Cisco TEO—Process Automation Guide for Incident Analysis for SAP

Release 2.2
September 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24785-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco TEO—Process Automation Guide for Incident Analysis for SAP

CONTENTS

New and Changed Information vii

Preface ix

Organization ix

Conventions x

Product Documentation xi

Documentation Formats xi

Guides and Release Notes xi

Online Help xi

Open Source License Acknowledgements xi

Obtaining Documentation and Submitting a Service Request xii

CHAPTER 1 Importing Automation Packs 1-1

Accessing the Automation Pack Import Wizard 1-2

Opening the Import Wizard After Running Setup Wizard 1-2

Opening the Import Wizard from Console 1-2

Importing the Core Automation for SAP.tap 1-4

Importing the Incident Analysis for SAP.tap 1-7

CHAPTER 2 Understanding the Automation Pack Content 2-1

Accessing Automation Pack Properties 2-2

Viewing Automation Pack Content and Dependencies 2-3

Viewing Automation Pack Content 2-3

Incident Analysis for SAP Processes 2-5

Incident Analysis for SAP Extended Target Properties 2-17

Incident Anaysis for SAP Target Groups 2-24

Incident Analysis for SAP Knowledge Base Articles 2-25

Viewing Automation Pack Dependencies 2-25

Incident Analysis for SAP Reports 2-26

CHAPTER 3 Getting Started Using the Automation Pack 3-1

Creating Runtime Users 3-2

Creating an SAP User Account 3-2

Creating a Runtime User Account 3-3

Creating SAP System Targets 3-4

Using Task Rules for Assignments and Notifications 3-8

Accessing Task Rules View 3-8

Configuring Task Rules 3-9

SAP Default Assignment 3-9

Creating a New Task Rule 3-11

Managing Task Rule Definitions 3-19

Enabling a Task Rule 3-19

Disabling a Task Rule 3-19

Creating a Copy of a Task Rule 3-20

Sorting Task Rules 3-20

Deleting a Task Rule 3-20

Enabling Notification Based on Assignment Processes 3-21

Managing Extended Target Properties 3-22

Accessing Extended Target Properties 3-22

Configuring Extended Target Properties 3-23

Managing Global Variables 3-27

Accessing Global Variables 3-27

Configuring Global Variables 3-28

SAP Alert Suppression Time Properties 3-28

Transaction Analyzer Report Location 3-29

CHAPTER 4 Managing Incident Analysis for SAP Processes 4-1

Accessing Incident Analysis for SAP Processes 4-2

Filtering Processes by Category 4-3

Managing SAP Processes 4-4

Enabling a Process 4-4

Disabling a Process 4-4

Modifying Process Instance Archival 4-5

Modifying a Process Schedule 4-6

Running Processes 4-9

Starting a Process 4-9

Viewing Running Process 4-11

Viewing Process Results 4-13

Accessing Process View 4-13

Viewing Activity Results 4-14

Viewing Incidents 4-15

Viewing Automation Summary 4-17

APPENDIX A Installing TEO SAP Monitoring Management Pack In SCOM A-1

Prerequisites A-1

Configuring the SCOM Environment A-2

Configuring Security Settings A-2

Creating A Run As Account A-2

Distributing Run As Account A-7

Importing Management Pack A-9

Creating a Profile for TEOProcess Database Run As Account A-12

Enabling SAP Alerts on Windows Event Log Process A-16

APPENDIX B Installing the SPI for HP OpenView B-1

Prerequisites B-1

Installing TEO HP OpenView SPI B-2

Configuring HP OpenView B-5

Configuring Services B-5

Deploying TEO Policies B-8

Enabling SAP Alerts on Windows Event Log Process B-9

APPENDIX C Understanding the Core Automation for SAP Content C-1

Automation Pack Content C-1

Core Automation for SAP Task Rules C-1

Core Automation for SAP Global Variables C-2

Core Automation for SAP Processes C-2

Core Automation for SAP Target Groups C-3

Core Automation for SAP Categories C-4

Automation Pack Dependencies C-4

INDEX

New and Changed Information

The following table describes new and changed information in this guide for the Cisco TEO Automation Pack for Incident Analysis for SAP 2.2.

Table 1 Cisco TEO Automation Pack for Incident Analysis for SAP 2.2 Feature Changes

Feature	Location
Updated guide name, automation pack name, and added Text Part Number to document.	All
Changes/Updates to Importing the Automation Pack include: • Disable all imported processes during import feature. • New Default Incidents Assignee Setup panel in Automation Pack Import Wizard (Core Automation for SAP TAP).	Chapter 1, "Importing Automation Packs"
Renamed and reorganized content in the Understanding Automation Pack Objects chapter; included reports in this chapter.	Chapter 2, "Understanding the Automation Pack Content"
New chapter on getting started using the automation pack; includes information about runtime users, targets, task rules, extended target properties, and global variables.	Chapter 3, "Getting Started Using the Automation Pack"
Merged information from Managing Global Variables chapter into Getting Started Using the Automation Pack chapter.	Chapter 3, "Getting Started Using the Automation Pack"
Removed section on Creating Automation Pack for New Processes section. See the *Tidal Enterprise Orchestrator Reference Guide* for information on this feature.	Chapter 4, "Managing Incident Analysis for SAP Processes"
Added appendix that includes information on the content in the Core Automation for SAP automation pack.	Appendix C, "Understanding the Core Automation for SAP Content"

Preface

Cisco TEO automation pack files are a collection of Tidal Enterprise Orchestrator (TEO) processes (workflows) authored by subject matter experts that work out-of-the-box to automate best practices for a particular technology. The automation pack files also include configuration objects that are used in the processes, such as variables, categories, target groups and knowledge base articles.

The Cisco TEO Automation Pack for Incident Analysis for SAP contains the content used to automate best practices for identifying and analyzing availability and performance problems within your SAP environment. TEO provides event correlation and root cause analysis capabilities, and intelligently manages the flood of incoming incidents by analyzing them in the context of the other incidents, events and metrics. When critical problems are detected, you are notified with a thorough description of the problem and recommendations for resolving it using language approproate for both administrators and operators.

This guide is intended to provide information on importing and using the Incident Analysis for SAP automation pack in TEO.

Organization

This guide includes the following sections:

Chapter 1	Importing Automation Packs	Provides instructions for installing the automation packs during or after the initial installation of TEO.
Chapter 2	Understanding the Automation Pack Content	Provides information on the content included in the automation pack.
Chapter 3	Getting Started Using the Automation Pack	Provides information on configuring the objects in TEO that are referenced by the content in the automation pack—runtime users, targets, task rules, extended target properties, and global variables.
Chapter 4	Managing Incident Analysis for SAP Processes	Provides information on using and managing the SAP processes.

Appendix A	Installing TEO SAP Monitoring Management Pack In SCOM	Provides instructions for setting up your SCOM environment, and installing and configuring the management pack.
Appendix B	Installing the SPI for HP OpenView	Provides instructions for installing the TEO modules for HPOV, configuring HPOV services and deploying the policies.
Appendix C	Understanding the Core Automation for SAP Content	Provides information on the content included in the Core Automation for SAP automation pack.

Conventions

This guide uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Product Documentation

Documentation Formats

Documentation is provided in the following electronic formats:

- Adobe® Acrobat® PDF files
- Online help

You must have Adobe® Reader® installed to read the PDF files. Adobe Reader installation programs for common operating systems are available for free download from the Adobe Web site at www.adobe.com.

Guides and Release Notes

You can download the product documentation in PDF format from the product CD.

Online Help

Online help is available and can be accessed using the following methods:

- Click the **Help** button on any dialog box box in the application to open the help topic in a pane to the right of the dialog box box.
- In the Tidal Enterprise Orchestrator console:
  - Click the **Help Pane** tool on the toolbar to open the help topic in a pane to the right of the console results pane.
  - Click **Help** on the menu bar.

Open Source License Acknowledgements

Licenses and notices for open source software used in Tidal Enterprise Orchestrator 2.2 can be found in the *Open Source Licensing Acknowledgements* document on the product CD. If you have any questions about the open source contained in this product, please email external-opensource-requests@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Importing Automation Packs

The *Tidal Enterprise Orchestrator Installation and Administration Guide* provides instructions for installing Tidal Enterprise Orchestrator (TEO) and the core components. During the initial installation of TEO, you can choose to import the automation packs, or import them later from within the Console.

The Cisco TEO Automation Pack for Incident Analysis for SAP has a dependency on the Cisco TEO Automation Pack for Core Automation for SAP. Therefore, this automation pack much be imported before the Incident Analysis for SAP automation pack.

This chapter guides you through importing the automation packs. It includes the following sections:

- Accessing the Automation Pack Import Wizard, page 1-2
- Importing the Core Automation for SAP.tap, page 1-4
- Importing the Incident Analysis for SAP.tap, page 1-7

Note It is recommended that you review the system requirements and prerequisites before importing automation packs. *See* the *Cisco TEO Getting Started Guide for SAP*.

Accessing the Automation Pack Import Wizard

You use the Automation Pack Import Wizard to import the automation packs (tap files). You can open the wizard immediately after installing TEO or from within the Console.

Opening the Import Wizard After Running Setup Wizard

Step 1 After running the Setup wizard to install the product, ensure that the **Launch automation pack import wizard now** check box is checked before closing the wizard.

The Select Automation Packs dialog box displays the available automation packs. All automation packs are checked by default.

Step 2 Ensure that the following check boxes are checked and then click **OK** to launch the Automation Pack Import Wizard:

- Core Automation for SAP
- Incident Analysis for SAP

Note *See* the *Tidal Enterprise Orchestrator Installation and Administration Guide* for instructions on importing and configuring the Core components for the product.

Proceed to Importing the Core Automation for SAP.tap, page 1-4.

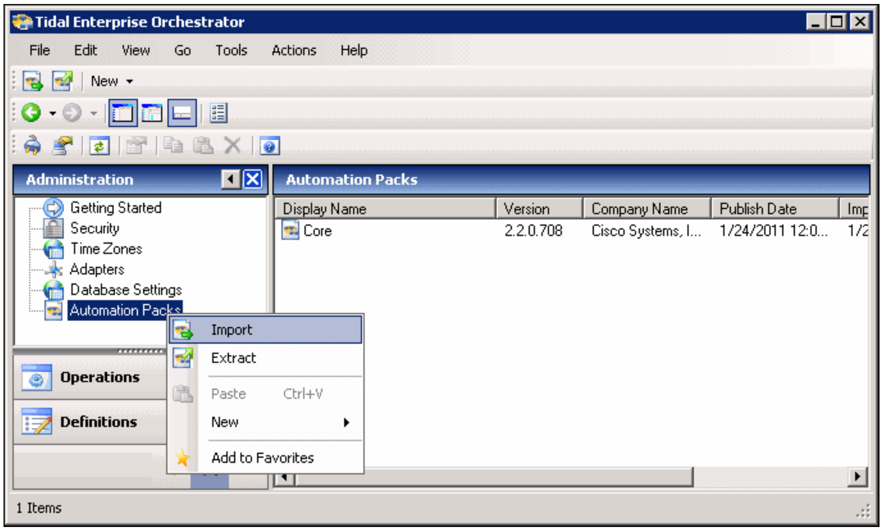
Opening the Import Wizard from Console

You can open the Automation Pack Import Wizard from within the Console after installing product. When importing automation packs from within the Console, you must re-open the Automation Pack Import Wizard for each automation pack that you are importing.

Because the Incident Analysis for SAP automation pack has a dependency on the Core Automation for SAP automation pack, you must first import this automation pack.

Step 1 In the Administration workspace on the Console, click **Automation Packs** in the navigation pane.

Figure 1-1 Automation Packs View—Import Menu



Display Name	Version	Company Name	Publish Date	Imp
Core	2.2.0.708	Cisco Systems, I...	1/24/2011 12:0...	1/2

Step 2 Use one of the following methods to open the Automation Pack Import Wizard:

- In the navigation pane, right-click **Automation Packs** and choose **Import**.
- On the Menu bar, choose **Actions > Import**.

Step 3 On the Windows Open dialog box, select the **Core Automation for SAP.tap** file and click **Open** to launch the Automation Pack Import Wizard.

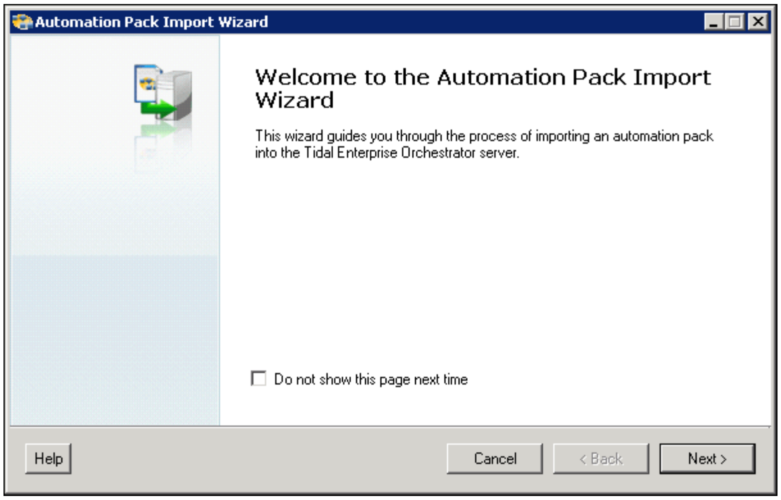
Proceed to Importing the Core Automation for SAP.tap.

