation point in a red circle.
- 3 Do one of the following:
  - From the tool bar, click the Details button.
  - Right-click the selected component and choose Details.
  - From the Components menu, choose Details.  
The Component Information window opens.



#### 4 Open the Dependencies tab.

In the Requires section, missing components are marked with an exclamation point in a red circle.

#### 5 From the Internet or private source, find the packages that provide the missing components.

If the package is a PKG, expand it and tar the directory.

#### 6 Add the packages to the local knowledge base.

When all missing dependencies are uploaded, the icon of the local component changes to standard.

## Troubleshooting NCOs

### Cannot Attach NCO

**Description:** Upload of the Attach procedure failed with the following error:

Package-Name mismatch. Use Add button.

**Cause:** The selected component and the RPM you selected to attach have different names.

**Workaround:** Use the Add feature instead of Attach.

### Attached NCO is Marked with an Exclamation Point in a Red Circle

**Description:** Upload succeeded, but the package icon is marked with an exclamation point in a red circle.

The rules of this RPM show that dependent components are missing from the local knowledge base.

**Workaround:** See [“To Fix Local Software Missing Dependencies”](#) on page 100.

## Cannot Find NCO

**Description:** Upload of the Attach procedure succeeded, but the NCO is not listed under Local RPMs or under Local PKGs.

A CO (under Software, rather than under Local) has the same name, version, and release. Your NCO was added to the package group of the appropriate name under Software.

**Workaround:** Run the Local Software Review predefined test (see [“Predefined Profiles”](#) on page 136), or use the Find feature to find this software component and to check that the listing is correct for your component.

## Cannot Delete an NCO Component

**Description:** When you try to delete a selected Local component, you receive the following error message:

Cannot be deleted.If an NCO is installed on any managed host within the selected distributions, it will be detected and uploaded again. To prevent Sun Update Connection – Enterprise from undoing your delete command, the message reminds you to uninstall the software component from all hosts before deleting it from the knowledge base.

**Workaround:** Do the following:

1. Open the Inventory panel (View -> Inventory).
2. From the Components list, right-click the software component and choose Component Properties. The Component Information window opens. In the Installed tab, see the list of all managed hosts that have this component installed.
3. Create and deploy a job to uninstall this component from the listed hosts.
4. Return to the main window and delete the component.

# Managing Local Files

In this section, users with full or admin permissions add, edit, and delete local files.

*Local files* are scripts, binaries, executables, and files that are private to your enterprise or otherwise unknown to the universal server. The following table explains the categories.

TABLE 5-2 Local File Categories

Category	Description	Use
Configuration files	Installs a version of a configuration file	Install configuration file versions for efficient change management on a customized environment
Macros	Outputs a value into a local configuration file	Install a local configuration file that includes a macro sign and the sign will be replaced with the local value
Post-action	Performs an action on the host after the job tasks are carried out	Run action scripts or binaries on hosts to fulfill a post-job requirement
Pre-action	Performs an action on the host before the job tasks are carried out	Run action scripts or binaries on hosts to fulfill a pre-job requirement
Probe	Runs a test on a host; if returns success, the job tasks are begun	Run test on hosts to make sure they can do a job before the tasks begin

## Actions

An action is a script, binary, or executable that does something to a host. You categorize your actions as either Pre or Post.

Pre-actions are run before the tasks of a job begins. If a pre-action finishes successfully, it returns a value of zero and the next actions of the job are carried out. If a pre-action returns a non-zero value, the job stops.

Post-actions are run after the other tasks of a job are completed. If a post-action returns a non-zero value, the job ends with a failure status.

For example, you want to install the Apache server. A prerequisite of Apache installation is that /home be unmounted. After it is installed, you want to run other applications that need /home to be mounted.

You create a pre-action `unmount_home.sh`:

```
#!/bin/sh -f
# unmount home from remote server
umount server01:/home
    if [ $?==0]; then exit 0; fi
```

You create a post-action `mount_home.sh`:

```
#!/bin/sh -f
# mount home to remote server
mount server01:/home
    if [ $?==0]; then exit 0; fi
```

You upload these actions. Then you create a profile to install Apache, and add these actions to the job basket. The job does the following:

1. runs any probes that you put in
2. unmounts /home
3. installs Apache
4. mounts /home

## Writing Actions

Make sure the action returns zero (0) on success.

Make the name of the action understandable and descriptive. You can view it in the Jobs panel as a task that either succeeded or failed.

## Uploading Actions

In this procedure you upload an existing executable as a Pre-Action or Post-Action to the knowledge base. You can create a category under Pre-Actions or Post-Actions before uploading an action (see [“Adding Categories” on page 79](#)).

### ▼ To Add an Action

- 1 **Log in with full permissions or as the `admin` user.**
- 2 **From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows Local components applied to the selected distribution.
- 3 **From the Components list select Local/Post-Actions | Pre-Actions/[category].**
- 4 **Do one of the following:**
  - From the tool bar, click the Add Component button.
  - Right-click the selected category and choose Local -> Add.
  - From the Components menu, choose Local -> Add.  
The Add Post Action or the Add Pre Action window opens.
- 5 **Type a name for the component that will point to your Post-action or Pre-action. This should not be the complete file name. The name should be a name that is easily understood.**
- 6 **Type a free-text description.**
- 7 **Check each distribution to which this file should be applied.**



**8 Select a source machine:**

- If the console has access to the file, select Console.
- If a remote managed host has access to the file, select Managed Host.

---

**Note** – Remote upload is limited to 5 Mbytes. Console upload is unlimited. It is recommended that you upload from the console whenever possible.

---

**▼ To Upload a Post-action or a Pre-action from the Console Machine**

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Upload a Post-action or a Pre-action from a Managed Host”](#) on page 105.

**1 Click the Select File button of the File Name field. The Choose File window opens.****2 Browse to and select the relevant file.****3 Click Open.**

The Choose File window closes, and the path name appears in the File Name field of the Add Pre Action or Add Post Action window.

**4 Click Apply.**

The Status column indicates when the upload is done.

**5 Click Close to close the window, or Reset to add more.****▼ To Upload a Post-action or a Pre-action from a Managed Host**

If you selected Managed Host, follow this procedure.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the file, and click OK.**

The Host Selection window closes. The host name appears in the Host Name field of the Add Pre Action or Add Post Action window.

**3 In the File Name field, type the full path name of the file.****4 Click Apply.**

The Status column indicates when the upload is done. Click Close to close the window, or Reset to add more.

### Example 5-3 Uploading a Post-action or a Pre-action with the CLI

The Add Target Local command is the same for Pre-actions, Post-actions, Configuration files, Macros, and Probes. The following syntax is for Pre-actions and Post-actions. The `-tP` parameter is for Pre-actions; `-tS` is for Post-actions. The example script adds a Post-action.

In the CLI syntax, a category under the default Local categories is mandatory. See the procedure: [Example 5-1](#) on for the Add Local Category CLI command. See [“Add Target Local \(-atl\) Command”](#) on page 270.

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}

function distro {
    echo "Active distributions are:"
    uce_cli -ld -u "$user" -p "$password"
    echo -n "To which distro should this script be added?"
    read distro
    echo
}

function category {
    echo "Under which category should this Post-action be added?"
    echo "Valid answers: any subcategory under Post-actions. See list:"
    uce_cli -fc -T "Post-actions" -sons -D $distro -u "$user" -p "$password" #> tmp.file
    sed "s/ROOT/Local/Post-actions/" tmp.file
    echo -n "Start your answer with / ::"
    read parent #rm tmp.file
    echo
}

function setup {
    echo -n "Type the full path name of the file to upload:"
    read pathname
    echo -n "Type a display name for the local file:"
    read displayName
}

login
distro
category
setup
uce_cli -atl -f "$pathname" -pT "Post-actions$parent" -tS "$displayName" -D $distro -u "$user" -p "$password"
```

## Probes

A probe is a script or binary that tests whether a host fulfills prerequisites for successful completion of a job.

If a probe returns zero, the next tasks of the job are carried out. This ensures that only hosts that currently meet your requirements will run jobs.

If a probe returns 1, the job fails on the host. The probe name is displayed in the Status window as the point of failure. Now you can easily troubleshoot the host.

### EXAMPLE 5-4 Creating a Probe

You create a probe that tests disk space. It returns zero if there is more than the minimum defined in the script.

```
#!/bin/csh -f
set minimum_space=1000000000
set actual_space=\Qdf -k | awk '{print $4}' | tail -1\Q
if ( $actual_space > $minimum_space ) then
    echo $actual_space
    exit 0
endif
exit 1
```

Upload this probe. Create a job that includes the probe. The tasks are carried out if the available space of the host meets your requirements.

## Writing Probes

Make sure the action returns zero (0) on success and one (1) on failure.

Make the name of the probe a boolean statement, to make it as clear as possible; users will view it in the Jobs panel as a task that either succeeded or failed.

Sun Update Connection – Enterprise might run a probe many times during a job. To ensure that operations are efficient, make sure that your probes are as short and fast as possible.

## Uploading Probes

In this procedure you add probes to the local knowledge base. You can create a category under Probes before uploading a probe (see [“Adding Categories” on page 79](#)).

## ▼ To Add a Probe

**1 Log in with full permissions or as the admin user.**

**2 From the drop-down list in the tool bar, select a distribution-architecture.**

The Components list shows Local components applied to the selected distribution.

**3 From the Components list select Local/Probes/[category].**

**4 Do one of the following:**

- From the tool bar, click the Add Component button.
- Right-click the selected category and choose Local -> Add.
- From the Components menu, choose Local -> Add.

The Add Probe window opens.

**5 Type a display name for the component that will point to your probe.**

This should not be the complete file name, but it should be a name that is easily understood.

**6 Type a free-text description.**

**7 Check each distribution to which this file should be applied.**

**8 Select a source machine:**

- If the console has access to the file, select Console.
- If a remote managed host has access to the file, select Managed Host.

Note: remote upload is limited to 5Mb; console upload is unlimited. It is recommended that you upload from the console whenever possible.

## ▼ To Upload a Probe from the Console Machine

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Upload a Probe from a Managed Host” on page 109](#).

**1 Click the Select File button of the File Name field.**

The Choose File window opens.

**2 Browse to and select the relevant file.**

**3 Click Open.**

The Choose File window closes, and the path name appears in the File Name field of the Add Probe window.

**4 Click Apply.**

The Status column indicates when the upload is done. Click Close to close the window, or Reset to add more.

**▼ To Upload a Probe from a Managed Host**

If you selected Managed Host, follow this procedure.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the software, and click OK.**

The Host Selection window closes. The host name appears in the Host Name field of the Add Probe window.

**3 In the File Name field, type the full path name of the file.****4 Click Apply.**

The Status column indicates when the upload is done. Click Close to close the window, or Reset to add more.

**Example 5–5 Uploading a Probe with the CLI**

The Add Target Local command is the same for Pre-actions, Post-actions, Configuration files, Macros, and Probes. The following syntax is for Probes.

In the CLI syntax, a category under the default Local categories is mandatory. See the procedure [Example 5–1](#) for the Add Local Category CLI command. See [“Add Target Local \(-atl\) Command”](#) on page 270.

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}

function distro {
    echo "Active distributions are:"
    uce_cli -ld -u "$user" -p "$password"
    echo -n "To which distro should this script be added?"
    read distro
    echo
}
}
```

```
function category {
    echo "Under which category should this Probe added?"
    echo "Valid answers: any subcategory under Probes. See list:"
    uce_cli -fc -T "Probes" -sons -D $distro -u "$user" -p "$password" > tmp.file
    sed "s/ROOT\Local\Probes//" tmp.file
    echo -n "Start your answer with / ::"
    read parent
    rm tmp.file
    echo
}

function setup {
    echo -n "Type the full path name of the file to upload:"
    read pathname
    echo -n "Type a display name for the local file:"
    read displayName
}

login
distro
category
setup
uce_cli -atl -f "$pathname" -pT "Probes$parent" -tR "$displayName" -D $distro -u "$user" -p "$password"
```

## Configuration Files

The configuration files of a Linux or Solaris machine determine everything about the environment: the kernel version, the bootloader, the file system, the printers, and so on. All of these files are writable, to a system administrator with permissions and knowledge. Change management in a Linux or Solaris environment usually includes managing files as well as applications.

A local *configuration file* is any file that you want to store on the knowledge base and distribute to multiple hosts for simultaneous and consistent configurations. Macros (see [“Macros” on page 116](#)) are used to localize these files for values relevant to each managed host.

### EXAMPLE 5-6 Updating Configuration Files

Your enterprise with 200 Linux servers is reorganizing; personnel are changing offices and floors. Everyone wants their machine to print to the closest printer. Instead of reconfiguring every `printcap` file for every host (probably more than once, as the printers and the staff are moved around the complex), you make different versions of this file.

You change `printcap` slightly for each version:

```
# /etc/printcap
# Version for RH 9 on 12th floor West
lp:\
```

**EXAMPLE 5-6** Updating Configuration Files (Continued)

```

:sd=/var/spool/lpd/lp:\
:mx#0:\
:sh:\
:rm=printer12
:rp=pr1:

```

A second version:

```

# /etc/printcap
# Version for RH WS3 on 10th floor Main
lp:\
  :sd=/var/spool/lpd/lp:\
  :mx#0:\
  :sh:\
  :rm=printer10
  :rp=pr1:

```

And so on. You create a file declaration for `/etc/printcap`. Then you upload the versions of the file to the file declaration.

Now you can change the printer configuration of any host within seconds, by selecting the appropriate version and sending it to the hosts that need it. The contents of their old `printcap` is overwritten with the contents of the version that you selected.

## Creating File Declarations

A *file declaration* holds a path name for installation on remote hosts. When you select a local Configuration File to install on remote hosts, the file is installed in the path and under the name that is determined by the file declaration. Thus, a file declaration can hold multiple versions of the same file; or different files that you want to be installed in the same path name on different hosts. This allows you to simultaneously manage configuration files of a heterogenous environment.

You can create a sub-category under Configuration Files before uploading a Configuration file (see “Adding Categories” on page 79).

### ▼ To Add a File Declaration

- 1** Log in with full permissions or as the `admin` user.
- 2** From the drop-down list in the tool bar, select a distribution-architecture.  
The Components list shows Local components applied to the selected distribution.
- 3** From the Components list select `Local/Configuration Files/[category]`.

**4 Do one of the following:**

- From the tool bar, click the Add Component button.
- Right-click the selected category and choose Local -> Add.
- From the Components menu, choose Local -> Add.

The Add Target File Declaration window opens.

**5 In the *Target File path name* text-field, type the path name where you want the files that will be held under this declaration to be installed on the target hosts. Do not delete the starting back-slash.****6 Type a free-text description.****7 Check each distribution to which this file should be applied.****8 Click Apply.**

The status column indicates when the file declaration is uploaded to the knowledge base.

**9 Click Close.**

The Add Target File Declaration window closes.

The file declaration is created. A file with a suffix of *-Unknown* is also created. This is a placeholder and prevents accidental overwrites.

**Example 5-7 Adding a File Declaration with the CLI**

You may add a file declaration to all distributions (default; do not use the `-D` parameter) or to a single distribution. If you choose to add a file declaration to a single specified distribution, you can add the Configuration files only to that distribution. Remember that a file declaration, declares the target path name for installation; it does not upload the file itself.

In the CLI syntax, a category under the default Local categories is mandatory. See the procedure: [Example 5-1](#) on for the Add Local Category CLI command. See [“Add File Declaration \(-afd\) Command”](#) on page 269.

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}

function distro {
    echo "Active distributions are:"
    uce_cli -ld -u "$user" -p "$password"
    echo -n "To which distro should this be added?"
```



```

    read distro echo
}
function category {
    echo "Under which category should this File Declaration be added?"
    echo "Valid answers: any subcategory under Configuration files. See list:"
    uce_cli -fc -T "Configuration files" -sons -D $distro -u "$user" -p "$password" > tmp.file
    sed "s/ROOT\Local\Configuration files//" tmp.file
    echo -n "Start your answer with / :)"
    read parent
    rm tmp.file
    echo
}
function setup {
    echo -n "Type the full path name for target installation:"
    read path name
}
login
distro
category
setup
uce_cli -afd -tftp "$pathname" -pT "Configuration files$parent" -D $distro -u "$user" -p "$password"

```

## Uploading Local Configuration Files

The File Declaration declares the full target path name for installation of a file on hosts; it is not the file itself. In this procedure you upload your local versions of Configuration files to the local knowledge base.

### ▼ To Add a Local Configuration File

- 1 **Log in with full permissions or as the admin user.**
- 2 **From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows Local components applied to the selected distribution.
- 3 **From the Components list, select Local/Configuration Files/*category*/file declaration.**
- 4 **Do one of the following:**
  - From the tool bar, click the Add Component button.
  - Right-click the selected category and choose Local -> Add.
  - From the Components menu, choose Local -> Add.  
The Add Configuration File window opens.

**5 Type a display version-name for the file.**

This text field is called Version (rather than Name), because the files that you add to a specific file declaration should all be different versions of one file. The Version value will be displayed in the Components list as a suffix to the file name.

When you install this file on a remote host, it is installed under the full path name of the file declaration.

**6 Type a free-text description.****7 Check each distribution to which this file should be applied. Make sure that the file declaration is on all the selected distributions.****8 Select a source machine:**

- If the console has access to the file, select Console.
- If a remote managed host has access to the file, select Managed Host.

Note: remote upload is limited to 5Mb; console upload is unlimited. It is recommended that you upload from the console whenever possible.

**▼ To Upload a Configuration File from the Console Machine**

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Upload a Configuration File from a Managed Host”](#) on page 114.

**1 Click the Select File button of the File Name field.**

The Choose File window opens.

**2 Browse to and select the relevant file.****3 Click Open.**

The Choose File window closes, and the path name appears in the File Name field of the Add Configuration File window.

**4 Click Apply.**

The Status column indicates when the upload is done. Click Close to close the window, or Reset to add more.

**▼ To Upload a Configuration File from a Managed Host**

If you selected Managed Host, follow this procedure.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the software, and click OK.**

The Host Selection window closes. The host name appears in the Host Name field of the Add Configuration File window.

**3 In the File Name field, type the full path name of the file.****4 Click Apply.****Example 5–8 Uploading a Configuration File with the CLI**

The Add Target Local command is the same for Pre-actions, Post-actions, Configuration files, Macros, and Probes. The following syntax is for Configuration files. This command creates a file declaration automatically. It cannot be used to add a file to an existing declaration.

In the CLI syntax, a category under the default Local categories is mandatory. See [Example 5–1](#) on for the Add Local Category CLI command. See [“Add Target Local \(-atl\) Command”](#) on page 270.

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}

function distro {
    echo "Active distributions are:"
    uce_cli -ld -u "$user" -p "$password"
    echo -n "To which distro should this file be added?"
    read distro
    echo }

function category {
    echo "Under which category should this file be added?"
    echo "A file declaration will be created automatically."
    echo "Valid answers: any subcategory under Configuration files. See list:"
    uce_cli -fc -T "Configuration files" -sons -D $distro -u "$user" -p "$password" > tmp.file
    sed "s/ROOT/Local/Configuration files/" tmp.file
    echo -n "Start your answer with / ::"
    read parent
    rm tmp.file
    echo
}

function setup {
    echo -n "Type the full path name of the file to upload: "
    read pathname
    echo -n "Type a version suffix for this version of the file: "
    read version
```

```
echo -n "Type a display name for the local file: "  
  read displayName  
}  
login  
distro  
category  
setup  
uce_cli -atl -f "$pathname" -pT "Configuration files$parent" -tF "$displayName" -v "$version" \  
-D $distro -u "$user" -p "$password"
```

## Macros

A macro is a short script that outputs a single line. This output replaces a macro sign in a local Configuration file.

The macro value is used to customize a Configuration file for its host machine. You create a job that installs a Configuration file on multiple hosts.

This Configuration file has `<^AM^>macro<^AM^>` in its content, where *macro* is the name of the macro in the knowledge base.

Each Agent sees the `<^AM^>` sign and runs the named macro script. The result of the macro run is a line of local data. The value of the macro is entered in place of the macro sign.

### EXAMPLE 5-9 Using Macros

You are reorganizing your network servers. You will be reconfiguring the `/etc/hosts` file for multiple hosts, perhaps several times. Instead of changing this file for every host every time, you create versions of this file and upload them as Configuration files. In each version, you replace the specific local host name with: `<^AM^>hostname<^AM^>`

You create a script named `hostname.sh`:

```
#!/bin/sh -f  
# find local host name  
hostname
```

You upload `hostname.sh` as a macro called `hostname` to the local knowledge base. You send the Configuration file as part of a job. Each agent that receives the file, gets the macro sign, downloads the `hostname` macro, and executes `hostname.sh`, which replaces `<^AM^>hostname<^AM^>` with the real local host name on each host.

## Writing Macros

When writing macros:

- Make sure that the name of the macro script is the same as the macro sign in the files.
- Make sure the macro outputs the appropriate string.

The value of the macro, that is seen in the Configuration file, is the value that was given when the Configuration file was installed and the agent ran the macro from the knowledge base. If you create a macro that changes its value dynamically (or if you edit the content of the macro file), changes do *not* apply to the remote host files. If you want to change the content of the Configuration files with a new macro, you will have to upload the macro to the knowledge base and re-install the file on the hosts, letting the agents run the new macro.

## Uploading Macros

In this procedure you add macros to the local knowledge base. Use this procedure to store local macro scripts, which will later be automatically downloaded and run on multiple hosts. You can create a category under Macros before uploading a macro (see “[Adding Categories](#)” on page 79).

### ▼ To Add a Macro

- 1 **Log in with full permissions or as the admin user.**
- 2 **From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows Local components applied to the selected distribution.
- 3 **From the Components list, select Local/Macros/[category].**
- 4 **Do one of the following:**
  - From the tool bar, click the Add Component button.
  - Right-click the selected category and choose Local -> Add.
  - From the Components menu, choose Local -> Add.  
The Add Macro window opens.
- 5 **Type a display name for the component that will point to the macro.**  
This should not be the complete file name, but it should be a name that is easily understood.
- 6 **Type a free-text description.**
- 7 **Check each distribution to which this file should be applied.**
- 8 **Select a source machine:**
  - If the console has access to the file, select Console.
  - If a remote managed host has access to the file, select Managed Host.

---

**Note** – Remote upload is limited to 5Mb; console upload is unlimited. It is recommended that you upload from the console whenever possible.

---

### ▼ **To Upload a Macro from the Console Machine**

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Upload a Macro from a Managed Host”](#) on page 118.

**1 Click the Select File button of the File Name field.**

The Choose File window opens.

**2 Browse to and select the relevant file.**

**3 Click Open.**

The Choose File window closes, and the path name appears in the File Name field of the Add Macro window.

**4 Click Apply.**

The Status column indicates when the upload is done. Click Close to close the window, or Reset to add more.

### ▼ **To Upload a Macro from a Managed Host**

If you selected Managed Host, follow this procedure.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the file, and click OK.**

The Host Selection window closes. The host name appears in the Host Name field.

**3 In the File Name field, type the full path name of the file.**

**4 Click Apply.**

The Status column indicates when the upload is done. Click Close to close the window, or Reset to add more.

#### **Example 5–10 Adding a Macro with the CLI**

The Add Target Local command is the same for Pre-actions, Post-actions, Configuration files, Macros, and Probes. The following syntax is for Macros.

In the CLI syntax, a category under the default Local categories is mandatory. See [Example 5–1](#) on [Example 5–1](#) for the Add Local Category CLI command. See “Add Target Local (-atl) Command” on page 270.

```
#!/bin/bash

function login {
    echo -n "Type your user name:"
    read user
    echo -n "Type your password:"
    read password
}

function distro {
    echo "Active distributions are:"
    uce_cli -ld -u "$user" -p "$password"
    echo -n "To which distro should this script be added?"
    read distro
    echo
}

function category {
    echo "Under which category should this Macro be added?"
    echo "Valid answers: any subcategory under Macros. See list:"
    uce_cli -fc -T "Macros" -sons -D $distro -u "$user" -p "$password" > tmp.file
    sed "s/ROOT/Local/Macros/" tmp.file
    echo -n "Start your answer with / :)"
    read parent
    rm tmp.file
    echo
}

function setup {
    echo -n "Type the full path name of the file to upload:"
    read pathname
    echo -n "Type a display name for the macro:"
    read displayName
}

login
distro
category
setup
uce_cli -atl -f "$pathname" -pT "Macros$parent" -tM "$displayName" \
-D $distro -u "$user" -p "$password"
```

## Editing Files

After you have added local files to your knowledge base, you may edit them in various ways. You may edit the files on the knowledge base. Any editing you do will affect the file that is stored to the knowledge base, not the original file.

You may edit the files you installed on managed hosts, making the changes directly on the hosts. These files are known as Host files. You may open and save changes to the content of a Host file using Sun Update Connection – Enterprise, but the changes will not be affected in the knowledge base unless you add the file as a knowledge base file.

## Editing Local File Properties

In this procedure, you edit the properties of Configuration files, File Declarations, Macros, Post-actions, Pre-actions, and Probes in the knowledge base. If your environment changes, you can use this procedure to change the distributions to which Local Files are applied.

### ▼ To Edit Local File Properties

- 1 Log in with full permissions or as the admin user.**
- 2 From the drop-down list in the tool bar, select a distribution-architecture.**  
The Components list shows Local components applied to the selected distribution.
- 3 From the Components list, under Local/default category/[user category>], select the relevant Post-action, Pre-action, Probe, Macro, Configuration file, or File Declaration.**
- 4 Do one of the following:**
  - From the tool bar, click the Edit Local Component button.
  - Right-click the selection and choose Local -> Edit.
  - From the Components menu, choose Local -> Edit.  
A Properties window opens.
- 5 Change the list of selected active distributions.**
- 6 Change any of the displayed properties.**
- 7 Click Apply.**

The changes are uploaded to the knowledge base. If you added more distributions to the selected list, the file itself is uploaded to the knowledge base of the new distributions.

## Editing Knowledge Base Files

In this procedure you edit the contents of a Post-action, Pre-action, Probe, Macro, or Configuration file that has already been uploaded to the local knowledge base.



## ▼ To Edit a Local File

- 1 Log in with full permissions or as the `admin` user.
- 2 From the drop-down list in the tool bar, select a distribution-architecture.  
The Components list shows Local components applied to the selected distribution.
- 3 From the Components list, under `Local/default category/[user category]/`, select the relevant Post-action, Pre-action, Probe, Macro, or Configuration file.
- 4 Do one of the following:
  - From the tool bar, click the Open knowledge base File button.
  - Right-click the selected component and choose Local -> Open -> Knowledge Base File.
  - From the Components menu, choose Local -> Open -> Knowledge Base File.  
The Knowledge Base File window opens, displaying the contents of the file that is in the knowledge base.
- 5 Make any changes to the contents of the knowledge base file.
- 6 Check each distribution to which the changes should be applied.
- 7 Click Apply.  
The Status column indicates when the upload is done.
- 8 Click Close to close the window, or Reset to make more changes.

## Replacing Knowledge Base Files

In this procedure, you attach new files to existing listings of Post-actions, Pre-actions, Probes, Macros, and Configuration files. Use this procedure to replace a knowledge base file with a different one from a managed host.

## ▼ To Replace Knowledge Base Files

- 1 Log in with full permissions or as the `admin` user.
- 2 From the drop-down list in the tool bar, select a distribution-architecture.  
The Components list shows Local components applied to the selected distribution.
- 3 From the Components list, under `Local/default category/[user category]/`, select the relevant Post-action, Pre-action, Probe, Macro, or Configuration file.

**4 Do one of the following:**

- From the tool bar, click the Upload KnowledgeBase File button.
- Right-click the selected file and choose Local -> Upload.
- From the Components menu, choose Local -> Upload.

The Attach Target File window opens.

**5 Select a source machine:**

- If the console has access to the file, select Console.
- If a remote managed host has access to the file, select Managed Host.

---

**Note** – Remote upload is limited to 5 Mbytes. Console upload is unlimited. It is recommended that you upload from the console whenever possible.

---

▼ **To Attach a File from the Console Machine**

If you selected console, follow this procedure. If you selected Managed Host, go to [“To Upload a Macro from a Managed Host” on page 118](#).

**1 Click the Select File button of the File Name field.**

The Choose File window opens.

**2 Browse to and select the relevant file.**

**3 Click Open.**

The Choose File window closes, and the path name appears in the File Name field of the Attach Target File window.

**4 Check the distributions to which you want to apply these changes.**

If you check a distribution that does not have the original file, the attach will fail but no damage will be done.

**5 Click Apply.**

The Status column indicates when the upload is done.

**6 Click Close to close the window.**

▼ **To Attach a File from a Managed Host**

If you selected Managed Host, follow this procedure.

**1 Click the Select Host button of the Host Name field.**

The Host Selection window opens.

**2 Select the managed host that has the file, and click OK.**

The Host Selection window closes. The host name appears in the Host Name field.

**3 In the File Name field, type the full path name of the file.****4 Check the distributions to which you want to apply these changes.**

If you check a distribution that does not have the original file, the attach will fail but no damage will be done.

**5 Click Apply.**

The Status column indicates when the upload is done.

**6 Click Close to close the window.**

## Deleting Knowledge Base Files

You can remove anything that you (or another user) added to the Local knowledge base, but before deletion, make sure the component is not already included in a profile or scheduled job. Deleting a local file that will be referenced later will cause the job to fail. In this procedure you delete Post-actions, Pre-actions, Probes, Macros, Configuration files, or File Declarations.

### ▼ To Delete a Local File

**1 Log in with full permissions or as the `admin` user.****2 From the drop-down list in the tool bar, select a distribution-architecture.**

The Components list shows Local components applied to the selected distribution.

**3 From the Components list, select the component you want to delete.****4 Do one of the following:**

- From the tool bar, click the Delete Local Component button.
- Right-click the selected component and choose Delete.
- From the Components menu, choose Delete.

The Delete Local Component window opens.

**5 Check the distributions from which you want to delete the component.**

You may leave it on the component list of some distributions and delete it from others, or delete it from all.

**6 Click Apply.**

The Status column indicates when the change is done. You might have to wait until the console is updated with the changes; time depends on your local environment configuration.

## Opening Host Files

After you have uploaded Local Configuration files to the knowledge base (see [“Uploading Local Configuration Files” on page 113](#)), and installed these files on managed hosts (see [“Distributing Local Files” on page 168](#)), you can access the files from the hosts. This feature allows you to view, edit, and save-as the content of files on remote hosts, directly on their hosts.

Make sure that:

- The file is installed on the managed host
- The managed host is online
- The managed host is not busy with a job

### ▼ To Access a File from a Remote Host

**1 Log in with full permissions or as the admin user.****2 From the drop-down list in the tool bar, select a distribution-architecture.**

The Components list shows Local components applied to the selected distribution.

**3 Select a host. You can view files from only one host at a time.****4 From the Components list, select Local/Configuration files/[category]/file declaration.**

The Configuration files on the knowledge base are versions for knowledge base organization. Select the File Declaration to point to the installed file on the remote host.

Local

-->Configuration Files

---->[category]

----->File Declaration (**path name of file on host**)

----->File version (on knowledge base)

**5 Do one of the following:**

- From the tool bar, click the Open Host File button.
- Right-click the File Declaration and choose Local -> Open -> Open Host File.
- From the Components menu, choose Local -> Open -> Open Host File.

The Remote File Editor window opens. Wait until the contents of the remote file are uploaded and displayed.

**6 Change the text as needed.**

**7 Do one of the following:**

- Click Cancel, to close the file without changing it.
- Click Save As, to save a copy of the file, with any changes included. The Save As window opens, from where you can determine the path name of the copy.
- Click Save, to overwrite the file on the selected remote host.  
The File Editor window closes.



## Solaris Baselines

---

This chapter describes how to use Solaris baselines to update your Solaris hosts with patches.

### Using Baselines to Update a Solaris Host With Patches (Task Map)

A *Solaris baseline* is a dated collection of patches, patch metadata, and tools. Sun releases Solaris baselines on a monthly basis. When you install the patches of a baseline on a host, that host is considered to be *compliant* with that baseline.

Baselines *only* pertain to Solaris hosts.

Using Solaris baselines enables you to easily know the patch level of your hosts. For example, you install some test hosts with a particular baseline. Then, you test these hosts for a period of time to see whether the patches in this baseline are stable enough to be used on your production hosts. When the testing reveals that this baseline is stable, you can install the same baseline you tested on your production hosts.

You can modify a baseline to create a custom patch set by the use of black lists and white lists. A *black list* is a list of patch IDs that you never want to be applied to a host. A *white list* is a list of patch IDs that you always want to be applied to a host.

Solaris baselines appear as a category in the Components list. The Solaris Baselines category contains a list of dated baselines. Each dated baseline contains these three patch sets:

- **Full** – Includes all Solaris patches
- **Recommended** – Includes Solaris recommended patches and security patches
- **Security** – Includes only Solaris security patches

Selecting a baseline patch set and choosing Details from the Components menu shows you the list of the patches in the baseline.

An installed baseline appears in the Components list marked as (Installed). If you install the baseline and use a policy as a black list, the baseline is not marked as (Installed) even though it has been installed.

The following table identifies the tasks that you might perform when using Solaris baselines to update a system with patches.

Task	Description	For Instructions
Create a white list of patches.	Your white list must include the baseline you want to install and can optionally include any patches that you want to always install.	<a href="#">“To Create a Solaris Baseline White List” on page 128</a>
(Optional) Create a black list of patches.	You can optionally create a black list that includes the patches that are never to be installed.	<a href="#">“To Create a Solaris Baseline Black List” on page 130</a>
Perform a Solaris baseline compliance analysis.	The result of this analysis is a list of the number of patches to be installed to bring it in to compliance with the baseline, the white list, and the black list you specify.	<a href="#">“To Perform a Solaris Baseline Compliance Analysis” on page 131</a>
Install a Solaris baseline on a managed host.	This procedure describes how to use the white list and black list you created to deploy a Solaris baseline to selected Solaris hosts.	<a href="#">“To Install a Solaris Baseline” on page 132</a>
View details about a baseline installation job.	You must have run a Solaris baseline deployment job or a Solaris baseline compliance analysis job that has successfully completed before you can view details.	<a href="#">“To View a Summary of a Baseline Installation Job” on page 133</a>

## ▼ To Create a Solaris Baseline White List

This procedure uses the profile mechanism to create a white list that contains a baseline and an optional white list.

For information about working with Solaris baselines, see the following:

- [“To Create a Solaris Baseline Black List” on page 130](#)
- [“To Perform a Solaris Baseline Compliance Analysis” on page 131](#)
- [“To Install a Solaris Baseline” on page 132](#)

---

**Note** – The terms update and patch are the same.

---



- 1 **From the Hosts list, select the host or group for which you want to create a baseline white list.**  
Note that the white list *must* contain a baseline and can *optionally* include a list of patches to install.
- 2 **Select the baseline you want to install.**
  - a. **From the Components list, expand the Solaris Baselines category.**
  - b. **Find and expand the dated baseline you want to install.**
  - c. **Select one of the following patch sets:**
    - **Full** – Includes all Solaris patches
    - **Recommended** – Includes Solaris recommended patches and security patches
    - **Security** – Includes only Solaris security patches
  - d. **(Optional) View the contents of the baseline, by choosing Details from the Components menu.**  
The Details window opens.
  - e. **Add the baseline to the Action list by choosing Required from the Components menu.**

---

**Note** – You can select only one baseline to for installation on a host, hosts, group or groups. If you select another baseline for the same host, hosts, group, or groups and choose Required from the Components menu, an error message appears.

---

- **To replace the current baseline with the one you just selected, click OK.**
  - **To use the original baseline, click Cancel.**
- 3 **(Optional) Add one or more patches to the white list.**
    - a. **From the Components list, expand the Patches category.**
    - b. **Find and expand the patch ID range for the patch or patches you want.**
    - c. **(Optional) View a description of the patch.**  
Choose Details from the Components menu.  
The Component Information window opens. This window presents information on the following tabbed pages:
      - **General tab** – Shows the patch ID, the size of the patch, and the platform for which the patch was created.
      - **Incident tab** – Shows the patch ID, the patch type, and a URL to the patch README file.
      - **Dependencies tab** – Shows any patches that depend on the one you selected.
      - **Installed tab** – Shows you the list of hosts on which the patch has been installed.



- 8 Repeat Steps 6 and 7 for each patch you want to add to the black list.
- 9 Click OK to save the policy on the Policies window.

## ▼ To Perform a Solaris Baseline Compliance Analysis

This procedure describes how to perform a Solaris baseline compliance analysis. The result of this analysis is a list of the number of patches to be installed to bring it in to compliance with the baseline, the white list, and the black list you specify.