Importing the Core Automation for SAP.tap

You must first import the Core Automation for SAP automation pack (Core Automation for SAP.tap). If you opened the Automation Pack Import Wizard from the Setup Completed panel, the wizard will guide you through importing each automation pack.

Step 1 On the Automation Pack Import Wizard Welcome panel, click **Next**.

Figure 1-2 Welcome to the Automation Pack Import Wizard



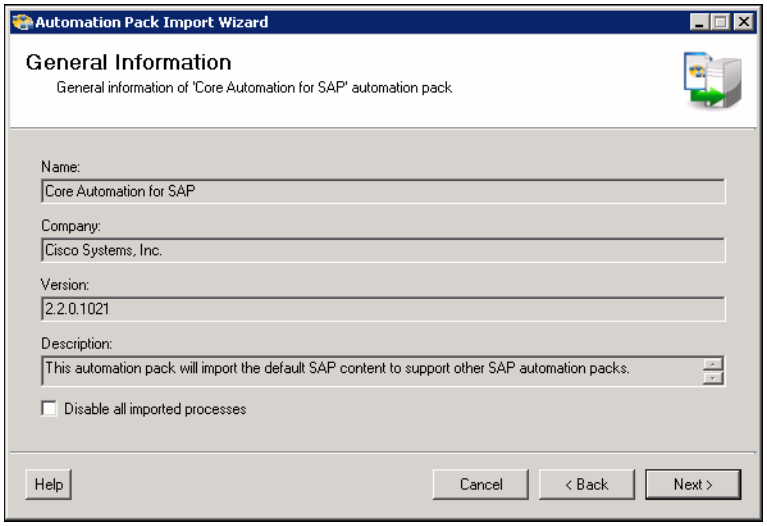
Welcome to the Automation Pack Import Wizard

This wizard guides you through the process of importing an automation pack into the Tidal Enterprise Orchestrator server.

☐ Do not show this page next time

Note If you do not want to display the Welcome panel the next time the wizard is opened, check the **Do not show this page next time** check box.

Figure 1-3 General Information—Core Automation for SAP



General Information

General information of 'Core Automation for SAP' automation pack

Name: Core Automation for SAP

Company: Cisco Systems, Inc.

Version: 2.2.0.1021

Description: This automation pack will import the default SAP content to support other SAP automation packs.

☐ Disable all imported processes

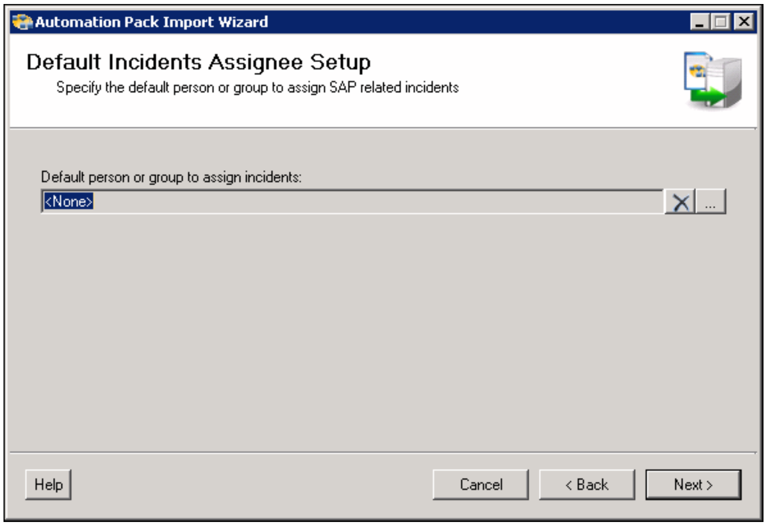
Step 2 On the General Information panel, review the information about the automation pack.

Step 3 If you want to disable all the processes that are imported with the automation pack, check the **Disable all imported processes** check box.

> **Note** If you disable all the imported processes, you will need to manually enable the processes in the Console before they can execute.

Step 4 Click **Next** to continue.

Figure 1-4 Default Incidents Assignee Setup—Core Automation for SAP



Automation Pack Import Wizard

Default Incidents Assignee Setup

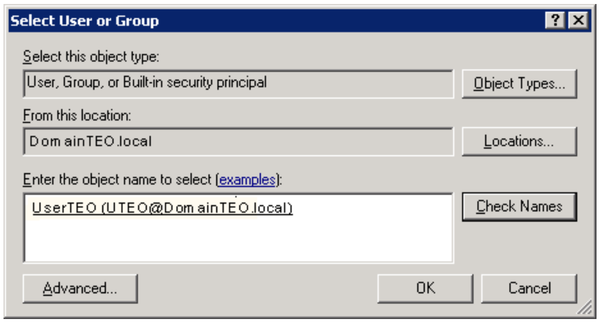
Specify the default person or group to assign SAP related incidents

Default person or group to assign incidents: <None>

Use the Default Incidents Assignee Setup panel to specify the default person who should be assigned SAP-related incidents.

Step 5 Click the **Browse** ... button to specify the user.

Figure 1-5 Select User or Group



Select User or Group

Select this object type: User, Group, or Built-in security principal

From this location: DomainTEO.local

Enter the object name to select (examples): UserTEO (UTEO@DomainTEO.local)

Step 6 On the Select User or Group dialog box, click **Location** and choose the location from which the user will be selected.

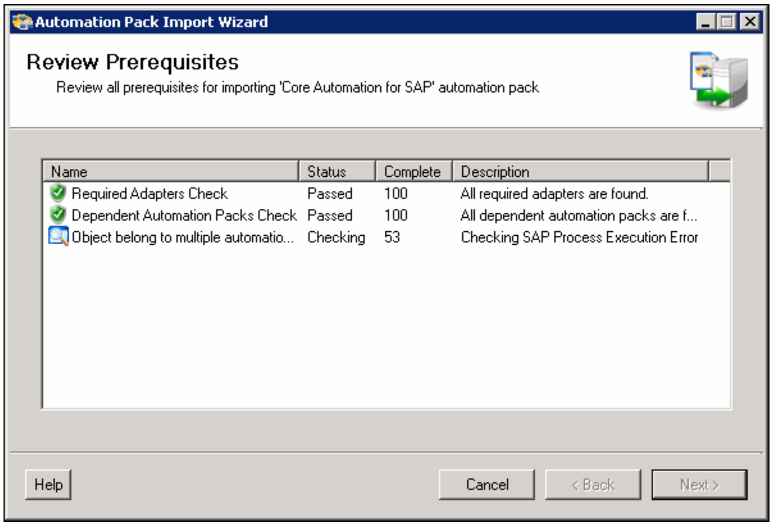
Step 7 In the text box, enter the user name and click **Check Names**.

If the name is found, the box will be populated with the appropriate email address.

Step 8 Click **OK** to close the Select User or Group dialog box.

Step 9 On the Default Incidents Assignee Setup panel, click **Next**.

Figure 1-6 Review Prerequisites—Core Automation for SAP



Review Prerequisites

Review all prerequisites for importing 'Core Automation for SAP' automation pack

Name	Status	Complete	Description
✓ Required Adapters Check	Passed	100	All required adapters are found.
✓ Dependent Automation Packs Check	Passed	100	All dependent automation packs are f...
Object belong to multiple automatio...	Checking	53	Checking SAP Process Execution Error

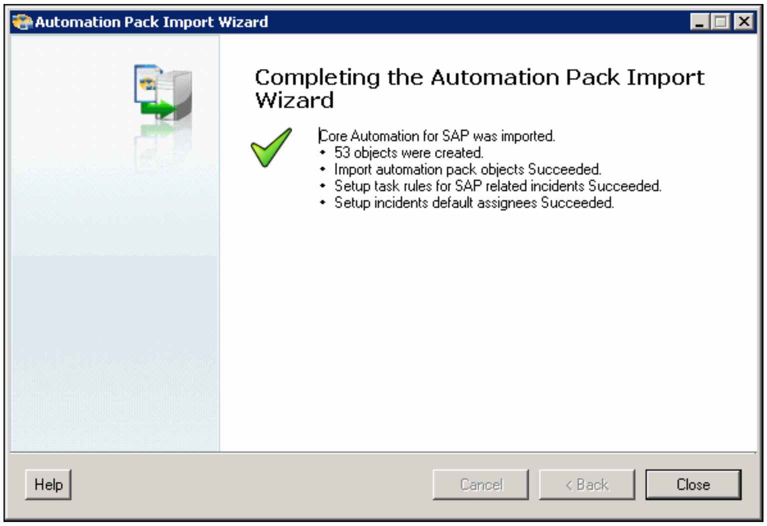
The Review Prerequisites panel displays the prerequisites for the automation pack being imported. The green check mark indicates that the prerequisite was found on the computer.

The red X indicates that the prerequisite was not found on the computer. When this occurs, the import process is stopped and cannot continue until all prerequisites have been met.

If all prerequisites are passed, the wizard automatically continues to the next panel.

Note If you opened the Automation Pack Import Wizard from the Setup Completed panel, the wizard displays the General Information panel (Figure 1-9 on page 1-8) for the next automation pack.

Figure 1-7 Completing the Automation Pack Import Wizard—Core Automation for SAP



Completing the Automation Pack Import Wizard

Core Automation for SAP was imported.

- 53 objects were created.
- Import automation pack objects Succeeded.
- Setup task rules for SAP related incidents Succeeded.
- Setup incidents default assignees Succeeded.

Step 10 After the objects have been imported, review the information on the Completing the Automation Pack Import Wizard panel to verify that it is correct and then click **Close** to close the wizard.

Importing the Incident Analysis for SAP.tap

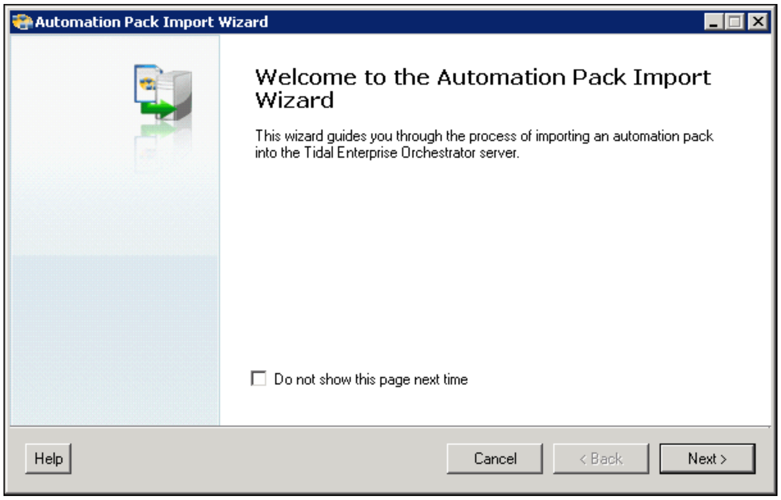
If you are importing the automation packs from within the Console, you must re-open the Automation Pack Import Wizard to import the Incident Analysis for SAP automation pack.

Step 1 Use one of the following methods to open the Import Automation Pack Wizard:

- In the navigation pane, right-click **Automation Packs** and choose **Import**.
- On the Menu bar, choose **Actions > Import**.

Step 2 On the Windows Open dialog box, select the **Incident Analysis for SAP.tap** file and click **Open** to launch the Automation Pack Import Wizard.

Figure 1-8 Welcome to the Automation Pack Import Wizard



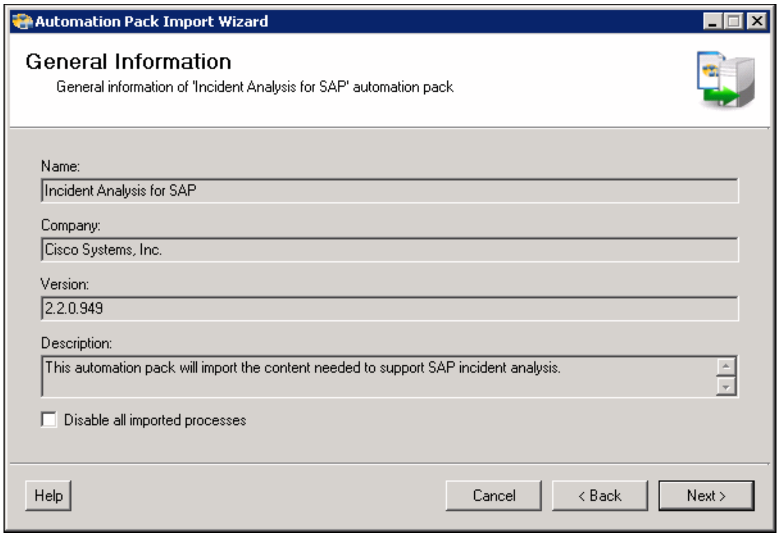
Welcome to the Automation Pack Import Wizard

This wizard guides you through the process of importing an automation pack into the Tidal Enterprise Orchestrator server.

☐ Do not show this page next time

Step 3 On the Welcome panel, click **Next**.

Figure 1-9 General Information—Incident Analysis for SAP



General Information

General information of 'Incident Analysis for SAP' automation pack

Name: Incident Analysis for SAP

Company: Cisco Systems, Inc.

Version: 2.2.0.949

Description: This automation pack will import the content needed to support SAP incident analysis.

□ Disable all imported processes

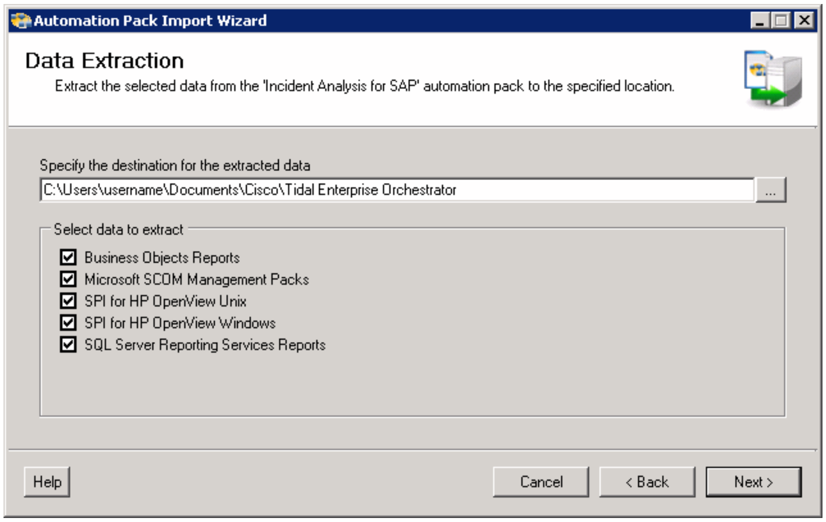
Step 4 On the General Information panel, review the information about the automation pack.

Step 5 If you want to disable all the processes that are imported with the automation pack, check the **Disable all imported processes** check box.

Note If you disable all the imported processes, you will need to manually enable the processes in the Console before they can execute.

Step 6 Click **Next** to continue.

Figure 1-10 Data Extraction—Incident Analysis for SAP



Data Extraction

Extract the selected data from the 'Incident Analysis for SAP' automation pack to the specified location.

Specify the destination for the extracted data: C:\Users\username\Documents\Cisco\Tidal Enterprise Orchestrator

Select data to extract

☑ Business Objects Reports
☑ Microsoft SCOM Management Packs
☑ SPI for HP OpenView Unix
☑ SPI for HP OpenView Windows
☑ SQL Server Reporting Services Reports

Use the Data Extraction panel to specify the destination for the extracted data and the data to be extracted. The Incident Analysis for SAP automation pack provides the following data that can be extracted and the check boxes are checked by default:

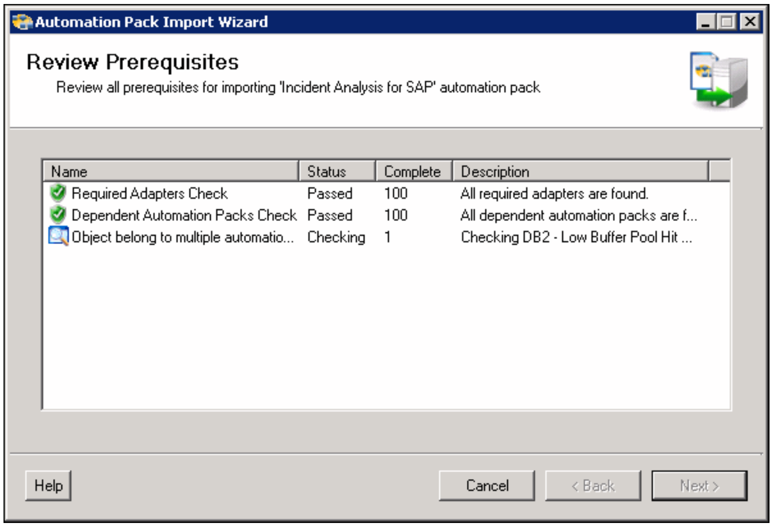
- Business Objects Reports—Extracts the report files to be imported into BusinessObjects after the automation pack has been imported.
- Microsoft SCOM Management Packs—Extracts management packs for integration with the Microsoft System Center Operations Manager 2007 framework.
- SPI for HP OpenView Unix—Extracts the SPI for integration with the HP OpenView Unix framework.
- SPI for HP OpenView Windows—Extracts the SPI for integration with the HP OpenView Windows framework.
- SQL Server Reporting Services Reports—Extracts the report files to be imported into SQL Server Reporting Services after the automation pack has been imported.

Step 7 On the Data Extraction panel, accept the default location or click **Browse** to specify a new destination.

Step 8 In the Select data to extract area, verify that the check boxes are checked for the data that you want to extract. If you *do not* want to extract specific data, uncheck the check box.

Step 9 Click **Next**.

Figure 1-11 Review Prerequisites—Incident Analysis for SAP



Automation Pack Import Wizard

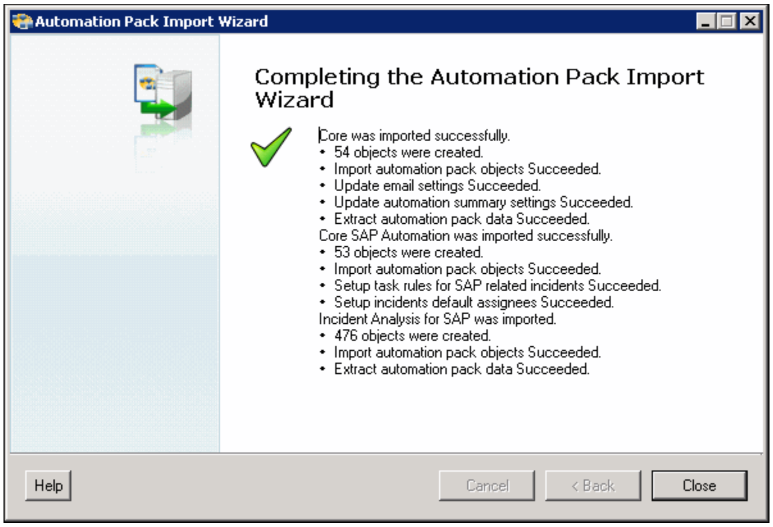
Review Prerequisites

Review all prerequisites for importing 'Incident Analysis for SAP' automation pack

Name	Status	Complete	Description
Required Adapters Check	Passed	100	All required adapters are found.
Dependent Automation Packs Check	Passed	100	All dependent automation packs are f...
Object belong to multiple automatio...	Checking	1	Checking DB2 - Low Buffer Pool Hit ...

If all prerequisites are passed, the wizard automatically continues to the next panel.

Figure 1-12 Completing the Automation Pack Import Wizard Panel



Completing the Automation Pack Import Wizard

Core was imported successfully.
- 54 objects were created.
- Import automation pack objects Succeeded.
- Update email settings Succeeded.
- Update automation summary settings Succeeded.
- Extract automation pack data Succeeded.

Core SAP Automation was imported successfully.
- 53 objects were created.
- Import automation pack objects Succeeded.
- Setup task rules for SAP related incidents Succeeded.
- Setup incidents default assignees Succeeded.

Incident Analysis for SAP was imported.
- 476 objects were created.
- Import automation pack objects Succeeded.
- Extract automation pack data Succeeded.

Step 10 After the objects have been imported, review the information on the Completing the Automation Pack Import Wizard panel to verify that it is correct and then click **Close** to close the wizard.

Note After you have completed importing the automation pack, you can import the Incident Analysis for SAP reports from the Console. For instructions on importing reports, *see* the *Tidal Enterprise Orchestrator Installation and Administration Guide*.

CHAPTER 2

Understanding the Automation Pack Content

The Incident Analysis for SAP automation pack includes the content used to automate best practices for identifying and analyzing availability and performance problems within your SAP environment. TEO provides event correlation and root cause analysis capabilities, and intelligently manages the flood of incoming incidents by analyzing them in the context of the other incidents, events and metrics. When critical problems are detected, you are notified with a thorough description of the problem and recommendations for resolving it using language approproate for both administrators and operators.

This chapter provides information about the content included in the Incident Analysis for SAP automation pack. It contains the following sections:

- Accessing Automation Pack Properties, page 2-2
- Viewing Automation Pack Content and Dependencies, page 2-3
- Incident Analysis for SAP Reports, page 2-26

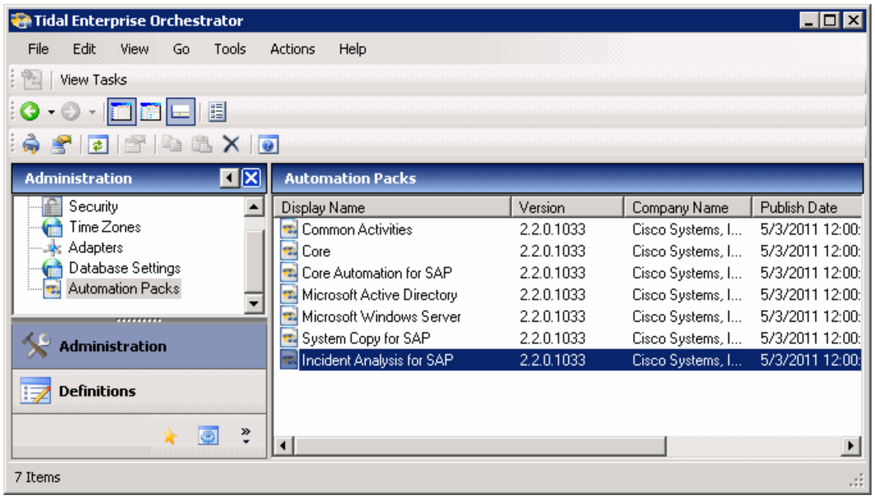
Note See Appendix C, "Understanding the Core Automation for SAP Content" for information on the content included in the Core Automation for SAP automation pack.

Accessing Automation Pack Properties

Users can access the automation pack properties from the Administration—Automation Packs view in the console. The automation pack properties dialog box displays general information about the automation pack, version number, publish date, list of content (objects), the dependencies of the automation pack, and the history of changes made to the automation pack.

Step 1 On the Administration workspace, click **Automation Packs** in the navigation pane to display the installed automation packs in the Automation Packs pane.

Figure 2-1 Accessing Automation Packs



Display Name	Version	Company Name	Publish Date
Common Activities	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:
Core	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:
Core Automation for SAP	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:
Microsoft Active Directory	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:
Microsoft Windows Server	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:
System Copy for SAP	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:
Incident Analysis for SAP	2.2.0.1033	Cisco Systems, I...	5/3/2011 12:00:

Information about the automation packs display in the following columns:

Column	Description
Company Name	Name of the company that released the automation pack.
Publish Date	Date the automation pack was created or exported to a file.
Version	Version number of the automation pack.
Display Name	Name of the automation pack.
ID	Identification number of the automation pack.
Import Date	Date the automation pack was imported into the product.
Licensed	Indicates whether the automation is a licensed product in TEO.
Description	Text description of the automation pack.

Step 2 Select the automation pack in the Automation Packs pane, right-click and choose **Properties**.

Step 3 On the Properties dialog box, click the appropriate tab to view the automation pack properties:

Tab	Description
General	Displays general information about the automation pack.
Objects	Display a list of the content included in the automation pack.
Dependencies	Display a list of automation packs and adapters referenced by the objects in the automation pack.
History	Displays when the automation pack was created or modified, and audit log entries that are relevant to the automation pack.

Step 4 When you have completed viewing the automation pack properties, click **Close** to close the dialog box.

Viewing Automation Pack Content and Dependencies

Use the automation pack Properties dialog box to view the content (objects) included in the automation packs and the dependencies associated with the automation pack.

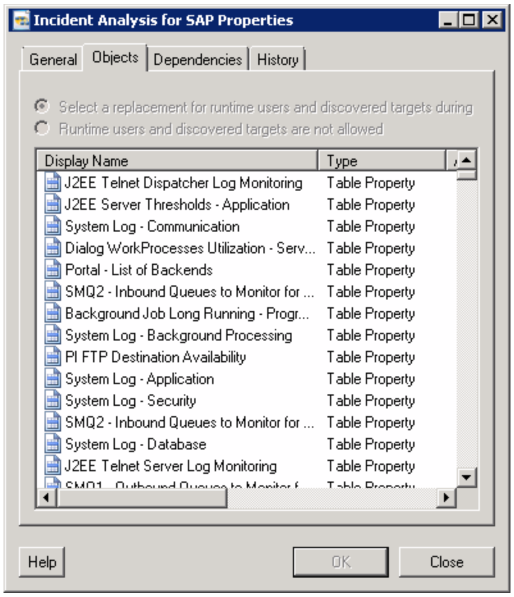
Viewing Automation Pack Content

Use the Objects tab to view a list of the content provided by the automation pack.

Step 1 On the Administration—Automation Packs view, select **Incident Analysis for SAP**, right-click and choose **Properties**.

Step 2 On the Incident Analysis for SAP Properties dialog box, click the **Objects** tab.