**Before You Begin** You must have a Solaris baseline white list and an optional black list to perform this task. For more information about creating these lists, see the following:

- [“To Create a Solaris Baseline White List” on page 128](#)
- [“To Create a Solaris Baseline Black List” on page 130](#)

---

**Note** – The terms update and patch are the same.

---

- 1 Open the New Job window by choosing New from the Jobs menu.
- 2 Select Simulate to run the job in simulation mode.
- 3 Open the Task Editor window by clicking the Add (New) Task button.
  - a. Choose your white list from the Profiles drop-down menu.
  - b. (Optional) Choose your black list from the Policy drop-down menu.
  - c. Open the Select Hosts window by clicking the Host Select button.
  - d. Select the host or group, click the Add button (right-facing arrow) to add it to the list, and then click OK.
  - e. Click OK to save the task.
- 4 Repeat Step 3 for each baseline compliance analysis task you want to run as part of this job.
- 5 (Optional) Click the Options tab to specify the task execution parameters.

If you plan to have more than one task in this job to run analyses against more than one baseline, you can select Parallel to run the tasks simultaneously. By default, tasks are run sequentially.
- 6 Click OK to submit the job.

- 7 (Optional) View the progress of the job running on the host by choosing Host Progress from the Host list.
- 8 View the job summary when the job completes.  
For more information, see [“To View a Summary of a Baseline Installation Job”](#) on page 133.

## ▼ To Install a Solaris Baseline

This procedure describes how to deploy a Solaris baseline to selected Solaris hosts.

**Before You Begin** You must have a Solaris baseline white list and an optional black list to perform this task. For more information about creating these lists, see the following:

- [“To Create a Solaris Baseline White List”](#) on page 128
- [“To Create a Solaris Baseline Black List”](#) on page 130

---

**Note** – The terms update and patch are the same.

---

- 1 Open the New Job window by choosing New from the Jobs menu.
- 2 Select Deploy to deploy the baseline to the selected hosts.
- 3 Open the Task Editor window by clicking the Add Task button.
  - a. Choose your white list from the Profiles drop-down menu.
  - b. (Optional) Choose your black list from the Policy drop-down menu.
  - c. Open the Select Hosts window by clicking the Host Select button.
  - d. Select the host or group, click the Add button (right-facing arrow) to add it to the list, and then click OK.
  - e. Click OK to save the task.
- 4 Repeat Step 3 for each baseline deployment task you want to run as part of this job.
- 5 Click OK to submit the job.
- 6 (Optional) View the progress of the job running on the host by choosing Host Progress from the Host list.

**7 View the job summary when the job completes.**

For more information, see “[To View a Summary of a Baseline Installation Job](#)” on page 133.

**8 (Optional) Perform a profile compliance check of the selected hosts.**

See “[To Check Profile Compliance](#)” on page 74.

---

**Note** – Perform this check *only* if you used a profile to install the baseline and white list. If you also used a policy to specify a black list, this check will show the host to be non-compliant.

---

## ▼ To View a Summary of a Baseline Installation Job

**Before You Begin** You must have run a Solaris baseline deployment job or a Solaris baseline compliance analysis job that has successfully completed.

- “[To Perform a Solaris Baseline Compliance Analysis](#)” on page 131
- “[To Install a Solaris Baseline](#)” on page 132

---

**Note** – The terms update and patch are the same.

---

**1 Select the job for which you want view a summary from the Jobs list.****2 Open the Job Summary window by choosing Summary from the Jobs menu.****3 View the following summary information for each task:**

- **Host** – Shows the host name on which you ran the task.
- **Distribution** – Shows the operating system and platform architecture of the host.
- **Task** – Shows the task type.
- **Number of Changes** – Shows the number of changes made or will be made to the host.

**4 (Optional) View details about a task.****a. Select a task from the table, and click the View Changes button.**

The Host Changes Report window opens.

**b. Select a patch ID from the table, and click the Component Info button.**

The Incident Information window opens.

**c. View information about the patch by clicking one of the following tabs:**

- **README** – Shows the URL to the patch README file.
- **General** – Shows the patch ID, patch category, and release date.
- **CVE ID** – Shows the CVE ID of the patch.

- **Package** – Shows the packages modified by the patch.
  - **Obsolete** – Shows the patches that this patch renders obsolete.
- d. **Click Close to dismiss the Incident Information window.**
  - e. **Click Close to dismiss the Host Changes Report window.**
- 5 **Repeat Step 4 for each task for which you want to view details.**
  - 6 **Click Close to dismiss the Job Summary window.**

# System Management Profiles

---

This chapter describes the predefined profiles and how you can deploy them to run system-wide checks and remote restarts.

The following profiles are described:

- Check Bugs Fix
- Check Security
- Check System
- Check Withdrawn Patches
- Local Software Review
- Perform Restart
- Perform Restart + Reconfigure
- Upgrade All Components

The procedures in this chapter include some advanced features, which will be explained in more detail in later chapters. They are given here to help you get started with execution of predefined profiles even before you are familiar with the details of Sun Update Connection – Enterprise environment management.

This chapter covers the following topics:

- “Terms” on page 136
- “Predefined Profiles” on page 136
- “Creating Policies for Predefined Profiles” on page 138
- “Running Predefined Profiles” on page 140
- “Running Restart Predefined Profiles” on page 143
- “Confirming Actions” on page 142
- “Handling Large Jobs” on page 145

# Terms

This chapter uses the following terms:

Conflict	When different components need different dependent components and these dependencies cannot exist on the same system together (for example, two different packages need two different versions of the same library), there is a conflict. Sun Update Connection – Enterprise solves such conflicts by finding a version of the dependent components that works for both base components.
Dependency	Most Linux and Solaris components depend upon the prior installation of existing libraries or other packages to operate in known system configurations. These other components are <i>dependent components</i> , or dependencies.
Predefined Profile	Set of compliance mappings provided with Sun Update Connection – Enterprise that performs a full-system check and fix, a remote restart, or a remote restart with reconfiguration.

## Predefined Profiles

Sun Update Connection – Enterprise provides various profiles already predefined. While you will be creating profiles that define system functions (profiles for web servers, printer servers, and so on), the predefined profiles check complete systems for specific issues or preform restarts on the remote hosts.

The following table briefly describes the predefined profiles.

Profile Name	Finds, and Fixes on Deploy	Sun Update Connection – Enterprise Actions
Check System	Dependencies	Installs or upgrades missing dependent components, according to the rules of the knowledge base of the selected distribution.
Check Security	Software to be patched against security holes	Every security instance known to the knowledge base of the selected distribution is checked, to see whether it can fix installed components.
Check Bug Fixes	Software to be patched for known bugs	Every bug fix patch known to the knowledge base of the selected distribution is checked, to see whether it can fix installed components.



Profile Name	Finds, and Fixes on Deploy	Sun Update Connection – Enterprise Actions
Local Software Review	Local software that is in Software, rather than Local RPMs or Local PKGs, to be replaced with a same-named certified software	Your local components are checked against the knowledge base of the selected distribution.  This profile helps you find the local components under Software.  If you confirm the actions of this profile, Sun Update Connection – Enterprise replaces the local version with a certified version.
Upgrade All Components	Software to be upgraded	Every installed component is checked against the knowledge base of the selected distribution, to see if installed components can be upgraded.
Check withdrawn patches (relevant to Solaris systems only)	Patches and updates that have been withdrawn by the vendor and should not be used	Installed patches are checked against the knowledge base of the selected distribution to see if the vendor has withdrawn the patch. A patch might be withdrawn due to a better patch or version making the withdrawn one obsolete, or due to bugs in the patch itself. Sun Update Connection – Enterprise will upgrade to the correct patch, if available. Or if not, downgrade back to the vendor supported version.
Perform Restart	Restarts selected hosts	If an action in a job needs a restart to have the deployment applied to the computer, you will see a reminder in the job To Do list that you should run a restart profile.  The Notifications category in the tree will show which hosts should be restarted.
Perform Restart + Reconfigure (relevant for Solaris systems only)	Restarts Solaris hosts and performs specific post-installation reconfigurations	If an action in a job needs a restart to have the deployment applied to the computer, you will see a reminder in the job To Do list that you should run a restart profile.  The Notifications category in the tree will show which hosts should be restarted.

## Policies for Predefined Profiles

You can deploy, or simulate deployment, of predefined profiles in jobs. When setting up the job, you include a policy. A policy determines how the job handles dependencies. During predefined profiles, all components are considered dependencies, so the policy determines the trends and automation of the deployment of the predefined profile as a whole.

## Creating Policies for Predefined Profiles

In this procedure you create a policy designed to be used in jobs that deploy predefined profiles.

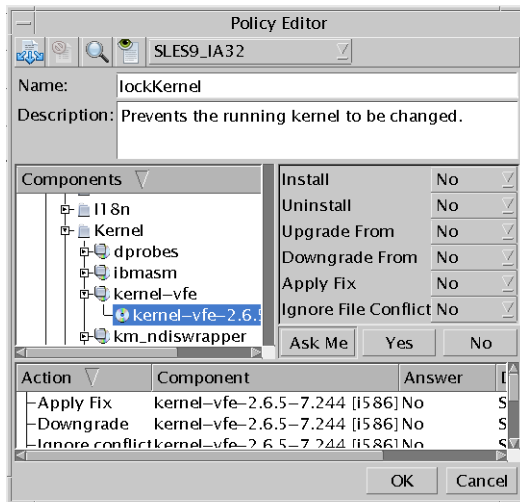
### ▼ To Create a Policy for Predefined Profiles

- 1 Log in as any user.
- 2 Do one of the following:
  - From the tool bar, click the Policies button.
  - From the Tools menu, choose Policies.

The Policies window opens.

- 3 Click the New button.

The Policy Editor window opens.



- 4 Select a distribution and type a name for the policy.

- 5 Set the policy according to the policy recommendations.

See [“Policy Recommendations for Predefined Profiles”](#) on page 139.

To set a policy, select an item in the Components list and then select a predefined answer (Ask Me, Yes, No) for the listed Sun Update Connection – Enterprise actions (Install, Uninstall, Upgrade From, Downgrade From, Apply Fix, Ignore File Conflict).

- 6 To make this policy applicable to multiple distributions, click the Multi Distro button.**  
See “To Align Component Settings for Multiple Distributions” on page 210.

**7 Click OK.**

The Policy Editor window closes. The new policy is listed in the Policies window.

## Policy Recommendations for Predefined Profiles

To automate component handling of jobs that deploy a predefined profile, set Yes policies to Software or to Local for specific deployment actions.

TABLE 7-1 Automating Predefined Profiles

Profile Name	Component	Set YES to:
Check System	Software and Local	Apply Fix
Check Security	Software and Local	Apply Fix
Check Bug Fixes	Software and Local	Apply Fix
Upgrade All Components	Software and Local	Upgrade From
Check withdrawn patches	Software and Local	Apply Fix, Upgrade From, Downgrade From

- **Local Software Review Policy Recommendations**

Fully automating the Local Software Review predefined profile without checking what the components are that you are going to replace, is not the best handling method. A better method is to check the local components and set a relevant policy.

When you run the Local Software Review, Sun Update Connection – Enterprise finds the complete list of uncertified components (NCOs) that are listed under Software, rather than under Local RPMs or Local PKGs. This placement is done if you upload an NCO that has the same name as a certified component.

If you are ready to replace local software with certified software (have better deployment rules) from the universal server, set Upgrade From and Downgrade From to Yes.

- **No Policies for Restart Profiles**

Perform Restart and Perform Restart and Reconfigure are different from the profiles. These are not tests. They do not perform actions on individual components, so no policy is relevant.

- **Ignore File Conflicts Policy**

Be wary of setting a Yes policy to the Ignore File Conflicts action. This action needs you to take responsibility for results of forcing an action, regardless of the knowledge base rules. It is recommended that you always leave this action as Ask Me.

- **Locking Components from Change**

If you automate a job with the policy recommended here, you do not have to set the policy to all Software, all Local RPMs, or all Local PKGs. In the components list, set a general policy on categories. Find the package groups or versions that you want to lock from change and give them a No policy. All packages in a category inherit the policy of the parent, except for those with a different policy.

## Creating a Policy With the CLI

The CLI command to create a policy for a predefined profile is the same as for creating any policy, `-aca`. The parameter that sets a policy for Apply Fixes is `-fix`. The following example shows how to set Apply Fixes to Yes for all Software. See [“Add Policy Attribute \(-aca\) Command” on page 271](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
echo -n "Enter the name of a policy or create a new one:"
read policyName
uce_cli -aca -C "$policyName" -T "Software" -fix yes -u "$user" -p "$password"
```

## Predefined Profiles in Jobs

Jobs that include predefined profiles function differently than other Complex Jobs. The following tasks explain how to set up and handle these jobs.

## Running Predefined Profiles

### ▼ To Create Job with a Predefined Profile

In this procedure you deploy predefined profiles on managed hosts, with a policy you created in the previous task. You will use the Complex Jobs feature, but this procedure will give the simplest steps. If you are restricted to run simulation jobs only, you can perform this task by using Simulate instead of Deploy.

---

**Note** – The Check System predefined profile, especially, should be run before you use a host as a source in a clone job (see [“Cloning Inventories” on page 158](#)), to ensure that you are not cloning a host with dependency issues.

---

**Before You Begin** Before you begin a job on a Solaris machine, make sure the PKG deployment preferences are appropriate for your local needs. See [“Host Preferences – PKGs” on page 301](#).

**1 Do one of the following:**

- From the tool bar, click the New Job button.
- From the Jobs menu, choose New.

The New Job window opens.

**2 Type a name for the job.****3 Choose a job mode:**

- To discover the list of issues, without touching the hosts, check Simulate.
- To discover and fix the issues by changing host inventories, check Deploy.

(If you are restricted to run simulation jobs only, the mode options are disabled. The job will be run in simulate mode.)

**4 Type a free-text description.****5 Open the Task Editor.****6 Type a name for the first task of the job.****7 In the Profile drop-down list, select one of the Predefined Profiles.****8 Click the Hosts button next to the Hosts field.**

The Select Hosts window opens.

**9 Select a host or group and click the Add button.**

The host or group is added to the Selected Hosts list.

Add as many hosts and groups as you want.

**10 Click OK.**

The Hosts window closes. Selected hosts are displayed in the Hosts field of the Tasks tab.

**11 In the Policy drop-down list, select a policy:**

- Select the Always ask me policy to be asked for confirmation before anything is done. This also allows you to see the full list of actions and to break up a large job if needed.
- Select a policy that you created (Yes to Apply Fixes, for example), if you want the job to be done automatically, without your confirmation.

**12 Click the Add Task button.**

The task name appears in the tasks list.

If you want to run multiple predefined profiles on the selected hosts, you can create more tasks, each with a different profile. However, it is recommended that you run only one predefined profile the first time, to ensure that the job is not so big that it times out.

### 13 Click OK.

The New Job window closes and the job begins. See the Jobs panel in the main window.

## Example 7-1 Running a Predefined Profile With the CLI

The CLI submit job command is used to deploy or simulate a predefined profile. The example given here deploys the Check System profile with the Always ask me policy. See [“Submit Job \(-sj\) Command” on page 274](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo -n "Type a name for this job:"
read jobName
echo "The list of hosts is:"
uce_cli -lah -u "$user" -p "$password"
echo "The list of groups is:"
uce_cli -lg -u "$user" -p "$password"
echo "Do you want to do this check on a host or on a group (h | g)?"
read hostgroup
echo "Copy the name of a host or group to be checked"
read selected

uce_cli -sj -j "$jobName" -P "Check system" -C "Always ask me" -$hostgroup "$selected" \
-us -dp -u "$user" -p "$password"
```

## Confirming Actions

### ▼ To Confirm Actions

If you selected the Always ask me policy, or if the job found actions to do on dependencies for which you did not set a policy, the job pauses, waiting for you to confirm or deny suggested fixes.

---

**Note** – If your user account has Notify when: Job pauses selected, you will receive an email when you need to confirm actions to continue a job. Therefore, you can schedule the predefined profile to run during idle hours and confirm the actions when you receive notification. See [“To Create a Full-Permission User Account” on page 47](#) for details on notification, and [“To Create a Feature-Rich Complex Job” on page 203](#) for details on scheduling jobs.

---

- 1 Make sure the Jobs panel of the main window is available: from the View menu, choose Jobs.**
- 2 From the Jobs list (left-hand frame), click a job name with the confirmation icon.**  
The tasks of the job appear in the Tasks list (middle frame).
- 3 Select a task name with the confirmation icon.**
- 4 Do one of the following:**
  - From the tool bar, click the Confirmation button.
  - Right-click the selected task and choose Confirmation.
  - From the Jobs menu, choose Tasks -> Confirm.

The Confirmation window opens and shows suggested actions.
- 5 If a confirmation question deals with a component for which you need more information, select the question and click the Details button.**  
The Component Information window opens.
- 6 Take note of relevant data and then click OK to close the Component Information window and return to the Confirmation window.**
- 7 In the Confirmation window, select Yes to the questions you confirm and No to those you do not want Sun Update Connection – Enterprise to perform on the selected hosts.**
  - If the job was in Deploy mode, the confirmed actions are done on the selected hosts.
  - If the job was in Simulate mode, the actions and results are calculated, giving you an accurate estimation of the required changes.

## Running Restart Predefined Profiles

### ▼ To Create a Job with a Restart Predefined Profile

In this procedure you run the predefined profiles that restart remote hosts. This procedure starts with the Notifications category in the Inventory panel.

**Before You Begin** Before you begin a job on a Solaris machine, make sure the PKG deployment preferences are appropriate for your local needs. See [“Host Preferences – PKGs” on page 301](#).

- 1 In the main window, make sure the Inventory panel is visible by choosing Inventory from the View menu.**
- 2 From the Hosts list, select All Hosts and from the Component list, select Notifications or Restart.**  
If Restart is marked Installed, there are hosts that should be restarted.
- 3 To see the names of these hosts, right-click Restart and then click Details.**  
The Component Information window opens. The Installed tab lists hosts that need a restart. Make a note of these hosts and close the Component Information window.
- 4 From the tool bar, click the New Job button.**  
The New Job window opens.
- 5 Type a name and description for the job.**
- 6 Click the Deploy radio button.**
- 7 Open the Task Editor.**
- 8 Type a name for the task of the job.**
- 9 In the Profile drop-down list, select Perform Restart (or Perform Restart + Reconfigure, for Solaris hosts, and only if the notification mentioned a needed reconfiguration).**
- 10 Click the Hosts button next to the Hosts field.**  
The Select Hosts window opens.
- 11 Select the hosts you noted from the Notification or Restart list and click Add.**  
You can add any host that you want to restart, even if it was not marked in Notifications.
- 12 Click OK.**  
The Hosts window closes. Selected hosts are displayed in the Hosts field of the Tasks tab.
- 13 Click the Add Task button.**  
The task name appears in the tasks list.
- 14 Click OK.**  
The New Job window closes and the job begins. The selected hosts are restarted.



## Handling Large Jobs

Jobs that execute predefined profiles can build up a list of hundreds of actions to do. This procedure explains how to handle such large jobs, by breaking up a large system-wide fix into smaller, faster jobs. Use this procedure if you get a confirmation list with many actions (for example, more than 30 action items). It is applicable only for predefined profiles; in other jobs, if you answer No to a confirmation question, the Dependency Resolver will search for a different solution or fail the job.

### ▼ To Handle Large Predefined Profile Jobs

- 1 In the Confirmation window, select Yes for some actions and No to others.
- 2 Click OK to start the job.
- 3 Wait for the job to finish, as shown by the Finished icon in the Jobs list, and then select it.
- 4 Do one of the following:
  - From the tool bar, click the Rerun Job button.
  - Right-click the job name and choose Run.
  - From the Jobs menu, choose ReRun.

The Rerun window opens.

- 5 Give the job a new, meaningful name and description.
- 6 Check the Deploy mode.
- 7 Click OK.

The predefined profile runs again. In the Confirmation window of the continuation job, you will see the actions to which you answered No in the previous run of this task.
- 8 Answer Yes or No to the actions in the list and click OK to run the job.

You can run a predefined profile in as many jobs as you want.



# Inventories

---

This chapter describes the details of inventories and explains how to control hosts through management of individual components.

The following topics are covered:

- “Terms” on page 147
- “Understanding Inventories” on page 148
- “Inventory Jobs” on page 154
- “Inventory Jobs with Local Scripts and Files” on page 166

## Terms

This chapter uses the following terms:

Cost-Effective	Manner in which the dependency resolver decides which solution is optimal for a host; cost effectiveness is measured in number of deployment changes needed by any one solution to fulfill a given request.
dependency resolver (DR)	Set of patented algorithms to describe a solution for a job. Initiated by the agent application when a job is received.
Deploy Mode	Job mode that can change host inventory.
Inventory	(1) List of components installed on a managed host. (2) List of components on the universal server.
Knowledge Base	Sub-system of the Sun Update Connection – Enterprise system dependency server, acts as a proxy server for the universal server, keeping dependency rules for CO deployment on managed hosts.  A local knowledge base is a private, on-site only, collection of NCO listings and their deployment rules as generated by the Local Expansion technology.

Policy	Set of confirmation rules for the implementation of the dependency resolver and level of automation of dependency handling.
Simulate Mode	Job mode that produces a test of what would have happened if the job had been in deploy mode.

## Understanding Inventories

Sun Update Connection – Enterprise provides access to the inventory of certified components (COs) in the universal server. Each supported distribution has its own knowledge base inventory.

You also have access to the inventory of every managed host, both COs and Non-Certified Components (NCOs). The agent on a host scans the machine and brings you an inventory of all installed components.

You can view the inventory of a managed host within the inventory of the universal server, quickly seeing what can be upgraded, installed, replaced, or uninstalled.

The inventory is displayed in the Components list layout. The levels are:

- **Category** – software components grouped together by function
- **Package group** – Holder of versions of a software
- **Package** – Points to one software component in the knowledge base

An inventory can contain different types of packages. The types are:

- **Certified Objects (CO)** – Under the Software category. COs are components certified by the Certification Lab. In Solaris, Software includes PKGs from the CDs and Sun Freeware.
- **Non Certified Objects (NCO)** – Under the Local RPMs and Local PKGs categories. NCOs are private, proprietary, or third-party components.
- **Local Files** – Under the Local/Pre-actions, Post-actions, Macros, Probes, and Configuration files categories. Local Files are private files, scripts, executables, binaries that you use often on multiple hosts.

Inventory jobs focus on the component level. You select a component from the inventory and then apply a setting to it. The component settings are described in the following tables.

**TABLE 8-1** Inventory Component Settings on Packages (RPM, PKG, NCO, Local File)

Setting	Result if Package Installed	Result if Package Not Installed
Required	Nothing is done.	DR finds solution to install it.
Not Allowed	DR finds solution to uninstall it.	Nothing is done.

**TABLE 8-1** Inventory Component Settings on Packages (RPM, PKG, NCO, Local File) *(Continued)*

Setting	Result if Package Installed	Result if Package Not Installed
Upgrade	If there is a newer version for an installed package, the package is upgraded.  If there is more than one version newer than this package, the most cost-effective version is chosen.	Nothing is done.

**TABLE 8-2** Inventory Component Settings on Categories and Package Groups

Setting	Result if Packages Installed	Result if Packages Not Installed
Required	If at least one package is installed, nothing is done.	If no package in category/group is installed, the one that is most cost-effective is installed.
Not Allowed	All packages within category/group are uninstalled.	If no package in category/group is installed, nothing is done.
Upgrade	All installed packages within category/group are upgraded if newer versions exist.	Nothing is done.

For example, you want to install the `cURL` utility on your FTP servers. You select the FTP group in the Hosts list. In the Components list, you select `curl` and apply the Required setting to it. You right-click the action and choose Run on Selected Hosts. The job installs `curl` on the FTP hosts that do not have it yet. It also makes sure that a list of dependent components is installed.

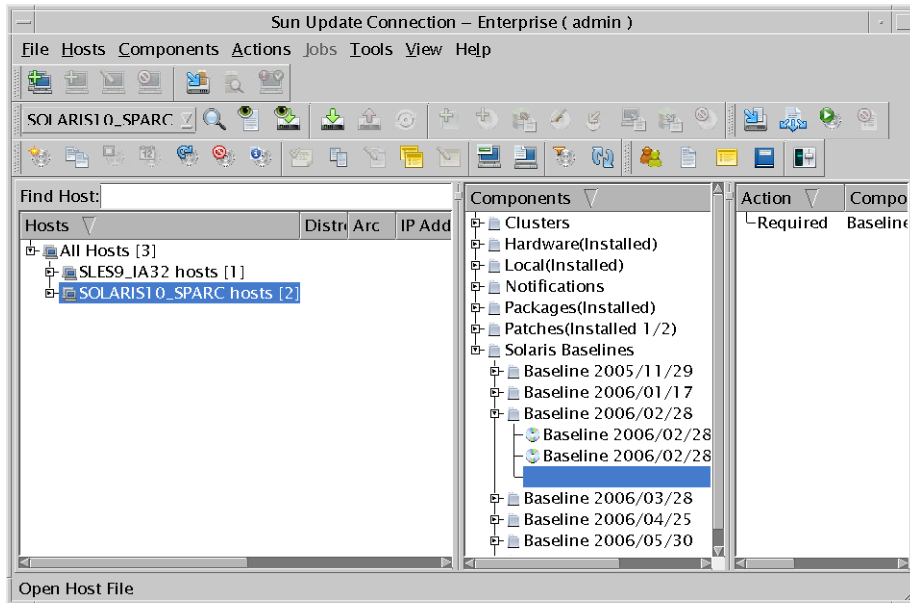
You can see the list of dependencies. Open the Inventory window, right-click the `curl` version you want to install and choose Details. The Dependencies tab of the Component Information window lists the components that are required by `curl`.

## Viewing Inventories

### ▼ To View the Inventory of the universal server

Each agent discovers the installed inventory on its managed host and sends it to the dependency manager (DM), which updates the console. This procedure describes the Inventory panel of the console's main window.

- 1 From the View menu, make sure Inventory is selected.



- 2 From the drop-down list on the tool bar, select a distribution-architecture.

The Components list shows the components of the selected distribution.

- 3 Make sure no host is selected in the Hosts list, and that the Show Installed Components button is deselected.

The Components list shows all components in the knowledge base of the selected distribution.

- 4 To see more information about a selected component, do one of the following:

- From the tool bar, click the Details button.
- Right-click the selection and choose Details.
- From the Components menu, choose Details.

The Component Information window opens.

## ▼ To View the Installed Inventory of Selected Hosts

- 1 From the View menu, make sure Inventory is selected.
- 2 In the Hosts list, select a managed host, group, or multiple hosts and groups (use Shift or Control to select multiple items).
- 3 From the drop-down list in the tool bar, select a distribution-architecture.  
The Components list shows the components of the selected distribution.

#### 4 Choose the type of list you want to view:

- **Filtered** – Click the Show Installed Components button, if you want to see only those components which are installed on the selected managed hosts.
- **Complete** – Leave this button deselected, if you want to see all components available for download.

### Further Understanding

- If you are a user with permissions restricted to specific groups, you see only the hosts of your authorized groups.
- Components that are Solaris patches might have a Notifications category in the Rules tab of the Component Information window, which explains if the host must be restarted (and possibly reconfigured) to apply the patch or to complete a successful installation of the patch.
- If you have a local, private version of a certified component, it is not listed under Local, but under Software. The name of your component is *namebuild-date*. You can use the Local Software Review predefined profile to find these components (see “Predefined Profiles” on page 136).
- Some distributions contain components with the same name on multiple architectures. In the Inventory display, these components are named *namearchitecture*
- Components are marked with different installation indicators:
  - **Installed** – At least one package of this package group or category is installed on at least one selected managed host
  - **No Installed mark** – Component is not installed on any selected managed host but is available for installation from the universal server
  - **A ratio** – Some, but not all, selected hosts have this component installed
    - The first number shows how many of the selected hosts have this component installed
    - The second number shows how many hosts were selected
 For example, you select 105 hosts from different groups. The System Environment component is marked with (Installed 93/105). 93 of the selected hosts have System Environment components installed on them.

### Viewing an Inventory with the CLI

The CLI command to view an inventory is for one specific host at a time. It outputs package names only, not categories or package-groups. See “List Host Inventory (-lhi) Command” on page 259.

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
```

```
echo "The list of hosts is:"
uce_cli -lah -u "$user" -p "$password"
echo -n "Copy the name of the host whose inventory you want to see:"
read hostname

uce_cli -lhi -h "$hostname" -u "$user" -p "$password"
```

## Saving Inventories

### ▼ To Save an Inventory

In this procedure, you save an inventory of a host or of a group. Saving an inventory allows you to restore a host to a previous state if needed, or to clone the inventory of a host or a group onto another host (see [“Restoring Managed Hosts” on page 161](#)). Sun Update Connection – Enterprise automatically saves inventories before deploying a job on a host. Automatic inventories have this naming convention:

- For a host: *hostname\_Job\_jobname\_yymmdd\_time*
- For a group: *groupname\_Job\_jobname\_yymmdd\_time*

Use this procedure to save an inventory record with a meaningful name.

**Before You Begin** Before saving an inventory, you should run the Check System predefined profile on the host or group. This will ensure that the saved inventory does not have dependency issues. If you will be managing Solaris hosts, you should run the Check Withdrawn Patches profile. This will replace withdrawn Solaris patches with appropriate operating software. See [Chapter 7](#).

- 1 From the Hosts list, select a single host or a group.**
- 2 Do one of the following:**
  - From the tool bar, click the Save Inventory to File button
  - Right-click the selected host or group and choose Save Inventory ->To File.
  - From the Hosts menu, choose Save Inventory ->To File.  
A dialog box opens with the date entered in the text-entry box.
- 3 Type a name for this inventory and then click OK.**

### Example 8–1 Saving a Host Inventory with the CLI

The CLI command to save host inventory saves a record of the inventory of a single host. See [“Save Host Inventory \(-shi\) Command” on page 275](#).



```

#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of hosts is:"
uce_cli -lah -u "$user" -p "$password"
echo -n "Copy the name of the host whose inventory you want to save:"
read hostname
echo -n "Type a name for the inventory record:"
read savedInven

uce_cli -shi -h "$hostname" -s "$savedInven" -u "$user" -p "$password"

```

### Example 8-2 Saving a Group Inventory with the CLI

The CLI command to save group inventory saves a record of the inventory for each host of the group. This does not create a composite record. It creates a separate file for each host. The files are named according to this convention *hostname\_suffix\_mmdyyytime*. You create the suffix, a name or number to identify this as a group inventory save. See [“Save Group Inventory \(-sgi\) Command” on page 276](#).

```

#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of groups is:"
uce_cli -lg -u "$user" -p "$password"
echo -n "Copy the name of the group whose hosts inventories you want to save:"
read groupname
echo -n "Type a group suffix for the inventory saves:"
read suffix

uce_cli -sgi -g "$groupname" -sn "$suffix" -u "$user" -p "$password"

```

# Inventory Jobs

You can manipulate inventory components to create quick jobs. Use Inventory jobs to install, uninstall, upgrade, or downgrade specific components.

Although Inventory jobs are quickly created and deployed, more control and features are available with Complex jobs, which options offer more efficient environment management. For more details, see [Chapter 11](#).

## Creating Inventory Jobs

### ▼ To Change the Inventory of a Host or Group

This procedure explains how to create an inventory job to manage the installed components of hosts.

Before you begin a job on a Solaris machine, make sure the PKG deployment preferences are appropriate for your local needs. See “[Host Preferences – PKGs](#)” on page 301.

**1 From the View menu, make sure Inventory is selected.**

**2 From the drop-down list on the tool bar, select a distribution-architecture.**

The Components list changes to display components of the selected distribution.

**3 In the Hosts list, select groups or hosts.**

**4 In the Components list, select a component.**

**5 Assign an action to the selected component.**

Do one of the following:

- From the tool bar, click the Required, Not Allowed, or Upgrade button.
- Right-click the selected component and choose Required, Not Allowed, or Upgrade.
- From the Components menu, choose Required, Not Allowed, or Upgrade.

See [Table 8-1](#) for more explanations of these options.

The action-component setting appears in the Actions list.

**6 Enter as many component actions as you want.**

**7 To make the inventory job applicable to hosts of different distributions:**

- To select specific components from different distributions, change the selection of the drop-down list of distributions in the tool bar. Find the relevant components and add the action settings to the Actions list.

- To let Sun Update Connection – Enterprise find components from other distributions that are comparable to the ones you have in the Actions list, click the Multi Distribution button (see [“To Align Component Settings for Multiple Distributions”](#) on page 210).

**8 Do one of the following:**

- From the tool bar, click the Run Job button.
- Right-click in the Actions list and choose Run on Selected Hosts.
- From the Actions menu, choose Run on Selected Hosts.

The Run Job window opens.

**9 Give the job a name and an optional, free-text description.**

**10 Select a mode for the job:**

- **Deploy** – Do the actions on the selected hosts
- **Simulate** – Simulate the actions to estimate job time and full job actions  
(If you have restricted permissions to run simulation only jobs, these options are disabled. The job will be run in simulate mode.)

**11 Click OK.**

The Run Job window closes. The job starts.

## Comparing Inventories

### ▼ To Compare Inventories

The Inventory Comparison feature shows the differences of installed components between two hosts. The hosts must be of the same distribution-architecture, both in console and in CLI commands.

Comparing inventories offers the following features:

- Check that managed hosts of same functions have same software.
- Run a job that replicates the software deployment of one host to another.
- Rollback a managed host to a saved inventory.
- Compare the inventory of a host with the inventory of a group of hosts. Make a single host like the rest of the hosts in a group.

There are different types of inventories to choose from. The following table describes each type.

- **Current Inventory** – Installed software as-is
- **Automatically Saved Inventory** – Before a job, Sun Update Connection – Enterprise automatically saves a record of the inventory of selected hosts indicated by AU: at the beginning of the inventory name

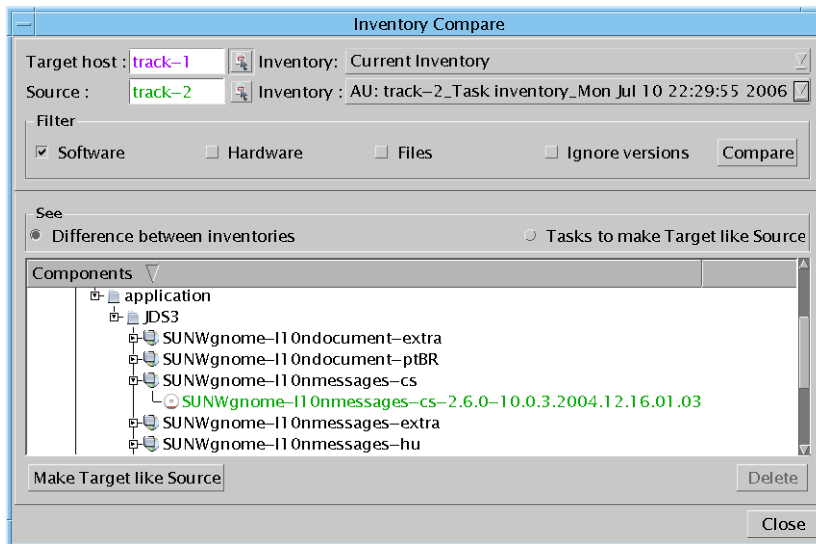
- **Saved Host Inventory** – User initiated saved record of the inventory of a selected host
- **Saved Group Inventory** – User-initiated saved record of the inventory of a group; a composite list of software installed on all hosts of the group

**Before You Begin** Before comparing inventories, you should run the Check System profile on the host or group. This will ensure that the source inventory does not have dependency issues. If you will be managing Solaris hosts, you should run the Check Withdrawn Patches profile. This will replace withdrawn Solaris patches with appropriate operating software. See [Chapter 7](#).

In addition, if you will be comparing Solaris machines, you should edit the PKG settings (see “[Host Preferences – PKGs](#)” on page 301) to ensure that the deployment operates as expected.

- 1 **Make sure the Inventory panel is open in the main window. From the View menu, choose Inventory.**
- 2 **Do one of the following:**
  - From the tool bar, click the Compare Inventories button.
  - Right-click in the Hosts list and choose Compare Inventories.
  - From the Hosts menu, choose Compare Inventories.

The Inventory Comparison window opens.



- 3 **Click the Host Select button to the right of the Target host field.**  
The Host Selection window opens.
- 4 **Select the host you want to change and then click OK.**  
The Host Selection window closes. The selected host name appears in the Target host field.

**5 From the Inventory drop-down list, select a stored inventory or the current inventory.**

If you want to create a job from the comparison, select Current Inventory.

**6 Click the Host Select button to the right of the Source field.**

The Host Selection window opens.

**7 Select the managed host you want to use as the source and then click OK.**

The Host Selection window closes. The selected host name appears in the Source field.

**8 From the Inventory drop-down list, select a saved inventory.**

(If the source host is different from the target host, you can select the current inventory.)

**9 In the Filter section, select the types of components you want to be in the comparison:**

- Software packages
- Hardware drivers
- Configuration Files
- whether you want the comparison to ignore differences in Versions of the same packages

**10 Click Compare.**

The results of the inventory comparison are displayed.

**11 Under the See section of the Inventory Comparison window, select Tasks to Make Target like Source.**

If the results include at least one difference between the selected inventories which can be converted to an action (differences in configuration files cannot be converted), more features are available. See the following procedures.

**Example 8–3 Comparing Inventories with the CLI**

The compare host inventories CLI command outputs two lists: what is installed in the source inventory and not in the target inventory, and what is in the target inventory and not in the source inventory.

Both hosts must be of the same distribution. Both the source host and the target host may be the same host, but the inventories must be different.

If you do not use the -s or the -ts parameters, the current inventories are used by default. See [“Compare Hosts and Inventories \(-chi\) Command” on page 277](#).