Figure 2-2 Incident Analysis for SAP Properties—Objects Tab



Incident Analysis for SAP Properties

● Select a replacement for runtime users and discovered targets during
○ Runtime users and discovered targets are not allowed

Display Name	Type
J2EE Telnet Dispatcher Log Monitoring	Table Property
J2EE Server Thresholds - Application	Table Property
System Log - Communication	Table Property
Dialog WorkProcesses Utilization - Serv...	Table Property
Portal - List of Backends	Table Property
SMQ2 - Inbound Queues to Monitor for ...	Table Property
Background Job Long Running - Progr...	Table Property
System Log - Background Processing	Table Property
PI FTP Destination Availability	Table Property
System Log - Application	Table Property
System Log - Security	Table Property
SMQ2 - Inbound Queues to Monitor for ...	Table Property
System Log - Database	Table Property
J2EE Telnet Server Log Monitoring	Table Property
SMQ1 - Outbound Queues to Monitor f	Table Property

Step 3 On the Objects tab, review the information about the content included in the Incident Analysis for SAP automation pack.

Columns	Description
Display Name	Name of the object (processes, global variables, knowledge base).
Type	Object type.
Action Required	Action required to successfully import or export the objects.
Description	Text description of the object.
Version	Object version.

Incident Analysis for SAP Processes

The following table contains the processes that are imported by the Incident Analysis for SAP automation pack.

Process Name	Description
ABAP ShortDumps Last 1 hour - DB2	Detects the number of shortdumps occuring in the last one hour.
ABAP ShortDumps Last 1 hour - DB2 Mainframe	Detects the number of shortdumps occuring in the last one hour.
ABAP ShortDumps Last 1 hour - Oracle	Detects the number of shortdumps occuring in the last one hour.
ABAP ShortDumps Last 1 hour - SQL Server	Detects the number of shortdumps occuring in the last one hour.
ABAP Terminations (ShortDumps)	Detects when an ABAP program terminates abnormally.
Active Work Processes	Collects number of active work processes.
Aging Exclusive Transaction Lock (Oracle)	Detects and analyzes the cause of exclusive database locks. This process examines the system work processes to identify the process holding the lock.
APO LiveCache Properties	This process periodically gathers the configuration attributes of LiveCache APO systems such as current state, last restart, data and log space.
Application Server Properties	This process periodically gathers the system configuration attributes of SAP servers (instances) such as Kernel version, OS, host name, and number of work processes.
Applications System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to applications.
Background Job Duration Monitor	Every hour the process 'Background Job Duration Monitor' compares running background jobs against thresholds defined in the global variable 'Background Job Maximum Duration' to determine which background jobs are running longer than expected. A threshold may be defined for each background job to monitor.
Background Job Schedule Monitor	Compares SM37 results with global variable 'Background Job Schedule Monitor' to determine if background jobs started and ended in the time boundaries defined in the variable.
Background Processing Errors	Scans the job log for defined error messages to determine why a job aborted. The process will only analyze jobs defined in the global variable 'Background Jobs Aborted - List of Jobs'. The process is triggered by a CCMS alert when a job aborts.
Background Processing Server Metrics	Collects background processing performance metrics of each application server.
Background Processing System Metrics	Collects performance metrics of the system-wide background processing system.

Process Name	Description
Background System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to background processing.
Bad DB Indexes	Detects LiveCache defective database indexes.
BasisSystem System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the basis subsystem.
BatchInput System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the batch input (BDC) subsystem.
Blocked Queues	Detects and analyzes qRFC blocked CCMS alerts. This process creates an incident only if another CCMS queue blocked incident did not happen in the last 15 minutes.
Blocked Integration Server qRFC Queues	Analyzes the status of the XI integration server qRFC queues.
Buffer Hit Rate: "CUA"	Examines the status of SAP application server buffers for user interface elements. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "FieldDescription"	Examines the status of SAP application server buffers for field descriptions. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "GenericKey"	Examines the status of SAP application server buffers for buffered database tables. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "InitialRecords"	Examines the status of SAP application server buffers for initial record layouts. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "Program"	Examines the status of SAP application server buffers for compiled ABAP programs (PXA). This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "Screen"	Examines the status of SAP application server buffers for ABAP screen pages. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "ShortNameTAB"	Examines the status of SAP application server buffers for shortname tables. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "SingleRecord"	Examines the status of SAP application server buffers for cached database table records. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Hit Rate: "TableDefinition"	Examines the status of SAP application server buffers for SAP database table definitions. This process analyzes the buffer hit rate percentage to accurately identify buffer utilization.
Buffer Pool Hit Ratio (DB2)	Detects low chace hit ratio, library cache hit rate.
Buffer Swap Check	Detects object swaps in the application buffers.
Buffers Metrics	Collects buffers metrics.

Process Name	Description
CA Wily Alert Notifications	Monitors Computer Associates Wily alerts that are sent to a mailbox.
Canceled Update Record	Detects when the system has too many cancelled updates.
CCMS Availability Monitoring: Instances	Utilizes Availability Monitoring via the CCMSPING agent to detect whether remote instances are available for work from the Alert Monitor of your Central Monitoring System (CEN).
CCMS Availability Monitoring: Systems	Utilizes Availability Monitoring via the CCMSPING agent to detect whether remote systems are available for work from the Alert Monitor of your Central Monitoring System (CEN).
CCMS System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the CCMS subsystem.
Check Space (MSSQL)	Detects when the database file system utilization is over the threshold.
Cluster Management - Process Time	Analyzes the J2EE cluster's average waiting time for data to be transferred from the dispatcher to the server to detect possible communication performance problems.
Commit Charge (Windows)	Analyzes the cause of low available virtual memory on Windows operating systems. This process examines the commit charge, page in rate, running work processes, other environmental conditions analyzed by TEO to accurately identify the cause of the high commit charge utilization.
Commit Charge Metrics	Collects performance metrics from the Windows memory management.
Communication System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the communications subsystem.
Concurrent Users Metrics	Collects statistics for number of users logged on to the system.
Configuration Manager - Cache	Analyzes the hit rate of the J2EE configuration manager cache, an indication J2EE engine modules are retrieving data from disk too frequently.
CPU Load Average	Measures and analyzes general efficiency of the SAP work processes. This process examines work processes, CPU utilization, and other performance conditions analyzed by TEO to accurately identify the cause of high number of processes waiting to be processed by the CPU.
CPU Utilization	Measures and analyzes CPU utilization averaged across all CPUs. This process examines work processes, user load, paging and other performance samples analyzed by TEO to accurately identify the cause of consistently high CPU utilization.
CPU Utilization Performance Metrics	Collects CPU utilization metrics.
Customer Syslog Messages	Detects messages in the SAP system log (custom) that match parameter Syslog - Customer.

Process Name	Description
Daily Average Workload: Background	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: BufferSync	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: Dialog	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: RFC	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: Spool	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: Total	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: Update	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Daily Average Workload: Update2	Collects previous day number of steps, response time, CPU time, wait time, load time and database request time.
Database Backup (MSSQL)	Detects when the backup has not executed successfully for more than the specified number of days.
Database Backup (DB2 MF)	Detects when the backup has not executed successfully.
Database Backup (DB2)	Detects when the backup has not executed successfully for more than the specified number of days.
Database Backup (Oracle)	Detects when the backup has not executed successfully for more than the specified number of days.
Database Consistency (DB2)	Detects and analyzes differences between the SAP data dictionary and the physical database.
Database Consistency (Informix)	Detects and analyzes differences between the SAP data dictionary and the physical database.
Database Consistency (MSSQL)	Detects and analyzes differences between the SAP data dictionary and the physical database.
Database Consistency (Oracle)	Detects and analyzes differences between the SAP data dictionary and the physical database.
Database Consistency (SAP DB)	Detects and analyzes differences between the SAP data dictionary and the physical database.
Database Consistency: Missing Items (DB2)	Detects and analyzes differences between the SAP data dictionary and the physical database. This process examines detects items in the SAP data dictionary that are missing from the database.
Database Consistency: Missing items (Oracle)	Detects and analyzes differences between the SAP data dictionary and the physical database. This process examines detects items in the SAP data dictionary that are missing from the database.
Database CPU Metrics - MSSQL	Collects database CPU metrics.
Database Deadlock Detected (DB2 MF)	Detects deadlocks reported by the database.

Process Name	Description
Database Disk Free Space (MSSQL)	Detects when the disk drive used by database files or TempDB are running out of space.
Database Disk Metrics - MSSQL	Collects database disk metrics.
Database Disk Metrics - Oracle	Collects database disk metrics.
Database File Systems Monitor (DB2)	Detects when disk space of storage paths or disk space of the file system where the log directory is located are nearing their capacity and must be extended in order to prevent service disruption.
Database Lock (Oracle)	Detects and analyzes SAP process waiting on database lock. This process examines the system work processes, and the Oracle locks table to accurately identify the cause of the locks potentially impacting response time.
Database Lock (DB2)	Detects and analyzes SAP process waiting on database lock.
Database Locks (MSSQL)	Detects and analyzes SAP process waiting on database lock.
Database Request Time	Detects and analyzes the cause of long database request time. This process examines current database workload, database CPU utilization, and other database metrics analyzed by TEO to accurately identify the cause of performance degradation.
Database Size Metrics - MSSQL	Collects database size metrics.
Database System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to applications.
Dialog Performance Metrics	Collects performance information related to online user response time.
Dialog Response Time	Detects and analyzes the cause of slow dialog response time.
Dialog WorkProcesses Utilization	Detects when the number of server dialog processes is reaching a threshold defined on parameter "Dialog WorkProcesses Utilization".
Dispatcher Queue Monitor	Monitors the Dispatcher System Thread Manager queues. It monitors the WaitingTaskQueue (number of tasks for which there are no threads available) and number of tasks that are not receiving any more space in the WaitingTaskQueue.
Enqueue Frequency	Detects and analyzes the frequency enqueue operations (logical data locks) per minute that are coming from another instance to the central instance. This process examines the enqueue to identify the source of enqueue overload.

Process Name	Description
Enqueue Queue Length	Detects when the number of enqueue requests is approaching the capacity of the enqueue server. This process examines the percentage length of the wait queue for the enqueue service to accurately identify enqueue capacity problems.
Enqueue Table Size	Analyzes the number of lock entries in the enqueue table. This process examines the size of the enqueue table to detect lock backlogs.
Error Message (Oracle)	Examines the Oracle alert log and detects Oracle error messages.
File System	Monitors file system resources such as percentage used and free space.
Free Active Alert Slots in Shared Memory	Detects CCMS alerts for the number of free active alert slots in shared memory.
Gateway Reader	Examines the gateway process and detects when the maximum possible number of clients for the gateway nears capacity.
Gateway Reader Metrics	Collects Gateway Reader metrics.
Generic SAP Telnet Command	Used to execute SAP telnet commands on J2EE servers.
GRMG - Availability Monitoring	Used to execute SAP telnet commands on J2EE servers.
GRMG - Availability Scenario Monitoring	Detects URL availability alerts generated by GRMG (Generic Request Message Generator).
Monitoring	Detects URL availability alerts generated by GRMG (Generic Request Message Generator).
ICM Queue	Examines the internet communication manager wait queue and detects when the number of requests waiting for ICM worker threads nears capacity.
IDoc Inbound Backlog (ALE)	Examines the inbound IDoc queue and detects backlogs of inbound IDocs that have not been processed or are in an error state.
IDoc Inbound Error Backlog (ALE)	Detects inbound IDoc application posting failure backlogs. This process inspects the inbound IDoc queue for backlogs of inbound IDocs in error state.
IDoc Inbound Processing (ALE)	Examines the inbound IDoc queue and detects when the number of inbound IDocs in a each processing status exceeds threshold.
IDoc Outbound Backlog (ALE)	Examines the outbound IDoc queue and detects backlogs of outbound IDocs that have not been sent or are in an error state.
IDoc Outbound Error Backlog (ALE)	Detects outbound IDoc error backlogs. This process inspects the outbound IDoc queue for backlogs of outbound IDocs in error state.
IDoc Outbound Processing (ALE)	Examines the outbound IDoc queue and detects when the number of outbound IDocs in a each processing status exceeds threshold.