```
#!/bin/bash
echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
```

```
read password

echo "What distribution are you working on?"
uce_cli -ld -u "$user" -p "$password"
echo -n "Copy the distribution name you want:"
read distroGroup
echo "The list of hosts in this distribution is:"
uce_cli -lgh -g "$distroGroup hosts" -u "$user" -p "$password"
echo -n "Copy the name of the source host:"
read sourcehost
echo -n "Copy the name of the target host:"
read targethost

echo "The list of saved inventories is:"
uce_cli -lss -g "$distroGroup hosts" -u "$user" -p "$password"
echo -n "Copy the name of the source inventory:"
read sourceInven
echo -n "Copy the name of the target inventory:"
read targetInven

uce_cli -chi -h "$sourcehost" -s "$sourceInven" -t "$targethost" -ts "$targetInven" \
-u "$user" -p "$password"
```

## Cloning Inventories

### ▼ To Clone Software Inventory

If the results of a Compare Inventory include differences which can be converted to tasks, and if the target inventory is a Current Inventory of a host, you can make the target inventory like the source inventory. This operation does not dump everything on the target as a traditional clone feature would. It allows for a more secure job. It shows you which components are on the source that are not on the target, and could be installed; and which are on the target which could be uninstalled.

#### 1 Compare a source inventory to the Current Inventory of a target host.

If the source inventory can be cloned onto the target inventory, the Make Target Like Source button is enabled.

#### 2 Click Make Target like Source.

The Run Job window opens.

The actions under Deploy source's inventory on target->Profile Data show the components to be installed, uninstalled, upgraded, or downgraded on the target to make its inventory similar to the source inventory.

You may continue with the job now, if this is the only type of action to be done:

- Comparison is of Linux inventories
- Differences are of software, not Solaris patches
- Tasks are for only install, with no uninstall of Solaris patches

If the tasks displayed in the Run Job window include Maintain target's patches, see [“Patch Management in Solaris Comparisons”](#) on page 159 before continuing with this procedure.

**3 Type a new name for the job.**

**4 Select Deploy or Simulate.**

**5 Click OK.**

The job installs, uninstalls, upgrades, and downgrades components on the target managed host to make its inventory consistent with that of the source.

## Patch Management in Solaris Comparisons

Solaris patches are installed and handled differently than Linux components. An inventory comparison will result in patch comparisons only if the selected inventories have identical software components.

If patches are compared and differences found:

- If the only actions to take on patches are to install them on the target, you may continue the job; return to Step 3.
- If there is at least one patch which should be uninstalled from the target, you should understand implicit patch installations before continuing with the job.

For example, patch \*-05 is installed on a Solaris machine. It is upgraded to patch \*-20. All of the patches between 05 and 20 are implicitly installed. They are not on the machine, but the machine is affected as though they were. If you uninstall 20, you lose those effects and go back to 05; but according to what you have seen, you might believe that 19 should be on the machine.

To handle implicit patch installations, Sun Update Connection – Enterprise will first uninstall the patch that was not in the source and then install a comparable patch seen on the inventory of the source.

You see the following in the Run Job window:

```
Maintain target's patches -> Profile Data ->Install patch
```

## Troubleshooting Clone Inventory Jobs

- Cannot Create Solaris Patch Job
  - **Situation** – The job cannot be created because there are conflicts in patch management actions.

- **Error** – Cannot create job due to patch conflicts.
- **Explanation** – One Solaris patch can affect multiple software. In one job, you could see tasks to both install the patch for one software and uninstall the same patch for another software. This job cannot be done through the Compare Inventory feature.
- Job Too Big
  - **Situation** – If the job contains too many actions, the following message is displayed
  - **Error** – The job exceeds the recommended size of 20 tasks. Do you want to continue?
  - **Explanation** – For every action that is sent as part of a job, more actions are added, to automatically handle dependency issues. If a job contains too many actions, there is a larger possibility that the job will fail on timeout.
  - **Solution** – You can click Continue and try to run the job as is. Or, you can break up the job into smaller ones:
    1. Click Cancel and then delete some of the actions from the panel.
    2. Click Make Target like Source again and run the job.
    3. Create a job to run the remaining actions.

---

**Note** – You can change the default minimum of 20 actions in the Preferences window (see “[Console Preferences – Jobs](#)” on page 299).

---

- No Tasks for Job
  - **Situation** – The job cannot be created because there are no actions, even if the comparison did find some differences.
  - **Explanation** – Some differences in inventory will not be translated into actions. These are the following:
    - Uninstall Local files
    - Install Local Unrecognized files
    - Change hardware support components
  - **Solution** – Rerun the comparison filter. If such components are the only differences between the two inventories, they are actually already very similar.

If you still want to make the managed hosts duplicates of each other, select the Difference between inventories radio button, take note of the list of differences, and create separate jobs to complete the cloning.
- Cannot Locate Software Component
  - **Situation** – The job cannot be created because the components that you selected cannot be located.
  - **Error** – Cannot locate the following components.

Make sure they are added to the Local Components tree.



- **Explanation** – The components that you selected are known because the SDS added them to the knowledge base. However, the software component itself was not uploaded, or was removed from the local machines. Therefore, there is no available software to be installed.
- **Solution** – To add the software component to the knowledge base:
  1. Log into the console as a user with full permissions or as admin.
  2. From the Components list, select Local/Local RPMs or Local/Local PKGs and then click Attach.
  3. In the Attach Target File window, browse to the managed host and path where the software component is stored and then click OK.

## Restoring Managed Hosts

### ▼ To Roll Back an Inventory

After you run a job and decide that the changes are not what you need, you can roll back the component inventory of a managed host to a previously saved inventory. Inventories are saved automatically before job changes, and you can save an inventory on demand (see [“Saving Inventories” on page 152](#)).

- 1 **Make sure the Inventory panel is open in the main window by choosing Inventory from the View menu.**

- 2 **Do one of the following:**

- From the tool bar, click the Compare Inventories button.
- Right-click in the Hosts list and choose Compare Inventories.
- From the Hosts menu, choose Compare Inventories.

The Inventory Comparison window opens.

- 3 **Click the Host Select button to the right of the Target host field.**

The Host Selection window opens.

- 4 **Select the host you want to restore and then click OK.**

The Host Selection window closes. The selected host name appears in the Target host field.

- 5 **From the Inventory drop-down list, select Current Inventory.**

- 6 **Click the Host Select button to the right of the Source field.**

The Host Selection window opens.

- 7 **Select the same managed host you want to restore and then click OK.**

The Host Selection window closes. The selected host name appears in the Source field.

- 8 From the Inventory drop-down list, select the optimal stored inventory of the host or of a group to which the host belongs.
- 9 Filter the inventories for the type that you want to restore, or select all the inventory options.

---

**Note** – If the hosts are Solaris machines, you can rollback only Software or only Patches at one time.

---

**10 Click Compare.**

Check the results of the inventory comparison. If the differences between the inventories can be converted to component management tasks, the Make Target like Source button is enabled.

**11 Click Make Target like Source.**

The Run Job window opens.

**12 In the Run Job window, select Deploy and then click OK.**

The restore job begins.

If you are a user with restricted permissions to run only simulation jobs, you do not have this option.)

#### **Example 8–4 Restoring a Host with the CLI**

The CLI command `submit compare job` can clone the inventory (or part of it) from one host or saved inventory to another host. It can also restore a host to a previously saved inventory. This example shows a restore inventory job. See [“Submit Compare Job \(-scj\) Command” on page 278](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "What distribution are you working on?"
uce_cli -ld -u "$user" -p "$password"
echo -n "Copy the distribution name you want:"
read distroGroup
echo "The list of hosts in this distribution is:"
uce_cli -lgh -g "$distroGroup hosts" -u "$user" -p "$password"
echo -n "Copy the name of the host to restore:"
read host

echo "The list of saved inventories is:"
uce_cli -lss -g "$distroGroup hosts" -u "$user" -p "$password"
echo -n "Copy the name of the inventory to which $host is be restored:"
read sourceInven
```

```
uce_cli -scj -h "$host" -s "$sourceInven" -t "$host" -j "Restore $host" -C "Always ask me" \
-dp -u "$user" -p "$password"
```

## Saving Inventory Settings as Profiles

### ▼ To Save Inventory Settings as a Profile

Inventory jobs allow you to quickly manage hosts based on specific components. You can also manage hosts using Complex Jobs (see [Chapter 11](#)), which allow for more features in one management task. To do this, you need a profile. In this procedure, you save a inventory action list as a re-usable profile.

- 1 Make sure the Inventory panel is open in the main window by choosing Inventory from the View menu.**
- 2 From the drop-down list on the tool bar, select a distribution-architecture.**  
The Components list changes to display components of the selected distribution.
- 3 In the Components list, select a component.**
- 4 Assign an action to the selected component.**  
Do one of the following:
  - From the tool bar, click the Required, Not Allowed, or Upgrade button.
  - Right-click the selected component and choose Required, Not Allowed, or Upgrade.
  - From the Components menu, choose Required, Not Allowed, or Upgrade.  
The action-component setting appears in the Actions list.
- 5 Enter as many component settings as you want.**
- 6 To make the inventory job applicable to hosts of different distributions:**
  - To select specific components from different distributions, change the selection of the drop-down list of distributions in the tool bar. Find the relevant components and add the action settings to the Actions list.
  - To let Sun Update Connection – Enterprise find components from other distributions that are comparable to the ones you have in the Actions list, click the Multi Distribution button.  
See [“To Align Component Settings for Multiple Distributions”](#) on page 210.
- 7 Do one of the following:**
  - From the tool bar, click the Save As Profile button.
  - Right-click in the Actions list and choose Save as Profile.

- From the Actions menu, choose Save as Profile.

The Profile Editor window opens.



- Type a new name for the profile, and type a free-text description.
- Check that the component actions in the bottom panel are what you want. You can change the profile before saving it.
- Click OK.

The profile is saved. The Profile Editor closes.

### Example 8–5 Saving a Host Inventory as a Profile

This Copy Inventory to Profile CLI command takes a host as a parameter. Everything that is installed on the host is marked as Required in the profile. All remaining components in the knowledge base of the distribution of the selected host that are not installed on that host are marked as Not Allowed in the profile. Use this profile to make an inventory cloning job on multiple hosts.

Note that in the following script example, the existence of a policy is assumed.

Make sure to execute a Check System for dependency issues before you save the inventory as a profile, either in the CLI or in the console. In addition, if the host is a Solaris machine, execute a Check Withdrawn Patches profile. See “Convert Inventory to Profile (-cip) Command” on page 277.

```

#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of hosts is:"
uce_cli -lah -u "$user" -p "$password"
echo -n "Copy the name of the host you want:"
read host
echo "The inventory of this host will be saved as a profile."
echo -n "Type a name for this profile:"
read profileName

echo "Checking $host for dependency issues..."
uce_cli -sj -P "Check system" -C "YesToAll" -h "$host" -dp -u "$user" -p "$password"
# Always run the System Test for Dependency Issues before saving an inventory.
# YesToAll is a policy that says Yes to all actions on SW and Local.
uce_cli -cip -h "$host" -P "$profileName" -u "$user" -p "$password"

```

### Example 8–6 Saving a Saved Inventory as a Profile

This Copy Snapshot as Profile CLI command takes the name of a saved inventory (known as a *snapshot* in the CLI) as a parameter. Everything that was installed on the host when the inventory was saved, is marked as Required in the profile. This profile could be used for a mass clone job.

Make sure to execute a Check System for dependency issues before you save the inventory as a profile, either in the CLI or in the console. In addition, if the host is a Solaris machine, execute the Check Withdrawn Patches profile. See [“Convert Snapshot to Profile \(-csp\) Command” on page 277](#).

```

#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo "The list of hosts is:"
uce_cli -lah -u "$user" -p "$password"
echo -n "Copy the name of the host you want:"
read host

echo "The saved inventories of this host are:"
uce_cli -lss -h "$host" -u "$user" -p "$password"
echo -n "Copy the saved inventory that you want to save as a profile"
read inven
echo -n "Type a name for this profile:"

```

```
read profileName

echo "Checking $host for dependency issues..."
uce_cli -sj -P "Check system" -C "YesToAll" -h "$host" -dp -u "$user" -p "$password"
# Always run the System Test for Dependency Issues before saving an inventory.
# YesToAll is a policy that says Yes to all actions on SW and Local.
uce_cli -csp -h "$host" -s "$inven" -P "$profileName" -u "$user" -p "$password"
```

## Inventory Jobs with Local Scripts and Files

Efficient system and network administrators often maintain a repository of scripts that they use to run typical host management tasks. They might also keep a repository of configuration files that they have changed for various situations, allowing them to quickly manage peripherals and do other frequent environment modifications.

Sun Update Connection – Enterprise allows you to store your scripts and files in your local Sun Update Connection – Enterprise knowledge base, as explained in [“Managing Local Files” on page 102](#). The following tasks show how you can easily create Inventory jobs to execute your scripts or install your file versions on multiple hosts. Using such techniques, you could manage complex, time-consuming tasks with one-click and be done within minutes: route fifty computers to a new printer, add nodes to a cluster, change the dynamics of on-demand services, and so on.

## Executing Scripts on Hosts

### ▼ To Execute a Local File on Multiple Hosts

In this procedure you will run Probes, Pre-actions, and Post-actions on managed hosts, using Inventory jobs. You could include these files in jobs that include installation components (RPMs, PKGs); this procedure shows the difference between Sun Update Connection – Enterprise install of installations and Sun Update Connection – Enterprise install of executions. The local file you want must already be in the Components list, under Local.

- 1 Make sure the Inventory panel is open in the main window by choosing Inventory from the View menu.**
- 2 From the drop-down list on the tool bar, select a distribution-architecture.**  
The Components list changes to display components of the selected distribution.
- 3 In the Hosts list, select the hosts upon which you want to execute the script.**
- 4 In the Components list, expand Local and then expand the relevant category: Probes, Pre-actions, or Post-actions.**
- 5 Select the probe or action that you want.**

**6 Do one of the following:**

- From the tool bar, click the Required button.
- Right-click the selected file and choose Required.
- From the Components, choose Required.

The action setting appears in the Actions list.

**7 Add as many Probes, Pre-actions, or Post-actions as you want.****8 To execute the files on hosts of different distributions:**

- To select specific files from different distributions, change the selection of the drop-down list of distributions in the tool bar. Find the relevant files and add the action settings to the Actions list.
- To let Sun Update Connection – Enterprise automatically add the same files that you uploaded to multiple distributions, click the Multi Distribution button. See [“To Align Component Settings for Multiple Distributions”](#) on page 210.

**9 Do one of the following:**

- From the tool bar, click the Run Job button.
- Right-click in the Actions list and choose Run on Selected Hosts.
- From the Actions menu, choose Run on Selected Hosts.

The Run Job window opens.

**10 Type a name and description for the job.****11 Check the bottom panel of the Run Job window and make sure it will execute the actions or probes you want. Although the action says Install, the actions and probes are not installed, but are executed on the remote hosts.****12 Select Deploy mode. As this job will execute scripts, a simulation will not do anything on the hosts.****13 Click OK.**

The job begins.

Probes are executed first.

If they succeed, Pre-actions are executed next.

If the Pre-actions succeed, Post-actions are executed.

## Distributing Local Files

### ▼ To Install Configuration Files on Multiple Remote Hosts

In this procedure you will install local Configuration files on managed hosts with an inventory job. The version you want must already be on the Components list, under Local/Configuration files. If the file has a macro sign in its contents, make sure the appropriate macro is also uploaded to the knowledge base. You do not need to add the macros to the inventory job; macros are called and executed automatically by Sun Update Connection – Enterprise.

- 1 Make sure the Inventory panel is open in the main window by choosing Inventory from the View menu.**
- 2 From the drop-down list on the tool bar, select a distribution-architecture.**

The Components list changes to display components of the selected distribution.
- 3 In the Hosts list, select hosts on which the files will be installed.**
- 4 In the Components list, under Local/Configuration files select the file version that you want.**
- 5 Do one of the following:**
  - From the tool bar, click the Required button.
  - Right-click the selected file and choose Required.
  - From the Components menu, choose Required.  
The action setting appears in the Actions list.
- 6 To install the files on hosts of different distributions:**
  - To select specific files from different distributions, change the selection of the drop-down list of distributions in the tool bar. Find the relevant files and set them to Required.
  - To let Sun Update Connection – Enterprise automatically add to the Actions list the same files that you uploaded to multiple distributions, click the Multi Distribution button. See [“To Align Component Settings for Multiple Distributions”](#) on page 210.
- 7 Do one of the following:**
  - From the tool bar, click the Run Job button.
  - Right-click in the Actions list and choose Run on Selected Hosts.
  - From the Actions menu, choose Run on Selected Hosts.

The Run Job window opens.
- 8 Type a name and description for the job.**
- 9 Select Deploy mode.**



**10 Click OK.**

The job begins.

The files that were uploaded to the knowledge base are installed on the remote hosts in the path names provided by the File Declaration of each Configuration file version.

If a Configuration file has a macro sign, the macro is called after file installation. The macro executes, and its output replaces the macro sign in the Configuration file.

**Example 8-7 Distributing Local Files**

Your File Declaration is `/etc/printcap` and the local File is `printcap_01`. Use this job to install `printcap_01` on ten hosts. On the hosts, it installs a file named `/etc/printcap` that has the contents of `printcap_01`. The contents of each existing `printcap` file are overwritten with the contents of `printcap_01`.



# Profiles

---

This chapter explains how to use the powerful profile tool to manage multiple systems consistently while automating many tedious administration jobs.

This chapter covers the following topics:

- “Terms” on page 171
- “Working With Profiles” on page 172

## Terms

This chapter uses the following terms:

Component	Any logical unit that is, or can be, part of a machine; not only software and files, but also any logical construct of the component hierarchy.
Inventory	(1) List of components installed on a managed host. (2) List of components on the universal server.
Knowledge Base	Sub-system of the Sun Update Connection – Enterprise system dependency server, acts as a proxy server for the universal server, holding and updating deployment rules and certified components.
Profile	Definition of a component configuration for a type of machine; what is required and what is not allowed to be installed on this type of machine.
Predefined Profile	Profile provided with Sun Update Connection – Enterprise that performs a full-system check and fix.

## Working With Profiles

Create profiles to record the requirements of your enterprise and deploy the profiles to automatically create servers and workstations. Creation and deployment of profiles takes minutes, handles dependencies, and ensures consistency.

For example, you create a profile called Web Servers which defines that your web servers are required to have the httpd client and server, and must not have anonFtp. You deploy the profile. Sun Update Connection – Enterprise installs the necessary components, uninstalls those you do not want, and automatically handles dependent components.

You can schedule a job to deploy the profile on a routine basis, such as once a month. It will make sure that everything that you want (httpd) is still installed and does not have dependency conflicts. It will make sure that anonFtp is not installed.

Sun Update Connection – Enterprise profiles focus on the component level. You select a component from the knowledge base inventory and then apply a setting to it. The component settings are described in the following table.

**TABLE 9-1** Profile Component Settings

Setting	Setting on Package	Setting on Category/Package Group
Required	If package is not installed, DR finds solution to install it. If installed, nothing is done.	If at least one package is installed, nothing is done. If no package in category/group is installed, the one that is most cost-effective is installed.
Not Allowed	If package is installed, DR finds solution to uninstall it. If not installed, nothing is done.	All packages within category/group are uninstalled.
Upgrade	If there is a newer version for an installed package, the package is upgraded. If the package is not installed, nothing is done. If there is more than one newer version, the most cost-effective is chosen.	All packages within category/group are upgraded if newer versions exist.

A profile is used as a single job. Its settings (Required, Not Allowed, Upgrade) affect a managed host only during the actual deployment of the profile. After you deploy a profile, you could run another job that contradicts the settings of the profile.

If you build a profile that has multiple Required and Not Allowed components, the Dependency Resolver (DR) may find a solution for the Required components that demands that a Not Allowed component be installed. If this happens, the DR rejects the solution and looks for another, one that will conform to both the Required and the Not Allowed settings.

## ▼ To Create a Profile

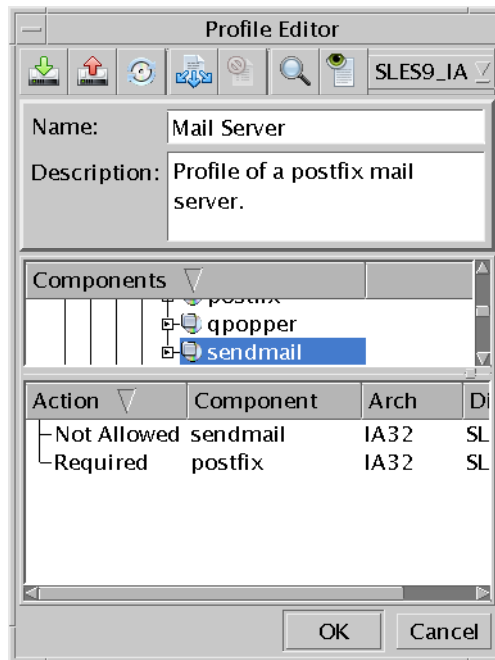
In this procedure, you will create and save a new profile, to be used later in a job. Users of all levels can perform this procedure in the console. Other users see your profiles as read-only. They can deploy or copy your profiles; they cannot delete or edit them. This restriction applies to users of all levels.

### 1 Do one of the following:

- From the tool bar, click the Profiles button.
- From the Tools menu, choose Profiles.  
The Profiles window opens.

### 2 Do one of the following:

- From the tool bar on the Profiles window, click the New button.
- Right-click a blank space in the Profiles window and choose New.  
The Profile Editor window opens.



### 3 From the drop-down list on the tool bar, select a distribution-architecture.

The Components list shows the components of the selected distribution.

**4 Type a name for the profile and an optional free-text description.**

**5 In the Components list, select a component.**

**6 Assign a profile action to the selected component.**

Do one of the following:

- **From the tool bar, click the Required, Not Allowed, or Upgrade button.**
- **Right-click the selected component and choose Required, Not Allowed, or Upgrade.**

The component setting appears in the Actions list of the Profile Editor.

To make the profile applicable to hosts of different distributions:

- To select specific components from different distributions, change the selection of the drop-down list of distributions in the tool bar. Find the relevant components and add the action settings to the Actions list.
- To let Sun Update Connection – Enterprise find components from other distributions that are comparable to the ones you have in the Actions list, click the Multi Distribution button. See [“To Align Component Settings for Multiple Distributions” on page 210.](#)

**7 Click OK.**

The Profile Editor window closes. The profile is created and appears in the Profiles window.

### **Example 9-1** Creating a Profile with the CLI

The CLI command to create a profile allows for only one component and its setting. See [“Add Profile Attribute \(-apa\) Command” on page 271.](#)

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
echo -n "Enter a string to search for exact component name:"
read comp2find
uce_cli -fc -T $comp2find -u $user -p $password
echo -n "Copy the exact component name that you want to add to a profile:"
read comp2use
echo -n "Enter the name of a profile or create a new one:"
read profileName
echo "What do you want to do with the component?"
echo "Make it Required, Not Allowed,"
```

```

echo "or Upgraded when possible?"
echo -n "Enter the setting (-R | -N | -U) (case-sensitive):"
read setting
uce_cli -apa -P "$profileName" -T "$comp2use" $setting -u "$user" -p "$password"

```

## ▼ To Edit a Profile

In this procedure you will edit an existing profile that you created. Users of all levels can perform this procedure in the console.

You cannot edit a profile in the following circumstances:

- The profile was created by another user.
- The profile is currently in an active job.
- The profile is a Predefined System Test Profile (see [Chapter 7](#)).  
If you edit a profile that is scheduled for later deployment, the users who deploy that profile decide whether to use the original profile or the edited one.

### 1 Do one of the following:

- **From the tool bar, click the Profiles button.**
- **From the Tools menu, choose Profiles.**  
The Profiles window opens.

### 2 Select a profile from the list.

### 3 Do one of the following:

- **From the tool bar of the Profiles window, click the Edit button.**
- **Right-click the selected profile and choose Edit.**  
The Profile Editor window opens.

### 4 From the drop-down list on the tool bar of the Profile Editor, select a distribution-architecture.

The Components list changes to display components of the selected distribution.

### 5 Change as many component settings as you want.

See [Table 9-1](#).

To add a component setting, select the component and do one of the following:

- From the tool bar of the Profile Editor, click the Required, Not Allowed, or Upgrade button.
- Right-click the selected component and choose Required, Not Allowed, or Upgrade.

To delete a component setting, select an action in the Actions list and do one of the following:

- From the tool bar of the Profile Editor, click the Delete button.
- Right-click the selected action and choose Delete.

To change a component setting, delete the action from the Actions list and then add a new action for the component setting you want.

#### **6 Add as many component settings as you want.**

To make the profile applicable to hosts of different distributions:

- To select specific components from different distributions, change the selection of the drop-down list of distributions in the Profile Editor tool bar. Find the relevant components and add the action settings to the Actions list.
- To let Sun Update Connection – Enterprise find components from other distributions that are comparable to the ones you have in the Actions list, click the Multi Distribution button. See [“To Align Component Settings for Multiple Distributions” on page 210](#).

#### **7 Click OK.**

The Profile Editor window closes. The profile is edited.

### **Example 9–2 Editing a Profile with the CLI**

The CLI command to edit a profile is the same as to create a profile. See [“To Create a Profile” on page 173](#).

## **▼ To Edit a Scheduled Profile**

You can edit a profile that you created, even if you deleted it from the profiles list, so that future deployments or simulations of the profile will be different from the original profile. Use this procedure to change scheduled jobs.

You can edit scheduled profiles only when the following are all true:

- The job that deploys/simulates the profile is scheduled for future runs.
- The options of the job are set to automatically accept changes.
- You are the owner of the profile.
- The profile is not in a currently active job.
- The profile is not a Predefined System Test Profile.

See [Chapter 7](#).

#### **1 Make sure the Jobs panel is open in the main window by choosing Jobs from the View menu.**

#### **2 Select a job name in the Jobs list and then select one of the tasks that appear in the Tasks list.**



**3 Do one of the following:**

- **From the tool bar, click the Edit Scheduled Profile button.**
- **Right-click the selected task and choose Edit Profile.**
- **From the Jobs menu, choose Tasks -> Edit Scheduled Profile.**  
The Profile Editor window opens.

**4 Edit the profile as needed.****5 Click OK.**

The Profile Editor window closes. The profile is edited for the next run of the job.

## ▼ To Copy a Profile

In this procedure you will copy an existing profile. Use this procedure when another user has created a profile that is useful to your own deployment and management jobs, but you want to be able to edit it. You could also use this procedure on your own profiles, to create a new profile based on a prior one. You cannot copy a Predefined System Test Profile (see [Chapter 7](#)). Users of all levels can perform this procedure in the console.

**1 Do one of the following:**

- **From the tool bar, click the Profiles button.**
- **From the Tools menu, choose Profiles.**  
The Profiles window opens.

**2 Select a profile from the list.****3 Do one of the following:**

- **From the tool bar of the Profiles window, click the Copy button.**
- **Right-click the selected profile and choose Copy.**  
The Profile Editor window opens.

**4 Edit the profile as needed, or simply change the name.****5 Click OK.**

The Profile Editor window closes. A copy of the profile with the new name appears in the Profiles window.

### Example 9-3 Copying a Profile with the CLI

The copy profile command in the CLI allows you only to save a profile under a new name, without making changes to the settings. See [“Copy Profile \(-cp\) Command” on page 272](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
echo -n "Enter a string to search for exact component name:"
read comp2find
uce_cli -fc -T $comp2find -u $user -p $password
echo -n "Copy the exact component name that you want to add to a profile:"
read comp2use
echo -n "Enter the name of a profile or create a new one:"
read profileName
echo "What do you want to do with the component?"
echo "Make it Required, Not Allowed,"
echo "or Upgraded when possible?"
echo -n "Enter the setting (-R | -N | -U) (case-sensitive):"
read setting
uce_cli -apa -P "$profileName" -T "$comp2use" $setting -u "$user" -p "$password"
```

## ▼ To Copy an Active Profile

You can copy any profile (except a Predefined System Test Profile), even if the owner deleted it from the profiles list or it is in a currently active job. Use this procedure to create new profiles from those used in jobs.

- 1 **Make sure the Jobs panel is open in the main window by choosing Jobs from the View menu.**
- 2 **Select a job name in the Jobs list and then select one of the tasks that appears in the Tasks list.**
- 3 **Do one of the following:**
  - **From the tool bar, click the Copy Profile button.**
  - **Right-click the selected task and choose Copy Profile.**
  - **From the Jobs menu, choose Tasks -> Copy Profile.**  
The Profile Editor window opens.
- 4 **Edit the profile as needed, or simply change the name.**

**5 Click OK.**

The Profile Editor window closes. The profile with the new name is added to the Profiles window.

## ▼ To Delete a Profile

In this procedure, you delete a profile that you created. Users of all levels can perform this procedure in the console.

You cannot delete profiles in the following circumstances:

- The profile was created by another user.
- The profile is currently being deployed in an active job.
- The profile is scheduled to be deployed, and the owner of the job selected that the job not be updated with profile changes.

**1 Do one of the following:**

- **From the tool bar, click the Profiles button.**
- **From the Tools menu, choose Profiles.**  
The Profiles window opens.

**2 Select a profile from the list.****3 Do one of the following:**

- **From the tool bar of the Profiles window, click the Delete button.**
- **Right-click the selected profile and choose Delete.**

**4 In the confirmation dialog box, click Delete again.**

### **Example 9-4** To Create a Postfix Mail Server Profile – Example

The previous procedures explained how to create, edit, copy, and delete profiles, in general. This procedure is a specific example of a profile for a mail server.

1. To open the Sun Update Connection – Enterprise Console, type `uce_console` in a terminal shell and log in with a valid user name and password.
2. From the Tools menu, choose Profiles.  
The Profiles window opens.
3. Right-click in the Profiles window and choose New.  
The Profile Editor window opens.

4. From the drop-down list in the tool bar of the Profile Editor, select a distribution.
5. Give the profile a name.  
For example, you might name the profile `PostfixMailServer`.
6. Type a description of the profile.
7. In the components list, find `postfix`, right-click it and choose `Required`.  
See [“To Find Components” on page 212](#) for details on searching the Components list.  
`Required postfix` appears in the Actions list.
8. Find `sendmail`, right-click it and choose `Not Allowed`.  
`Not Allowed sendmail` appears in the Actions list.
9. Right-click in the Actions list and choose `Multi-Distribution`.  
The Multi Distributions window opens. Your locally active distributions are listed. Those that are listed in green have a component match.
10. Click `OK`.  
The Multi Distributions window closes. The Actions list in the Profile Editor now includes more actions for the additional distributions.
11. In the Profile Editor, click `OK`.  
The Profile Editor closes. `PostfixMailServer` appears in the Profiles list.  
To deploy the Mail Server Profile, see [Chapter 11](#).

# Policies

---

This chapter explains how to create, edit, copy, and delete policies. A policy enables you to predefine how a job is performed. It allows you to determine which solutions are unacceptable, and it allows you to set the automation level of the job.

This chapter covers the following topics:

- “Terms” on page 181
- “Working With Policies” on page 182

## Terms

This chapter uses the following terms.

Component	Any logical unit that is, or can be, part of a machine; not only software and files, but also any logical construct of the component hierarchy.
Cost-effective solution	Deployment solution that has the least requirements for number of dependency issues, time, and resources, to fulfill a job.
Policy	Set of confirmation rules for the implementation of the dependency resolver and level of automation of jobs.
dependency resolver (DR)	Set of patented algorithms to describe a solution for a job. Initiated by agent application when a job is received.
Inventory	(1) List of components installed on a managed host. (2) List of components on the universal server.
Knowledge Base	Sub-system of the Sun Update Connection – Enterprise system dependency server, acts as a proxy server for the universal server, holding and updating deployment rules and certified components.

## Working With Policies

When you send a job to managed hosts, each selected agent runs the dependency resolver (DR) to find the most cost-effective solution for its own host to complete the job.

Creating a policy enables you to add your own rules to how the DR should determine what is the best solution.

- You can predefine some actions as unacceptable. The DR rejects any solution that contains these actions. Thus, you can determine trends for the DR, without giving up on the automation.
- You can predefine some actions as automatic, to be carried out without asking for user-intervention.

Sun Update Connection – Enterprise policies focus on the component level. You select a component from the knowledge base inventory, select a possible deployment action, and then apply a deployment policy setting to the pair. If the selected component is a category or a package-group, the setting applies to all packages contained in the category or package-group.

### EXAMPLE 10-1 Example

You want to install the latest version of a security software on a hundred hosts. You create a policy that protects your kernel from any changes.

```
Running Kernel Install - No
Running Kernel Uninstall - No
Running Kernel Upgrade From - No
Running Kernel Downgrade From - No
```

When you run the job on the group of hosts, the policy forces those hosts with old kernels either to find a way to install the new software in the present environment, or to fail the job.

**TABLE 10-1** Policy Component-Action Settings

	Ask Me	Yes	No
Install or Uninstall	Pause the job for confirmation before installing or uninstalling the selected component.	Install or uninstall the selected component automatically, as required by solution.	Find a solution that does not install or uninstall the selected component.
Upgrade from or Downgrade from	Pause the job for confirmation before changing the version of the selected component.	Upgrade or downgrade the selected component automatically, as required by solution.	Find a solution that does not upgrade or downgrade the selected component.

TABLE 10-1 Policy Component-Action Settings (Continued)

	Ask Me	Yes	No
Apply Fix	Pause the job for confirmation before fixing dependency, security, or bug issues on selected component.	Deploy fix automatically as needed.	Find a solution that does not deploy a fix on the selected component.
Ignore File Conflict <sup>1</sup>	Pause the job for confirmation, so you see the conflict and decide run-time whether to ignore it and continue the job, or to fail the job.	The conflict is understood and known to be unimportant. Continue the job without pause.  <b>Caution</b> – Do not set Yes to this action unless you know the conflict.	Find a solution that does not allow for any file conflicts.

<sup>1</sup> If the selected component provides a file that cannot be installed on a machine with a file provided by another component that is already installed, there is a file conflict.

If both components are certified, the rules of the knowledge base handle deployment without conflicts. If one or both are local components not in the knowledge base, the conflict will cause the job to fail.

## ▼ To Create a Policy

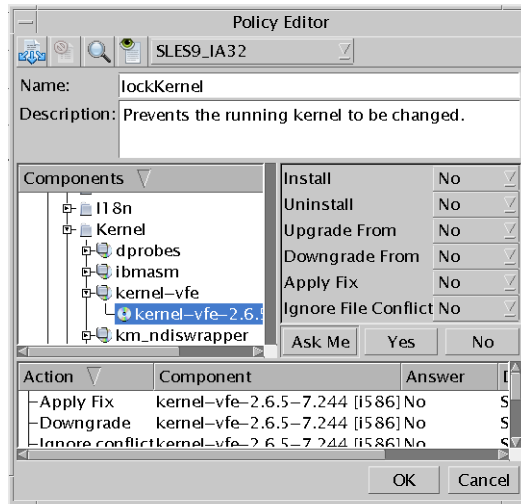
In this procedure, you will create a policy to be used later in jobs. Users of all levels can perform this procedure in the console. Other users see your policies as read-only. They can use or copy your policies; they cannot delete or edit them. This restriction applies to users of all levels.

### 1 Do one of the following:

- **From the tool bar, click the Policies button.**
- **From the Tools menu, choose Policies.**  
The Policies window opens.

### 2 Do one of the following:

- **From the tool bar on the Policies window, click the New button.**
- **Right-click a blank space in the Policies window and choose New.**  
The Policy Editor window opens.