Process Name	Description
Installed Components (adhoc)	Lists the installed components, releases and patch levels.
Installed Components (report)	Lists the installed components, releases and patch levels. The process will create an alert per components and it is used in reports.
IView Response Time	Samples IView response time for a custom defined set of IViews. This process analyzes the sample averages to detect the potential cause of slow response time.
J2EE Application and System Threads Manager Metrics	Collects Application Thread Pool performance metrics.
J2EE Cluster Management Metrics	Collects Cluster Management performance metrics.
J2EE Connections Manipulator Metrics	Collects Connections Manipulator performance metrics.
J2EE Memory Service Metrics	Collects Memory Service performance metrics.
Lan Collisions Metrics	Collects network performance metrics - Collisions.
Lan Packets In Metrics	Collects network performance metrics - Inbound Packets.
Lan Packets Out Metrics	Collects network performance metrics - Outbound Packets.
LCA - Data Cache Hit Rate Metrics	Collects "Live Cache - Data Cache Hit Rate" metrics.
LCA - Data Cache Usage Metrics	Collects "LiveCache - Data Cache Used" metrics.
LCA - Heap Usage Metrics	Collects "LiveCache - Heap Usage" metrics.
LCA - Used Data Space Metrics	Collects "LiveCache - Used Data Space" metrics.
LCA - Used Log Space Metrics	Collects "LiveCache - Used Log Space" metrics.
LCA Data Space	Detects LCA data area storage shortages that could potentially cause LiveCache to hang.
LCA Log Space	Detects LCA log space storage shortages that could potentially cause LiveCache to hang.
LiveCache Error	Examines the livecache alert monitor and detects LiveCache errors.
LiveCache State	Detects operational state changes in LiveCache that put production operation at risk.
Location Availability Alert	Raises an incident when a location is unavailable.
Location Availability Data Collection for Reports	Collects data for location availability reports.
Location Availability Execution	Starts the process that monitors location availability. This process will be executed in the targets included in the Location Availability Monitors target group.
Long Running Background Work Process	Detects if any background job runtime has exceeded 12 hours. This process examines the system work processes to identify such background processes.
Long Running Dialog Process	Detects when an update process is running longer than the threshold defined on variable "Update Maximum Duration".

Process Name	Description
Long Running Update	Detects when an update process is running longer than the threshold defined on variable "Update Maximum Duration".
Memory Constraint (MSSQL)	Analyzes the database buffer cache hit rate. This process examines the database to detect low buffer hit rate, an indication the server is retrieving data from disk too frequently.
Memory Metrics	Collects memory management metrics.
Memory Service - Used Memory	Examines memory used by the J2EE engine and detects when the current allocation for the virtual machine is nearing total utilization.
Miscellaneous System Log Messages	Detects all messages in the SAP system log that generate alerts not classified to subsystem category.
Monitor Cluster Status	Monitors the status of the J2EE cluster nodes.
Monitor Generic J2EE File	Monitors the status of the J2EE cluster nodes.
Monitor J2EE Dispatcher Logs	Monitors patterns on J2EE dispatcher logs specified on TEO global variables.
Monitor J2EE Server Logs	Monitors patterns on J2EE server logs specified on TEO global variables.
Number of work Processes	Samples the number of work processes of each type on each server.
Object Roll and Paging Metrics	Collects object roll and paging area metrics.
Old Enqueue Entries	Analyzes lock entries entries in the enqueue table over four hours old. This process examines enqueue locks properties to help identify potentially orphaned enqueues.
OMS Data Cache HitRate	Detects and analyzes the data cache rate object management store. This process examines the data cache hit rate and data cache usage to identify the reason for the low cache hit rate.
OMS Heap Usage	Detects when object managment system heap memory utilization is nearing allocated memory capacity.
Open Change Pointers (ALE)	Detects and identifies backlogs in change pointer processing. This process inspects the change pointer tables (BDCP and BDCPS) for open change pointers and counts the number of unprocessed change pointers per message type. Open change pointers indicate master data documents needing to be analyzed and converted into IDocs to be sent to other systems.
Operational Instance Status	Detects instance status availability. This process examines the system log entries to identify the cause of the availability problems.
OS Collector Status	Examines the status of the SAP operating system collector.
Out of Memory Exception	Monitors and detects memory exceptions thrown when the object management system heap size reaches memory capacity.

Process Name	Description
Package and Catalog Cache HitRatio (DB2)	Detects low chace hit ratio, library cache hit rate.
Page In	Detects and analyzes excessive operating system paging. This process examines the average number of page-ins per second, memory utilization, work processes, and other environmental conditions analyzed by TEO to accurately identify the cause of the high paging rate.
Page Out	Detects and analyzes excessive operating system paging. This process examines the average number of page-outs per second, memory utilization, work processes, and other environmental conditions analyzed by TEO to accurately identify the cause of the high paging rate.
Paging Metrics	Collects OS paging statistics.
PI Application Error Monitor	Detects XI messsage processing errors. It is similar to the SXMB_MONI transaction.
PI Business Process Engine Status	Monitors the overall status of the PI business process engine component.
PI FTP Destination Availability	Proactively checks connectivity of selected FTP Destinations. This process is disabled by default and will not work if enabled because it has an invalid runtime user to connect to the FTP Server. You will need to make a copy of the process for each different runtime user that will connect to the FTP Server and update the activity "Test FTP Destination".
PI Queue Monitor	Detects errors in the XI queues.
PI Server Component Availability	Pings internal exchange infrastructure server components for availability and detects if any core server components are unavailable.
PI tRFC Destination Availability	Proactively checks connectivity of selected RFC Destinations. This process issues an RFC connection test and identifies which RFC destinations have lost connectivity.
Portal Availability	Proactively checks connectivity of selected portals. This process issues a connection test (SM59 - HTTP) and identifies which destinations have lost connectivity.
Portal Checklist	Automates the most important and frequent tasks for monitoring SAP portal health.
RFC Destination Availability	Proactively checks connectivity of selected RFC Destinations. This process issues an RFC connection test and identifies which RFC destinations have lost connectivity.
RFC Destination Availability - HTTP	Proactively checks connectivity of selected RFC Destinations. This process issues a connection test and identifies which destinations have lost connectivity.
Runstats (DB2 MF)	Detects when runstats is need.

Process Name	Description
SAP Administrator Checklist	Automates the most important and frequent SAP administration tasks for monitoring SAP system health. This process detects and analyzes common error conditions that typically need to be addressed by system administrators.
SAP Connection Errors	Monitors TEO connection errors to SAP systems.
SAP License Check	Checks for an expiring installed license.
SAP System Properties	Periodically gathers the system configuration attributes of SAP systems, such as license information, installed SAP components, release and patch levels and DB platform information.
SAPConnect monitoring - per Status	Detects transmission errors reported by transaction SCOT. **Note** The process is disabled by default because it calls function "SX_SNDREC_SELECT" and it is not available in all SAP versions/sp levels.
SAPConnect monitoring - per Type	Detects transmission errors reported by transaction SCOT. **Note** The process is disabled by default because it calls function "SX_SNDREC_SELECT" and it is not available in all SAP versions/sp levels.
Security Audit Log Messages	Detects all messages in the SAP system log that generate alerts relevant to security audit exceptions. This process is disabled by default because it can generate a large volume of incidents. It depends on system configuration (SM20). **Note** There is no rule in the monitoring framework to collect events generated by this process.
Security System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the security subsystem.
Server Availability	Raises an incident when a server is unavailable.
Server Availability (for report)	Monitors SAP application servers availability. It monitors ABAP stack availability.
Server Queue Monitor - Application	Monitors the Server System and Application Thread Manager queues. It monitors the WaitingTaskQueue (number of tasks for which there are no threads available) and number of tasks that are not receiving any more space in the WaitingTaskQueue.
Server Queue Monitor - System	Monitors the Server System Thread Manager queues. It monitors the WaitingTaskQueue (number of tasks for which there are no threads available) and number of tasks that are not receiving any more space in the WaitingTaskQueue.
Shared Pool Memory (Oracle)	Detects analyzes low shared pool memory. This process examines the row chace hit ratio, library cache hit rate, and free memory to identify the cause of the shared pool memory shortage.

Process Name	Description
Slow SQL Statements (MSSQL)	Analyzes SQL execution and fetch times to detect poorly executing SQL statements.
SMQ1 - Outbound Queue Error Monitor	Detects errors in the outbound queues.
SMQ1 - Outbound Queue Hanging Monitor	Detects queues on states set for monitoring on global variable "SMQ1 - Outbound Queues to Monitor for Hanging - Status to Monitor".
SMQ2 - Inbound Queue Error Monitor	Detects errors in the inbound queues.
SMQ2 - Inbound Queue Hanging Monitor	Detects queues on states set for monitoring on global variable "SMQ2 - Inbound Queues to Monitor for Hanging - Status to Monitor".
Spool Device Message	Detects and analyzes the cause of spool device errors.
Spool Device Metrics	Collects spool devices metrics.
Spool File Number	Detects when the spool file number range interval is near range limits.
Spool High Volume Group Pages Metrics	Collects Spool High Volume Group Pages metrics.
Spool High Volume Group Requests Metrics	Collects Spool High Volume Group Requests metrics.
Spool Service Metrics	Collects system wide spool service metrics.
Spool Service Status	Detects and analyzes the cause of the spool status. This process examines the spool wait time, system log, and other error conditions analyzed by TEO to accurately identify the cause of the spool service error.
Spool Service Wait Time	Detects and analyzes high spool wait time.
Spool System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the spool subsystem.
Spool Wait Time Metrics	Collects average wait time of the spool service metrics.
SQL Error Message (MSSQL)	Examines the SQL Server logs and detects level 17 or higher errors.
Swap Space (Unix)	Detects and analyzes low available swap space on Unix operating systems. This process examines the swap free space and memory paging rates to accurately identify the cause of low swap space.
Swap Space (Unix) Metrics	Collects swap space metrics.
System Log Message Frequency	Detects an increase in the rate of messages written to the system log.
System Wide Background Processing	Detects and analyzes the cause of backlogs or bottlenecks in system-wide background processing. This process examines the background processing queue, work processes configuration, and other system resources analyzed by TEO to accurately identify the cause of the backlogs or bottlenecks.
Table or Index Reorganization (DB2 MF)	Detects when table space on index reorganization is needed.

Process Name	Description
Table Space (DB2)	Detects when a DB2 tablespace is over the threshold.
Table Space (Oracle)	Detects when the Oracle tablespace size is approaching its capacity and must be increased to prevent service disruption.
Tablespace Monitor - 46C (Oracle)	Detects when the Oracle tablespace size is approaching its capacity and must be increased to prevent service disruption.
Tablespace Monitor (Oracle)	Detects when the Oracle tablespace size is approaching its capacity and must be increased to prevent service disruption.
Transaction Response Time Monitoring	Samples system-wide dialog response time for a custom defined set of transactions. This process analyzes the sample averages for work process, wait time, CPU time, database time, and load time to detect the potential cause of slow system-wide dialog response time.
TransportSystem System Log Messages	Detects all messages in the SAP system log that generate alerts relevant to the change and transport subsystem.
tRFC Error Monitoring for Customized Targets	Monitors tRFC errors (CPICERR or SYSFAIL) for specific targets. It compares SM58 results with the list of targets on parameter "Targets for tRFC error check".
tRFC Errors (Communication)	Eetects and analyzes the cause of transactional RFC connection failures. This process examines the RFC error log and tests RFC destination connectivity to identify the cause of the RFC connection error.
tRFC Errors (Execution)	Detects and analyzes the cause of transactional RFC program failures. This process examines the RFC error log to identify the cause of the RFC connection error.
tRFC Queue (Remote Calls Waiting)	Examines the tRFC queue size and reports when a backlog of tRFC calls waiting to be sent occurs.
Update Performance Metrics	Collects update process metrics.
Update Process Errors	Detects and analyzes the cause of errors in the update work processes. This process examines the update process for work process, database, program, and other error conditions analyzed by TEO to accurately identify the cause of the update error.
Update Process Performance	Monitors the performance characteristics of the update processes. This process examines the update work processes and update queue length to detect and identify the cause of update backlogs.
Update Service Status	Detects the shutdown of the update service. This process examines the update queue, system log, and update work processes to accurately identify the cause of the service shutdown.

Process Name	Description
URL Ping	Analyzes availability and response time of a specified URL and detects connection or HTTP protocol failures.
Work Process Analysis	Detects when the number of work processes in Hold or Stopped state for a selected reason is reaching a threshold defined on parameter "Work Processes Status Analysis".

Incident Analysis for SAP Extended Target Properties

The following table contains the extended target properties that are imported by the Incident Analysis for SAP automation pack. The extended target properties that do not have a value defined must be configured by the user prior to using them in processes.

Note For information on configuring extended target properties, see Managing Extended Target Properties, page 3-22.