- 3 **Type a name for the policy.**
- 4 **From the drop-down list on the tool bar, select a distribution-architecture.**  
The Components list shows the components of the selected distribution.
- 5 **In the Components list, select a component, and for each action, set a policy for the selected component; do one of the following:**
  - **Select Ask Me, Yes, or No from the drop-down list of the action**
  - **Click the Ask Me, Yes, or No button for all actions.**  
To make the policy applicable to hosts of different distributions:
    - To select specific components from different distributions, select from the drop-down list of distributions. Find components and add settings to the Actions list.
    - To let Sun Update Connection – Enterprise find components from other distributions that are comparable to the ones you have in the Actions list, click the Multi Distro button (see [“To Align Component Settings for Multiple Distributions”](#) on page 210).
- 6 **Click OK.**  
The Policy Editor window closes. The policy is created and appears in the Policies window.

### Example 10–2 Creating a Policy in the CLI

The CLI command to create a policy allows for only one component-action and its setting. See [“Add Policy Attribute \(-aca\) Command”](#) on page 271.



```

#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
echo -n "Enter a string to search for exact component name:"
read comp2find
uce_cli -fc -T $comp2find -u $user -p $password
echo -n "Copy the exact component name that you want to add to a
policy:"
read comp2use
echo -n "Enter the name of a policy or create a new one:"
read policyName
echo "What action is relevant for this component?"
echo "(install|downgrade|fix|remove|upgrade|ignore)"
echo -n "Type the exact action, case-sensitive:"
read action
echo -n "Enter the setting (yes|no|ask_me) (case-sensitive):"
read setting
uce_cli -aca -C "$policyName" -T "$comp2use" -$action $setting -u "$user" -p
"$password"

```

## ▼ To Edit a Policy

In this procedure, you will edit a policy and save the changes. Users of all levels can perform this procedure in the console.

You cannot edit a policy in the following circumstances:

- The policy was created by another user.
- The policy is currently in an active job.
- The policy is the Predefined Always ask me policy.

If you edit a policy that is scheduled for later deployment, the users who deploy that policy decide whether to use the original policy or the edited one.

### 1 Do one of the following:

- **From the tool bar, click the Policies button.**
- **From the Tools menu, choose Policies.**  
The Policies window opens.

### 2 Select a policy from the list.

**3 Do one of the following:**

- **From the tool bar of the Policies window, click the Edit button.**
- **Right-click the selected policy and choose Edit.**

The Policy Editor window opens.

**4 From the drop-down list on the tool bar of the Policy Editor, select a distribution- architecture.**

The Components list changes to display components of the selected distribution.

**5 Change as many component settings as you want.**

See [Table 10-1](#).

To add a component setting, select the component and set a policy for each deployment action. Do one of the following:

- Select Ask Me, Yes, or No from the drop-down list of the action
- Click the Ask Me, Yes, or No button for all actions.

To delete a component setting, select an action in the Actions list and click the Delete Selected button.

To change a component setting, delete the action from the Actions list and then add a new action for the component setting you want.

**6 Add as many component settings as you want.**

To make the policy applicable to hosts of different distributions:

- To select specific components from different distributions, change the selection of the drop-down list of distributions. Find the relevant components and add the settings to the Actions list.
- To let Sun Update Connection – Enterprise find components from other distributions that are comparable to the ones you have in the Actions list, click the Multi Distro button (see [“To Align Component Settings for Multiple Distributions”](#) on page 210).

**7 Click OK.**

The Policy Editor window closes. The policy is edited.

## ▼ To Edit a Scheduled Policy

You can edit a policy that you created, even if you deleted it from the policies list, so that future runs of a job will have different confirmation policies. Use this procedure to change the policy of scheduled jobs.

You can edit scheduled policies only when the following are all true:

- The job that deploys/simulates the policy is scheduled for future runs.
- The options of the job are set to automatically accept changes.
- You are the owner of the policy.
- The policy is not in a currently active job.
- The policy is not the Always ask me policy.

**1 Make sure the Jobs panel is open in the main window. From the View menu, choose Jobs.**

**2 Select a job name in the Jobs list and then select one of the tasks that appears in the Tasks list.**

**3 Do one of the following:**

- **From the tool bar, click the Edit Policy button.**
- **Right-click the selected task and choose Edit Policy.**
- **From the Jobs menu, choose Tasks -> Edit Scheduled Policy.**  
The Policy Editor window opens.

**4 Edit the policy as needed.**

**5 Click OK.**

The Policy Editor window closes. The policy is edited.

### **Example 10–3** Editing a Policy in the CLI

The CLI command to edit a policy is the same as to create a policy. See [Example 10–2](#).

## **▼ To Copy a Policy**

In this procedure you will copy an existing policy. Use this procedure when another user has created a policy that is useful to your own deployment and management jobs, but you want to be able to edit it. You could also use this procedure on your own policies, to create a new policy based on a prior one. You cannot copy the Predefined Always ask me policy. Users of all levels can perform this procedure in the console.

**1 Do one of the following:**

- **From the tool bar, click the Policies button.**
- **From the Tools menu, choose Policies.**  
The Policies window opens.

- 2 **Select a profile from the list.**
- 3 **Do one of the following:**
  - **From the tool bar of the Policies window, click the Copy button.**
  - **Right-click the selected policy and choose Copy.**  
The Policy Editor window opens.
- 4 **Edit the policy as needed, or simply change the name.**
- 5 **Click OK.**  
The Policy Editor window closes. The policy is edited.

#### **Example 10–4** Copying a Policy with the CLI

The copy policy command in the CLI allows you only to save a policy under a new name, without making changes to the settings. See [“Copy Policy \(-cc\) Command” on page 273](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password
echo "The list of existing policies is:"
uce_cli -lc -u $user -p $password
echo -n "Type the exact name of the policy you want to copy:"
read sourceP
echo -n "Type a name for the new policy:"
read targetP
uce_cli -cc -sC "$sourceP" -tC "$targetP" -u "$user" -p "$password"
```

## ▼ **To Copy an Active Policy**

You can copy any policy (except the default Always ask me policy), even if the owner deleted it from the policies list or it is in a currently active job. Use this procedure to create new policies from those used in jobs.

- 1 **Make sure the Jobs panel is open in the main window by choosing Jobs from the View menu.**
- 2 **Select a job name in the Jobs list and then select one of the tasks that appears in the Tasks list.**

- 3 Do one of the following:**
  - **From the tool bar, click the Copy Policy button.**
  - **Right-click the selected task and choose Copy Policy.**
  - **From the Jobs menu, choose Tasks -> Copy Policy.**  
The Policy Editor window opens.
- 4 Edit the policy as needed, or simply change the name.**
- 5 Click OK.**  
The Policy Editor window closes. The policy is edited.

## ▼ To Delete a Policy

In this procedure you will delete a policy that you created. Users of all levels can perform this procedure in the console.

You cannot delete policies in the following circumstances:

- The policy was created by another user.
- The policy is currently being deployed in an active job.
- The policy is scheduled to be used in a job, and the owner of the job selected that it not be updated with policy changes.

If a scheduled job is set to accept changes, you may delete the policy. On the next scheduled run, the job will use the default Always ask me policy.

- 1 Do one of the following:**
  - **From the tool bar, click the Policies button.**
  - **From the Tools menu, choose Policies.**  
The Policies window opens.
- 2 Select a policy from the list.**
- 3 Do one of the following:**
  - **From the tool bar of the Policies window, click the Delete button.**
  - **Right-click the selected policy and choose Delete.**
- 4 In the confirmation dialog box, click Delete again.**





# 11

## CHAPTER 11

# Complex Jobs

---

This chapter explains how to manage hosts in the most consistent and efficient manner. Complex jobs are not difficult to create or use; they are complex because they combine several objects into one command from the user interface to the system dependency server. Complex jobs maintain consistency throughout the environment and to make sure that even the most complicated lifecycle management missions are orderly and error-free. Complex jobs allow you to include multiple tasks, each task combining a set of objects and operation options.

This chapter covers the following topics:

- “Terms” on page 191
- “Complex Job Processes” on page 192
- “Complex Job Objects” on page 194
- “Creating Complex Jobs” on page 194
- “Saving Job Templates” on page 201
- “Copying Jobs” on page 201
- “Creating Complex Jobs” on page 202

## Terms

This chapter uses the following terms:

Agent	Application of Sun Update Connection – Enterprise that is installed on every managed host and that runs the Dependency Resolver, finding solutions specific to its host.
Cost-effective	Deployment solution that has the least requirements for number of dependency issues, time, and resources, to fulfill a job.
dependency manager (DM)	Sub-system of the Sun Update Connection – Enterprise system dependency server, responsible for managing jobs on hosts and communications between the user interface and agents.
dependency resolver (DR)	Set of patented algorithms to describe a solution for a job. Initiated by agent application when a job is received.

Mode	Job option that determines whether the job changes hosts (Deploy) or tests the action list on hosts (Simulate).
Job	Collection of actions and tests to be run on selected managed hosts by agents.
Knowledge Base	<p>Sub-system of the Sun Update Connection – Enterprise system dependency server, acts as a proxy server for the universal server, keeping dependency rules for CO deployment on managed hosts and the COs themselves.</p> <p>A local knowledge base is a private, on-site only, collection of NCO listings and their deployment rules as generated by the Local Expansion technology.</p>
Policy	Set of confirmation rules for the implementation of the dependency resolver and level of automation of jobs.
Profile	Definition of a component configuration for a type of machine; what is required and what is not allowed to be installed on this type of machine.
system dependency server (SDS)	The complete management system for Sun Update Connection – Enterprise. Its sub-systems include the Server, the dependency manager, and the knowledge base.
Task	Part of a job that contains a profile, a hostlist, a policy, an optional schedule, and performance options.

## Complex Job Processes

You create a single job to be run on one or multiple hosts. Each agent that receives the job runs it individually, optimizing on the software configuration of the host.

To fulfill a job, an agent uses rules and components from the knowledge base. The agent runs the dependency resolver, which takes into account installed inventory, selected policy, and selected profile.

The dependency resolver is a set of algorithms that describes the best possible solution for an agent to complete a job. The best possible solution includes:

- The most cost-effective package to deploy, matching component rules in the knowledge base to the existing configuration of the host
- The most cost-effective way to fulfill dependency requirements, ensuring that the managed host will operate correctly after the job

When you create a job, the agent of each selected managed host picks up the job and runs the following processes. Each agent performs these actions only for the components of its



distribution-architecture; irrelevant components are ignored. Therefore, you can safely create a multiple distribution job and send it to a mixed group of hosts.

The job process of each agent, for each task, is as follows:

- Reads the knowledge base to find rule and component updates
- Sends the software component inventory of the host to the dependency manager
- Runs probes to test that host resources can fulfill the job, if you selected probes
- Runs dependency resolver
- Builds a tasklist (if a simulation job, job ends after this step)
- Saves an inventory of each host to be changed
- Gets confirmation for tasks, either from a policy or interactively
- Runs local pre-actions, if you selected any
- Installs local Configuration files, if you selected any
- Customizes local Configuration files with macros, if any are called upon
- Installs requested knowledge base components
- Runs local post-actions, if you selected any
- Runs post-fix actions, if applicable (see “[Post-Fix Actions](#)” on page 193)
- Sends job status (success/failure) and new inventory to the DM

## Post-Fix Actions

A post-fix action is a binary that performs an action on hosts when a specific package has been installed. Sun Update Connection – Enterprise runs post-fixes without user intervention. Post-fixes ensure machine functionality after changes.

### EXAMPLE 11-1 Using Post-Fix Actions

You create a job that upgrades the kernel. Before the job ends, a post-fix action is triggered, which updates the boot-loader file for the new kernel version.

## Agent Queuing

While an agent is running a job, it cannot perform other Sun Update Connection – Enterprise actions:

- It cannot upload its files to the File Browser window.
- It cannot upload its parameters to the Host Settings window.

- It cannot upload an updated inventory to the console. The inventory of the managed host will be updated on the console after the job is done.  
You may assign more jobs to this host, and the jobs will be queued.

## Complex Job Objects

A complex job is made up of one or more tasks, a schedule, and a set of performance options. At the time that you create the job, you set the schedule (see “[To Set Job Schedules](#)” on page 196) and the options (see “[To Set Job Options](#)” on page 198). On the other hand, you may create the objects of the tasks either on the fly, as you create the tasks, or before you begin to create the job.

A task needs a profile:

- You can create or copy a profile beforehand. See [Chapter 9](#)
- You can use Predefined Profiles. See [Chapter 7](#)

A task needs a policy:

- You can create or copy a policy beforehand. See [Chapter 10](#)
- You can use the default Always ask me policy.

A task needs a hostlist:

- You can select groups to ensure hosts of similar functionality receive consist jobs. See [Chapter 4](#)
- You can select one or more hosts (using the Shift or Control keys) from the New Job window.
- Users with restricted permissions over groups can select only groups and hosts of their authorized groups.

## Creating Complex Jobs

In the following procedures, you will select the objects and options of a job and then run the job on selected hosts.

Before you begin a job on a Solaris machine, make sure the PKG deployment preferences are appropriate for your local needs. See “[Host Preferences – PKGs](#)” on page 301 on “[Host Preferences – PKGs](#)” on page 301.

This procedure is broken up into the following parts:

- “[To Set Up the Objects of a Job](#)” on page 195
- “[To Create the Tasks of a Job](#)” on page 195
- “[To Set Job Schedules](#)” on page 196
- “[To Set a Single Schedule](#)” on page 197
- “[To Set a Recurring Schedule](#)” on page 198

- [“To Set Job Options” on page 198](#)
- [“Running a Job with the CLI” on page 200](#)

## ▼ To Set Up the Objects of a Job

- 1 Make sure the Jobs panel is available in the main window by choosing Jobs from the View menu.
- 2 Do one of the following:
  - From the tool bar, click the New Job button.
  - Right-click in the Jobs list and choose New Job.
  - From the Jobs menu, choose New.  
The New Job window opens.
- 3 Give the job a name and a free-text description.
- 4 Select a mode for the job:
  - Deploy – Perform the tasks on the selected hosts
  - Simulate – Test the job to estimate time and full action list  
A user may be restricted to executing jobs only in Simulate mode.
- 5 Do the following:
  - a. Create tasks for the job.  
See [“To Create the Tasks of a Job” on page 195](#).
  - b. Set job options or leave the default settings.  
See [“To Set Job Options” on page 198](#).
  - c. Set a schedule or leave the default Now schedule.  
See [“To Set Job Schedules” on page 196](#).

## ▼ To Create the Tasks of a Job

- 1 In the Tasks tab of the New Job window, click Add Task.  
The Task Editor opens.

- 2 Type a name for a task.**
- 3 Select a profile from the drop-down list, or click the profile editor button to open the Profile Editor and create a new profile.**

If you select a user-defined profile and then click the button, you can edit an existing profile.
- 4 Select a policy from the drop-down list, or click the policy editor button to open the Policy Editor, to create or edit a policy as you would a profile.**
- 5 Click the Hosts button to the right of the Hosts field.**

The Select Hosts window opens.
- 6 Select hosts and groups and then click the Add button.**

The hosts or groups are added to the Selected Hosts list.
- 7 When the Selected Hosts list contains the hosts or groups that you want to receive this job, click OK.**

The Hosts window closes. The selected hosts and groups appear in the Hosts field of the Tasks tab.
- 8 Click OK.**

The task is added to the Tasks list of the job. Add as many tasks as you want.

The order of the tasks in the list is the order that they will be executed. To change this order, select a task name and click the Up or Down buttons.

To edit a task, select the task and click the Edit button.

To remove a task from the job, select the task and click the Delete button.
- 9 Decide how to continue:**
  - If you want to run the job with default settings, click OK now.
  - If you want to set a deployment schedule, go to [“To Set Job Schedules” on page 196.](#)
  - If you want to view and edit the job options, go to [“To Set Job Options” on page 198.](#)
  - If you want to save the tasks as a job template, click Save Template.

## ▼ To Set Job Schedules

- 1 Open the Schedule tab.**

- 2 Select a schedule type:
  - Single – have the job run at a future date and time.
  - Recurring – have the job run on a recurring basis.

## ▼ To Set a Single Schedule

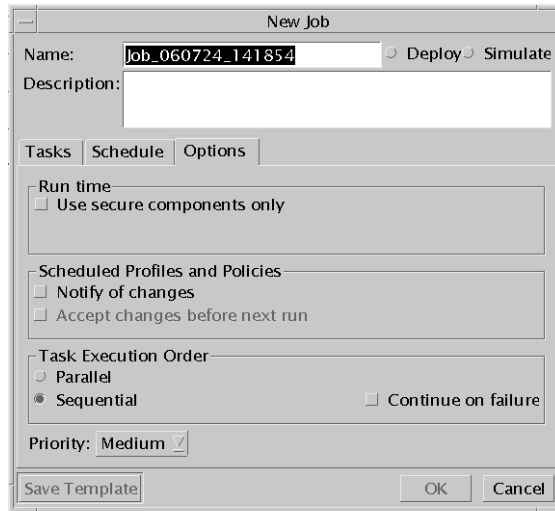
- 1 Select Single.
- 2 In the Time text box, select the hour and the minutes.  
Type in the desired time, or use the arrows to change the selection. The time settings are by 24 hours: 13:00 = 1pm, 14:00 = 2pm, ... 00:00 = midnight.
- 3 Click the button to the right of the Date box.  
The Calendar opens.
- 4 Select a date and then click OK.  
The Calendar closes. The selected date appears in the Date field.
- 5 In the New Job window, click OK or set job options.  
See “To Set Job Options” on page 198.  
The job will begin on the selected time and date.

## ▼ To Set a Recurring Schedule

- 1 Select Recurring.
- 2 In the Month drop-down list, select either Every Month (all year schedule) or a specific month (monthly schedule).
- 3 Select days of the month:
  - Every day – Job runs every day of the month, or year (if Every Month was selected).
  - Day in week – Select the days of the week on which the job will be run.
  - Day in month – Select dates in the month on which the job will be run.
- 4 Select time of the day:
  - Earliest – Set a time (hour:minutes) for the first run of the job.
  - Interval – Set a minute interval, to have the job run multiple times during a day.
  - Latest – Set a time for the latest run of the job, if an interval for multiple runs was selected.

## ▼ To Set Job Options

- 1 Open the Options tab.



- 2 Select Use Secure Components only if you want to give priority to secure versions. Deselect it to give priority to cost-effective versions, which makes the job run faster.
- 3 If you set a recurring schedule for the job, decide how the job should be handled if selected profiles and policies are changed between now and the next run of the job.

Option	Selected Function	Deselected Function
Notify of changes	If the owner of the profiles or policies changes them, you will get an email notification. Select if using profiles/policies that other users created.	You are not notified of changes. Deselect if you own the selected profiles or policies and do not want the reminder emails.
Accept changes before next run	Use updated profiles or policies. Select for consistency and automation.	Use the profiles or policies as they were when you created the job. Deselect for predictability.

- 4 Specify how you want the task to run in relation to other tasks and how to handle failures.

Option	Selected Function	Deselected Function
Parallel	Run the job simultaneously with other jobs. Do <i>not</i> run jobs that depend on the results of other jobs in parallel. Run such jobs in sequential mode only.	Run the job after the previous job completed. By default, a job is run sequentially.
Sequential	Run the job after other jobs have completed.	Run the job in parallel mode.

Option	Selected Function	Deselected Function
Continue on failure	Continue to run a job even if one of the steps or tasks experienced a failure. This option is only available for jobs that run in sequential mode.	Terminate a job if a step or task experiences a failure.
Priority	Select or change a priority for a job. Values are Low, Medium, and High.	By default, the priority is set to Medium.

## Running a Job with the CLI

The CLI command to submit a job runs one task on a single selected host or group. See [“Submit Job \(-sj\) Command” on page 274](#).

```
#!/bin/bash

echo -n "Enter your user name:"
read user
echo -n "Enter your password:"
read password

echo -n "Type a name for this job:"
read jobname
echo -n "Do you want to run this job on a host or a group? (h|g):"
read hostgroup
if [ $hostgroup = "h" ];then
    echo "Hosts are:"
    uce_cli -lah -u "$user" -p "$password"
else
    echo "Groups are:"
    uce_cli -lg -u "$user" -p "$password"
fi
echo -n "Copy host or group name to receive job:"
read selected

echo "Profiles are:"
uce_cli -lp -u "$user" -p "$password"
echo -n "Copy profile to use:"
read profile
echo "Policies are:"
uce_cli -lc -u "$user" -p "$password"
echo -n "Copy policy to use:"
read policy

echo "Simulating $jobname"
uce_cli -sj -j "$jobname" -P "$profile" -C "$policy" -$hostgroup "$selected"
```