Extended Target Properties	Description	Value Defined?
Average Dialog Response Time	Threshold for the average dialog response time per server. This variable is used by processes that are started by dialog response time CCMS alerts. If the variable value is less than the CCMS threshold, an incident will be created. Enter the threshold value (milliseconds).	Yes
Background Job Long Running - Programs To Ignore	Monitors long-running background processes. Enter the list of programs that can be ignored when running longer than the threshold entered on variable "Background Job Long-Running - Threshold." Wildcards are not accepted.	No
Background Job Long Running - Threshold	Monitors long-running background processes. Enter the threshold value (seconds).	Yes
Background Job Maximum Duration	Specify a list of background jobs to monitor and their maximum duration in seconds.	No
Background Job Schedule Monitor	Specify a list of background jobs to monitor the start time and end time. TEO will raise an incident when the job does not execute and it is over the start time threshold or job is executing and it is over the end time threshold. Format for start time and end time is HH:mm:ss (24 hours format), for example, 18:00:00 for 6:00 PM.	No

Extended Target Properties	Description	Value Defined?
Background Jobs Aborted - List of Jobs	Specify background jobs to monitor. Incidents will be raised only when aborted jobs are in the list. Wildcards are accepted (for example, if you want to match all jobs that begin with JOB01, enter JOB01*). **Note** Job name is case sensitive.	Yes
Buffer Hit Ratio Threshold	Threshold percentage for buffer hit ratio	Yes
Buffer Swaps Threshold	Threshold for number of swaps in the application buffers.	Yes
CPU Queue Length	Threshold for SAP application server CPU queue length. Enter the threshold value.	Yes
Database Free Space	Threshold for minimum database free space (percentage). This is the file system free space in SQL Server databases and the table space free space in Oracle databases.	Yes
Dialog WorkProcesses Utilization	Maximum percentage of dialog work processes utilization per server.	Yes
Dialog WorkProcesses Utilization - Servers to Ignore	List of servers to ignore when monitoring dialog work process utilization. Enter the full server name (for example, sapr3e02_R3E_00).	No
Enqueue Lock Age	Threshold for how long an object can be held by an enqueue lock. Enter the value in minutes.	Yes
Enqueue Locks - Maximum Number	Threshold for number of locks.	Yes
File System to Ignore	File System to ignore when CCMS raises an alert for File System Utilization that has exceeded the threshold. Wildcards are accepted (for example, if you want to match all file systems starting with "e:" enter e:*).	No
IDOC Monitoring - Inbound	Monitors the number of Inbound IDocs received but not yet processed in the last 24 hours. Enter a list of Inbound IDoc types and the threshold to raise an incident.	No
IDOC Monitoring - Outbound	Monitors the number of Outbound IDocs submitted but not yet sent in the last 24 hours. Enter a list of Outbound IDoc types and the threshold to raise an alert.	No
J2EE Buffer Cache HitRate	Threshold for buffer cache hit rate.	Yes

Extended Target Properties	Description	Value Defined?
J2EE Cluster Management AverageProcessTime	Threshold for Cluster Management AverageProcessTime (High Average MS Process Time indicates a long waiting period for the data to be transferred from the dispatcher to the server). The unit is milliseconds.	Yes
J2EE Dispatcher Thresholds	Thresholds for dispatcher queues (number of runnable tasks waiting for available thread in the threads pool).	Yes
J2EE Memory Used	Threshold for percentage of used memory in the server.	Yes
J2EE Server Thresholds - Application	Thresholds for server queues (number of runnable tasks waiting for available thread in the threads pool). It monitors the Application Thread Manager queues.	Yes
J2EE Server Thresholds - System	Thresholds for server queues (number of runnable tasks waiting for available thread in the threads pool). It monitors the System Thread Manager queues.	Yes
J2EE Telnet Dispatcher Log Monitoring	J2EE dispatcher logs to be monitored via SAP telnet. Enter the list of logs to monitor (log), the pattern to match via grep command (pattern), the number of logs of each type that are created in the application server and a comma delimited list of wildcards to filter out matches (exclude). TEO monitors logs at usr/…/cluster/<dispatcher>/log/system.	Yes
J2EE Telnet File Monitoring	J2EE files to be monitored via SAP telnet. Enter the full path for the files to be monitored (file), the pattern to match via grep command (pattern) and a list of widcards to filter out matches (exclude).	No
J2EE Telnet Server Log Monitoring	J2EE server logs to be monitored via SAP telnet. Enter the list of logs to monitor (log), the pattern to match via grep command (pattern), the number of logs of each type that are created in the application server and a comma delimited list of wildcards to filter out matches (exclude). TEO monitors logs at usr/…/cluster/<server>/log/system.	Yes
Long Running Dialog Process	Monitors long-running dialog processes. Enter the threshold value (seconds).	Yes
Number of ABAP Shortdumps	Threshold for the number of ABAP short dumps per hour.	Yes

Extended Target Properties	Description	Value Defined?
Page-In per sec	Threshold for the "Page-In per sec" alert. This variable is used by processes that are started by Page-In CCMS alerts. If the variable value is less than the CCMS threshold, an incident will be generated. Enter the threshold value.	Yes
Page-Out per sec	Threshold for the "Page-Out per sec" alert. This variable is used by processes that are started by Page-Out CCMS alerts. If the variable value is less than the CCMS threshold, an incident will be generated. Enter the threshold value.	Yes
PI Application Error - Period to Monitor	Enter the number of minutes to check for PI application errors. (Last X minutes)	Yes
PI Application Error - Receiver Interfaces to Monitor	List of PI Receiver Components and Interfaces. TEO will match components and interfaces as seen on transaction SXMB_MONI. Wildcard expressions are accepted (for example, if you want to match all sender interfaces that start with MI_SALES, enter MI_SALES*).	No
PI Application Error - Sender Interfaces to Monitor	List of PI Sender Components and Interfaces. TEO will match components and interfaces as seen on transaction SXMB_MONI. Wildcard expressions are accepted (for example, if you want to match all sender interfaces that start with MI_SALES, enter MI_SALES*).	No
PI FTP Destination Availability	Monitors the availability of an FTP destination. Enter the FTP destinations to be monitored by TEO for availability. Destination is the IP address of the FTP server. Account is the user account for connecting to the FTP server. The PI FTP Destination Availability process is disabled by default. You will need to make a copy of the process for each runtime user that will connect to the FTP server.	No
PI Queues to Monitor	Enter Queue name to be compared to the errors on SMQ2. Matches will raise incidents with queue owner in the incident description. Wildcard expressions are accepted (for example, if you want to match all quese starting with PI_TEST, enter PI_TEST.	No

Extended Target Properties	Description	Value Defined?
PI tRFC Destination Availability	Monitors the availability of specific destinations. Enter a list of destinations to be monitored by TEO for availability.	No
Portal - IView Response Time	Monitors the average response time for specific iViews. Enter a list of iViews to be monitored and the average response time threshold (milliseconds). TEO monitors average response time in 10-minute intervals. Wildcard expressions are accepted (for example, if you want to match all iViews starting with EP:PRT_init:com.sap.portal, enter EP:PRT_init:com.sap.portal*.	No
Portal - List of Backends	List of SAP ABAP backends that will be accessed by Portal applications. Enter SystemID (for example, enter PRD).	No
Portal Availability	Monitors the availability of Portal Important: Portal will be monitored from an ABAP system. Use overrides to select an ABAP system to monitor the Portal. Enter a list of Portals to monitor: Destination: Portal name (you can enter any name that will make it easy to identify the portal) Host : Portal IP or host name Service: 50x00 (port to connect to portal) Path: /irj/portal Pattern: status_code200	No
SCOT - Transmission Errors per Status	Monitors the number of transmission errors reported by transaction SCOT. Enter a list of Statuses, the threshold to raise an incident and the description to add to the incident. If you only want to monitor total transmission errors, enter "Total Errors" as the sender type. Note that the process (SAPConnect Monitoring) is disabled by default because it calls function "SX_SNDREC_SELECTwhich is not available in all SAP versions/service pack levels.	Yes

Extended Target Properties	Description	Value Defined?
SCOT - Transmission Errors per Type	Monitors the number of transmission errors reported by transaction SCOT in the last 1 hour. Enter a list of Address Types and the threshold to raise an incident. If you only want monitor total transmission errors, enter "Total Errors" as the sender type. Note that the process (SAPConnect Monitoring) is disabled by default because it calls function "SX_SNDREC_SELECT" which is not available in all SAP versions/service pack levels.	Yes
SMQ1 - Outbound Queues to Monitor for Errors	Enter Queue Name to be compared to the errors on SMQ1. Matches will raise incidents with queue owner in the incident description. Wildcard expressions are accepted (for example, if you want to match all queues starting with XI_TEST, enter XI_TEST*).	No
SMQ1 - Outbound Queues to Monitor for Hanging - Queues to Monitor	Enter Queue Name to be compared to SMQ1 and the status entered on the variable "SMQ1 - Outbound Queues to Monitor for Hanging - Status to Monitor". Matches will raise incidents. Wildcard expressions are accepted (for example, if you want to match all queues starting with TEST, enter TEST*).	No
SMQ1 - Outbound Queues to Monitor for Hanging - Status to Monitor	Enter Status to be compared to queue status in SMQ1 and the threshold for how long (minutes) the queue can be in the status (for example, Status = Ready, Time in Status = 30).	No
SMQ2 - Inbound Queues to Monitor for Errors	Enter Queue Name to be compared to the errors on SMQ2. Matches will raise incidents with queue owner in the incident description. Wildcard expressions are accepted (for example, if you want to match all queues starting with XI_TEST, enter XI_TEST*).	No
SMQ2 - Inbound Queues to Monitor for Hanging - Queues to Monitor	Enter Queue Name to be compared to SMQ2 and the status entered on the variable "SMQ2 - Outbound Queues to Monitor for Hanging - Status to Monitor". Matches will raise incidents. Wildcard expressions are accepted (for example, if you want to match all queues starting with TEST, enter TEST*).	No
SMQ2 - Inbound Queues to Monitor for Hanging - Status to Monitor	Enter Status to be compared to queue status in SMQ2 and the threshold for how long (minutes) the queue can be in the status, like for example Status = Ready, Time in Status = 30.	No

Extended Target Properties	Description	Value Defined?
System Log - Application	Enter the system log number and the incident name.	No
System Log - Background Input	Enter the system log number and the incident name.	No
System Log - Background Processing	Enter the system log number and the incident name.	Yes
System Log - Basis	Enter the system log number and the incident name.	Yes
System Log - CCMS	Enter the system log number and the incident name.	No
System Log - Communication	Enter the system log number and the incident name.	Yes
System Log - Customer	Monitors custom message IDs created in the SAP system log (customer). When there is a match, it creates an incident that is appended to the description in the Alert field.	No
System Log - Database	Enter the system log number and the incident name.	Yes
System Log - Miscellaneous	Enter the system log number and the incident name.	No
System Log - Security	Enter the system log number and the incident name.	Yes
System Log - Spool	Enter the system log number and the incident name.	Yes
System Log - Transport	Enter the system log number and the incident name.	No
Targets for tRFC error check	Monitors tRFC errors (CPICERR or SYSFAIL) for specific Targets. Enter the list of Targets to be compared with SM58 results. Wildcards are accepted (for example, if you want to match all targets starting with FAX, enter FAX*).	No
Transaction Response Time	Monitors the average response time for specific ABAP transactions. Enter a list of transactions to be monitored and the average response time threshold (milliseconds). TEO monitors average response time in 10 minute intervals.	No
tRFC Destination Availability	Monitors the availability of specific destinations. Enter a list of destinations to be monitored by TEO for availability.	No
tRFC Destination Availability - HTTP	Monitors the availability of specific HTTP destinations. Enter a list of destinations to be monitored by TEO. The entries are similar to SM59 for HTTP destinations. Pattern can be wildcard or a substring that you are looking for in the report result. Note that it will strip off all the white spaces (blank, tab, new line) and the "|" character from the report before matching it against the pattern. Pattern example: status_code200	No

Extended Target Properties	Description	Value Defined?
tRFC Source	The name of the server where the destination check tests are executed. Enter the full name of the server (ServerName_SID_SysNo) where the destination check tests will be executed. The value is case sensitive.	No
tRFC Source - HTTP	The name of the server where the destination check tests are executed. Enter the full name of the server (ServerName_SID_SysNo) where the destination check tests will be executed. The value is case sensitive.	No
Update Maximum Duration	Threshold for the time an update is in state of "running". The process will check time via SM66. Enter the threshold value in seconds.	Yes
Update Queue Time	Threshold for the update queue time per server. This variable is used by processes that are started by dialog response time CCMS alert. If the variable value is less than the CCMS threshold, an incident will be generated. Enter the threshold value.	Yes
URL Ping	Monitors URL availability (HTTP ping). Enter the URL address (for example: http://<ServerName>:50000/irj/portal).	No
Work Processes Analysis	Monitors work processes for HOLD status reasons. Enter a list of work process Hold status reasons to be monitored. Enter thresholds for "Max Number" of working processes in the system running longer than "Max Duration" seconds on the specified "Status".	Yes

Incident Anaysis for SAP Target Groups

The following target group is imported by the Incident Analysis for SAP automation pack.

Target Group Name	Description
CA Wily Email Account	Includes the email targets that will be monitored by CA Wily alerts.

Incident Analysis for SAP Knowledge Base Articles

The knowledge base articles provide information to help understand the results of an activity or process, including a summary of what has occurred, the possible cause of the results, and suggested actions to take to resolve issues. The Incident Analysis for SAP automation pack contains the Knowledge Base articles that are included in the SAP activities.

To view the knowledge base articles for Incident Analysis for SAP, use the Administration—Knowledge Base Articles view. See the *Tidal Enterprise Orchestrator Reference Guide* for additional information on knowledge base articles.

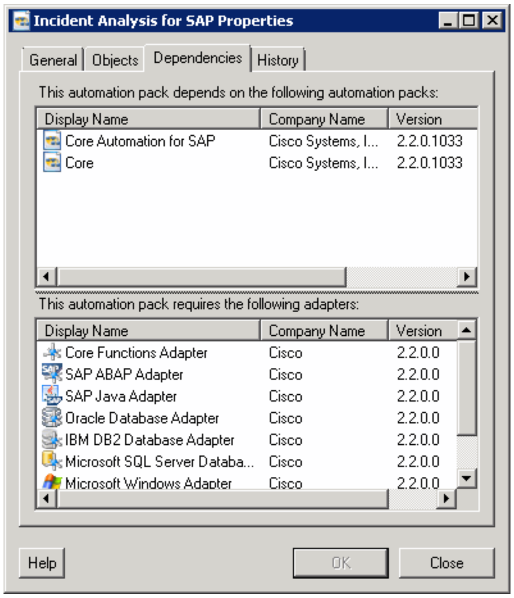
Viewing Automation Pack Dependencies

Use the Dependencies tab to view the automation packs and adapters referenced by the objects in the automation pack. These object must be installed prior to importing the Incident Analysis for SAP automation pack.