```

    -us -sm -u "$user" -p "$password"
echo -n "Do you want to deploy $jobname? (y|n)"
read yes
if [ $yes = "y" ]; then
    uce_cli -sj -j "$jobname Deployed" -P "$profile" -C "$policy" -$hostgroup
    "$selected" -us -dp -u "$user" -p "$password"
fi

```

## Saving Job Templates

### ▼ To Save a Job Template

After you have set up the objects of a job, you can save it as a template. Using a job template, you can run the job, with or without edits, whenever you want. Use this procedure if you have the job requirements, but are unsure of when it should be run, or if the hosts are not yet online.

#### 1 Open the New Job window and create tasks.

If you want, you can set a schedule and select options.

#### 2 With any tab of the New Job window open, click Save Template.

Sun Update Connection – Enterprise saves the job without running it, and sends you a message when the save is complete.

The template name appears in the Jobs list, with an icon to indicate that it is not a running job.

To create a job from the template, select the template and then right-click and select Rerun. Select Deploy or Simulate and then click OK.

## Copying Jobs

### ▼ To Copy a Job

You can use a job to be the base of another job. Use this procedure if you have a complex job that would fulfill new requirements with a few changes, rather than creating a new job.

#### 1 In the Jobs list, select a job to use as the source and then right-click and select Copy.

The New Job window opens with the objects and settings of the selected job.

The profile is listed as Based on <source profile> from <date time>. This is to notify you that the job will be based on the profile as it was at the date and time that the source job was created. If the profile has been changed since then, this new job will not reflect those changes.

If the profile is listed as `Task's Profile`, the job was not a complex job. It was created by applying job settings to inventory components. You can make a copy of this job, but you cannot view its `ToDo` basket.

**2 Make any changes to the job that you want and then click OK.**

The job is added to the Jobs list and begins according to its schedule settings.

---

**Note** – If you do make changes to the copied job, there is no indication in the Job list. See the Job Log for details of how the changes were translated into actions.

---

## Creating Complex Jobs

### ▼ To Create a Simple Complex Job

This procedure is a specific example of executing Complex Jobs. This example is of a very simple job. You could follow it even if you have not yet created profiles, policies, and groups.

**1 Make sure the Jobs panel of the main window is open by choosing Jobs from the View menu.**

**2 From the tool bar, click the New Job button.**

The New Job window opens.

**3 Name the job `CheckAllHosts`. In the description, type This job checks all hosts for missing dependencies.**

**4 Select `Simulate`.**

This job will find any missing dependencies on any of the hosts and give you an idea of how long the actual job would take.

**5 In the Tasks tab, click `Add Task` and a task with:**

- **Name:** `SingleCheck`
- **Profile:** `Check System`
- **Policy:** `Always ask me`
- **Hosts:** `All Hosts`

**6 Click `OK` in the Tasks tab.**

The `SingleCheck` task is added to the job.

**7 Click OK in the New Job window.**

The job is sent to all managed hosts. Each host will be checked to see whether it has any missing or conflicting dependencies.

**8 Check the progress of the hosts as they run the job, and the job log of each host when it is done.**

See [“To Monitor a Current Job” on page 218](#).

If the results of the simulation are satisfactory, rerun the job in Deploy mode. See [“To Rerun a Job” on page 220](#).

The DR finds a solution to fix any missing or conflicting dependencies. You will be asked to confirm the fixes before they are deployed. See [“To Confirm Tasks” on page 214](#)). On confirmation, the actions are carried out and all dependencies are fixed on all hosts.

**▼ To Create a Feature-Rich Complex Job**

This procedure is a specific example of using the Complex Job feature. This example is of a more feature-rich job.

This example assumes the following:

- You have a profile with your requirements of an NFS server (`NfsServer`) and a profile for an NFS client (`NfsClient`).
- You have created a policy to automatically apply fixes (`AutoFix`).
- You have created a group of machines destined to be NFS servers (`nfs servers`) and a group for NFS clients (`nfs clients`). The machines may be of differing distributions and architectures. You would have aligned the profile requirements for the different active distributions before creating this job. See [“To Align Component Settings for Multiple Distributions” on page 210](#).

**1 Make sure the Jobs panel of the main window is open by choosing Jobs from the View menu.****2 Click the New Job button.**

The New Job window opens.

**3 Name the job: NFS Environment.**

In the description, type This job provisions NFS servers and NFS clients.

**4 Select Deploy.**

As the profiles are your own or the predefined profiles for system management, you have a good idea of what will be done on the hosts; you do not need to simulate the job before deploying it.

Before anything is changed on any host, Sun Update Connection – Enterprise saves its inventory. If you do not like the results of the job, you can easily restore it to its previous inventory. See [“Restoring Managed Hosts” on page 161](#).

**5 In the Tasks tab, click Add Task and a task with:**

- **Name:** IntegrityCheck
- **Profile:** Check System
- **Policy:** AutoFix
- **Hosts:** nfs servers and nfs clients groups

**6 Click OK.**

The IntegrityCheck task is added to the job.

**7 Add another task:**

- **Name:** ProvisionNfsServer
- **Profile:** NfsServer
- **Policy:** Always ask me
- **Hosts:** nfs servers groups

**8 Click OK.**

The ProvisionNfsServer task is added to the job.

**9 Add another task:**

- **Name:** NfsClient
- **Profile:** NfsClient
- **Policy:** Always ask me
- **Hosts:** nfs clients groups

**10 Click OK.**

The ProvisionNfsClients task is added to the job.

Now you have a job with three tasks: check hosts for missing dependencies, provision the NFS server profile on the nfs servers group, and then provision the NFS client on the nfs clients group.

Let's set a schedule for this job. If the job is run on a recurring basis, it will make sure that the hosts in the web servers group always comply with the web server profile. If they do comply, nothing is changed and the job finishes on success. If there has been an error in change management, the recurring run will find it.

- 11 Open the Schedule tab.**
- 12 Select Recurring.**
- 13 Select Every Month.**
- 14 Select Day in week, and then select Monday.**
- 15 Set Earliest to 7 : 00.**  
The job will now run every Monday, early in the morning. Let's look at the job options now.
- 16 Open the Options tab.**
- 17 Select Use secure components only.**
- 18 If you are the owner of the profiles and of the AutoFix policy, you can leave the Notify of changes option deselected. They cannot be changed by any other user.**
- 19 Select Accept changes before next run.**

If the requirements of an NFS server change, you need only change the profile once. This option ensures that the job will automatically use any changes you make to the profile.

You now have a re-usable job, with multiple tasks to be run on multiple hosts in a specific order, according to what is relevant to the inventory, distribution, and hardware architecture of each managed host. The job has a schedule. You will be notified by email if there are any tasks to do or if a host goes down. The job options have been set to optimize this specific set of tasks. To execute the job, click OK in the New Job window.



## Common Job Operations

---

This chapter explains how to perform operations that are common to all Sun Update Connection – Enterprise jobs: Inventory-based, Complex, and scheduled.

This chapter covers the following topics:

- “Job Preparation” on page 207
- “Job Management Features” on page 214
- “Troubleshooting Jobs” on page 225

### Job Preparation

While you are preparing the settings for a job, either an Inventory-based job or the objects of a Complex job, you can access features to make the procedures more efficient; or in the case of Solaris PKG preference settings, to make the jobs succeed at all.

Procedures in this section include:

- “To Set PKG Preferences” on page 208
- “To Align Component Settings for Multiple Distributions” on page 210
- “To Find Components” on page 212
- “To Use Regular Expressions” on page 214

### Settings for PKG Jobs

This procedure is essential for any job that installs, uninstalls, upgrades, or downgrades Solaris PKGs or patches.

#### Solaris admin File

The PKG preferences in the Solaris admin file describe how Solaris PKGs are deployed on Solaris machines. When you install the Sun Update Connection – Enterprise Agent on a Solaris machine, the path name of the Solaris admin file is `/opt/local/uce/agent/config_files/admin`.

You can change these parameters in the Preferences -> Host -> PKGs window, to change the parameters individually for a specific host; or you can point Sun Update Connection – Enterprise to your own customized Solaris admin file.

## Configure Agents on Idle

This procedure explains the steps for changing the Sun Update Connection – Enterprise preferences of Solaris agents in your environment. You cannot do the steps if the agent is busy with an Sun Update Connection – Enterprise job. Make sure the agents are idle before continuing.

### ▼ To Set PKG Preferences

In this procedure you will access and edit Preferences as needed. This procedure must be done before you deploy PKGs on hosts.

**1 From the Tools menu, choose Preferences.**

The Preferences window opens.



**2 In the Preferences window, select the Host radio button.**

The Host Selection window opens.

**3 Select one of the hosts to receive the job and then click OK.**

The Host Selection window closes and you are returned to the Preferences window. Wait while the Preferences values of the selected agent are uploaded to the console and displayed in the Preferences window.

**4 In the Category list, click PKGs.**

The PKGs preferences are displayed.

**5 Make appropriate changes and then click Submit.**

The Preferences Confirmation window opens.

The listed Target will be Host. The bottom panel lists the PKG parameters that you changed, with their new values.

**6 Check Restart Agent on target hosts.**

**7 Click Submit.**

Wait for the agent to restart and come back online and then select the same host again in the Host Selection window.



**8 Click Select target hosts.**

The Select Hosts window opens.

**9 Add the hosts to receive PKG deployment to the Selected Hosts list and then click OK.**

The preferences that you changed in the original host are copied to the selected hosts.

- **Mail address** – Notification emails will be sent to these addresses when PKGs are installed.
- **Package install basedir** – Base directory where relocatable packages are to be installed.
- **Instance** – If the PKG to install already exists on this machine, this parameter determines what Sun Update Connection – Enterprise will do and has the following options:
  - **Quit** – Do not install the PKG
  - **Overwrite** – Install the PKG again
  - **Unique** – Install the PKG as a unique instance
- **Partial** – If a partial install of a PKG is already on this machine, you can do the following:
  - **Nocheck** – Do not check for partially installed PKGs
  - **Quit** – Do not install the PKG if it is already partially installed
- **RunLevel** – If the system status is not correct for installing or uninstalling a PKG, you can choose one of the following:
  - **Nocheck** – Do not check run level
  - **Quit** – Do not install or uninstall if run level requirement is not met
- **Install Depend** – If other PKGs depend on the one being installed, you can choose one of the following:
  - **Nocheck** – Do not check for dependencies
  - **Quit** – Do not install a PKG if its dependencies are not met
- **Remove depend** – If other PKGs depend on the one that you want to uninstall, you can choose one of the following:
  - **Nocheck** – Do not check for dependencies
  - **Quit** – Do not uninstall a PKG that is needed by others
- **Check space** – If the disk space of this managed host does not meet the requirements of the PKG to install, you can choose one of the following:
  - **Nocheck** – Do not check disk space requirements (install will fail if the machine runs out of space)
  - **Quit** – Do not install the PKG if the listed space requirements are not met
- **Setuid flags** – The setuid and setgid flags are used in Solaris programming for security. If a PKG should enable these flags after installation, you can choose one of the following:
  - **Nocheck** – Do not check for setuid/setgid executables
  - **Quit** – Do not install the PKG if it will turn on these flags
  - **Nochange** – Install the PKG, but override the flags
- **Check conflicts** – If the installation of a PKG will overwrite a file provided by a previous PKG and create a conflict between files, you can choose one of the following:

- **Nocheck** – Do not check for conflicts and force install
- **Quit** – Do not install the PKG if file conflicts are detected
- **Nochange** – Install the PKG, but do not install conflicting files
- **Action scripts** – If an install of a PKG provides an action script that contains possible security impacts, you can choose one of the following:
  - **Nocheck** – Do not check for security impact of action scripts
  - **Quit** – Do not install the PKG if its action scripts could negatively impact security
- **Custom admin file full path name** – Path name of a customized Solaris admin file; if none, leave default.

## Multiple Distribution Host Lists

Sun Update Connection – Enterprise has the ability to simultaneously manage machines of different operating systems and architectures. You can create a single job and send it to any or all of your hosts. A single agent will ignore the components that are irrelevant to its distribution.

You can create Inventory-based jobs, profiles, and policies that contain components of several distributions, by selecting a new distribution in the drop-down list. However, Sun Update Connection – Enterprise offers a feature to make multiple distribution management easier.

For example, if you have a group of web servers, some of which are Red Hat 9.0 and others are Red Hat Enterprise Linux 3.0 Advanced Server, you can create one profile for web servers.

While you create the profile, you can apply settings to components of either of the distributions. Then, rather than searching for the same components in the other distribution, you can use the multiple distribution feature. It will automatically align the selected components with similar components on the other distribution. You can either accept the automatic alignment or intervene with checks and changes of your own.

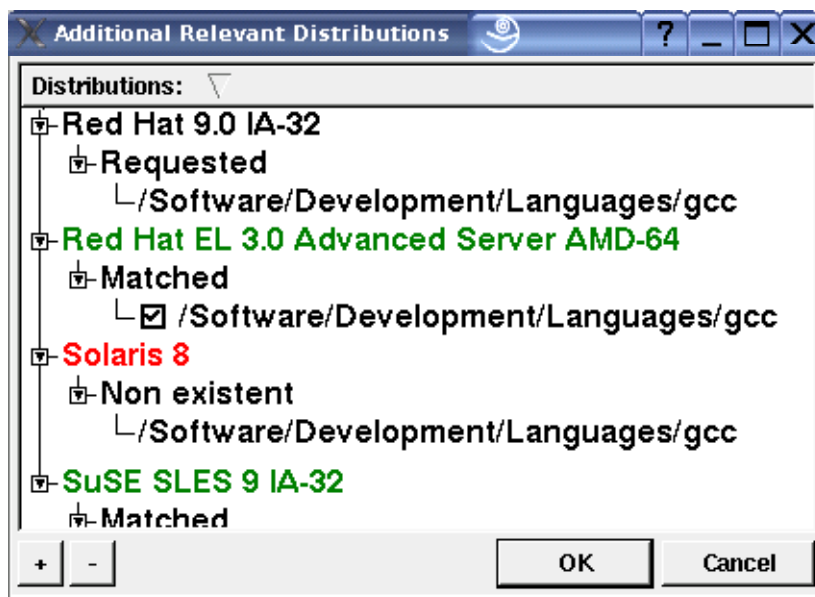
### ▼ To Align Component Settings for Multiple Distributions

In this procedure, you will make the component settings of a profile, policy, or inventory job applicable to hosts of multiple distributions. This will enable you to simultaneously manage hosts of different distributions in a consistent manner. This feature is available from the Profile Editor, the Policy Editor, and the Inventory panel of the main window.

- 1 **In the Components list, select the component and the setting or action that you want.**  
The component and the action appear in the Actions list.
- 2 **Do one of the following:**
  - **From the tool bar (main window or Profile Editor), click the Multi Distributions button.**

- Right-click in the Actions list and choose Multi Distributions.
- From the bottom of the Policy Editor, click the Multi Distro button.
- From the Actions menu of the main window, choose Multi Distributions.

The Multiple Distribution window opens.



The list of distributions is color-coded to show which have the selected components and which do not.

- 3 Expand the distributions that have the components (shown in green or yellow).
  - Check those components that you want to be aligned.
  - Leave unchecked the components that you do not want to be aligned.
- 4 Click OK to close the window.

You are returned to the Profile Editor, Policy Editor, or Inventory window. The aligned component settings are added to the Actions list.

- 5 To add more components from the distributions that did not have similar components (shown in red in the Multi Distribution window), select a new distribution in the drop-down list.**

The components list changes to show components from that distribution. Select the ones you want and add them to the Actions list. You can add as many component settings, from multiple distributions, as you choose.

## Component Search

At any time that you are focused on a Components list, the Find feature is available. It operates on the list of components that is currently active, according to the distribution that you selected. As each list contains thousands of components, the Find feature is indispensable.

### ▼ To Find Components

Sun Update Connection – Enterprise jobs are based on the component level. You decide what the requirements are for each type of machine, or for each individual machine, by selecting components and setting actions on them. In this procedure you will search the active components list for a component name or partial string.

- 1 Make sure that the active components list is of a relevant distribution.**

If it is not, change the selected distribution in the drop-down list on the tool bar.

- 2 Do one of the following:**

- **From the tool bar (main window or Profile Editor), click the Find button.**
- **Right-click in the Actions list and choose Find.**
- **From the Components menu, choose Find.**

The Find Components window opens.



**3 In the text field, type a component name or partial string.**

**4 Select the options that you want.**

Option	Checked	Unchecked
Match upper/lower case	Case-sensitive	Case-insensitive
Include versions	Results include package versions, categories, and package groups	Results include categories and package groups
Filter for empty names	Results include non-certified objects that have no software components associated with them	Results include categories and package groups
Limit search to selected component	Search within selected category or package group	Search throughout the entire list
List results in new window	Display results in Search Result window	First result highlighted in Components list

**5 Click Find.**

The Find window closes.

If the list results in the new window are checked, the Search Result window opens and shows all matching components.

- Double-click a result item to highlight it in the Components list.
- Click Close in the Search Result window to apply a setting on the component.
- To find the next matching component, press F3.

If the list results in the new window are unchecked, the first matching component is highlighted in the Components list.

- To find the next matching component, press F3.
- To find the previous match, press Shift + F3.

## To Use Regular Expressions

The Find feature supports regular expressions and pattern matching wildcards.

Sun Update Connection – Enterprise assumes that all search strings might be partial strings. You do not need a wildcard for “any characters”. For example, if you search for `gimp`, the results include `gimp`, `gimp-print`, and `xsane-gimp`.

If you want to restrict the default behavior, to search only for packages that begin with `gimp`, use: `^gimp`. The carrot (outside of brackets) indicates that the string must be the beginning of the pattern.

- `[char]` – Find any of the characters in the brackets.  
To find packages dealing with markup languages, either `xml` or `html`, search for `[xht]ml`.
- `[^char]` – Find any of the characters not in the brackets.  
If you want to find `http` packages, but do not want the list of `httpd`, search for `http[^d]`
- `[char-char]` – Find a range of characters.  
A regular expression of `c[a-u]p` results in a list that includes `cups`, `cdparanoia-libs`, `cipe`, and `libcap`.

## Job Management Features

The following procedures explain how to use various Sun Update Connection – Enterprise features that enable you to monitor and manage jobs after they have been created.

If your user account is restricted to simulate jobs only, you will not be able to perform all these features. Users with full permissions can use all the procedures.

Procedures in this section include:

- “To Confirm Tasks” on page 214
- “To Monitor a Current Job” on page 218
- “To View Job Log” on page 219
- “To Rerun a Job” on page 220
- “To Filter the Jobs Panel” on page 221
- “To Delete Jobs” on page 222
- “To Refresh the Jobs List” on page 223
- “To Reschedule Recurring Jobs” on page 223
- “To Install Interactive Solaris Patches” on page 224

### ▼ To Confirm Tasks


If you create a policy, you can predefine which actions should be done automatically (see “To Create a Policy” on page 183). If you chose the predefined Always ask me policy, or if the selected policy did not answer all actions, the job will pause for your confirmation. In this procedure, you will confirm or deny actions of a task of a job. The confirmation answers apply to all hosts selected for the job.

- 1 Make sure the Jobs panel of the main window is available. From the View menu, choose Jobs.**
- 2 From the Jobs list, click a paused job, indicated with the confirmation icon.**  
The tasks of the job appear in the Tasks list.
- 3 Select a task name with the confirmation icon.**
- 4 Do one of the following:**
  - **From the tool bar, click the Confirmation button.**
  - **Right-click the selected task and choose Confirmation.**
  - **From the Jobs menu, choose Tasks -> Confirm.**  
The Confirmation window opens, displaying suggested actions.

**Confirmation**

Job: check and fix security  
Task: security

Question ▾	Yes	No
Apply Fix acroread (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix cups-client (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix cups-libs (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix cups (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix curl (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix enscript (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix gpg2 (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix gpg (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix htdig (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix ImageMagick (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix imlib2-loaders (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix imlib2 (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix iproute2 (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix kdebase3 (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix kdegraphics3-fax (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix kdelibs3 (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix kernel-default-nongpl (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No
Apply Fix kernel-default (SUSE92 IA32)	<input type="radio"/> Yes	<input type="radio"/> No



- 5 If a confirmation question deals with a component for which you need more information, select the question and click the Details button.  
The Component Information window opens.
- 6 When you have the information you need, click OK to close the Component Information window. You are returned to the Confirmation window.
- 7 In the Confirmation window, select Yes to the questions you confirm and No to those you do not want Sun Update Connection – Enterprise to perform on the selected hosts.  
There are different types of questions, and your answers will cause different effect.



Question	Yes	No
Install, Uninstall, Upgrade, Downgrade	Sun Update Connection – Enterprise will perform this action.	The DR will execute again, searching for a solution that does not include these actions. If another solution is not found, the job fails.
Apply Fix	Sun Update Connection – Enterprise will fix the dependency, security, or bug issue.	Sun Update Connection – Enterprise will not apply the fix in this job.
Perform <i>action</i> (Mandatory)	Sun Update Connection – Enterprise will perform some action that is necessary to apply the deployment on the selected hosts.	The job will fail.
Perform <i>action</i> (without Mandatory)	Sun Update Connection – Enterprise will perform some action that is necessary to apply the deployment on the selected hosts.	The Host Progress window shows <b>Attention!</b> You do the listed action manually.
Accept	You accept that you have to do the special action manually. Until you handle the action, the job will be marked as failed.	This action does not concern you; possible effects: <ul style="list-style-type: none"> <li>■ The Host Progress window will show a reminder that this action should be done by someone at some point.</li> <li>■ If the action is mandatory, the job will fail.</li> </ul>

## 8 Click OK.

# More Information About Confirmation

## What Happens After Task Confirmation

If the job was in Simulate mode, the actions and results are calculated, giving you an accurate estimation of the required time and changes, and whether your answers will allow the job to succeed.

If the job was in Deploy mode, the confirmed actions that Sun Update Connection – Enterprise can do automatically are done on the selected hosts. If you have confirmed an Acknowledge question, the Host Progress windows shows **Acknowledged: <action>**. Remember that the results of the job might not be applied to the hosts until you actually do the acknowledged action.

If the Host Progress window shows **Attention! <action>**, you should do the action to have the results applied. Some actions can be done through Sun Update Connection – Enterprise. For others, you should ask make sure the action is done at some point, by someone.

If a job fails because you said No to a question, the reason given in the Host Log is: **Resolve failure - cannot resolve solution. User request.**

## ▼ To Monitor a Current Job

After you send a single job to be done on a list of hosts, the agent installed on each host finds an individual solution for the job. You can monitor the progress of each host, separately, as it performs the actions of a task in a job. You can also view the job log of each host. This procedure explains how to open and understand the Host Progress window and the Job Log window for a host.

**1 Make sure the Jobs panel of the main window is available. From the View menu, choose Jobs.**

**2 From the Jobs list, select a job.**

The tasks of the job appear in the Tasks list.

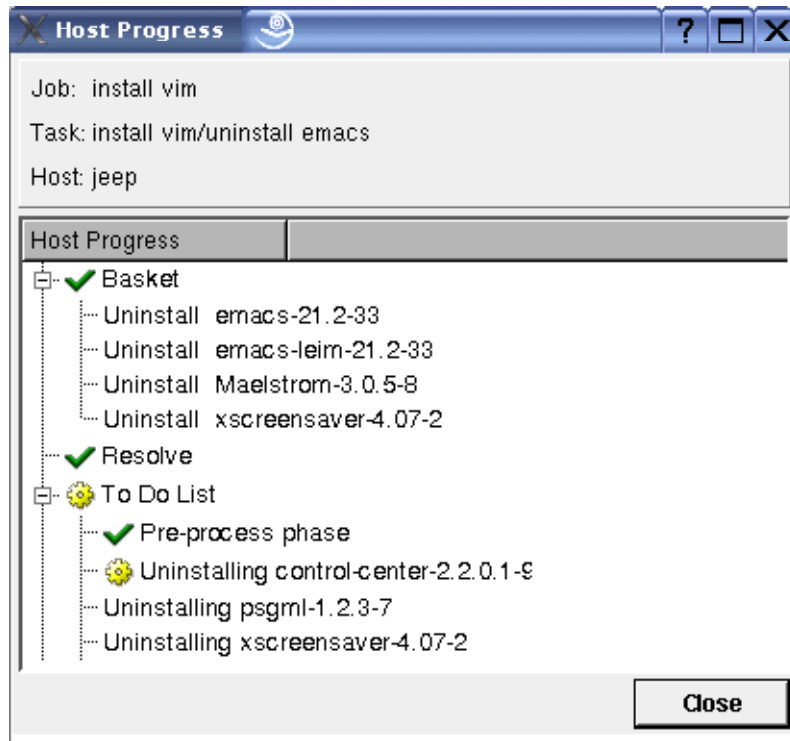
**3 From the Tasks list, select a task.**

The hosts running this task appear in the Hosts list of the Jobs panel.

**4 Select a host.**

**5 Do one of the following:**

- **From the tool bar, click the Host Progress button.**
- **Right-click the selected host and choose Host Progress.**
- **From the Jobs menu, choose Hosts -> Show Progress.**  
The Host Progress window opens.



## 6 Monitor the actions of the host for the selected task:

- **Basket** – The actions that you requested.
- **Resolve** – Status of the dependency resolver finding a solution.
- **To Do List** – List of actions to be taken to fulfill the solution. This list might contain special actions. If it is Perform <action>, Sun Update Connection – Enterprise does the action automatically. If the To Do item is Attention! <action>, you are expected to handle the action yourself before the job will continue.

If there is a problem, you can click the Stop Job button. The job will stop at a safe place.

## ▼ To View Job Log

When a job is done, either on success or failure, you can see the log of actions for all tasks of the job on the selected host. Each host may have a different log for the same job.

- 1 **Make sure the Jobs panel of the main window is available. From the View menu, choose Jobs.**

**2 From the Jobs list, select a job.**

The tasks of the job appear in the Tasks list.

**3 From the Tasks list, select a task.**

The hosts running this task appear in the Hosts list of the Jobs panel.

**4 Select a host.**

**5 Open the Job Log. Do one of the following:**

- **From the tool bar, click the Job Log button.**
- **Right-click the selected host and choose Show Log.**
- **From the Jobs menu, choose Hosts -> Show Log.**

The Job Log window opens.

The Job Log shows each phase and whether it started and finished successfully. If there are any errors, they are listed.

To send the log to technical support, click Save As, save the log on the console machine, and email it with all relevant details.

If the failure reason is User request, run the job again with different Confirmation answers or a different Policy. This error indicates that you denied actions that were necessary to the success of the job.

## ▼ **To Rerun a Job**

Rerun a job that has completed, either successfully or with a failure.

**1 Make sure the Jobs panel of the main window is available.**

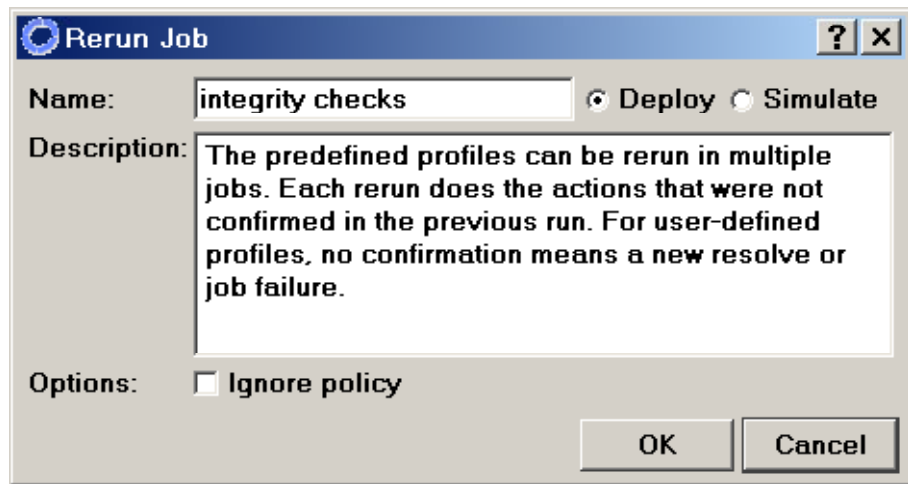
From the View menu, choose Jobs.

**2 From the Jobs list, select a job.**

**3 Do one of the following:**

- **From the tool bar, click the Rerun button.**
- **Right-click the selected job and choose Rerun.**
- **From the Jobs menu, choose Rerun.**

The Rerun window opens.



- 4 Give the job a new name and an optional description.
- 5 Select a mode for the job:
  - Deploy – Execute the job actions
  - Simulate – Test the job
- 6 If the job failed because the policy did not allow certain components to be changed, check Ignore Policy to ensure that the job has a chance to succeed.
- 7 Click OK.

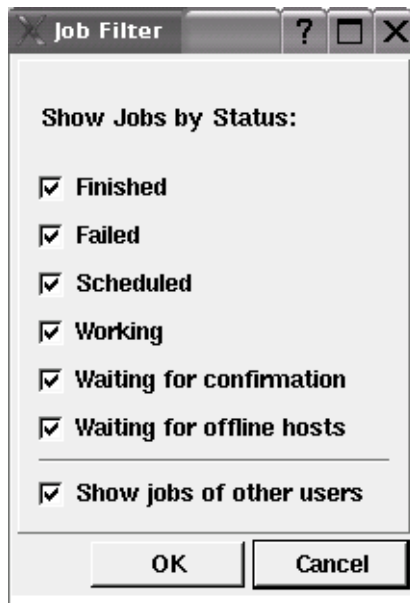
The Rerun window closes and the new job is added to the Jobs list. This job runs the same tasks, on the same host list, as the original job.

## ▼ To Filter the Jobs Panel

Set the filters to show the information you want in the Jobs panel. This enables you to easily find information about jobs, tasks, and hosts in the Jobs list that is important to you.

- 1 **Make sure the Jobs panel of the main window is available.**  
From the View menu, choose Jobs.
- 2 **Do one of the following:**
  - **From the tool bar, click the Filter button.**

- **Right-click in the Jobs list and choose Filter.**
- **From the Jobs menu, choose Filter.**  
The Jobs Filter window opens.



- 3 **Check options to filter the list for jobs by status and by owner.**
- 4 **Click OK.**

The Jobs list changes to display only the jobs that match the checked filtering options.

---

**Note** – You can organize the Jobs list by dragging columns in any order you choose. You can click a column header to order the list alphanumerically.

---

## ▼ **To Delete Jobs**

In this procedure, you will delete job listings that are no longer relevant. When you delete a job listing, the data remains in the system dependency server. You can query job history from reports (see “[Job History Reports](#)” on page 249).

---

**Note** – You can use the profiles and policies of jobs that are in the list, so do not delete jobs until you are sure they are no longer relevant.

---

- 1 Make sure the Jobs panel of the main window is available.**

From the View menu, choose Jobs.

- 2 From the Jobs list, select a job that is no longer current.**

- 3 Do one of the following:**

- **From the tool bar, click the Delete Job button.**

- **Right-click in the Jobs list and choose Delete.**

- **From the Jobs menu, choose Delete.**

The job listing is removed from the Jobs window.

## ▼ To Refresh the Jobs List

The Jobs list is updated for current dynamics on a schedule. If you want to make sure that the list is accurate, use this procedure to force the update and refresh the list.

- 1 Make sure the Jobs panel of the main window is available. From the View menu, choose Jobs.**

- 2 Do one of the following:**

- **From the tool bar, click the Refresh button.**

- **Right-click in the Jobs list and choose Refresh.**

- **From the Jobs menu, choose Refresh.**

The list is updated, if necessary.

## ▼ To Reschedule Recurring Jobs

If you set a Complex job for a recurring schedule, you can change the schedule at any time after it is in the Jobs list.

- 1 Make sure the Jobs panel of the main window is available. From the View menu, choose Jobs.**

- 2 Do one of the following:**

- **From the tool bar, click the Reschedule button.**

- **Right-click in the Jobs list and choose Reschedule.**

- **From the Jobs menu, choose Reschedule.**  
The Reschedule window opens.
- 3 **Select days of the month:**
    - **Every day** – Job runs every day of the month, or year (if Every Month was selected).
    - **Day in week** – Select the days of the week on which the job will be run.
    - **Day in month** – Select dates in the month on which the job will be run (use Shift or Control to select multiple dates).
  - 4 **Select time of the day:**
    - **Earliest.** Set a time (*hour:minute*) for the first run of the job.
    - **Interval.** Set a minute interval to have the job run more than one time a day.
    - **Latest.** Set a time for the latest run of the job if you specified an interval for multiple runs.
  - 5 **Click OK.**

## ▼ To Install Interactive Solaris Patches

You can install Solaris patches as an inventory-based job or as a complex job. Some patches are handled automatically by Sun Update Connection – Enterprise, while other patches demand user interaction.

When you need to install an interactive Solaris patch, Sun Update Connection – Enterprise downloads the patch for you, but you must handle the manual intervention actions yourself.

- 1 **Create a job to install the patches.**
- 2 **Run the job.**  
The job will pause with confirmation questions.
- 3 **From the Jobs panel, select the task that contains the patch and click the Confirmation button.**  
The Confirmation window opens.  
One of the following questions will appear:
  - `Accept Install of patch requires manual intervention for component`
  -



Accept Uninstall of patch requires manual intervention for *component*

**4 Click Yes for this question.**

This means that you accept the responsibility for handling this patch. If you select No, the job fails.

**5 In the Confirmation window, click OK.**

The job begins. It downloads the patch you requested to the `/opt/local/uce/agent/blobs.save` directory on the selected Solaris machines.

When the job reaches the point where it would install the patch, it is marked as failed and stops.

**6 On the Solaris machines, manually install `/opt/local/uce/agent/blobs.save/patchname-ver.`**

**7 On the console machine, right-click the job in the Jobs panel and choose Rerun.**

The Rerun window opens.

**8 Select Deploy and then click OK.**

Sun Update Connection – Enterprise runs the job again, recognizes the installed required patch, and continues.

## Troubleshooting Jobs

In the Jobs panel, you might see that a job failed on a host. There are various reasons for a failed job, and different ways in which you can handle the issue.

To which troubleshooting procedure is most relevant, open the Job Log (see [“To Monitor a Current Job” on page 218](#)).

Procedures in this section include the following:

- [“Handling Resolve Failures” on page 225](#)
- [“Handling Failures Due to Cost” on page 226](#)
- [“Handling Missing Components” on page 226](#)
- [“Handling Installation Issues” on page 227](#)

## Handling Resolve Failures

If a job failure occurs during the resolve stage, troubleshoot the solution offered by the Dependency Resolver with these checks.

- Open the Host Progress window of a failed host and check for manual intervention points. Handle the manual procedures and rerun the job.
- Open the Job Log of a failed host. Carefully check components and actions in the job. For example, you might have created a profile that demanded conflicting actions on some components. Recreate the job without the problematic components.

- Change or create a policy that causes the agent to look for a different DR for the job. The confirmation policy should Not Allow the components listed under the failure reason to receive the failed actions.

You might find it helpful to review the Resolve Log of the failed host. Open the Preferences window of the selected host to find the directory and file name of this log (see [“Host Preferences – Logs” on page 301](#)).

## Handling Failures Due to Cost

Sometimes a failed DR cannot be fixed. The message cost in change too high indicates that the DR found so many components that would have had to be changed, that it will not go on.

- If you requested many components, break up your request into smaller jobs.
- If you requested only a few components, try making a job of each component separately. You will probably find one that demands too many dependency fixes. Perhaps you can select an alternative component.

## Handling Missing Components

Sometimes a component cannot be installed or uninstalled. One of the following errors might appear to explain the DR failure:

- ```
component is not installable by current KB
```

- ```
component is not removable by current KB
```

Only Local components may be not installable or not removable. To handle these issues, open the Local category in the Components list of the main window. Expand the subcategories until you find the problematic components.

- The Components list might include listings for which you do not have the software component: an NCO without an attached software, a 3rd-Party application for which you do not have a license, a tool without an uploaded script, and so on.

If this is the problem, the package will be marked with an empty software icon.

If you see one of these icons, upload the required software component.

See [“Fixing Local Dependencies” on page 100](#).

- The local component might be in the knowledge base, but missing dependencies according to the deployment rules.

If this is the problem, the package will be marked with an exclamation point in a red circle.

Right-click the component and choose Component Details.

---

The Component Information window opens, displaying the missing requirements in the Dependencies tab.

## Handling Installation Issues

If the job failed during installation, use these checks to find a solution.

- Check the permissions needed by the component for install. The permissions might conflict with the permissions of the logged-in user. The Job Log of the failed host will show permissions as the reason for failure.
- Try to install the component manually with Linux terminal commands. Afterwards, run a Check System (see [“Running Predefined Profiles” on page 140](#)) to handle dependency issues.  
If the installation fails for an NCO (non-certified component), the Job Log might provide one of the following reasons.
  - **Conflict with.** Listed NCO has possible conflicts with a component from the To Do list.
  - **Downgrade.** Listed NCO appears to be a newer version of a component from the To Do list.
  - **Possible Unavailability.** Installing one of the components from the To Do list might cause the listed NCO to become inoperable.
- Run the Local Software Review predefined profile and replace NCOs with COs, or uninstall the NCOs.
- Make sure that the NCO has been detected and added to the components list. If the local software package is not under Local RPMs or Local PKGs, search for it under a CO listing in Software (see [“To Find Components” on page 212](#)). If the NCO is not in the components list, add it (see [“Adding Undetected Linux Software” on page 85](#)).



# Reports

---

This chapter describes Sun Update Connection – Enterprise reports. This chapter defines each report, shows how to access them, customize them, and understand the report results. Reports enable you to better manage your machines, with regards to patch and incident management.

This chapter covers the following topics:

- “Terms” on page 229
- “Report Explanations” on page 230
- “Generating Reports” on page 231
- “Filtering and Viewing Incident Reports” on page 232
- “Incident Compliance Reports” on page 236
- “Host Compliance Reports” on page 240
- “CVE Compliance Reports” on page 242
- “Package Compliance Reports” on page 244
- “Service Pack Compliance Reports” on page 247
- “Job History Reports” on page 249
- “Managing Reports” on page 250

## Terms

This chapter uses the following terms:

Enhancement	Package provided by and defined by a distribution vendor as a fix that is neither security nor bug fix, but which enhances an earlier package.
Patch	Sun Solaris binary, named in a numbering system, that adds some type of fix to an already installed PKG.
Nonpatch	RPMs from Linux advisories or PKGs from Sun Freeware, which provide a fix to an existing package; not as a binary to be added to a package, but as a standalone package.

Incident	Fix for an application or feature that may include a number of packages.
Channel	Linux distribution version or Solaris version, and hardware architecture.
CVE ID	Patches and packages from the list of candidates to be published as common vulnerabilities and security exposure incidents (also known as CVE ID). See <a href="http://cve.mitre.org/cve/index.html">http://cve.mitre.org/cve/index.html</a> .
Compliant	Host has the patch, package, incident, or profile installed.
Service Pack	Mass release of packages by a distribution vendor, which when installed will solve various incident issues.

## Report Explanations

Reports offer access to the latest patches, fixes, and incidents. There is also a report type for Sun Update Connection – Enterprise job history, for general job auditing.

When you ask that a report be generated, you select the criteria that are relevant to you, such as host list and whether you want to know which hosts have a specific patch or whether you want to know which do not. The report that is generated is a table of information that you can easily review for efficient, up-to-date management of all your hosts.

- **Incidents** – Basic information of all known distribution and local incidents.
- **CVE Compliance** – Incidents that belong to a given CVE ID.
- **Host Compliance** – Reports on whether hosts are compliant to security and bug fix incidents.
- **Incidents Compliance** – Mapping between selected incidents and selected hosts; to find if incidents are installed.
- **Package Compliance** – Incidents relevant to selected packages.
- **Service Pack** – Incidents created by the publication and release of a service pack by a vendor.
- **Jobs History** – History of installs and uninstalls done by Sun Update Connection – Enterprise on managed hosts.

Reports enable you to check for new patches, security advisories, and so on. You can get a general report, or test a host or installed package for available fixes. You can search for specific Solaris patches by their CVE IDs.

# Generating Reports

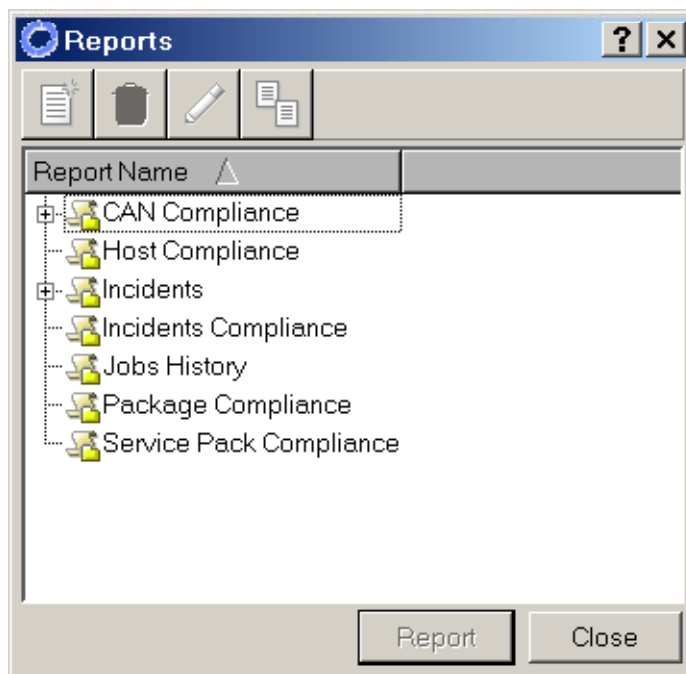
When you open the Reports window, there is a list of types of reports. You select the type that you want, fill in the criteria options, and then decide whether you want to generate the report immediately, or save the criteria as a report template.

## ▼ To Access Reports

1 Do one of the following:

- From the tool bar, click the Reports button.
- From the Tools menu, choose Reports.

The Reports window opens.



2 Select one of the report types.

**3 From the tool bar of the Reports window, click the New button.**

A Report Editor window opens where you choose the criteria to create the new report. Each report type opens a different Report Editor window.

**4 Type a unique name for the new report and an optional, free-text description.**

**5 Choose the relevant criteria.**

**6 Do one of the following:**

▪ **Click Report.**

A report is displayed in a Report Result window. The columns of this window differ between the types of reports.

▪ **Click Save.**

The report criteria are saved as a template, under the report type. Select the report template and click Report to get current results, as often as you like.

## Filtering and Viewing Incident Reports

Generate Incident reports to get a list of incidents linked to packages, CVE IDs, or just a general list of incidents. This report does not tell you if your hosts are compliant with the incidents. It provides information about incidents of filtered categories and types, or a complete list of incidents for a channel.

When an incident is published by a vendor, it contains more than the packages; it also contains information on the source issue of the incident and why the packages included are needed. You can access this information as well through the Incident report.

### ▼ To Filter an Incident Report

Filter an incident report in the Incident Report Editor window. The criteria that you select can create a large general list or a specific query.

**1 In the Reports window, select Incidents and then click the New button.**

The Incidents Report Editor opens.



**Incidents Report Editor**

Name:

Description:

Incidents

Category:  Security  Bug fix  Enhancement  Service Pack  CD

Type:  Nonpatch  Patch

Released:

Channel:

Incident:

Package:

CAN Id:

- 2 **Select categories and types of incidents that are relevant to the report.**  
You must select at least one category and one type.
- 3 **Click Report now if you do not want to apply more filters.**

## ▼ To Filter a Report by Date

- 1 **Click the Select Dates button.**  
The Select Dates window opens.
- 2 **Select a date range:**
  - **Relative.** Specify how many days since the incident was published.

- **Range.** Click the **Select Dates** buttons to specify a start date and an end date for the time range.

If the date is not important, leave the default Any date selected.

## ▼ **To Filter a Report by Channel**

- 1 **Click the Select button next to the Channel box.**

The Channel Select window opens.

- 2 **Select relevant channels.**

To select multiple channels, use the Shift key or the Ctrl key. To select all, type Ctrl+A.

- 3 **Click OK.**

The selected channels appear in the Channel box of the Report Editor.

## ▼ **To Filter a Report by Specific Package, CVE ID, or Incident**

- 1 **Click a Select button.**

The Select window opens and shows the filter names.

- 2 **Select relevant items and click Add.**

- 3 **Click OK.**

## **Viewing Incident Reports**

After you select the criteria in the Incident Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

Incident	Category	Type	Channel	Release	#Pkgs
abiword-51808	Security	Non-patch	SUSE92_IA32	2005-05-03	1
acroread-52336	Security	Non-patch	SUSE92_IA32	2005-07-15	1
apache-52347	Security	Non-patch	SUSE92_IA32	2005-07-20	1
apache2-51791	Security	Non-patch	SUSE92_IA32	2005-05-03	4
apache2-52356	Security	Non-patch	SUSE92_IA32	2005-07-27	3
apache2-mod_php4-52329	Security	Non-patch	SUSE92_IA32	2005-07-08	9
apache2-mod_python-52012	Security	Non-patch	SUSE92_IA32	2005-05-03	1
bogofilter-51771	Security	Non-patch	SUSE92_IA32	2005-05-03	1
bzip2-52249	Security	Non-patch	SUSE92_IA32	2005-06-14	1
compat-curl2-52287	Security	Non-patch	SUSE92_IA32	2005-06-15	1
cups-51982	Security	Non-patch	SUSE92_IA32	2005-05-03	4
cyrus-sasl-51738	Security	Non-patch	SUSE92_IA32	2005-05-03	2
dnsmasq-52135	Security	Non-patch	SUSE92_IA32	2005-05-03	1
enscript-52005	Security	Non-patch	SUSE92_IA32	2005-05-03	1

FIGURE 13-1 Report Window – Incidents

Each line in the Report shows the incident name (defined by vendor), category, type, channel, and release date. It shows the number of packages that belong to this incident.

To see package details of an incident, select an incident name in the report and then click Details. A new Report window opens, displaying the packages needed for the selected incident. The Recommended columns list the latest incident name and package version that is recommended for you to install. If an incident is a newer fix to a previous incident, the recommended incident shows which incident (and installation of its packages) will bring your systems most up-to-date.

To see informational details of an incident, select a line in the new report list and click Incident Information. The Incident Information window opens.

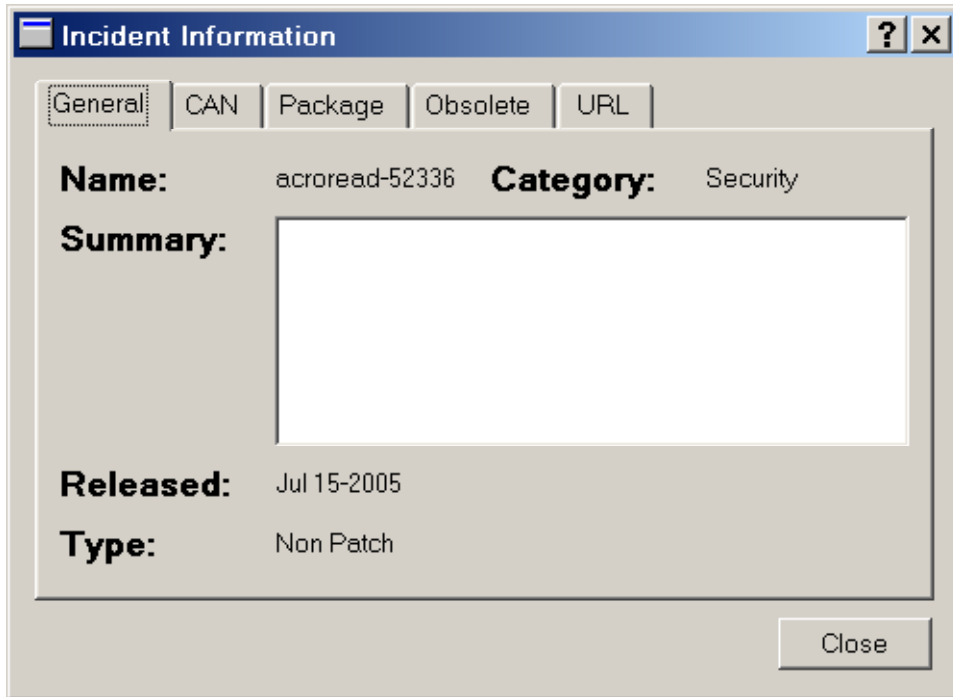


FIGURE 13-2 Incidents Information

The Incident Information window has the following tabs:

- **General.** Includes the name, category of incident, summary (if the vendor published one), date released, and type (nonpatch or patch).
- **CVE.** Shows the ID in the CVE list.
- **Package.** Shows the list of packages that are related to this incident.
- **Obsolete.** Shows the list of incidents that are made obsolete by this incident.
- **URL.** Shows the reference to more information published by the vendor.

## Incident Compliance Reports

Generate Incident Compliance reports to discover which incidents should be installed, or have already been installed, on which of your hosts. The report provides relevant information. The Incident report shows all incidents. The Incident Compliance report filters the list for what is relevant to each selected host.

## ▼ To Filter an Incident Compliance Report

Filter an incident compliance report in the Incident Compliance Report Editor window. This report requires that you filter for incident name. You may choose all available incidents, to make a very general report; or you may choose a specific incident to get a report of host compliance on this particular set of packages.

- 1 In the Reports window, select Incident Compliance and then click the New button.**  
The Incident Compliance Report Editor opens.

The screenshot shows a dialog box titled "Incidents Compliance Report Editor". It has a standard Windows-style title bar with a minimize button, a maximize button, and a close button. The dialog is divided into several sections:

- Name:** A text box containing "suse-enhancements".
- Description:** A text box containing "this report shows nonpatch enhancements to my suse channel, and the hosts on that channel that need these to be installed".
- Hosts:** A section with a "Hosts:" label and a text box containing "SUSE92\_IA32 hosts". To the right of the text box is a small icon of a document with a plus sign. Below this is a "Status:" label with two radio buttons: "Compliant" (unselected) and "Not Compliant" (selected).
- Incidents:** A section with two radio buttons: "Select Incidents" (unselected) and "Filter" (selected). Below these are several controls:
  - Category:** Three checkboxes: "Security" (unselected), "Bug fix" (unselected), and "Enhancement" (checked).
  - Type:** Two checkboxes: "Nonpatch" (checked) and "Patch" (unselected).
  - Released:** A text box containing "Any date" with a small icon of a calendar.
  - Package:** A text box with a small icon of a document with a plus sign.
  - CAN Id:** A text box with a small icon of a document with a plus sign.

At the bottom of the dialog are three buttons: "Save", "Report", and "Cancel".

FIGURE 13-3 Incident Compliance Report Editor

**2 Click the Select button by the Hosts box.**

The Select Hosts window opens.

**3 Select relevant hosts and click the Add button to add them to the Selected list.**

**4 Click OK.**

The selected hosts appear in the Hosts box.

**5 Select one of the following status options:**

- **Compliant. Show hosts that have the selected incidents installed.**
- **Not Compliant. Show hosts that should have the incidents installed.**

**6 To check compliance with specific incidents, select the Select Incidents radio button and click the Select button next to the Name box.**

The Select window opens and shows incident names. Add the incidents on which you want the report.

**7 To check compliance with incidents of categories or types, select the Filter radio button and then select categories and types of incidents (you must select one of each).**

Optionally, you can filter the incidents for date (see [“To Filter a Report by Date” on page 233](#)), included packages, and CVE ID (see [“To Filter a Report by Specific Package, CVE ID, or Incident” on page 234](#))

## Viewing Incident Compliance Reports

After you select the criteria in the Incident Compliance Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

Each line in the Report shows the incidents you selected, or those that matched your filters, and the number of hosts with the compliance status that you selected (compliant or not compliant). If you selected compliant for status, the report shows how many of the selected hosts have this incident installed. If you selected not compliant, the report shows how many of the selected hosts should have this incident installed.

To see which hosts are counted in the row, select an incident name in the report and then click Details. A new Report window opens, displaying the host names and the number of packages needed for the selected incident.

To see package details, click Details again. The Report window is cleared, and then it displays the packages needed for the selected incident. It shows the versions that are currently installed and lists the versions that should be installed to finalize this incident.

To see informational details of an incident, select a line in the new report list and click Incident Information. The Incident Information window opens.

## ▼ To Create an Incident Compliance Job

From the Incident Compliance report, you can create a job to install the packages that are related to a selected incident on the hosts selected in the report editor.

- 1 In the Incident Compliance Report Editor, select Not Compliant for the Status.**
- 2 Select the remaining criteria for the report and then generate the report.**
- 3 Select a specific incident and then click Details.**  
The report shows the noncompliant hosts.
- 4 Select hosts and then click Details.**  
The report shows the packages to install on the hosts.
- 5 Select packages and then click Send Job.**  
The job installs the recommended version.

## Host Compliance Reports

Generate Host Compliance reports to discover hosts should be updated for security fixes. You may choose to get a report that lists hosts that are compliant; or a report of those that need to be fixed. The security issues could be of those incidents that are security; or it could include both security and bug fixes.

## ▼ To Filter a Host Compliance Report

Filter a host compliance report in the Host Compliance Report Editor window. This report requires that you filter select an option from each filter.

- 1 In the Reports window, select Host Compliance and then click the New button.**  
The Host Compliance Report Editor opens.



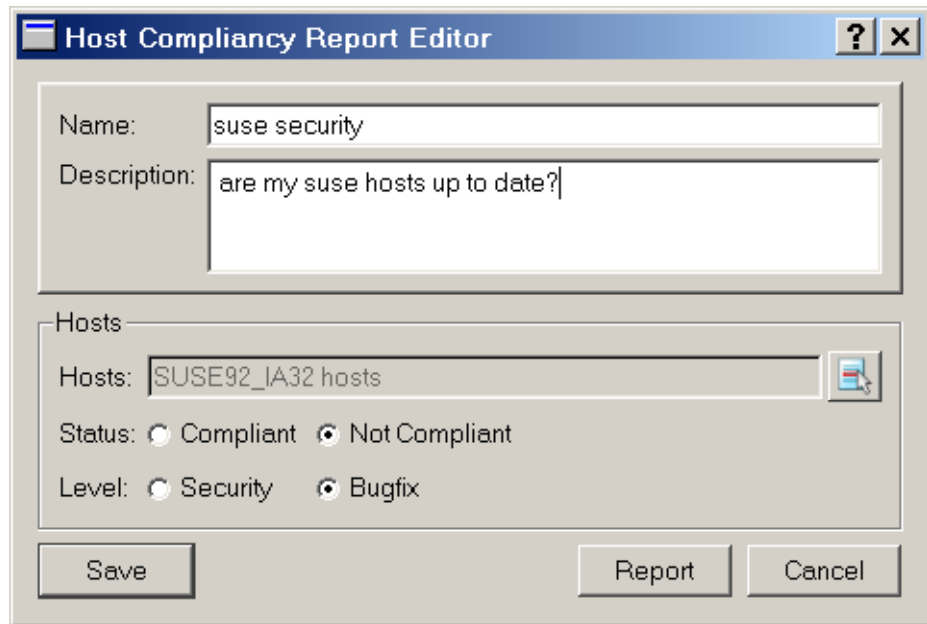


FIGURE 13-4 Host Compliance Report Editor

**2 Select hosts for the report.**

See “[To Filter an Incident Compliance Report](#)” on page 237.

**3 Select status options:**

- **Compliant.** Show hosts that are compliant with known security incidents.
- **Not Compliant.** Show hosts that need management to be compliant.

**4 Select level of incidents:**

- **Security.** Show security incidents
- **Bug fix.** Show security and bug fix incidents

## Viewing Host Compliance Reports

After you select the criteria in the Host Compliance Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

Each line in the Report shows the hosts you selected and the number of incidents with the compliance status that you selected (compliant or not compliant). If you selected compliant for status, the report shows how many incidents have been installed on each of the selected hosts; if you selected not compliant, the report shows how many incidents should be installed on each host.

To see which incidents are counted in the row, select a host name in the report and then click Details. The report displays the incident names.

To see package details, click Details again. The report displays the packages needed for the selected incident. It shows the versions that are currently installed and lists the versions that should be installed to finalize this incident.

To see informational details of an incident, select a line in the new report list and click Incident Information. The Incident Information window opens.

## ▼ To Create a Host Compliance Job

From the Host Compliance report, you can create a job that will install the packages related to needed incidents on the selected hosts.

- 1 **In the Host Compliance Report Editor, select Not Compliant for the Status.**
- 2 **Select the remaining criteria for the report and then generate the report.**
- 3 **Select a specific host and then click Send Job.**

The job installs the recommended version of each package.

Optionally, you can send the job from the report windows opened after clicking Details, to create a smaller job, of selected incidents, or selected packages.

# CVE Compliance Reports

Generate CVE Compliance reports to find incidents related to specific CVE IDs and the hosts that should have these incidents installed.

## ▼ To Filter a CVE Compliance Report

Filter a CVE compliance report in the CVE Compliance Report Editor window. This report requires that you filter select an option from each filter.

- 1 **In the Reports window, select CVE Compliance and then click the New button.**

The CVE Compliance Report Editor opens.

The screenshot shows a Windows-style dialog box titled "CAN Compliance Report Editor". It contains the following fields and controls:

- Name:** An empty text input field.
- Description:** A larger empty text input field.
- Hosts:** A text input field containing "All Hosts" and a small icon to the right.
- Status:** Two radio buttons: "Compliant" (unselected) and "Not Compliant" (selected).
- CAN:** A text input field containing "005-2364,CAN-2005-2365,CAN-2005-2366,CAN-2005-2367" and a small icon to the right.
- Buttons:** "Save", "Report", and "Cancel" buttons at the bottom.

- 2 **Select hosts for the report.**  
See [“To Filter an Incident Compliance Report”](#) on page 237.
- 3 **Select one of the following status options:**
  - **Compliant.** Show hosts that are compliant with known security incidents.
  - **Not Compliant.** Show hosts that need management to be compliant.
- 4 **Select the CVE IDs that you want Sun Update Connection – Enterprise to match to incidents.**  
See [“To Filter a Report by Specific Package, CVE ID, or Incident”](#) on page 234.

## Viewing CVE Compliance Reports

After you select the criteria in the CVE Compliance Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

The Report shows the CVE IDs you selected and the number of incident-packages with the compliance status that you selected (compliant or not compliant). If you selected compliant for status, the report shows how many packages have been installed on each of the selected hosts to be compliant with an incident. If you selected not compliant, the report shows how many packages should be installed on each host for incidents of this CVE ID.

To see which incidents are counted in the row, select a host name in the report and then click Details. The report displays the incident names and the packages of each incident.

To see informational details of an incident, select a line in the new report list and click Incident Information. The Incident Information window opens.

### ▼ To Create a CVE Compliance Job

From the CVE Compliance report, you can create a job that will install, on the selected hosts, the packages needed to resolve the CVE ID and the incidents related to it.

- 1 In the CVE Compliance Report Editor, select Not Compliant for the Status.**
- 2 Select the remaining criteria for the report and then generate the report.**
- 3 Select listed CVE IDs and then click Details.**  
The report shows the packages to install.
- 4 Select packages and then click Send Job.**  
The job installs the recommended version of each package.

## Package Compliance Reports

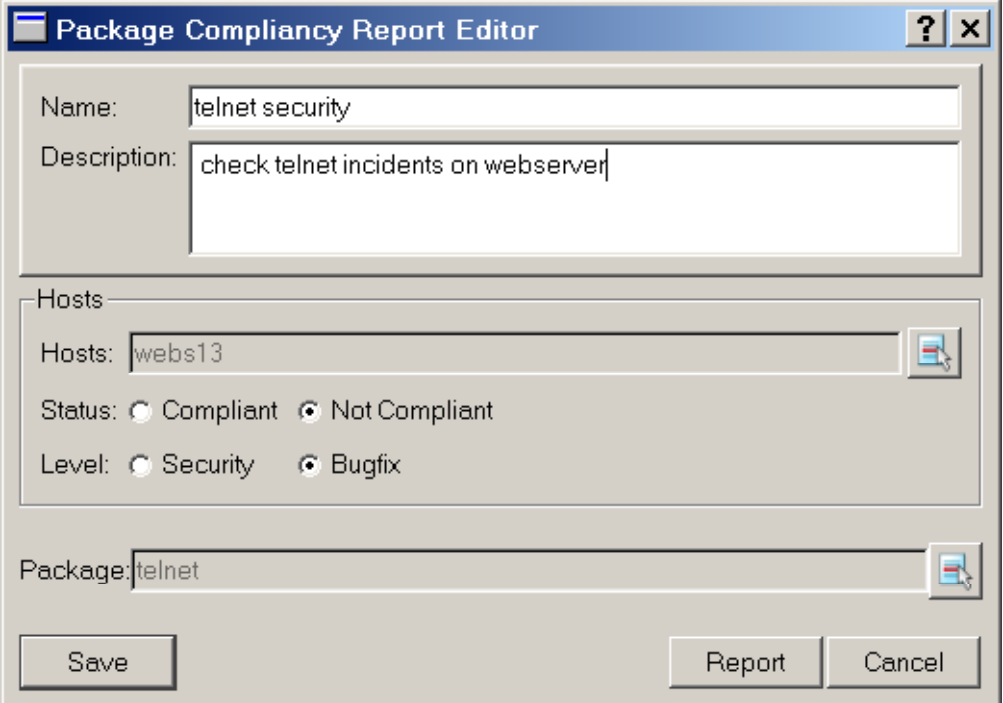
Generate Package Compliance reports to find incidents related to specific packages. For example, if you have a mission-critical application, use the Package Compliance Report to discover if there are new incidents related to this application and to make sure you have up-to-date versions of relevant packages.

## ▼ To Filter a Package Compliance Report

Filter a Package Compliance report in the Package Compliance Report Editor window. This report requires that you filter select an option from each filter.

- 1 In the Reports window, select Package Compliance and then click the New button.

The Package Compliance Report Editor opens.



The screenshot shows the 'Package Compliancy Report Editor' window. It has a title bar with a question mark and close button. The main area contains the following fields and options:

- Name:** telnet security
- Description:** check telnet incidents on webserver
- Hosts:** webs13
- Status:**  Compliant  Not Compliant
- Level:**  Security  Bugfix
- Package:** telnet

At the bottom, there are three buttons: 'Save', 'Report', and 'Cancel'.

- 2 Select hosts for the report.

See “To Filter an Incident Compliance Report” on page 237.

- 3 Select one of the following status options:

- **Compliant.** Show hosts that are compliant with known security incidents.
- **Not Compliant.** Show hosts that need management to be compliant.

- 4 Select one of the following level options:

- **Security.** Show security incidents.

- **Bug fix. Show security and bug fix incidents.**
- 5 Select the packages that you want Sun Update Connection – Enterprise to match to incidents.**  
See “[To Filter a Report by Specific Package, CVE ID, or Incident](#)” on page 234.

## Viewing Package Compliance Reports

After you select the criteria in the Package Compliance Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

The Report shows the packages you selected and the number of hosts and incidents with the compliance status that you selected (compliant or not compliant). If you selected compliant for status, the report shows how many hosts have this package to be installed; if you selected not compliant, the report shows how many hosts need this package to be installed.

To see which incidents and hosts are counted in the row, select a package name in the report and then click Details. The report displays host names and incidents, what is installed on the hosts and what is recommended for installation.

To see informational details of an incident, select a line in the new report list and click Incident Information. The Incident Information window opens..

## ▼ To Create a Package Compliance Job

From the Package Compliance report, you can create a job that will install, on the selected hosts, the package version need to resolve the incident.

- 1 In the Package Compliance Report Editor, select Not Compliant for the Status.**
- 2 Select the remaining criteria for the report and then generate the report.**
- 3 Select listed packages and then click Details.**  
The report shows the hosts on which the package should be installed.
- 4 Select packages and then click Send Job.**  
The job installs the recommended version of each package.

# Service Pack Compliance Reports

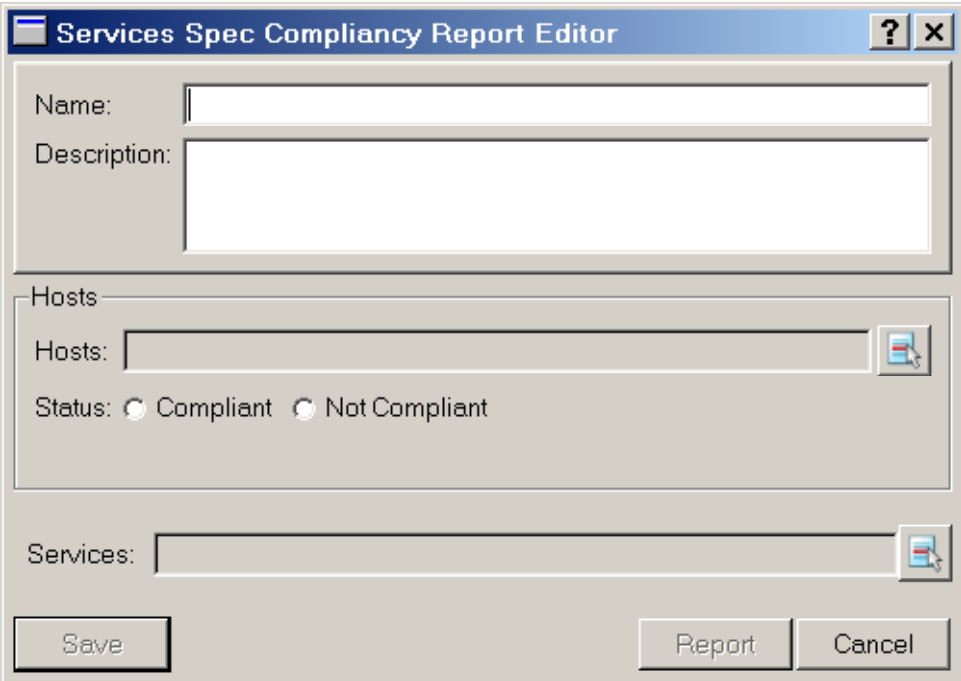
Generate Service Pack Compliance reports to find if your hosts have the latest service packs provided by vendors.

## ▼ To Filter a Service Pack Compliance Report

Filter a Service Pack Compliance report in the Service Pack Compliance Report Editor window. This report requires that you filter select an option from each filter.

- 1 In the Reports window, select Service Pack Compliance and then click the New button.

The Service Pack Compliance Report Editor opens.



The screenshot shows the 'Services Spec Compliancy Report Editor' dialog box. It has a title bar with a question mark and a close button. The dialog contains several input fields and buttons:

- Name:** A single-line text input field.
- Description:** A multi-line text input field.
- Hosts:** A text input field with a search icon on the right.
- Status:** Two radio buttons labeled 'Compliant' and 'Not Compliant'.
- Services:** A text input field with a search icon on the right.
- Buttons:** 'Save', 'Report', and 'Cancel' buttons are located at the bottom of the dialog.

- 2 Select hosts for the report.

See [“To Filter an Incident Compliance Report”](#) on page 237.

- 3 Select one of the following status options:

- **Compliant.** Show hosts that are compliant with known security incidents.

- **Not Compliant. Show hosts that need management to be compliant.**
- 4 **Select the service packs that you want Sun Update Connection – Enterprise to match to the selected hosts.**  
See [“To Filter a Report by Specific Package, CVE ID, or Incident”](#) on page 234.

## Viewing Service Pack Compliance Reports

After you select the criteria in the Service Pack Compliance Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

The Report shows the service packs you selected and the number of packages with the compliance status that you selected (compliant or not compliant, with the service pack). If you selected compliant for status, the report shows how many packages of the service pack are installed on the host; if you selected not compliant, the report shows how many packages this host needs to install.

To see which packages are counted in the row, select a host name in the report and then click Details. The report displays host names and packages, what version is installed on the hosts and what version is recommended for installation.

## Running Service Pack Compliance Jobs

From the Service Pack Compliance report, you can create a job to install, on the selected hosts, the package version need to install the service pack contents.

### ▼ **To Create a Service Pack Compliance Job**

- 1 **In the Service Pack Compliance Report Editor, select Not Compliant for the Status.**
- 2 **Select the remaining criteria for the report and then generate the report.**
- 3 **Select listed packages and then click Details.**  
The report shows the hosts on which the packages should be installed.
- 4 **Select packages and then click Send Job.**  
The job installs the recommended version of each package.



## Job History Reports

Generate Job History reports to get a detailed history of the install and uninstall actions taken on hosts throughout Sun Update Connection – Enterprise management. This report also shows which user made the deployments, enabling you to track a team of operators.

### ▼ To Filter a Job History Report

Filter a Job History report in the Job History Report Editor window. This report requires that you filter select an option from each filter.

- 1 In the Reports window, select Job History and then click the New button.

The Job History Report Editor opens.

The screenshot shows the 'Jobs History Report Editor' dialog box. The 'Name' field contains 'last week'. The 'Description' field contains 'What was done on the web servers while I was on vacation?'. The 'Hosts' dropdown is set to 'All Hosts'. The 'Dates' dropdown is set to 'Interval days: 7'. Under the 'Action' section, both 'Installs' and 'Uninstalls' are checked. The 'Save', 'Report', and 'Cancel' buttons are visible at the bottom.

- 2 Select hosts for the report. See [“To Filter an Incident Compliance Report”](#) on page 237.
- 3 Select one of the following level options:
  - Security. Show security incidents.
  - Bug fix. Show security and bug fix incidents.

**4 Select relevant dates.**

See “To Filter a Report by Date” on page 233.

**5 Select one of the following action options:**

- **Installs. Show details of installations done on the selected hosts and dates.**
- **Uninstalls. Show details of uninstalls done on the selected hosts and dates.**

## Viewing Job History Reports

After you select the criteria in the Job History Report Editor, you can generate the report, or name it and save it as a template. If you save it as a template, you can select the template and then click Report in the Reports window. Whether you generate the report from the editor window or from a template, the same Report window opens.

The Report shows the date and time that an action was done, what the action was and on what component and host, the job that called for the action, and the user that created the job.

## Managing Reports

You can copy, edit, and delete report templates. You create a report template by saving the criteria of a report.

If you generate the report without saving, these features are not available. In addition, these features are not applicable to the default report types.

After a report is generated, you can perform various actions with it.

## Managing Report Templates

- To *delete* a report, select a report template that you created and then click the Delete button in the tool bar.
- To *edit* a report, select a report template that you created and then click the Edit button in the tool bar.
- To *create* a new report or report template based on a previously created template, select a report template shown under a default report type, and click the Copy button in the tool bar.

## Managing Report Results

- To *save* the report results in a text file, click the Save button.
- To *print* the report, click the Print button.
- To *email* the report, click the Send button.
- To *get more details* on a selected item in the report, click the Details button.
- To *create a job* that will fix the compliance issues, click the Run button.



# Command-Line Interface

---

The Command-line interface (CLI) is provided with the Sun Update Connection – Enterprise Suite. You can install it and activate it on any machine in the network that includes the other Sun Update Connection – Enterprise applications. The CLI enables Sun Update Connection – Enterprise Console functionality without opening the graphical user interface.

Sun Update Connection – Enterprise CLI commands can be run either as single lines or embedded in scripts.

This chapter covers The following topics:

- “Syntax” on page 253
- “Commands” on page 255

## Syntax

The command to initiate the CLI is `uce_cli`.

---

**Note** – You can also initiate the CLI with the `osc` command, which still exists for backward compatibility purposes. This `osc` command might be removed in future releases.

---

```
uce_cli -command -parameter value [...] [-flag][...] -u username -p password
```

The following command searches for a component with `apac` in its name:

```
# uce_cli -fc -T "apac" -u myname -p mypass
```

## Arguments

The `uce_cli` command has these two types of arguments:

- Parameter syntax is dash (-), name, space, value: *-param value*
- Flags have no value. If a flag is specified, it indicates a true value. If a flag is not specified, it indicates a false value. Flag syntax is dash, name: *-flag*

You can specify the `-verbose` flag with any command to produce troubleshooting information as part of the command output.

Some commands have an optional parameter for the delimiter of output. The delimiter is the separator between items in output. By default, the delimiter is a line feed, so each item appears on a separate line. You can change the delimiter in commands that offer this option to any set of characters or whitespace that meets your requirements.

If you want each item to appear in one line with commas, specify `-dlt ", "` as the delimiter in the command.

Some commands have a parameter (usually `-T` or `-pT`) whose value is a component in the knowledge base. When providing the name of a component, in particular, of a Local component, include its knowledge base path, to ensure that the name is unique. For example, specify the `-T` parameter as follows:

```
-T "Local/Configuration files/yourCat/yourDec/yourFile"
```

## User Names and Passwords

Every CLI command is accessed with an existing Sun Update Connection – Enterprise user name of a user with full permissions, or the `admin` user, and with its password. You may type these access details directly into the command with the `-u` and `-p` parameters.

If you do not provide the `-u` and `-p` parameters in the command, the CLI prompts for them:

<code># uce_cli -lg</code>	command to list all groups
Initializing ...	“Initializing” is output as notification.
Username: admin	“Username” is prompted.
Password:	“Password” is prompted. Input is hidden.

## Special Characters

If a parameter value has a space or a special character, close the value in straight quotation marks (“”).

The exclamation mark (!) is not a valid character even in quotes. To use it, you must protect it with a backward slash: \!.

Local components may have names with the forward slash (/). For example, you could create a category of Configuration files called "/etc", to show that these files have target installations in the /etc directory. In the CLI commands, when you use a component that has / in its name, protect it with a backslash (\), so that the CLI can identify it as part of a string rather than a path.

For example, say that you have a category named /etc, a file declaration named /etc/hosts, and a file version called /etc/hosts-5 in the Local components list.

The CLI requires that you refer to this hierarchy as the following:

```
ROOT/Local/Configuration files/\etc/\etc/hosts/\etc/hosts-5
```

## Commands

The CLI offers a set of commands to perform Sun Update Connection – Enterprise functions.

The commands can be divided into the following categories:

- “List and Find Commands” on page 255
- “Host and Group Commands” on page 265
- “Local Component Commands” on page 268
- “Policy Commands” on page 271
- “Job Commands” on page 274
- “Inventory Commands” on page 275
- “Help Commands” on page 279

## List and Find Commands

The commands in this section are useful for all the other commands. They are used to find the values of other parameters. For example, if you have a command that needs a distribution name, run the -ld command to get the list of valid input.

This section includes the following:

- “List Distributions (-ld) Command” on page 256
- “Find Component (-fc) Command” on page 257
- “List All Hosts (-lah) Command” on page 258
- “List Host Properties (-lh) Command” on page 258
- “List Host Inventory (-lhi) Command” on page 259
- “List Groups (-lg) Command” on page 259
- “List Group’s Hosts (-lgh) Command” on page 260
- “List Profiles (-lp) Command” on page 260
- “List Policies (-lc) Command” on page 261

- “List Profile Attributes (-lpa) Command” on page 261
- “List Policy Attributes (-lca) Command” on page 262
- “List Logs (-ll) Command” on page 263
- “List Jobs Status (-ljs) Command” on page 263
- “List Job Status Attributes (-ljsa) Command” on page 264
- “List Saved Snapshots (-lss) Command” on page 264

## List Distributions (-ld) Command

The list-distributions command outputs the supported distributions on your local system. If you add the -all flag, all Sun Update Connection – Enterprise supported distributions are output.

Use this command to get valid values for the -D (distribution) parameter used in other CLI commands.

<b>Flag</b>	-all – List all distributions supported by Sun Update Connection – Enterprise. Without this flag, only the distributions that have been locally activated are listed.
<b>Syntax</b>	<code>uce_cli -ld [-all] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -ld -u admin -p 123</code>
<b>Result Example</b>	Available Distributions: RH9_IA32 SLES8_S390
<b>Example</b>	<code>uce_cli -ld -all -u admin -p 123</code>



<b>Result Example</b>	Available Distributions: RH72_IA32 RH73_IA32 RH8_IA32 RH9_IA32 FC2_IA32 AS21_IA32 ES21_IA32 AS3_IA32 ES3_IA32 WS3_IA32 AS3_AMD64 WS3_AMD64 SUSE9_IA32 SUSE92_IA32 SLES8_IA32 SLES9_IA32 SLES7_S390 SLES8_S390 SLES8_AMD64 SUSE9_AMD64 SOLARIS8_SPARC
-----------------------	---

## Find Component (-fc) Command

The find-component command returns the exact names of components.

Use this command to get the values for the -T or -pT parameter used by other commands.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -T <i>component</i> – Specify the name of the component. If you type part of a name, without -sons, the output will be all components that have this string in their names. The value you specify is case-insensitive.</li> <li>▪ -dlt <i>delimiter</i> – Specify the delimiter for the output.</li> <li>▪ -D <i>distribution</i> – Specify the distribution to use. If not specified, the command operates on all distributions.</li> </ul>
<b>Flag</b>	<p>-sons – List the contained components of the component you specified with -T.</p> <p>This flag operates only if the component listed with -T is the complete name of a category or package group holding packages.</p> <p>If the -T value is not unique in the Components list, include the tree path; otherwise only the first component's sons are output.</p>
<b>Syntax</b>	<pre>uce_cli -fc -T "component" [ -sons ] [ -dlt "delimiter" ] [ -D distribution ] -u username -p password</pre>

<b>Example</b>	<code>uce_cli -fc -T "ROOT" -sons -dlt " , " -D RH9_IA32 -u admin -p 123</code>
<b>Result Example</b> finding categories	ROOT/, ROOT/ARCHITECTURES, ROOT/DISTRIBUTION, ROOT/FILESYSTEM, ROOT/HANDLER, ROOT/Hardware, ROOT/Local, ROOT/SPECIAL, ROOT/Software, ROOT/extensions
<b>Example</b>	<code>uce_cli -fc -T "httpd" -sons -u admin -p 123</code>
<b>Result Example:</b> finding packages	ROOT/Software/System Environment/Daemons/httpd/httpd-2.0.40-21 ROOT/Software/System Environment/Daemons/httpd/httpd-2.0.40-21.1 ROOT/Software/System Environment/Daemons/httpd/httpd-2.0.40-21.3 ROOT/Software/System Environment/Daemons/httpd/httpd-2.0.40-21.5 ROOT/Software/System Environment/Daemons/httpd/httpd-2.0.40-21.9
<b>Example</b>	<code>uce_cli -fc -T "local" -u admin -p 123</code>
<b>Result Example:</b> partial string	ROOT/Local ROOT/Local/Local RPMs ROOT/SPECIAL/active_rpmdb/Local RPM DataBase version 4.0 ROOT/Software/System/Libraries/glibc-locale ROOT/Software/System/Libraries/glibc-locale/glibc-locale-2.3.3-118 [i586]

## List All Hosts (-lah) Command

The list-all-hosts command outputs a complete list of all managed hosts in the system. Use this command to get values for the -h parameter of other parameters.

<b>Parameter</b>	<code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.
<b>Syntax</b>	<code>uce_cli -lah [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lah -u admin -p 123</code>

## List Host Properties (-lh) Command

The list-host command outputs the properties (such as IP address, distribution, and so on) of a given host.

<b>Parameter</b>	<code>-h <i>hostname</i></code> – Specify the host name.
<b>Syntax</b>	<code>uce_cli -lh -h <i>hostname</i> -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lh -h webserver2 -u admin -p 123</code>

<b>Result Example</b>	<pre>Host Data: Host ID = 1 Host Name = webserv2 Unique String = lnx013 Host IP = 127.0.0.2 Host Type is: standard Host (maybe Master) Host is Connected Distribution ID is 9 Master Group ID = 0 Master Host ID =0 listen on port 8001</pre>
-----------------------	---

To get valid values for the `-h` parameter, use the `-lah` command.

Note that even if a managed host is not connected to Sun Update Connection – Enterprise at the time of the command, the data is still retrieved. An error number will be given (example: `FailedErrCode = 34014464`) if the host is not online.

## List Host Inventory (`-lhi`) Command

The `list-host-inventory` command outputs the list of software installed on a given host.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-h <i>hostname</i></code> – Specify the host name.</li> <li>▪ <code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.</li> </ul>
<b>Syntax</b>	<code>uce_cli -lhi -h <i>hostname</i> [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lhi -h lnx013 -dlt " " -u admin -p 123</code>
<b>Result Example</b>	<code>up2date-gnome-2.1.7-1 wu-ftpd-2.6.1-6 shapecfg-2...</code>

To get valid values for `-h`, use the `-lah` command.

## List Groups (`-lg`) Command

The `list-group` command lists all the groups. Use this command to get values for the `-g` parameter used in other CLI commands.

<b>Parameter</b>	<code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.
<b>Syntax</b>	<code>uce_cli -lg [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lg -u admin -p 123</code>

<b>Result Example</b>	<pre>RH9_IA32 hosts SLES8_S390 hosts All Hosts topGroup topGroup/nestedGroup</pre>
-----------------------	--

Notice that nested groups are listed in a path. For any command that calls for the `-g` parameter to list a group, if you want a nested group, type its complete group path.

Groups that are named *distribution\_architecture* hosts are default distribution groups. When an agent registers with the SDS, its distribution is recognized and the host is added to the appropriate distribution group. Each distribution group contains all the managed hosts of that distribution. The distribution groups' host lists are system-defined and cannot be manually changed.

The All Hosts group is also a default group. It contains the complete list of managed hosts in your environment.

## List Group's Hosts (-lgh) Command

The list-group-hosts command outputs the hosts that are assigned to a given group.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-g <i>groupname</i></code> – Specify the name of the group.</li> <li>▪ <code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.</li> </ul>
<b>Syntax</b>	<code>uce_cli -lgh -g "<i>groupname</i>" [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lgh -g "topGroup/nestedGroup" -u admin -p 123</code>
<b>Result Example</b>	<pre>webserver2</pre> <p>(Note that quotations are required for group paths and for group names that contain spaces.)</p>
<b>Example</b>	<code>uce_cli -lgh -g "nestedGroup" -u admin -p 123</code>
<b>Result Example</b>	<pre>Error: Requested group not found.</pre> <p>(Error indicates that parent-group path is required for nested groups.)</p>

To get valid values for the `-g` parameter, use the `-lg` command.

## List Profiles (-lp) Command

The list-profiles command outputs a list of all existing profiles.

Use this command to get values for the `-P` parameter of other CLI commands.

<b>Parameter</b>	<code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.
<b>Syntax</b>	<code>uce_cli -lp [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lp -u admin -p 123</code>
<b>Result Example</b>	<pre> Check System Perform Restart Check Security Upgrade All Components Check Bugs Fix Perform Restart + Reconfigure Local Software Review Check Withdrawn Patches </pre>

Note that the profiles listed in the result example are the default, predefined profiles. Even if you have not yet created profiles, this command will have output.

## List Policies (-lc) Command

The list-policies command outputs a list of all existing policies, predefined answers for a dependency resolver (DR). Use this command to get values for the -C parameter of other CLI commands.

<b>Parameter</b>	<code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.
<b>Syntax</b>	<code>uce_cli -lc [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lc -dlt ", " -u admin -p 123</code>
<b>Result Example</b>	<code>autoSWchanges, lockKernelNode, Always ask me</code>

The Always Ask Me policy is the default policy. Even if you have not yet created policies, this command will have output.

## List Profile Attributes (-lpa) Command

The list-profile-attribute command outputs the attributes, the component-requirement combinations that make up a profile.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-P <i>profile</i></code> – Specify the name of an existing profile.</li> <li>▪ <code>-dlt <i>delimiter</i></code> – Specify the delimiter for the output.</li> </ul>
<b>Syntax</b>	<code>uce_cli -lpa -P "<i>profile</i>" [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>

<b>Example</b>	<code>uce_cli -lpa -P "create WebServer" -u admin -p 123</code>
<b>Result Example</b>	<pre> Profile name = createWebServer from node = httpd-devel (RH9_IA32) Install from node = httpd (RH9_IA32) Install from node = httpd-manual (RH9_IA32) Install from node = vsftpd (RH9_IA32) Uninstall from node = tftp (RH9_IA32) Uninstall from node = ftp (RH9_IA32) Install         </pre>

To get valid values for -P, use the -lp command.

If a predefined profile is used for the -P parameter, the output will be just the name of the profile.

Notice that the action is listed under the component (node). Although the action is listed as install or uninstall or upgrade or downgrade, a profile checks compliance. If the component is already installed and the action is "Install," nothing is done and the profile succeeds.

## List Policy Attributes (-lca) Command

The list-policy-attribute command outputs the attributes, the component-action-answer combinations, that make up a confirmation policy.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -C <i>policy</i> – Specify the name of the existing confirmation policy.</li> <li>▪ -dlt <i>delimiter</i> – Specify the delimiter for the output.</li> </ul>
<b>Syntax</b>	<code>uce_cli -lca -C "<i>policy</i>" [ -dlt "<i>delimiter</i>" ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -lca -C SWAutoYes -u admin -p 123</code>
<b>Result Example</b>	<pre> Policy name - SWAutoYes from node = Software (RH9_IA32) Install Yes from node = Software (RH9_IA32) Upgrade Yes from node = Software (RH9_IA32) Apply Fix Yes         </pre>

To get valid values for -C, use the -lc command.

## List Logs (-ll) Command

The list-logs command outputs logs for actions on selected components of a host or of a group. You might ask to see, for example, uninstallation actions on Local RPMs for the WebServers group, installations of Networking components on one host, or any install or uninstall of Software on All Hosts.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -A <i>action</i> – Specify the action. Legal values are All Actions, Installs, and Uninstalls.</li> <li>▪ -dlt <i>delimiter</i> – Specify the delimiter for the output.</li> <li>▪ -g <i>groupname</i> – Specify the name of the group.</li> <li>▪ -h <i>hostname</i> – Specify the name of the host.</li> </ul>
<b>Syntax</b>	<code>uce_cli -ll -A <i>action</i> [ -dlt "<i>delimiter</i>" ] ( -g <i>group</i>   -h <i>host</i> ) -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -ll -A Installs -h lnx13 -u admin -p 123</code>
<b>Result Example</b>	<pre>Tue May 4 16:32:17 2004 lnx13 Install httpd-devel-2.0.3-1 (RH9_IA32) Job_buildWebServer rochelle</pre> <p>Explanation: time, host name, action, component, distribution, job name, and user name.</p>

Use the -lg to get values for the -g. Use the -lah to get values for the -h. Use the -ld to get values for the -D. Use the -fc to get values for the -T.

## List Jobs Status (-ljs) Command

The list-job-status command outputs a list of jobs that you created with the current user name, according to the status criteria that you choose.

<b>Parameter</b>	-dlt <i>delimiter</i> – Specify the delimiter for the output.
<b>Flag</b>	<ul style="list-style-type: none"> <li>▪ -all – List all jobs.</li> <li>▪ -ok – List jobs that completed successfully.</li> <li>▪ -fl – List jobs that failed.</li> <li>▪ -pr – List jobs that are in process.</li> <li>▪ -wc – List jobs that are waiting for user confirmation.</li> </ul>
<b>Syntax</b>	<code>uce_cli -ljs [ -dlt "<i>delimiter</i>" ] ( -all   -ok   -fl   -pr   -wc ) -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -ljs -ok -u admin -p 123</code>

<b>Result Example</b>	<pre>makeWebServer Deploy Tue May 6 9:30:09 2004 All hosts finished successfully anotherJob Verify Tue May 6 11:32:15 2004 All hosts finished successfully  Explanation: job name, mode, start time, status; for two jobs: "makeWebServer" and "anotherJob."</pre>
-----------------------	--

### List Job Status Attributes (-ljsa) Command

The list-job-status-attributes command outputs status information (current status, profile data, and so on) of one job that you created with the current user name.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -j <i>jobname</i> – Specify the name of the job.</li> <li>▪ -dlt <i>delimiter</i> – Specify the delimiter for the output.</li> </ul>
<b>Syntax</b>	<code>uce_cli -ljsa -j "jobname" [ -dlt "delimiter" ] -u username -p password</code>
<b>Example</b>	<code>uce_cli -ljsa -j ProvServer -u admin -p 123</code>
<b>Result Example</b>	<pre>makeWebServer Deploy Tue May 6 9:30:09 2004 All hosts finished successfully  Explanation: job name, job mode, start time, and status.</pre>

To get valid values for the -j parameter, use the -ljs command.

If a host did not end successfully, more host and profile information is output.

### List Saved Snapshots (-lss) Command

The list-saved-snapshots command outputs a list of saved snapshots. When you save an inventory of a host or of a group, you create a *snapshot*. A snapshot is also saved, for each selected host, before a job is deployed.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -h <i>hostname</i> – Specify the name of the host.</li> <li>▪ -g <i>groupname</i> – Specify the name of the group.</li> <li>▪ -dlt <i>delimiter</i> – Specify the delimiter for the output.</li> </ul>
<b>Syntax</b>	<code>uce_cli -lss ( -g group   -h host ) [ -dlt "delimiter" ] -u username -p password</code>



<b>Example</b>	<pre>uce_cli -lss -g WebServers -u admin -p 123 uce_cli -lss -h lnxsrvr13 -u admin -p 123</pre>
----------------	---

You *must* specify either `-h` or `-g`.

To get valid values for the `-h` parameter, use the `-lah` command. To get valid values for the `-g` parameter, use the `-lg` command.

## Host and Group Commands

The following commands allow you to view and manage hosts and groups of hosts.

This section includes the following:

- “Add Host (`-ah`) Command” on page 265
- “Delete Host (`-dh`) Command” on page 265
- “Rename Host (`-rh`) Command” on page 266
- “Add Group (`-ag`) Command” on page 266
- “Add Host to Group (`-ahg`) Command” on page 266
- “Delete Group (`-dg`) Command” on page 267
- “Rename Group (`-rg`) Command” on page 267

### Add Host (`-ah`) Command

The add-host command adds predefined host data to the system before agent installation. The agent on the host adds the host automatically. If there is already a host in the system with the given host name, the command results in an error.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-h hostname</code> – Specify the name of the host.</li> <li>▪ <code>-D distribution</code> – Specify the distribution to use. If not specified, the command operates on all distributions.</li> </ul>
<b>Syntax</b>	<code>uce_cli -ah -h <i>hostname</i> -D <i>distribution</i> -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -ah -h wserver03 -D RH9_IA32 -u admin -p 123</code>

To get valid values for the `-D` parameter, use the `-ld` command. The value of `-h` must not already be in the output of the `-lah` command.

### Delete Host (`-dh`) Command

The delete-host command removes a host from the management of the system. This command is effective only if the agent has been stopped or uninstalled.

<b>Parameter</b>	<code>-h hostname</code> – Specify the name of the host.
<b>Syntax</b>	<code>uce_cli -dh -h hostname -u username -p password</code>
<b>Example</b>	<code>uce_cli -dh -h wserver03 -u admin -p 123</code>

To get valid values for the `-h` parameter, use the `-lah` command.

## Rename Host (- rh) Command

The `rename-host` command renames a host, from an existing name to a new name. The name of the host is not the DNS name (Unique String) of the machine, but the Sun Update Connection – Enterprise name of the host. You can change this name at any time without affecting the machine or its configurations.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-sH hostname</code> – Specify the source host name of an existing host.</li> <li>▪ <code>-tH hostname</code> – Specify the name of a target host.</li> </ul>
<b>Syntax</b>	<code>uce_cli -rh -sH hostname -tH hostname -u username -p password</code>
<b>Example</b>	<code>uce_cli -rg -sH lnx013 -tH mailserver_2 -u admin -p 123</code>

To get valid values for the `-sH` parameter, use the `-lah` command.

A valid value for the `-tH` parameter is a new, unique host name. This name must not appear in the output of the `-lah` command.

## Add Group (- ag) Command

The `add-group` command creates a new group of hosts.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-g groupname</code> – Specify the name of a group.</li> <li>▪ <code>-pG groupname</code> – Optionally specify the name of an existing parent group under which to create the group.</li> </ul>
<b>Syntax</b>	<code>uce_cli -ag -g "groupname" [ -pG "groupname" ] -u username -p password</code>
<b>Example</b>	<code>uce_cli -ag -g ApacheServers -pG WebServers -u admin -p 123</code>

To get valid values for the `-pG` parameter, use the `-lg` command.

## Add Host to Group (- ahg) Command

The `add-host-group` command assigns a managed host to a group.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-h hostname</code> – Specify the name of a host.</li> <li>▪ <code>-g groupname</code> – Specify the name of a group.</li> </ul>
<b>Syntax</b>	<code>uce_cli -ahg -h hostname -g "groupname" -u username -p password</code>
<b>Example</b>	<code>uce_cli -ahg -h wsrvr03 -g WebServers -u admin -p 123</code>

To get valid values for the `-h` parameter, use the `-lah` command.

Valid values and results for the `-g` parameter:

- If the group exists (use the `-lg` command), the host is added to it.
- If the group does not exist, it is created and the host is assigned to it.
- If the group exists, but has a parent not given in the CLI command, a new top-level group is created by the same name. You can have same-named groups of different hierarchies.
- If the named group is written as a nested group (“parent/nested”), and this group-path does not exist, all the groups are created.

## Delete Group (`-dg`) Command

The delete-group command deletes a group and its sub-groups from the system. It does not unregister the managed hosts. It cannot be used on default groups.

<b>Parameter</b>	<code>-g groupname</code> – Specify the name of the group.
<b>Syntax</b>	<code>uce_cli -dg -g "groupname" -u username -p password</code>
<b>Example</b>	<code>uce_cli -dg -g WebServers -u admin -p 123</code>

To get valid values for the `-g` parameter, use the `-lg` command.

## Rename Group (`-rg`) Command

The rename-group command renames a group, from an existing name to a new name.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-sG groupname</code> – Specify the source group name of an existing group.</li> <li>▪ <code>-tG groupname</code> – Specify the name of a target group. This name must be a new group.</li> </ul>
<b>Syntax</b>	<code>uce_cli -rg -sG "groupname" -tG "groupname" -u username -p password</code>
<b>Example</b>	<code>uce_cli -rg -sG WebServers -tG webserver -u admin -p 123</code>

To get valid values for the `-sG` parameter, use the `-lg` command.

A valid value for the `-tG` parameter is a new, unique group name. It must not appear in the output of the `-lg` command.

## Local Component Commands

The following commands are used to manage local software and files.

This section includes the following:

- “Add Local Category (-alc) Command” on page 268
- “Add Software Package (-asp) Command” on page 268
- “Add File Declaration (-afd) Command” on page 269
- “Add Target Local (-atl) Command” on page 270

### Add Local Category (-alc) Command

The add-local-category command creates a new category under Local, under Probes, Pre-actions, Post-actions, Macros, or Configuration Files.

Use this command if you want to upload scripts and files to the local knowledge base. You cannot upload a local file or script until you have created a category to hold it.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -T <i>component</i> – Specify the name of the component. If you type part of a name, without -sons, the output will be all components that have this string in their names. The value you specify is case-insensitive.</li> <li>▪ -ds <i>description</i> – Specify an optional description of the new category.</li> <li>▪ -pT <i>category</i> – Specify the parent category name in which to create the new category. Valid values are: Probes, Pre-actions, Post-actions, Macros, Configuration files, or one of these, with /<i>existing-subcategory</i>.</li> <li>▪ -D <i>distribution</i> – Specify the distribution to use. If not specified, the command operates on all distributions.</li> </ul>
<b>Syntax</b>	<code>uce_cli -alc -T "category" [ -ds "description" ] -pT "parent-category" [ -D distribution ] -u username -p password</code>
<b>Example</b>	<code>uce_cli -alc -T "PrintcapVersions" -ds "various config files to set up different printers" -pT "Configuration files" -u admin -p 123</code>

To get a list of the valid values for the -pT parameter, use the -fc command, with "Local" as the value of its -T parameter.

One or both of "ROOT/Local/Local RPMs" or "ROOT/Local/Local PKGs" is listed, but are not valid values for the -alc command; all the other items in this output are acceptable.

### Add Software Package (-asp) Command

The add-software-package command pushes a local software package to the local knowledge base.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-f <i>pathname</i></code> – Specify the full path name of the source RPM file.</li> <li>▪ <code>-T <i>category</i></code> – Specify the name of the category in which to add this RPM.</li> <li>▪ <code>-D <i>distribution</i></code> – Specify the distribution to use. If not specified, the command operates on all distributions.</li> </ul>
<b>Flag</b>	<code>-secure</code> – Security fix mark. If present, the local package is a security fix for a previous version.
<b>Syntax</b>	<code>uce_cli -asp -f "<i>pathname</i>" [ <code>-secure</code> ] -D <i>distribution</i> [ <code>-T <i>category</i></code> ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -asp -f "/usr/share/myApps/myApp01.05-73.rpm" -D RH9_IA32 -u admin -p 123</code>

To learn more about the security fix mark and when to use the `-secure` flag, see [“To Fix Local Software Missing Dependencies” on page 100](#) and [“Fixing Local Dependencies” on page 100](#).

To get valid values for the `-D` parameter, use the `-ld` command.

## Add File Declaration (`-afd`) Command

The `add-file-declaration` command adds a file declaration to the local knowledge base. A file declaration is the target path name for installation of a local Configuration file onto managed hosts.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-pT <i>category</i></code> – Specify the parent category name in which to create the new category. This value must be a user-defined category under Configuration files.</li> <li>▪ <code>-ds <i>description</i></code> – Specify an optional description of the new file.</li> <li>▪ <code>-tfp <i>pathname</i></code> – Specify the target path name for installation on remote hosts.</li> <li>▪ <code>-D <i>distribution</i></code> – Specify the distribution to which the file applies. If not specified, the command operates on all distributions.</li> </ul>
<b>Syntax</b>	<code>uce_cli -afd -pT "<i>category</i>" [ <code>-ds "<i>description</i>"</code> ] -tfp "<i>pathname</i>" [ <code>-D <i>distribution</i></code> ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -afd -pT "Configuration files/PrintcapVersions" -ds "install directory for printcap versions" -tfp "/etc/printcap" -u admin -p 123</code>

Before you can create a file declaration, you have to have a category under Configuration files. Use the `-alc` command to create a category. To see a list of categories, use the `-fc` command with `-T "Local/Configuration files" -sons`.

The output of this command would give valid values for the `-pT` parameter of the `-afd` command. You can shorten the path of the category component to `Configuration files/category`. You do not need to type the full path from the root.

## Add Target Local (-atl) Command

The add-target-local command adds a file or a script to the local knowledge base.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -pT <i>category</i> – Specify the parent category name in which to create the new category. Valid values are: Probes, Pre-actions, Post-actions, Macros, Configuration files with a user-defined subcategory.</li> <li>▪ -f <i>pathname</i> – Specify the full path name of the file to upload.</li> <li>▪ -ds <i>description</i> – Specify an optional description.</li> <li>▪ -D <i>distribution</i> – Specify the distribution for which this category is relevant. If not specified, the command operates on all distributions.</li> <li>▪ -tF – If -f is a configuration file, creates a file declaration.</li> <li>▪ -tM – If -f is a macro, use -tM with a display name for the macro.</li> <li>▪ -tP – If -f is a pre-action, use -tP with a display name for the pre-action.</li> <li>▪ -tR – If -f is a probe, use -tR with a display name for the probe.</li> <li>▪ -tS – If -f is a post-action, use -tS with a display name for the post-action.</li> <li>▪ -v <i>version</i> – Specify the version of the file. This is mandatory for configuration files only to supply a version suffix display name.</li> </ul>
<b>Syntax</b>	<code>uce_cli -atl -f "<i>pathname</i>" -pT <i>category</i> [ -ds "<i>description</i>&gt;" ] ( -tF   -tM   -tP   -tR   -tS <i>name</i> ) [ -v <i>version</i> ] [ -D <i>distribution</i> ] -u <i>username</i> -p <i>password</i></code>
<b>Example: Config file</b>	<code>uce_cli -atl -f "/home/admin/myFiles/print_v5" -pT "Configuration files/PrntVer" -ds "printcap Flr5" -tF "/etc/printcap" -v "05" -u admin -p 123</code>
<b>Example: Macro</b>	<code>uce_cli -atl -f "/home/admin/scripts/findhost.sh" -pT "hostname" -ds "finds local hostname for file localization" -tM "hostname" -u admin -p 123</code>
<b>Notes</b>	Before performing this procedure, you must have created the category PrntVer under Configuration files and the category hostname under Macros (see <a href="#">“Add Local Category (-alc) Command” on page 268</a> ). You must also have created a script to upload as a macro. The example shows a script that finds the host name of the local host.

To find a valid value for -pT, use -fc with -T "Local/default category>/" -sons.

To find a valid value for -D, use the -ld command. If you do not name a specific distribution, the named parent category (value of -pT) must also be in all distributions.

The -t\* parameter that you choose to use must match the -pT parameter. For example, if -pT is Macros/localhostname then use -tM to name the macro.

The -tM, -tP, -tR, and -tS parameters take any new name as a value.

The -tF parameter needs a file declaration as its value. If you use a new path name for this value, it creates a new file declaration. If you use -tF, you must use -v to give the Configuration file a display version.

## Policy Commands

The following commands are for profiles and confirmation policies.

This section includes the following:

- “Add Profile Attribute (-apa) Command” on page 271
- “Add Policy Attribute (-aca) Command” on page 271
- “Copy Profile (-cp) Command” on page 272
- “Copy Policy (-cc) Command” on page 273
- “Export (-exp) Command” on page 273
- “Import (-imp) Command” on page 274

### Add Profile Attribute (-apa) Command

The add-profile-attribute command edits an existing profile by adding a new component-setting to the profile. It may also be used to create a new profile.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -P <i>profile</i> – Specify the name of a new or existing profile.</li> <li>▪ -T <i>component</i> – Specify the name of the component to be included in this profile.</li> <li>▪ -D <i>distribution</i> – Specify the distribution for which this profile is relevant. If not specified, the command operates on all distributions.</li> </ul>
<b>Flag</b>	<ul style="list-style-type: none"> <li>▪ -N – Marks the component as Not Allowed.</li> <li>▪ -R – Marks the component as Required.</li> <li>▪ -U – Marks the component for upgrade if a newer version is available.</li> </ul>
<b>Syntax</b>	<code>uce_cli -apa -P "profile" -T "component" ( -N   -R   -U ) [ -D <i>distribution</i> ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<pre>uce_cli -apa -P myWebSvr -T "httpd" -R -u admin -p 123 uce_cli -apa -P myWebSvr -T "httpd" -U -u admin -p 123</pre>
<b>Result Example</b>	The myWebSvr profile now has two more settings than it originally had: now httpd components are Required and must be Updated. If the profile did not exist before, it is created.

To get a valid value for a name of an existing profile for the -P parameter, use the -lp command. To get a valid value for the -T parameter, use the -fc command. To get a valid value for the -D parameter, use the -ld command.

### Add Policy Attribute (-aca) Command

The add-policy-attribute command edits an existing policy, by adding a new component-action-answer to the policy. This command can also be used to create a new policy.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>■ -C <i>policy</i> – Specify the name of a new or existing policy.</li> <li>■ -T <i>component</i> – Specify the name of the component for which the policy answers questions.</li> <li>■ -D <i>distribution</i> – Specify the distribution for which this policy is relevant. If not specified, the command operates on all distributions.</li> <li>■ -install <i>answer</i> – Specify the policy value for installing a component. Valid values are yes, no, and ask_me.</li> <li>■ -downgrade <i>answer</i> – Specify the policy value for downgrading a component. Valid values are yes, no, and ask_me.</li> <li>■ -fix <i>answer</i> – Specify the policy value for fixing a component. Valid values are yes, no, and ask_me.</li> <li>■ -remove <i>answer</i> – Specify the policy value for removing a component. Valid values are yes, no, and ask_me.</li> <li>■ -upgrade <i>answer</i> – Specify the policy value for upgrading a component. Valid values are yes, no, and ask_me.</li> <li>■ -ignore <i>answer</i> – Specify the policy value for ignoring file conflicts. Valid values are yes, no, and ask_me.</li> </ul>
<b>Syntax</b>	<code>uce_cli -aca -C "policy" -T "component" ( -install   -downgrade   -fix   -remove   -upgrade   -ignore ) ( yes   no   ask_me ) [ -D <i>distribution</i> ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -aca -C newPolicy -T "User Interface" -remove no -u admin -p 123</code>

One action parameter, and only one, is mandatory, with a value of either yes, no, or ask\_me.

To get a valid value for an existing policy name for the -C parameter, use the -lc command; or use a new one to create a new policy. To get a valid value for the -T parameter, use the -fc command. To get a valid value for the -D parameter, use the -ld command.

## Copy Profile (-cp) Command

The copy-profile command copies an existing profile to a new one. You can then use -apa command to further customize the copied profile.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>■ -sP <i>source-profile</i> – Specify the name of an existing source profile.</li> <li>■ -tP <i>target-profile</i> – Specify the name of the target profile that receives settings of the source profile.</li> </ul>
<b>Syntax</b>	<code>uce_cli -cp -sP <i>source-profile</i> -tP <i>target-profile</i> -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -cp -sP webServer -tP webServerHTTP -u admin -p 123</code>



To get a valid value for the `-sP` parameter, use the `-lp` command.

## Copy Policy (-cc) Command

The `copy-policy` command copies an existing policy to a new one. You can then use the `-aca` command to further customize the copied policy.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-sC source-policy</code> – Specify the name of an existing source policy.</li> <li>▪ <code>-tC target-policy</code> – Specify the name of the target policy that receives settings of the source policy.</li> </ul>
<b>Syntax</b>	<code>uce_cli -cc -sC source-policy -tC target-policy -u username -p password</code>
<b>Example</b>	<code>uce_cli -cc -sC SWAutoYes -tC SWYesKernelNo -u admin -p 123</code>

To get valid values for the `-sC` parameter, use the `-lc` command.

## Export (-exp) Command

The `export` command allows you to export Profiles or Inventories to XML files. An Sun Update Connection – Enterprise object in XML format is easy to read and edit, and can be manipulated as a file.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-ent entity-type</code> – Specify the type of the entity. Valid values are <code>Profile</code> or <code>Inventory</code>.</li> <li>▪ <code>-f pathname</code> – Specify the full path name of the XML file to which to export.</li> <li>▪ <code>-T list</code> – Specify a comma-separated list of profiles to export or a list of hosts whose inventories are to be exported. If not specified, all objects of type <code>-ent</code> are exported.</li> </ul>
<b>Syntax</b>	<code>uce_cli -exp -ent ( "Profile"   "Inventory" ) -f pathname.xml [ -T "profile,profile,..."   "hostname,hostname,..." ] -u username -p password</code>
<b>Example</b>	<code>uce_cli -exp -ent "Profile" -f /home/stuff/httpSverProfile.xml -u admin -p 123</code>
<b>Example</b>	<code>uce_cli -exp -ent "Inventory" -f /home/stuff/myHost.xml -u admin -p 123</code>
<b>Example</b>	<code>uce_cli -exp -ent "Inventory" -T "\lnx13,\lnx10" -f /home/stuff/rpmsOf13-10.xml -u admin -p 123</code>

To get valid values for `-T`, use the `-lp` command to see profiles, or the `-lah` to see hosts.

Be aware that as this command creates a file outside of Sun Update Connection – Enterprise, the success of the command is dependent upon your user permissions: the machine user executing the command has to have permissions to write to the path give in the `-f` parameter.

## Import (-imp) Command

The import command allows you to import XML files into Sun Update Connection – Enterprise and convert them back to profiles.

<b>Parameter</b>	-f <i>filename</i> – Specify the full path name to the XML file to import.
<b>Syntax</b>	<code>uce_cli -imp -f path/filename.xml -u username -p password</code>
<b>Example</b>	<code>uce_cli -imp -f /home/stuff/httpSverProfile.xml -u admin -p 123</code>

## Job Commands

The following commands create and manage jobs and job tracking.

This section includes:

- “Submit Job (-sj) Command” on page 274
- “Delete Job (-dj) Command” on page 275

## Submit Job (-sj) Command

The submit-job command creates a job from a profile, a confirmation policy, and a selected host or group, and submits it to the dependency manager.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ -j <i>jobname</i> – Specify the name of the new job. If you do not supply this value, the job is given a name based on the date and time it was sent.</li> <li>▪ -P <i>profile</i> – Specify the name of an existing profile.</li> <li>▪ -C <i>policy</i> – Specify the name of an existing policy.</li> <li>▪ -h <i>hostname</i> – Specify a single host name on which to run the job. This parameter <i>cannot</i> be used with the -g parameter.</li> <li>▪ -g <i>groupname</i> – Specify a group name on which to run the job. This parameter <i>cannot</i> be used with the -h parameter.</li> </ul>
<b>Flag</b>	<ul style="list-style-type: none"> <li>▪ -us – Use only secure components to fulfill dependency requirements.</li> <li>▪ -dp – Run the job in deploy mode. You must specify this flag if you want the job to actually make changes to the target host.</li> <li>▪ -sm – Run the job in simulation mode. Jobs are run in simulation mode by default.</li> </ul>
<b>Syntax</b>	<code>uce_cli -sj [ -j "jobname" ] -P "profile" -C "policy" ( -g "groupname"   -h hostname ) [ -us ] ( -dp   -sm ) -u username -p password</code>

<b>Example</b>	<pre>uce_cli -sj -j MakeWebServer -P webserverApps -C autoSW -h lnx13 -us -dp -u admin -p 123  uce_cli -sj -j 31_12_2003 -P UpgradeApache -C "Always ask me" -g webservers -sm -u admin -p 123</pre>
----------------	--

Either `-h` or `-g` must be given. If you do not give either `-dp` or `-sm`, the default mode for the job is simulate (not deploy).

To get a valid value for the `-j` parameter, use the `-ljs` command. To get a valid value for the `-P` parameter, use the `-lp` command. To get a valid value for the `-C` parameter, use the `-lc` command. To get a valid value for the `-h` parameter, use the `-lah` command. To get a valid value for the `-g` parameter, use the `-lg` command.

## Delete Job (`-dj`) Command

The delete-job command deletes a completed job from the Status list (used to keep the output of `-ljs` relevant), or cancels and deletes an unfinished job.

<b>Parameter</b>	<code>-j <i>jobname</i></code> – Specify the name of the job.
<b>Syntax</b>	<code>uce_cli -dj -j "<i>jobname</i>" -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -dj -j "MakeWebServer" -u admin -p 123</code>

To get valid values for the `-j` parameter, use the `-ljs` command.

## Inventory Commands

The following commands allow you to access, save, and compare the inventory (list of installed software) of a host or of a group.

This section includes the following:

- “Save Host Inventory (`-shi`) Command” on page 275
- “Save Group Inventory (`-sgi`) Command” on page 276
- “Convert Inventory to Profile (`-cip`) Command” on page 277
- “Convert Snapshot to Profile (`-csp`) Command” on page 277
- “Compare Hosts and Inventories (`-chi`) Command” on page 277
- “Submit Compare Job (`-scj`) Command” on page 278

### Save Host Inventory (`-shi`) Command

The save-host-inventory command saves a snapshot (a record of the host’s inventory at the current time) of the given host.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-h hostname</code> – Specify the name of the host.</li> <li>▪ <code>-s snapshot-name</code> – Specify the name of the snapshot.</li> </ul>
<b>Syntax</b>	<code>uce_cli -shi -h hostname -s snapshot-name -u username -p password</code>
<b>Example</b>	<code>uce_cli -shi -h lnxsrvr13 -s beforeUpdate -u admin -p 123</code>

To get valid values for `-h`, use the `-lah` command.

## Save Group Inventory (-sgi) Command

The `save-group-inventory` command saves a snapshot of the inventory of each host in the given group.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-g groupname</code> – Specify the name of the group.</li> <li>▪ <code>-sn suffix-name</code> – Specify the name of the snapshot suffix. When you save a snapshot for a group, a snapshot is created with the following file name format: <i>hostname-suffix-timestamp.</i></li> </ul>
<b>Syntax</b>	<code>uce_cli -sgi -g "groupname" -sn suffix -u username -p password</code>
<b>Example</b>	<code>uce_cli -sgi -g WebServers -sn wsrvrs -u admin -p 123</code>
<b>Result Example</b>	<pre>lnx01-wsrvrs-932111203 lnx12-wsrvrs-933111203 admin0-wsrvrs-9341112033 web13-wsrvrs-93111203</pre>

To get valid values for `-g`, use the `-lg` command.

## Delete Saved Snapshot (-dss) Command

The `delete-saved-snapshot` command deletes a selected saved snapshot.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-h hostname</code> – Specify the name of the host.</li> <li>▪ <code>-s snapshot-name</code> – Specify the name of the snapshot.</li> </ul>
<b>Syntax</b>	<code>uce_cli -dss -h hostname -s snapshot -u username -p password</code>
<b>Example</b>	<code>uce_cli -dss -h lnxsrvr13 -s inventory_beforeRestore -u admin -p 123</code>

To get a valid value for the `-h` parameter, use the `-lah` command. To get a valid value for the `-s` parameter, use the `-lss` command.

## Convert Inventory to Profile (-cip) Command

The `convert-inventory-profile` command saves the software inventory of a host into a profile. All software installed on the host is marked as Required on the profile; everything else is marked as Not Allowed.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>■ <code>-h hostname</code> – Specify the name of the host.</li> <li>■ <code>-P profile</code> – Specify the name of the profile.</li> </ul>
<b>Syntax</b>	<code>uce_cli -cip -h hostname -P "profile" -u username -p password</code>
<b>Example</b>	<code>uce_cli -cip -h lnxsrvr13 -P lnxsrvrProfile -u admin -p 123</code>

To get valid values for the `-h` parameter, use the `-lah` command.

## Convert Snapshot to Profile (-csp) Command

The `convert-snapshot-profile` command converts a saved software inventory (a snapshot) of a host as a profile. All software listed in the snapshot is marked as Required on the profile; everything else is marked as Not Allowed.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>■ <code>-h hostname</code> – Specify the name of the host.</li> <li>■ <code>-s snapshot-name</code> – Specify the name of the snapshot.</li> <li>■ <code>-P profile</code> – Specify the name of the profile.</li> </ul>
<b>Syntax</b>	<code>uce_cli -csp -h hostname -s snapshot-name -P "profile" -u username -p password</code>
<b>Example</b>	<code>uce_cli -csp -h lnxsrvr13 -s beforeUp -P oldSrv -u admin -p 123</code>

To get a valid value for the `-h` parameter, use the `-lah` command. To get a valid value for the `-s` parameter, use the `-lss` command.

## Compare Hosts and Inventories (-chi) Command

The `compare-host-inventory` command compares the installed software of two hosts, or the snapshots of two hosts. You may also compare the inventory or snapshot of a host against the snapshot of a group. The result of this command is the set of differences.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>■ <code>-h hostname</code> – Specify the name of the source host.</li> <li>■ <code>-s snapshot-name</code> – Specify the name of the source snapshot.</li> <li>■ <code>-t hostname</code> – Specify the name of the target host.</li> <li>■ <code>-ts snapshot-name</code> – Specify the name of the target snapshot.</li> <li>■ <code>-dlt delimiter</code> – Specify the delimiter for the output.</li> </ul>
------------------	--

<b>Syntax</b>	<code>uce_cli -chi -h source-hostname [ -s source-snapshot ] -t target-hostname [ -ts target-snapshot ] [ -d\lt "delimiter" ] -u username -p password</code>
<b>Example</b>	<code>uce_cli -chi -h lnx13 -s lnxInvDec03 -t lnx29 -ts lnxInvDec18 -u admin -p 123</code>

To get valid values for the `-h` and `-t` parameters, use the `-lah` command. To get values for the `-s` and `-ts` parameters, use the `-lss` command.

Whether `-s` and `-ts` are optional or mandatory depends on the type of comparison you are making. Comparison matrix:

Type	-h	-t	-s	-ts
Compare two hosts, current inventories	Different hosts	Different hosts	Not used	Not used
Compare two hosts, saved snapshots	Different hosts	Different hosts	From <code>-lss</code> , each is a different snapshot	From <code>-lss</code> , each is a different snapshot
Compare current host to group snapshot	Host in source group	Target host	From <code>-lss</code>	Not used
Compare host at different stages of lifecycle	Same host named for both parameters	Same host named for both parameters	From <code>-lss</code> , each is a different snapshot	From <code>-lss</code> , each is a different snapshot

## Submit Compare Job (-scj) Command

The `submit-compare-job` command compares the installed software of two hosts, or the snapshots of two hosts, and then changes the inventory of the target host to duplicate the inventory of the source host. The result of this command is application provisioning to the target host.

If the hosts are Solaris machines, you can compare either Software or Patches in one compare job.

<b>Parameter</b>	<ul style="list-style-type: none"> <li>▪ <code>-h hostname</code> – Specify the name of the source host.</li> <li>▪ <code>-s snapshot-name</code> – Specify the name of the source snapshot.</li> <li>▪ <code>-t hostname</code> – Specify the name of the target host.</li> <li>▪ <code>-j jobname</code> – Specify the name of the job.</li> <li>▪ <code>-C policy</code> – Specify the name of the policy.</li> </ul>
<b>Flag</b>	<ul style="list-style-type: none"> <li>▪ <code>-sm</code> – Run the job in simulation mode. This is the default mode.</li> <li>▪ <code>-dp</code> – Run the job in deploy mode. If you want the job to actually make changes on the target host, you must use this flag.</li> </ul>

<b>Syntax</b>	<code>uce_cli -scj -h <i>source-hostname</i> [ -s <i>source-snapshot</i> ] -t <i>target-hostname</i> -j "<i>jobname</i>" -C "<i>policy</i>" [ -sm   -dp ] -u <i>username</i> -p <i>password</i></code>
<b>Example</b>	<code>uce_cli -scj -h lnxsrvr13 -t lnxsrvr29 -j Make29Like13 -C autoSW -dp -u admin -p 123</code>

To get a valid value for `-h` and `-t`, use the `-lah` command. To get a valid value for `-s`, use the `-lss` command. To get a valid value for `-j`, use the `-ljs` command. To get a valid value for `-C`, use the `-lc` command.

## Help Commands

The following commands access helpful information.

### Help (-h) Command

The help command outputs usage information. Notice that this command does not operate with a user name and password.

<b>Syntax</b>	<ul style="list-style-type: none"> <li>▪ <code>uce_cli -h</code> This line outputs the complete command list with descriptions.</li> <li>▪ <code>uce_cli</code> Without a specific command to work on, the CLI provides the command list and descriptions to help you enter the command you want in the correct format.</li> </ul>
---------------	--





# Sun Update Connection – Enterprise Scenarios

---

This chapter provides procedures for specific concepts. The steps can get into advanced features. Follow the cross-references to previous chapters for more details.

This chapter covers the following topics:

- “Clusters” on page 281
- “Floating Servers and Loads” on page 284
- “Cloning Servers” on page 286
- “Sharing Directories” on page 288
- “DB2” on page 290
- “WebSphere” on page 293

## Clusters

A cluster is a group of machines or other resources that act as one powerful system. Clustering provides high availability, continuous operations for a long time. There are many varieties of clusters.

This scenario uses openMosix, a Linux kernel extension for clustering. The openMosix cluster is a single-image cluster: multiple copies of a single operating system kernel.

openMosix joins Linux machines to function as one large multiple-processor computer. If you have a 12-node cluster, it is as though you had one computer with the CPU power of 12 computers. One process will not be 12-times faster, but you can run 12 processes simultaneously.

The openMosix package is not available from any one distribution. You can download it from the project site.

Notice that after the profile is set up, cluster creation is automated. You could create an opposite profile that would undo the actions of this scenario, thereby unclustering the machines. You could set both profiles to run on a schedule, which would cluster and uncluster your resources according to your needs.

## Creating an openMosix Cluster with Sun Update Connection – Enterprise

This procedure to create a cluster with nodes takes about two hours to complete. It might take less time if there are no unexpected problems or a little more time for different environments. Maintenance tasks on the cluster (for example, adding or changing a node) take about five to ten minutes.

### ▼ To Create an openMosix Cluster with Sun Update Connection – Enterprise

**1 Choose the machines that will be nodes of the cluster.**

Each machine should have a Linux distribution that is supported by Sun Update Connection – Enterprise and the kernel version supported by openMosix.

**2 Install Sun Update Connection – Enterprise (system dependency server [SDS], dependency manager [DM], the knowledge base, the console, and the agent) on one of the machines.**

See the *Sun Update Connection - Enterprise 1.0 Administration Guide*.

**3 Install the agent on the other machines.**

**4 Add the openMosix RPM to the local knowledge base.**

The Local Expansion technology creates deployment rules.

See “[Adding Undetected Linux Software](#)” on page 85.

**5 In a text editor, create `/etc/mosix.map`.**

This file maps a node number to each IP address.

**6 Add a file declaration called `/etc/mosix.map`**

See “[Creating File Declarations](#)” on page 111.

**7 Add the `/etc/mosix.map` file to the local knowledge base.**

See “[Uploading Local Configuration Files](#)” on page 113.

**8 In a text editor, create a version of `/etc/hosts` which includes the hosts to be in the cluster.**

**9 Add a `/etc/hosts` file declaration and add the version you just made to the local knowledge base.**

See “[Creating File Declarations](#)” on page 111 and “[Uploading Local Configuration Files](#)” on page 113.

**10 Write a script that changes the default boot kernel to `openMosix` in the grub table:**

```
OpenMosixAsDefault.sh
```

See “Writing Actions” on page 104.

**11 Add this script to Local/Pre-actions.**

See “Uploading Actions” on page 104.

**12 Add this script to Local/Post-actions.**

See “Uploading Actions” on page 104.

**13 Create a profile called `openMosixNode` that defines the following requirements of a node in the cluster:**

- Required: `openMosix` kernel and management tools
- Required: `/etc/mosix.map` (specifying local version)
- Required: `/etc/hosts` (specifying local version)
- Required: Pre-action `OpenMosixAsDefault.sh`

See “To Create a Profile” on page 173.

**14 Create a group called `Test`, which includes two of the machines, and then Create a group called `openMosixCluster`, which includes all the machines that are to be nodes in the cluster.**

See “To Create a Group” on page 62.

**15 Create a job that runs in `simulate` mode on the `Test` group, with the following profile tasks:**

- `openMosixNode` profile
  - Perform Restart
- Check the estimates and status of the job before continuing. See “Creating Complex Jobs” on page 194.

**16 Rerun the job in `deploy` mode on the `Test` group. Check the results and status of the hosts before continuing.**

See “To Rerun a Job” on page 220.

**17 Run the job again in `deploy` mode on the `openMosixCluster` group.**

All selected machines are now nodes of a cluster. See “Creating Complex Jobs” on page 194.

## ▼ To Add a Node to the Cluster

**1 Install the agent on the new machine.**

See the *Sun Update Connection - Enterprise 1.0 Administration Guide*.

**2 Add this managed host to the `openMosixCluster` group.**

See “To Edit a Group” on page 65.

- 3 Open the `mosix.map` knowledge base file and add a new node number and the IP of the new machine.**

Open the `/etc/hosts` knowledge base files and add the new host name.

See [“Opening Host Files” on page 124](#).

- 4 Run the job with the `openMosixNode` profile in deploy mode on the `openMosixCluster` group.**

Legacy data and applications are not touched by the job, but the new map and hosts files are downloaded to each node. See [“Creating Complex Jobs” on page 194](#).

## Floating Servers and Loads

Integrating Sun Update Connection – Enterprise with local environment resource monitoring tools provides Floating Servers and Loads, an implementation of the On-Demand Computing model. In general, the concept of On-Demand Computing enables enterprises to meet fluctuating resource demands efficiently, without adding hardware investments or keeping mostly-idle machines. Resources are made available as needed.

A servicing pool is a group of machines dedicated to a specific type of service: web servers, print servers, mail servers, and so on.

## Creating Floating Server Environment

In this procedure, you will use Sun Update Connection – Enterprise to install the needed server profile on the floating server when the load threshold has reached overload, and to uninstall the profile when the load threshold has reached idle.

### ▼ To Create a Floating Server

- 1 Using Sun Update Connection – Enterprise, create the profiles of your servers.**

Define what is required and what is not allowed to be on each type of server. For this scenario, define a `WebServerProfile` profile and a `TelnetServerProfile` profile.

See [“To Create a Profile” on page 173](#).

- 2 Create a profile that uninstalls the software of the other two profiles.**

No damage is caused by setting `Uninstall` to components that are not there. So, make an uninstall profile called `IdleServerProfile`.

- 3 If there are various distributions used in the server pools and in the floating servers, align the profiles for all relevant distributions.**

See [“To Align Component Settings for Multiple Distributions” on page 210](#).

- 4 **Create a policy that automates all actions (Yes to all actions on all Software) and call it YesToAll.**  
See “To Create a Policy” on page 183.
- 5 **Create groups for each pool of servers, and a group called Idle.**  
For this scenario, call the server groups WebServers and TelnetServers.  
See “To Create a Group” on page 62.
- 6 **In the Idle group, assign a spare server that is your floating server and name it floating.**  
See “To Assign a Host to Groups” on page 70 and “To Edit a Managed Host” on page 71.
- 7 **Write a script that takes the output of your local resource monitoring tool when the load threshold has been passed (either on overload or on idle) and runs a script similar to floatingServers.sh.**

### floatingServers.sh Script

This script is called by a local script that finds the group with an overload or an idle threshold pass. Its arguments are the group with the needed resources (source) and the group that needs the resource (target).

- If there is an overload on WebServers or TelnetServers, the source is Idle.
- If the server groups are idle, the source is the one containing the floating server.

Write your local script to call `floatingServers.sh`.

```
./floatingServers.sh source target
```

For example, the `floatingServers` script takes those arguments in the `findProfile` function, which tells which profile to use in the `deployServer` function. The profile either installs a web server, a telnet server, or uninstalls server software (to return floating server to idle).