Step 1 On the Administration—Automation Packs view, select **Incident Analysis for SAP**, right-click and choose **Properties**.

Step 2 On the Incident Analysis for SAP Properties dialog box, click the **Dependencies** tab.

Figure 2-3 Incident Analysis for SAP Properties—Dependencies Tab



This automation pack depends on the following automation packs:

Display Name	Company Name	Version
Core Automation for SAP	Cisco Systems, I...	2.2.0.1033
Core	Cisco Systems, I...	2.2.0.1033

This automation pack requires the following adapters:

Display Name	Company Name	Version
Core Functions Adapter	Cisco	2.2.0.0
SAP ABAP Adapter	Cisco	2.2.0.0
SAP Java Adapter	Cisco	2.2.0.0
Oracle Database Adapter	Cisco	2.2.0.0
IBM DB2 Database Adapter	Cisco	2.2.0.0
Microsoft SQL Server Databa...	Cisco	2.2.0.0
Microsoft Windows Adapter	Cisco	2.2.0.0

Step 3 Review the list of automation packs and adapters referenced by the Incident Analysis for SAP automation pack:

Object Type	Dependency
Automation Packs	• Core Automation for SAP • Core
Adapters	• Core Functions Adapter • SAP ABAP Adapter • SAP Java Adapter • Oracle Database Adapter • IBM DB2 Database Adapter • Microsoft SQL Server Database Adapter • Microsoft Windows Adapter • Web Service Adapter

Step 4 Click **Close** to close the dialog box.

Incident Analysis for SAP Reports

This section provides information on the reports that ship with the Incident Analysis for SAP automation pack. You can access the reports in Microsoft SQL Server Reporting Services or SAP BusinessObjects.

Note See the *Tidal Enterprise Orchestrator Reference Guide* for information about importing the reports.

Report Name	Description
ABAP Shortdumps per User	Displays the number of ABAP short dumps by User during a specified time period.
ABAP Shortdumps per Reason	Displays the number of ABAP short dumps by Error Code during a specified time period.
Administrator Checklist	Displays the Administrator Checklist incidents on a specified SAP system.
Application Server Availability	Displays the percentage of availability for all monitored SAP application servers. Click the link to view details about the server down time.
Availability Incidents	Displays the server unavailable incidents on a specified SAP system.
Background Analysis	Displays background utilization information for the specified SAP system.

Report Name	Description
CPU Utilization	Displays CPU utilization, CPU idle, and CPU queue on a specified SAP system.
Dialog Analysis	Displays dialog response time and resource utilization.
Dialog Response Time	Displays average response time of dialog service, front-end wait time, average dispatcher wait time per dialog step, average load and generation time for GUI objects, average time for processing logical database requests, and average time in network (excluding roundtrips).
Dialog Response Time Incidents	Displays dialog response time incidents on a specified SAP system.
Dialog WP Utilization	Displays the dialog work processes utilization on a specified system.
Installed Components	Displays the installed components on a specified SAP system.
Jobs Aborted (All)	Displays a list of aborted jobs on a specified SAP system.
Performance Analysis	Displays a history of any performance counter that has been collected by TEO.
Portal Response Time	Displays the iView response time on a specified SAP system.
Portal Response Time Incidents	Displays iView response time incidents on a specified SAP system.
SAP Background Jobs Aborted (All)	Displays a list of all aborted jobs on a specified SAP system.
SAP Background Jobs Aborted Incidents	Displays a list of aborted jobs on a specified SAP system that raised TEO incidents.
SAP Incidents	Displays a history of all TEO incidents that have occurred within a specified time period on a specified system for the specified incident level. You can click the link in the Time column to display detailed information about an incident.
SAP System Log Incidents	Displays events logged in the SAP system log that raised TEO incidents.
SAP System Log Incidents and Events	Displays all events logged in the SAP system log.
SAP System Overview	Displays a real-time portal for the specified SAP system where you can view the incidents that have occurred within a specified date. Click the link in the Time column to view detailed information about the incident.
Shortdumps per Reason	Displays the number of ABAP short dumps by Error Code during a specified time period.
Shortdumps per User	Displays the number of ABAP short dumps by User during a specified time period.

Report Name	Description
System Properties	Displays the system properties on a specified SAP system.
Users Logins	Displays the number of users logged in per SAP system and per server.
Workload Analysis	Displays overview of workload per system based on task.

CHAPTER 3

Getting Started Using the Automation Pack

Before you begin using the content that ships with the automation pack, you must create the objects in TEO that are referenced in the processes. These objects include targets, runtime users, task rules for assignments and notifications, and extended target properties.

This chapter provides basic information on defining the objects. It includes the following sections:

- Creating Runtime Users, page 3-2
- Creating SAP System Targets, page 3-4
- Using Task Rules for Assignments and Notifications, page 3-8
- Managing Extended Target Properties, page 3-22
- Managing Global Variables, page 3-27

For additional information about the objects discussed in this chapter, refer to the following documentation:

Document	Description
Tidal Enterprise Orchestrator Reference Guide	General information about Core product features.
Cisco TEO Adapter Guide for SAP ABAP	Information about the objects specific to SAP ABAP Adapter (runtime user, target, and activities).
Cisco TEO Adapter Guide for SAP Java	Information about the objects specific to the SAP Java Adapter (target and activities).
Cisco TEO Getting Started Guide for SAP	Information about configuring and managing the objects in TEO specific to SAP.

Creating Runtime Users

The runtime user account is used to connect to the targets on which the processes will execute. The type of runtime user account that is required depends on the type of target that is created. The following runtime users are required for the Incident Analysis for SAP processes:

Runtime User	Description
SAP User	Specifies the credentials required to access the SAP System target.
Runtime User	Specifies the credentials required to access the following SAP-related targets: • SAP Database • SAP Java Application Server

Creating an SAP User Account

You use the SAP User runtime user account to connect to the SAP System target.

Step 1 In the Definitions workspace, right-click **Runtime Users** and choose **New > SAP User** to open the New SAP User Properties dialog box.

Step 2 On the General tab, specify the following information:

Note The Required Field ❗ icon displayed on a tab or page indicates that the field is required and is missing a value.

Field	Description
Display name	Name for the user account.
User name	User name assigned to the SAP user account that connects to the SAP system or ABAP application server.
Password	Password assigned to the SAP user account that connects to the SAP system or ABAP application server.
Client	SAP client number assigned to the user account.
Description	A description of the user account.

Note The Used By tab displays objects used by the runtime user and will remain blank until used by an object.

The History tab displays the history of actions taken against the runtime user and will remain blank until after the initial creation.

Step 3 Click **OK** to close the dialog box.

Creating a Runtime User Account

You use the Runtime User account to connect to the SAP Database and SAP Java Application server targets.

Step 1 In the Definitions workspace, right-click **Runtime Users** and choose **New > Runtime User** to open the New Runtime User Properties dialog box.

Step 2 On the General tab, specify the following information:

Note The Required Field ! icon displayed on a tab or page indicates that the field is required and is missing a value.

Field	Description
Display name	Name for the user account. This field can populated with the information specified in the Domain and User name text fields, or you can enter a different name to display for the user account.
User name	User name assigned to the user account that connects to the SAP target.
Password	Check the check box and enter the password assigned to the user account. **Note** No password verification is done for the simple (generic) runtime user.
Description	A description of the user account.

Note The Used By tab displays objects used by the runtime user and will remain blank until used by an object.

The History tab displays the history of actions taken against the runtime user and will remain blank until after the initial creation.

Step 3 Click **OK** to close the dialog box.

Note For additional information on creating and managing runtime users, *see* the *Tidal Enterprise Orchestrator Reference Guide*.

Creating SAP System Targets

Before you can create or run processes, you must create the targets on which the processes will run. This section guides you through creating SAP System targets using the New SAP System Wizard.

You can create a target for an SAP system that uses an ABAP connection to the application server, an ABAP and Java connection to the application server, or a Java connection to application server. You can also configure to the SAP database that is associated with the SAP system.

Note The SAP Java Adapter requires certain SAP Java libraries, which are available on the SAP Installation CD. Before you can configure an SAP Java application server target, these files must be installed on the TEO server. For instructions on installing the SAP Java libraries, *see* the *Cisco TEO Adapter Guide for SAP Java*.

Step 1 In the Definitions view, right-click **Targets** and choose **New > SAP System** from the submenus to open the New SAP System Wizard Welcome panel.

Note The Required Field ❗ icon displayed on a tab or page indicates that the field is required and is missing a value.

Step 2 Click **Next** and specify the following information on the System Setup panel:

Field	Description
Display name	Enter a name for the SAP system. This is the name that will be displayed in the Targets pane.
System Components	
ABAP application servers	Check this check box if the SAP system uses an ABAP connection to the application servers. To monitor an ABAP+Java stack, this check box must be checked.
Java application servers	Check this check box if the SAP system uses a Java connection to the application servers. To monitor an ABAP+Java stack, this check box must be checked.
SAP database	Check this check box if you want to configure the SAP database that is associated with the SAP system.
Monitor as production system	The check box is checked by default. Certain processes will run only on production systems. If you want to monitor the system as a non-production system (development or sandbox), uncheck the check box.

Step 3 Click **Next**.

Step 4 On the ABAP Connection panel, specify the connection information for connecting to the SAP ABAP application server.

Note The system information entered on this panel must be unique. Otherwise, an error message displays informing you that the wizard detected another system already registered with the same information.

Field	Description
Connect using:	
Application server	Choose this option to connect to the SAP system using the SAP application server connection information.
Server name	Name of the SAP application server.
System number	SAP system number.
Logon group	Choose this option to establish a connection using a logon group, which contains a group of SAP system instances. When a user logs on to a logon group, the mesage server directs the users to the server of this group that currently has the lightest load.
System ID	SAP system ID (SID).
Message server	Determines which server a user logs on to and handles the communication between the application servers. For example, transport of update requests and lock requests.
Group name	Name of the Logon Group to be accessed. The name entered in this field is case-sensitive.
Router string (optional)	Enter the router string for accessing the SAP systems via SAPRouter. If you do not specify a router string, TEO accesses the SAP system directly. The router string must be formatted as: /H/host01/H/host02/H/ where host01 and host02 are the SAP systems that you want to access through the SAPRouter.
Default runtime user	Choose the user account that contains the credentials to connect to the target from the drop-down list. • To view the properties for the selected runtime user, click the **Properties** icon. • To create a new SAP User, click **New > SAP User**. *See* Creating an SAP User Account, page 3-2 for instructions.

Step 5 Click **Next**.

Step 6 On the Server Availability panel, specify the ABAP application servers that you want to monitor for availability and the ability to log in a user:

Field	Description
Servers available for monitoring	All detected servers are selected by default. Verify that the check box next to each server that you want to monitor is checked.
Add	If a server is offline during configuration, it will not be displayed in the list of available servers. To manually add the server, click **Add** and enter the name of the server.
Remove	If you want to remove a server from the list, select the server and click **Remove**.
Select All	If the check boxes have been unchecked and you want all servers to be monitored, click **Select All**.
Deselect All	If all the check boxes are checked and you want to uncheck all of them, click **Deselect All**.

Step 7 Click **Next**.

Step 8 If you selected to monitor the SAP database, specify the information for the type of database that is being configured. The fields that display depend on the database type.

Field	Description
Server	Enter the name of the SAP application server where the database resides.
Hostname or data source	Name of the host server or data source for the Oracle or Generic database.
SID	System ID for the server where the Oracle database resides.
Database name	Enter the name of the SAP database that is associated with the SAP system.
Database owner	Enter the name of the user that owns the rights to the database.
Database source	Enter the Data source to connect to the database.
Port Number	Enter the Port number used to connect to the database.
Default timeout for activities (seconds)	Enter the number of seconds before the activity times out. The default timeout period is 120 seconds.
Default runtime user	Choose the user account that contains the credentials to connect to the database from the drop-down list. • To view the properties for the selected runtime user, click the **Properties** tool. • To create a new runtime user, click **New > Runtime User**.
Connection string	If the database has a custom connection string label appended to the name, check the check box and modify the string in the text field.

Step 9 Click **Next**.

Step 10 On the Java Connection panel, click **New** to add the Java application server.

> **Note** If the SAP Java application server is already configured, it displays in the list box. Click **Next** to proceed.