```
# ./floatingServers.sh Idle WebServers
```

```
#!/bin/bash

host=floating
policy=YesToAll

function login {
  echo -n "Type your user name:"
  read user
  echo -n "Type your password:"
  read password
}

function deployServer {
  uce_cli -sj -P "$profile" -C "$policy" -h "$host" -dp -u "$user" -p
```

```
“$password”
}

function findProfile {
sourceG=$1
targetG=$2
if [ $sourceG = “Idle” -a $targetG = “WebServers” ]; then
    profile=“WebServerProfile”
elif [ $sourceG = “Idle” -a $targetG = “TelnetServers” ]; then
    profile=“TelnetServerProfile”
elif [ $sourceG = “WebServers” -o $sourceG = “TelnetServers” ]; then
    profile=“IdleServerProfile”
else
    echo “Source is not in automated script.”
    echo “From the following list of known profiles, select one to deploy on floating server”
    uce_cli -lp -u “$user” -p “$password”
    echo -n “Profile to deploy:”
    read profile
fi
}
login
findProfile $1 $2
echo “Deploying $profile on $host to make it part of $2”
deployServer
```

---

**Note** – If the servers in a pool are of one distribution, and the floating server is of another, you can use the BMI Server to recycle the floating server with a new Linux distribution while provisioning it with a profile. Consult with your Sun distributor for details.

---

## Cloning Servers

Because Sun Update Connection – Enterprise focuses on the component level, Sun Update Connection – Enterprise cloning enables you to maintain legacy data and applications. A management tool that focuses on the image level would simply overwrite the existing image with the source image. The Sun Update Connection – Enterprise feature provides a more discerning functionality.

Through the console, you can clone a single managed host to another host in a simple procedure. The scenario included here includes steps for changing Settings (see [Chapter 16](#)) that will ensure success of the cloning.

An additional scenario explains how to clone multiple hosts using the Sun Update Connection – Enterprise CLI.

## Before You Begin

Run the Check System profile on the host that you are using as the optimal host. This ensures that the comparison does not include conflicts or dependencies.

See [“Running Predefined Profiles” on page 140](#).

Run the Check Withdrawn Patches profile on Solaris machines.

### ▼ To Clone a Single Server

This procedure uses the Inventory Comparison feature.

**1 Make sure that the source managed host is online and as optimal as you think.**

Run the predefined system profiles on this host.

See [“Running Predefined Profiles” on page 140](#).

**2 Make sure the target managed host is online.**

**3 From the Tools menu, choose Preferences.**

The Preferences window opens. See [“Accessing and Editing Preferences” on page 297](#).

**4 In the Console preferences, Jobs category, increase the value of Max items in a job from 20 to 500.**

Submit and confirm the change.

See [“Console Preferences” on page 298](#).

**5 From the Hosts menu, choose Compare Inventories.**

The Inventory Comparison window opens. See [“Comparing Inventories” on page 155](#).

**6 Select the Target host and the Source host.**

**7 Select the current inventory for both hosts.**

**8 In the Filter field, select the full inventory (Software and Local) or use the Filter Select button to select pieces of the inventory to overwrite.**

**9 Click the Compare button and select the Tasks to Make Target like Source option.**

**10 Click the Make Target like Source button and send the clone job.**

## ▼ To Clone Multiple Servers

This procedure uses the CLI feature to create a profile from a complete host inventory. After you have the profile, you can delete requirements from it to lock legacy software and files from being overwritten during the clone job. Then the profile is sent to as many servers as you choose.

- 1 In a terminal window, type the CLI command to convert an inventory to a profile.

```
# uce_cli -cip -P new_profileName -h source_host -u user -p password
```

See “Convert Inventory to Profile (-cip) Command” on page 277.

- 2 View the attributes of the profile (what is required and what is not allowed).

```
# uce_cli -lpa -P profileName -u user -p password
```

See “List Profile Attributes (-lpa) Command” on page 261.

- 3 To protect legacy components on the target servers, delete the profile attributes that you do not want to clone over.

- a. Export the profile to an XML file name.

```
# uce_cli -exp -ent "Profile" -f path-and-filename.xml -T "profile" -u user -p password
```

- b. Edit the XML file. Delete the lines that mention components you want to protect on targets.

- c. Import the edited XML file as the profile.

```
# uce_cli -imp -f path-and-filename.xml -u user -p password
```

See “Export (-exp) Command” on page 273.

- 4 In the console, create a job that deploys the profile on selected hosts.

See “Creating Complex Jobs” on page 194.

## Sharing Directories

The Linux operating system is designed to be a network server or workstation. Sharing directories and files between computers, even of differing operating systems, is a relatively simple task. Although useful, it can be a daunting task for large environments. Sun Update Connection – Enterprise provides the tools to automate sharing and mounting, at the same time ensuring that the relevant machines have the necessary software and files to perform the tasks.



## Mounting an NFS Directory

This procedure shows how scripts can be used in Sun Update Connection – Enterprise jobs to make every-day administration tasks fast and easy. This scenario uses NFS to mount a Linux directory on a client Linux machine. It assumes an NFS server already exists.

### ▼ To Mount an NFS Directory

- 1 **Create a short script called `mntnfs.sh` that appends the appropriate line the `/etc/fstab`.**

```
#!/bin/bash
nfs=nfs_server_hostname
mntPnt=mounted_directory
fstab_line="$nfs: $mntPnt $mntPnt nfs nfsvers=2,rw 0 0"

echo $fstab_line >> /etc/fstab
/etc/init.d/netfs start
mount -a
```

- 2 **Upload the script as a Local -> Pre-Action -> `mntnfs`.**  
See [“Uploading Actions”](#) on page 104.
- 3 **Create a profile that requires `nfs-utils` and `mntnfs`.**  
See [“To Create a Profile”](#) on page 173.
- 4 **Make the profile applicable to all active distributions.**  
See [“To Align Component Settings for Multiple Distributions”](#) on page 210.
- 5 **Run a job on selected hosts that deploys the profile.**  
See [“Creating Complex Jobs”](#) on page 194.

## Mounting a Windows File System from Linux

This procedure shows how simple scripts can be used in Sun Update Connection – Enterprise jobs to make everyday administration tasks fast and easy. This scenario uses samba to mount a Microsoft Windows directory (that is previously set to Shared on Windows) from a Linux file system.

### ▼ To Mount a Windows Directory from a Linux Filesystem

- 1 **Create a short script called `mntWinSamba.sh` that turns on samba and runs the command to mount the directory.**

```
#!/bin/bash
user=linuxuser
pass=passwd4user
```

```
wincp=/win_hostname
winpath=/win_directory
linuxpath=/linux_mntdir
fstab_line=$wincp$winpath /mnt$linuxpath smbfs
    username=$user,password=$pass 0 0

/etc/init.d/smb start
echo $fstab_line >> /etc/fstab
mount -a
```

- 2 Upload the script as a Local -> Post-Action -> mntWin.**  
See [“Uploading Actions” on page 104.](#)
- 3 Create a profile that requires samba-client and mntWin.**  
See [“To Create a Profile” on page 173.](#)
- 4 Make the profile applicable to all active distributions.**  
See [“To Align Component Settings for Multiple Distributions” on page 210.](#)
- 5 Run a job on selected hosts that deploys the profile.**  
See [“Creating Complex Jobs” on page 194.](#)

## DB2

DB2 is a popular application. It is licensed, not Open Source, and therefore, it is not included in vendor distributions.

If you have the DB2 CD and a valid license, you can use this scenario to make installation faster and to ensure that your servers are completely managed by Sun Update Connection – Enterprise. After you have uploaded DB2 as an NCO to the local knowledge base, the Local Expansion Technology generates rules for it. These rules ensure that DB2 will work as an integral part of your environment.

### ▼ To Deploy DB2 on Multiple Machines

This procedure uses a script that calls up the DB2 license file during automated installation.

- 1 Upload the DB2 RPMs to the local knowledge base.**  
The RPMs are listed under Local -> Local RPMs. See [“Adding Undetected Linux Software” on page 85.](#)
- 2 Create a Local File Declaration that is the path where the license file should be installed.**  
For example, the file might be `/tmp/db2pe.lic`.

See “Creating File Declarations” on page 111.

### 3 Upload the license file as a Local Configuration File under the File Declaration.

See “Uploading Local Configuration Files” on page 113.

### 4 Create a script that does the following:

- Installs the license
- Creates DB2 users and instances
- Starts DB2

```
#!/bin/sh

OUTFILE="/tmp/db2_uce.out"

# Definitions
LICENSE_FILE="/tmp/db2pe.lic"
INST_DIR="/opt/IBM/db2/V8.1"

SERVICE_NAME=db2c_db2inst1
SERVICE_PORT=50000
INSTANCE_NAME=db2inst1
INSTANCE_USER=db2inst1
INSTANCE_GROUP=db2grp1 INSTANCE_HOME="/home/$INSTANCE_USER"
FENCED_USER=db2fenc1
FENCED_GROUP=db2fgrp1
FENCED_HOME="/home/$FENCED_USER"
ADMIN_USER=dasusr1
ADMIN_GROUP=dasadm1
ADMIN_HOME="/home/$ADMIN_USER"

# Install the DB2 license
$INST_DIR/adm/db2licm -a $LICENSE_FILE >> $OUTFILE 2>&1

# Fenced User Creation
groupadd $FENCED_GROUP
useradd -g $FENCED_GROUP -m -d $FENCED_HOME $FENCED_USER
chmod 755 $FENCED_HOME

# Instance User Creation
groupadd $INSTANCE_GROUP
useradd -g $INSTANCE_GROUP -m -d $INSTANCE_HOME $INSTANCE_USER
chmod 755 $INSTANCE_HOME

# Admin User Creation
groupadd $ADMIN_GROUP
useradd -g $ADMIN_GROUP -m -d $ADMIN_HOME $ADMIN_USER
chmod 755 $ADMIN_HOME
```

```

# Edit entry in /etc/services??
etc_serv=\Qgrep $SERVICE_NAME /etc/services | wc -l\Q
if [ $etc_serv -eq 0 ] ;
then
  echo "$SERVICE_NAME $SERVICE_PORT/tcp #DB2" >> /etc/services
fi

# Create db2 instance
$INST_DIR/instance/db2icrt -a SERVER -u $FENCED_USER -p $SERVICE_NAME
  $INSTANCE_NAME >> $OUTFILE 2>&1

# Admin instance creation
$INST_DIR/instance/dasCRT $ADMIN_USER >> $OUTFILE 2>&1

# Update DB manager configuration
$INST_DIR/instance/db2iexec $INSTANCE_NAME ". sqlllib/db2profile; db2
  update dbm
  cfg using svcname $SERVICE_NAME; db2set -i $INSTANCE_NAME
  db2comm=tcPIP; db2 terminate" >> $OUTFILE 2>&1

# Set DB2AUTOSTART=YES for $INSTANCE_NAME
$INST_DIR/instance/db2iset DB2AUTOSTART=YES -i $INSTANCE_NAME >>
  $OUTFILE 2>&1

# DB2 Start
$INST_DIR/instance/db2iexec $INSTANCE_NAME ". sqlllib/db2profile;
  db2stop; db2start " >> $OUTFILE 2>&1

# DB2 Admin Start
$INST_DIR/instance/db2iexec $ADMIN_USER ". das/dasprofile; db2admin
  start " >> $OUTFILE 2>&1

```

## 5 Upload the script under Local -> Post-actions -> postDB2.

See [“Uploading Actions” on page 104](#).

## 6 Create a profile that requires the following:

- All DB2 RPMs
- Local -> Configuration files -> license file
- Local -> Post-actions -> postDB2

See [“To Create a Profile” on page 173](#).

## 7 Run a job on selected hosts that deploys the profile.

See [“Creating Complex Jobs” on page 194](#).

# WebSphere

WebSphere is another popular licensed application that is not included in vendor distributions.

If you have the WebSphere CD and a valid license, you can use this scenario to make installation faster and to ensure that your servers are completely managed by Sun Update Connection – Enterprise. After you have uploaded WebSphere as an NCO to the local knowledge base, the Local Expansion Technology generates rules for it. These rules ensure that WebSphere will work as an integral part of your environment.

## ▼ To Deploy WebSphere on Multiple Machines

This procedure uses a script that calls up the WebSphere response file during automated installation.

### 1 Upload the WebSphere RPM to the local knowledge base.

The RPM will be listed under Local -> Local RPMs. See [“Adding Undetected Linux Software” on page 85](#).

### 2 Create a Local File Declaration that is the path where the response file should be installed.

For example, the path is `/tmp/WSresponse.txt`

See [“Creating File Declarations” on page 111](#).

### 3 Upload the response file as a Local Configuration File under the File Declaration.

See [“Uploading Local Configuration Files” on page 113](#).

### 4 Create a script that runs WebSphere integrated installation procedures with the response file and then starts WebSphere.

```
#!/bin/sh

# In this example, the installation directory should be
# on a local filesystem. Should be updated for NFS if
# moved to a non-standalone demo system

SOURCE_DIR="/root/demoscripts/websphere/WAS5Trial"
WS_DIR="/opt/WebSphere/AppServer/bin"

# Ensure that the installation directory is available

if [ ! -f $SOURCE_DIR/install ] ;
then
    echo "WebSphere installer not available."
    exit 1
fi
```

```
#Install WebSphere using response file

$SOURCE_DIR/install -options /tmp/wsresponse.rsp

# Start the WebSphere server

$WS_DIR/startServer.sh server1

exit 0
```

**5 Upload the script under Local -> Post-actions -> postinstallWS.**

See [“Uploading Actions” on page 104.](#)

**6 Create a script that creates WebSphere users and groups.**

```
#!/bin/sh

# In this example, the installation directory should be
# on a local filesystem. Should be updated for NFS if
# moved to a non-standalone demo system

SOURCE_DIR="/root/demoscripts/websphere/WAS5Trial"

# Users and groups needed if installing the Messaging Sub-system
# (MQ Series)

groupadd mqm
groupadd mqbrkrs

useradd -g mqm -G mqbrkrs mqm

# Ensure that the installation directory is available

if [ ! -f $SOURCE_DIR/install ] ;
then
    echo "WebSphere installer not available."
    exit 1
fi

exit 0
```

**7 Upload the script under Local -> Post-actions -> postsetupWS.**

See [“Uploading Actions” on page 104.](#)

**8 Create a profile that requires the following:**

- WebSphere RPM
- Local -> Configuration files -> response file

- Local -> Post-actions -> postinstallWS

See “To Create a Profile” on page 173.

**9 Create a profile that requires Local -> Post-actions -> postsetupWS.**

See “To Create a Profile” on page 173.

**10 Create a complex job that deploys the first profile and then the second profile on selected hosts.**

See “Creating Complex Jobs” on page 194.





# Customizing Preferences

---

This chapter describes how to set preferences to control Sun Update Connection – Enterprise operations.

---

**Note** – The preferences for the dependency manager can be viewed and edited only by the admin user.

---

This chapter covers the following topics:

- “Accessing and Editing Preferences” on page 297
- “Console Preferences” on page 298
- “Host Preferences” on page 300
- “Dependency Manager Preferences” on page 302
- “Submit Edits” on page 304

## Accessing and Editing Preferences

The following procedures explain how to access, edit, apply, and share changes among multiple hosts.

You can view and change the way the console behaves. You can view and change preferences for any agent application that is installed on a managed host, and then propagate the changes to other hosts.

If you have the admin user password, you can change the preferences for the dependency manager.

You can also set preferences for the Sun Update Connection – Enterprise server from the preferences of each of the applications. You can change the directories where downloads from the servers are kept and the protocol for the applications to communicate with each other.

## Opening the Preferences Window

### ▼ To Open the Preferences Window

**1 Log into the console.**

If you want to access the dependency manager parameters, log in as the admin user.

**2 Do one of the following:**

- **From the tool bar, click the Preferences button.**
- **From the Tools menu, choose Preferences.**

The Preferences window opens.



## Console Preferences

Console Preferences let you control how the Sun Update Connection – Enterprise GUI operates, where files are to be stored, how it communicates with the system dependency server, and advanced background job options.

### ▼ To Change Console Preferences

**1 In the Preferences window, select the Console radio button.**

The preferences for the console are accessible by default.

**2 Make the changes that you want.**

If you want to change various preferences in different categories of the selected entity, you can browse between the categories without clicking Submit every time. Your changes are remembered.

## Console Preferences – Files

These parameters determine file upload and download times and let you set the path name of the web browser.

- **File timeout.** Specifies the time limit in seconds for a file to upload to or download from a remote host (see “Opening Host Files” on page 124).

---

**Note** – Take into account local network traffic and physical distance when changing this value.

- **Path.** Specifies the path to the web browser that Sun Update Connection – Enterprise opens from the Component Information window.

---

**Note** – To find the path of the current browser, in a terminal window, type which *browser*.

- **Browser.** Specifies the browser that Sun Update Connection – Enterprise opens.

## Console Preferences – Jobs

These parameters are fine-tuning for running and monitoring jobs.

- **Max items in a job.** Specifies the warning limit for a job that is created in the Inventory Comparison window. The unit is the task items in a job.  
If no value is specified, the user is warned that job might be too big to succeed.
- **Prerequisite details.** Specifies whether to show data in the Host Progress window that is found by local probes.

---

**Note** – This preference is deselected by default to save on resources.

- **Status window refresh interval.** Specifies the time interval in seconds between data adjustment of jobs status in the Jobs panel.

## Console Preferences – Logs

These parameters are the path names and sizes for the console logs.

- **Error log file name.** Specifies the full path name of the error log of the console application.
- **Error log size.** Specifies the size limit in kbytes of the error log. If no value is specified, the log is deleted.
- **Job log file name.** Specifies the full path name of the job log.
- **Job log size.** Specifies the size limit in kbytes of the job log. If no value is specified, the log is deleted.

## Host Preferences

Host preferences manage how each agent handles Sun Update Connection – Enterprise jobs and logs, and how Sun Update Connection – Enterprise recognizes the host.

- You may view the preferences of only one host at a time.
- The host must be online and the agent must be connected to the SDS.
- The agent must not be busy at the time with an Sun Update Connection – Enterprise job.

### ▼ To Change Host Preferences

- 1 **In the Preferences window, select the Host radio button.**

The Host Selection window opens.

- 2 **Select a single host and then click OK.**

- 3 **Wait while the Preference values of the selected agent are uploaded to the console.**

---

**Note** – Preference values can be uploaded only if the agent is not busy with another command.

---

- 4 **Make the changes that you want.**

If you want to change various preferences in different categories of the selected entity, you can browse between the categories without clicking Submit every time. Your changes are remembered.

### ▼ To Share Host Preferences

You can change the preferences of one host, and apply those changes to multiple hosts. For example, if you want all managed hosts in one group to be configured for a new port, you can make the change once, and then share the new port number with all the other hosts in the group.

- 1 **Make the changes you want, submit them, restart the agent, and wait for changes to be uploaded.**

- 2 **Open the Preferences window again select the original host.**

- 3 **Click Select target hosts.**

The Select Hosts window opens.

- 4 **Add multiple hosts to the Selected Hosts list and then click OK.**

The preferences that you changed in the original host are copied to the selected hosts.

You can choose to share preferences with offline hosts. Their preferences are updated when they come online.

## Host Preferences – General

The following parameters offer various options for a specific host.

- **Listening port.** Specifies the port on which to listen for the dependency manager.
- **Clean-up after instal.** Specifies whether to delete no-longer needed RPM files after component is installed to save disk space.

## Host Preferences – Logs

These preferences point to the log files and set limits on their sizes. These logs are kept on the remote host.

- **Error log size.** Specifies the size in kbytes of the error log for this agent.
- **NCO log file size.** Specifies the size in kbytes of the log for local components installed on this managed host.
- **Job log size** – Specifies the size in kbytes of the job log for this agent.
- **Resolve log file size.** Specifies the size in kbytes of the log for each job action and for alternative job solutions.
- **Error log file name.** Specifies the full path name of the error log.
- **NCO log file name.** Specifies the full path name of the NCO log.
- **Job log file name.** Specifies the full path name of the job log.
- **Resolve log file name.** Specifies the full path name of the resolve log.

## Host Preferences – PKGs

The following parameters describe how Solaris packages are installed on Solaris machines. When you install the Sun Update Connection – Enterprise Agent on a Solaris machine, the path name of the Solaris admin file is `/opt/local/uce/agent/config_files/admin`. This file holds the answers for package deployment. You can change these parameters in the Preferences -> Host -> PKGs window, to change the parameters individually for a specific host, or you can point Sun Update Connection – Enterprise to your own customized Solaris admin file.

- **Mail address.** Specifies the address to which notification emails are sent when PKGs are installed.
- **Package install basedir.** Specifies the base directory where relocatable packages are to be installed.
- **Partial.** Specifies one of the following if a package is partially installed on this managed host.
  - **nocheck.** Do not check for partially installed packages.
  - **quit.** Do not install the package if it is already partially installed.
- **RunLevel.** Specifies one of the following if the system status is not correct for the installation or uninstallation of a package.

- **nocheck.** Do not check the run level.
- **quit.** Do not install or uninstall if run level requirement is not met.
- **Install depend.** Specifies one of the following if other packages depend on the one being installed.
  - **nocheck.** Do not check for dependencies.
  - **quit.** Do not install a package if its dependencies are not met.
- **Remove depend.** Specifies one of the following if other packages depend on the one that you want to uninstall.
  - **nocheck.** Do not check for dependencies.
  - **quit.** Do not uninstall a package that is needed by others.
- **Check space.** Specifies one of the following if the disk space of this managed host does not meet the installation requirements of the package.
  - **nocheck.** Do not check disk space requirements (install will fail if the machine runs out of space).
  - **quit.** Do not install the package if the listed space requirements are not met.
- **Setuid flags.** Specifies one of the following if a package should enable the setuid flag or the setgid flag after installation. These flags are used in Solaris programming for security.
  - **nocheck.** Do not check for the setuid executable or the setgid executable.
  - **quit.** Do not install the package if it will turn on these flags.
  - **nochange.** Install the package but override the flags.
- **Check conflicts.** Specify one of the following if the installation of a package will overwrite a file that is provided by another package that has been installed and will create a conflict between files.
  - **nocheck.** Do not check for conflicts and force the installation.
  - **quit.** Do not install the package if file conflicts are detected.
  - **nochange.** Install the package but do not install the conflicting files.
- **Action scripts.** Specify one of the following if the installation of a package provides an action script that contains possible security impacts.
  - **nocheck.** Do not check for security impact of action scripts.
  - **quit.** Do not install the package if its action scripts could negatively impact security.
- **Custom Admin file full path name.** Specify the path name of a customized Solaris `admin` file. If no path is specified, use the default.

## Dependency Manager Preferences

The Dependency Manager Preferences control how the current Dependency Manager (DM) works with consoles and agents.

You must be logged in as the `admin` user to access these Preferences.

## ▼ To Change DM Preferences

### 1 In the Preferences window, select the Dependency Manager radio button.

Wait while the values of the DM preferences are uploaded to the console from the SDS machine.

### 2 Make the changes that you want.

If you want to change various preferences in different categories of the selected entity, you can browse between the categories without clicking Submit every time. Your changes are remembered.

## DM Preferences – Clients

The DM acts as a server to the agents and to the console. These parameters determine connection behavior for the DM – Console and the DM – Agent.

- **Idle Console timeout.** Specifies the time limit in seconds before an idle console automatically logs out.
- **Force change password.** Automatically opens the Change Password window when a user first logs in to create a private password. This behavior is the default.
- **Auto-saved inventories limit.** Specifies the limit of the number of automatically saved inventories to be kept for comparisons and rollback. If no value is specified, older stored inventories are deleted.
- **All agents read-only.** Protects all hosts from change by executing all jobs done in simulate mode. This parameter is only applicable to certain testing environments..
- **Pause Scheduled Jobs.** Pauses all scheduled jobs while this checkbox is selected. Use this parameter before updating agents to ensure the application update is not interrupted by a job.  
When you clear this checkbox, scheduled jobs whose time to run has passed are run immediately

## DM Preferences – Logs

These parameters give the path names and sizes for the DM logs on the SDS machine.

- **Error log size.** Specifies the size limit in kbytes of the error log. If no value specified, the log is deleted.
- **Job log size.** Specifies the size limit in kbytes of the job log. If no value is specified, the log is deleted.
- **Error log file name.** Specifies the full path name of the error log of the DM application.
- **Job log file name.** Specifies the full path name of the job log of the DM application.

## Submit Edits

After changing the values of preference parameters of an application, submit the changes and restart the application.

### Submitting Preferences Customizations

In this procedure you submit the changes you made and restart the target application.

#### ▼ To Submit Changes

**1 In the Preferences window, click Submit.**

The Preferences Confirmation window opens.

If you want to make sure the changes are applied immediately, check the Restart/Logout option.

**2 In the Preferences Confirmation window, click Submit.**

The window closes.

Some setting changes are applied immediately. Some changes are applied only after restart. If you want to continue working and have the changes applied later, leave the Restart/Logout option in the Preferences Confirmation window deselected.

To restart the application later, use one of the following from the command line:

- **Agent** – `/etc/init.d/uce_agent restart`
- **Console** – `uce_console`
- **dependency manager** – `/etc/init.d/uce_engine restart`



# Index

---

## A

- add file declaration, CLI, 269
- add group, CLI, 266
- add host, 265
- add host to group, CLI, 266-267
- add local category, CLI, 268
- add policy, 271-272
- add policy attribute, 271-272
- add profile attribute, 271
- add software package, CLI, 268-269
- add target local, 270
- agent
  - All Hosts, 60
  - busy, 193
  - definition, 21
  - deploying confirmation policies, 182
  - distribution groups, 60
  - handling jobs, 226
  - jobs, 192
  - localizing files, 116
  - managed host, 67
  - read-only, 303
  - registering, 67
  - settings, 301
  - starting, 35
- Apply Fix, 138
- apply fix, policy recommendations, 139
- Auto-saved inventories limit, 303
- automation, jobs, 138

## B

- browser path, 299

- browser setting, 299

## C

- category
  - add to more distributions, 82
  - create, 79
  - create with CLI, 80
  - definition, CO, 148
  - definition, local, 76
  - delete, 82
  - edit, 81
  - properties, 81
- Certification Lab, 19
- Certified Object, see CO, 75
- change password
  - first login, 55
  - force, 303
- changing, managed host inventory, 42-43
- Check Bug Fixes, 136, 139
- Check Security, 136, 139
- Check System, 136
- check withdrawn patches, 137, 139
- clean-up after install, 301
- CLI
  - add file declaration, 269
  - add group, 266
  - add host, 265
  - add host to group, 266-267
  - add local category, 268
  - add policy, 271-272
  - add policy attribute, 271-272
  - add profile attribute, 271

CLI (*Continued*)

- add software package, 268-269
- add target local, 270
- compare hosts and inventories, 277-278
- convert snapshot to profile, 277
- copy policy, 273
- copy profile, 272-273
- delete group, 267
- delete host, 265-266
- delete job, 275
- find component, 257-258
- general notes, 16
- list all hosts, 258
- list distributions, 256-257
- list group's hosts, 260
- list groups, 259-260
- list host inventory, 259
- list host properties, 258-259
- list job status, 264
- list jobs status, 263-264
- list logs, 263
- list policies, 261
- list policy attributes, 262
- list profile attributes, 261-262
- list profiles, 260-261
- list saved snapshots, 264-265
- rename host, 266
- save group inventory, 276
- save host inventory, 275-276
- submit compare job, 278-279
- submit job, 274-275

## CLI command

- ag, add group, 266
- ah, add host, 258
- ahg, add host to group, 266-267
- asp, add software package, 268-269
- dg, delete group, 267
- dh, delete host, 265-266
- dj, delete job, 275
- fc, find component, 257-258
- h, help, 279
- lc, list policies, 261
- ld, list distributions, 256-257
- lg, list group, 259-260
- lgh, list group's hosts, 260
- lh, list host properties, 258-259

CLI command (*Continued*)

- lhi, list host inventory, 259
- ljs, list job status, 263-264
- ljsa, list job data, 264
- lss, list saved inventories, 264-265
- rg, rename group, 267
- rg, rename host, 266
- scj, submit compare job, 278-279
- sgi, save group inventory, 276
- shi, save host inventory, 275-276

CO

- definition, 75
- in Knowledge Base, 78, 147
- inventory, 76, 148
- Local Software Review handling, 227

compare hosts and inventories, 277-278

compare inventories, 155

component

- definition, 75
- details, 100

component information

- confirm tasks, 143
- open browser, 299
- viewing, 150

components list, 76

configuration file

- add, 110
- add with CLI, 115
- definition, 79

conflict, definition, 136

connect host to DM, 301

console

- definition, 21
- logging in, 35
- logs, 299
- preferences, 298
- starting up, 36

convert snapshot to profile, 277

copy policy, CLI, 273

copy profile, 272-273

**D**

- default group, definition, 59
- delete group, CLI, 267

delete host, 265-266  
 delete job, CLI, 275  
 delete RPMs after install, 301  
 Dependencies tab, 101  
 dependency  
   definition, 136  
   fix, 100  
 Dependency Manager  
   agent inventory, 149  
   definition, 191  
 dependency manager  
   disconnected host, 32  
 Dependency Manager  
   disconnected host in job, 34  
 dependency manager  
   functions, 21  
 Dependency Manager  
   jobs, 193  
   logs, 303  
 dependency manager  
   starting, 35  
 Dependency Manager  
   submit job to, 274  
 Dependency Resolver  
   definition, 147  
   in agent, 21  
   in job, 193  
   rejects conflicts, 172  
 disk space, saving, 301  
 distribution group, 59  
 distributions, list all, 256-257  
 DM, see Dependency Manager, 172  
 DR, see Dependency Resolver, 147, 172

## E

empty package, 88  
 enterprise Linux, 19  
 Error log  
   console, 299  
   DM, 303  
   host, 301  
 error message  
   Cannot be deleted, 102  
   Cannot locate the following components, 160

error message (*Continued*)  
   Cannot process command, 77  
   job exceeds the recommended size, 160  
   package-name mismatch, 101

## F

failed jobs, 34  
   confirmation no answers, 217  
   cost, 226  
   cost setting, 299  
   deleted local files, 123  
   file conflicts, 183  
   list with CLI, 263  
   log, 219  
   NCOs, 227  
   not installable, 226  
   permissions, 227  
   policy locked actions, 182  
   post-action returns, 103  
   probe returns, 107  
   rerun jobs, 220  
   resolve error, 225  
   Solaris disk space, 209, 302  
   user request, 217  
 features, 20  
 file declaration  
   add, 111  
   add with CLI, 112  
 files  
   errors in comparison jobs, 160  
   size limit, 298  
   time limit, 298  
 find component, 257-258  
 force change password, 303

## G

group  
   All Hosts, 60  
   create with CLI, 63  
   definition, 59  
   delete, 66  
   delete with CLI, 67, 267

**group** (*Continued*)

- edit, 65
  - edit with CLI, 65
  - in jobs, 60
  - list hosts with CLI, 260
  - list with CLI, 259-260
  - parent, 63
  - profile, 63
  - rename with CLI, 267
  - save inventory with CLI, 153, 276
  - user-defined, 60
- groups, managing, 61

**H**

- help command, CLI, 279
- homegrown applications, see also NCO, 19
- host

- assign to groups, 70
  - delete, 72
  - delete with CLI, 73, 265-266
  - edit, 71
  - icons, 61
  - list in group, 260
  - list inventory with CLI, 259
  - list properties with CLI, 258-259
  - list with CLI, 258
  - logs, 301
  - missing, 151
  - preferences, 300
  - profile compliance, 73
  - properties, 71
  - rename with CLI, 266
  - save inventory, 152
  - save inventory with CLI, 152, 275-276
  - technical definition, 67
  - view inventory with CLI, 151
  - viewing, 61
- hosts, managing, 67

**I**

- idle console timeout setting, 303
- Ignore File Conflict, 138

**install**

- delete packages after, 301
  - indicator, 151
- inventory
- auto save limit, 303
  - compare, 155
  - compare with CLI, 157
  - create jobs, 154
  - definition, 76
  - limit to stored, 303
  - list with CLI, 259
  - save, 152
  - save with CLI, 152
  - saving, 152
  - sending to Engine, 193
  - understanding, 149

**J****Job log**

- console, 299
- DM, 303
- host, 301

**jobs**

- automation, 138
- delete with CLI, 275
- inventory, create, 154
- list status details with CLI, 264
- list status of all jobs, 263-264
- settings, 299

**K**

- Knowledge Base, 161
  - components without rules, 226
  - contents, 148
  - definition, 76
- knowledge base, functions, 21
- Knowledge Base
  - jobs, 193
  - security, 77

**L**

- lifecycle, 19
- limit user to simulate jobs, 50
- list all hosts, 258
- list distributions, 256-257
- list group's hosts, 260
- list groups, 259-260
- list host inventory, 259
- list host properties, 258-259
- list jobs status, 263-264
- list logs, 263
- list policies, 261
- list policy attributes, 262
- list profile attributes, 261-262
- list profiles, 260-261
- list saved snapshots, 264-265
- listening port, 301
- local
  - files, categories, 103
  - fix dependency, 100
  - packages, add, 85
  - security fix, 99
  - software, 76
  - software, add with CLI, 87
  - software, see NCO, 88
  - software review check, 137
- Local Expansion technology, 76
- local expansion technology, functions, 21
- local files
  - definition, 76
  - delete, 123
  - edit from host, 124
  - edit from knowledge base, 120
  - edit properties, 120
  - replace, 121
  - see also configuration files, macros, probes, pre-actions, post-actions, 120
- logging in to the console, 35
- login timeout, 303
- logs
  - console, 299
  - DM, 303
  - hosts, 301
  - list with CLI, 263

**M**

- macro, 79
  - add, 116
  - add with CLI, 118
  - sign, 116
- macro\_sign, 116
- Maintain target's patches, 159
- managed host inventory
  - changing, 40, 42-43
  - saving, 40, 42
  - viewing, 40, 41-42
- managed hosts, 67
  - assign to groups, 70, 71
- managing groups, 61
- managing hosts, 67
- Max items in a job, 299
- middleware, 19

**N**

- NCO
  - add, 85
  - add to more distributions, 96
  - add with CLI, 87
  - check, 137
  - definition, 76
  - delete, 97
  - detection, 84
  - fix dependency, 100
  - handling, 227
  - host log, 301
  - linux
    - attach, 88
    - replace, 88
    - upload, 88
  - remove from distributions, 97
  - rule generation, 84
  - security, 84
  - technical definition, 77
- Non Certified Object, see NCO, 76
- notifications, actions, 76
- notifications, component information, 151
- notifications, email, 48
- notifications, performing needed restart, 143
- notifications, restart, 137

**O**

open source, 19

**P**

package, 76

    empty, 88

    inventory, 148

package group, 76

    edit, 95

password, change, 55

password, force setting, 303

Path setting, 299

Perform Restart, 137

Perform Restart + Reconfigure, 137

permissions

    full, 46

    limit, 45

permitted groups, user restrictions, 46

PKG, add, 90

policy

    add with CLI, 140

    copy with CLI, 273

    definition, 148, 182

    example, 182

    list attributes with CLI, 262

    list with CLI, 261

    predefined profiles, 138

port for agent, 301

post-action, 103

    add, 103, 104

    add with CLI, 106

pre-action, 103

    add, 103, 104

    add with CLI, 106

predefined profile, 137, 139

    confirm actions, 142

    execute with CLI, 142

    executing, 140

    large jobs, 145

    restart, 143

preferences

    agents, 300

    console, 298

    DM, 302

Prerequisite details setting, 299

probe, 103

    add with CLI, 109

    adding, 107

    results, 299

profile

    copy with CLI, 272-273

    create, 173

    from saved inventory, 277

    groups, 63

    host compliance, 73

    list attributes with CLI, 261-262

    list with CLI, 260-261

    purpose, 171

**R**

read-only hosts, 303

rename group with CLI, 267

rename host with CLI, 266

requires, 101

resolve, troubleshooting, 225

Resolve log, host, 301

return zero, 104, 107

rollback, 20

rule generation, 84

rules, 19

**S**

save group inventory, CLI, 276

save host inventory, CLI, 275-276

saving, managed host inventory, 42

SDS., *See* System Dependency Server

security fix, 98, 99

Show Installed

    deselect to see Local Inventory, 78

    viewing host inventory, 151

simulate, default setting, 303

snapshot, 165

snapshot, *see* saved inventory, 264-265

Solaris baselines, using, 128

Solaris post-patch install, 137

Solaris post-restart, 137

---

- starting applications, 35
- submit compare job, CLI, 278-279
- submit job, CLI, 274-275
- Sun Update Connection – Enterprise overview, 19
- System Dependency Server, 21
  - applications, 21
  - connected hosts, 67
  - functions, 21
- system dependency server, starting, 35

## T

- target file path name, 112
- testing host, 301
- third-party applications, 19
- timeout
  - console, 303
  - file, 298

## U

- uce\_console command, 36
- universal server
  - connect from SDS, 21
  - proxy to local, 21
- Unknown, 112
- updating jobs, 60
- upgrade software, check, 137, 139
- upload
  - file timeout, 298
  - packages from CD, 85
  - script, 103
- upload PKG, 90
- user
  - full permissions, 47
  - group limits, 51
  - read-only permissions, 49
  - simulate, 49
- user-defined groups
  - definition, 60
  - nested, 63
- user name, first login, 36
- user restrictions, 45

- users
  - managing, 46, 55
- using, Solaris baselines, 128

## V

- viewing, managed host inventory, 41-42