Step 11 On the SAP Java Application Server Connection panel, specify the information for connecting to the SAP Java application server:

Field	Description
Display name	Name of the server that will be displayed in the Targets pane.
Application server	IP address or name of the SAP Java application server.
JMX Connection	
JMX port	JMX port number used to connect to the Java application server.
Use credentials of the following runtime user	From the drop-down list, choose the default runtime user that contains the credentials to connect to the target. Click **New** to define a new runtime user. **Note** The runtime user must be a J2EE Admin account.
Monitor as Portal	Check the check box to run processes designed for portals on this Java server.
Central Instance	Check the check box to run processes designed for central instances on this Java server.
Telnet Connection	
Enable Telnet connection	Check the check box if you want to specify the Telnet connection information to connect to the Java application server.
Telnet port	Telnet port number used to connect to the Java application server
Use credentials of the following runtime user	From the drop-down list, choose the default runtime user that contains the credentials to connect to the target.

Step 12 Click **Finish**.

Step 13 After adding the Java application server, click **Next** on the Java Connection panel.

Step 14 On the Completing the New SAP System Wizard panel, verify that the information is correct and click **Finish** to complete the procedure.

Using Task Rules for Assignments and Notifications

Task rules are used to manage task assignments and notifications for tasks, such as incidents and alerts, that are generated from processes. When you import the Core Automation for SAP automation pack, you are prompted to specify the default user or group who should be assigned SAP incidents. By default, this person will receive all assignments unless task rules are created to specify alternate users or groups for specific tasks.

This section guides your through configuring the task rule that ships with the Core Automation for SAP automation pack and provides instructions for creating and managing task rules.

Note If you do not want to create task rules for email notifications, you can use the default notification based on assignment processes that ship with the Core automation pack. These processes are disabled by default and must be enabled if you want notifications to be sent (*see* Enabling Notification Based on Assignment Processes, page 3-21).

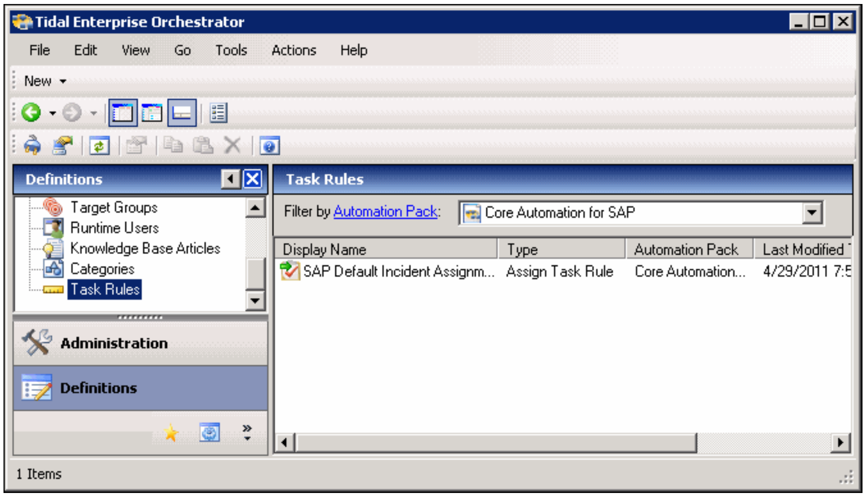
Accessing Task Rules View

The task rule that ships with the Core Automation for SAP automation pack can be accessed from the Definitions—Task Rules view.

Step 1 On the Console, select the Definitions workspace and click **Task Rules** in the navigation pane. By default, all the rules display in the Task Rules pane.

Step 2 Click the **Filter by** link and choose **Automation Pack > [Automation Pack Name]** to filter for only the task rules that ship with the specific automation pack.

Figure 3-1 Definitions—Task Rules View



Filter by Automation Pack: Core Automation for SAP

Display Name	Type	Automation Pack	Last Modified
SAP Default Incident Assignm...	Assign Task Rule	Core Automation...	4/29/2011 7:5

1 Items

The following information about the task rules displays by default:

Column	Description
Display Name	The name assigned to the task rule.
Enabled	Indicates whether the task rule is enabled (*True*) or disabled (*False*). A disabled task rule is unavailable for execution.
Type	Type of task.
Owner	User name of the person or group who assigned the task rule.
Last Modified Time	The date and time the task rule was last modified.
Last Modified By	The object or user name that last modified the task rule.
Id	Unique ID of the task rule.
Description	Brief description of the task rule.
Type Description	Brief overview of the task rule type.
Created Time	Time at which the task rule was created.
Created Date	Date the task rule was created.
Automation Pack	Name of the automation pack associated with the task rule.

Configuring Task Rules

Use the Task Rules view to configure the task rule that ships with the Core Automation for SAP automation pack.

SAP Default Assignment

The Core Automation for SAP automation pack ships with the Default SAP Assignment task rule, which is used to specify the default user or group who will be assigned all SAP-related incidents unless otherwise specified in task rules. This task rule can be configured during the import process on the Default Incidents Assignee Setup panel (Figure 1-4 on page 1-5) or from the Task Rules view in the Console.

Step 1 In the Definitions workspace, click **Task Rules** in the navigation pane to display the task rules in the results pane.

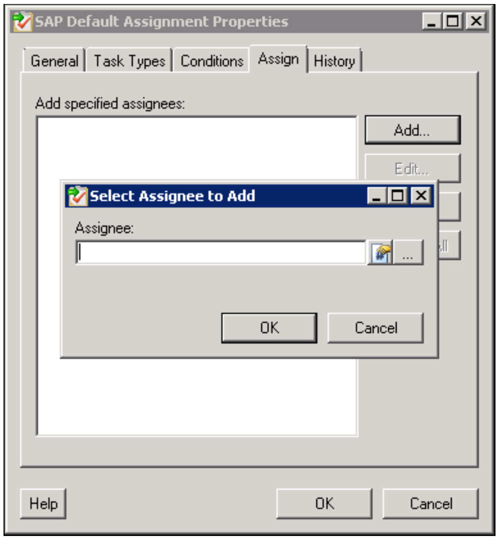
Step 2 Click the **Filter by** link and choose **Automation Pack**, and then choose **Core Automation for SAP** from the drop-down list to display the task rules that ship with the automation pack.

Step 3 Right-click the **SAP Default Assignment** task rule and choose **Properties** to open the SAP Default Assignment Properties dialog box.

Step 4 Click the **Assign** tab to specify the user or group that should receive assignments for incidents and alerts generated by the processes.

Step 5 On the Assign tab, click **Add** to open the Select Assignee to Add dialog box.

Figure 3-2 Adding Assignees to Task Rule



Step 6 On the Select Assignee to Add dialog box, specify the assignees using one of the following methods:

- Click the **Reference** tool to select the appropriate variable reference containing the assignee or list of assignees from the Insert Variable Reference dialog box.
- Click the **Browse** ... tool to launch the Select User or Group dialog box to add user to the list of assignees.

Step 7 Click **OK** to add the assignee to the task rule.

Step 8 When you have completed adding assignees to the task rule, click **OK** to close the dialog box.

Creating a New Task Rule

Use the Task Rules view to create a new task rule. The procedure is the same for all types of task rules with the exception of the task-specific tab (Assign, Notify, Update) for the type of task rule you are creating.

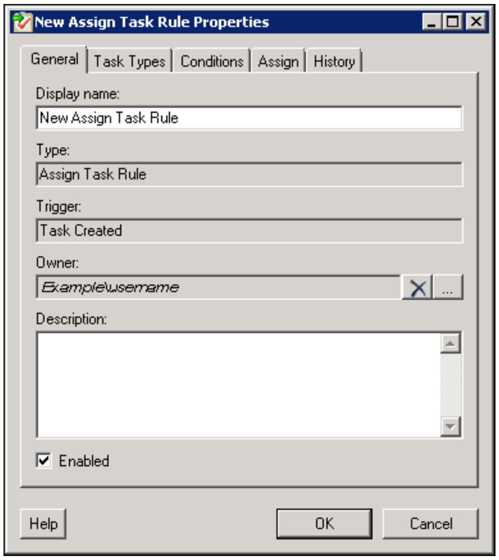
Note Only users with administrative rights can create task rules in TEO.

You can create the following types of task rules:

Task Rules	Description
Assign Task Rule	Assigns users to a task.
Notify Task Rule	Notifies users that a task has been created.
Update Task Rule	Specifies the properties to be updated in a task..

Step 1 In the Definitions workspace, right-click **Task Rules** and choose **New > [Task Rule Type]** to open the New Rule Properties dialog box.

Figure 3-3 New Rule Properties Dialog Box—General Tab


New Assign Task Rule Properties

Display name: New Assign Task Rule

Type: Assign Task Rule

Trigger: Task Created

Owner: Example\username

Description:

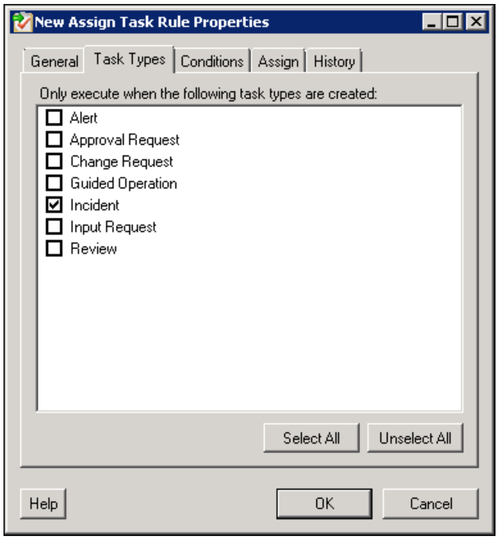
☑ Enabled

Step 2 On the General tab, enter the following information:

Field	Description
Display Name	Name of the task.
Type	*Display only.* Shows the type of object.
Trigger	*Display only.* Type of trigger associated with the task rule.
Owner	User name of the owner of the task rule. This is typically the person who created the task rule. Click the **Browse** ... tool to launch the Select User or Group dialog box to change the owner.
Description	A brief description of the task rule.
Enabled	The check box is checked by default to indicate that the task rule is available for execution. Uncheck the check box to disable the task rule. If the check box is unchecked, the task rule is disabled and will be unavailable for execution.

Step 3 Click the **Task Types** tab to specify the types of tasks to be executed by the rule.

Figure 3-4 New Rule Properties Dialog Box—Task Types Tab



Only execute when the following task types are created:

- ☐ Alert
- ☐ Approval Request
- ☐ Change Request
- ☐ Guided Operation
- ☑ Incident
- ☐ Input Request
- ☐ Review

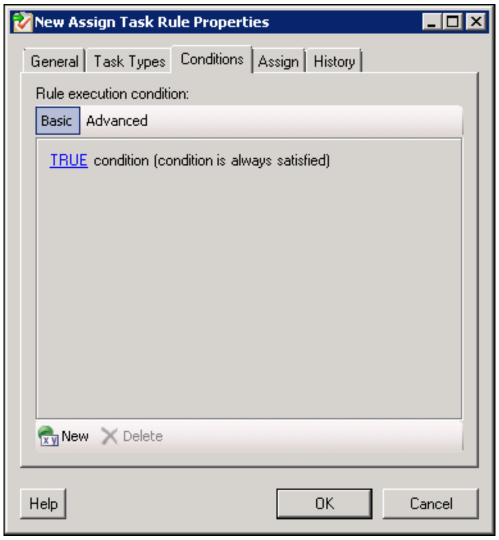
Step 4 Check the check box for the type of task that will execute the rule.

Task Type	Description
Alert	Alerts reflect potential problems that a user may want to investigate and possibly diagnose the problem.
Approval Request	Specifies the message and choices for the assignee who is approving the task.
Guided Operation	Details the steps a user takes to complete an assigned task.
Incident	Task requires an operator to take action in order to resolve an issue.
Input Request	Task requires input from an individual or group.
Review	Task assigns a document for review.

Step 5 Click the **Conditions** tab to specify the conditions of when the task rule action is to be taken based on an evaluation of the defined conditions.

Note The Required Value ❗ icon displayed on a tab or page indicates that the field is required and is missing a value.

Figure 3-5 New Rule Properties Dialog Box—Conditions Tab



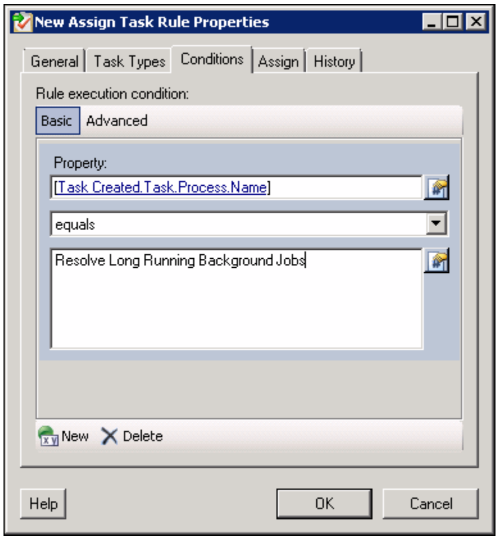
TRUE condition (condition is always satisfied)

Step 6 On the Conditions tab, define the conditions that must be met for the rule to execute.

Defining a Basic Condition:

a. On the Basic page, click **New** to add a new property for the condition that must be met.

Figure 3-6 New Rule Properties Dialog Box—Basic Condition



Rule execution condition:

Property:

[Task.Created.Task.Process.Name]

equals

Resolve Long Running Background Jobs

b. In the Property text field, click the **Reference** tool to choose a defined variable or reference an object on the Insert Variable Reference dialog box.

c. Choose the condition expression from the drop-down list.

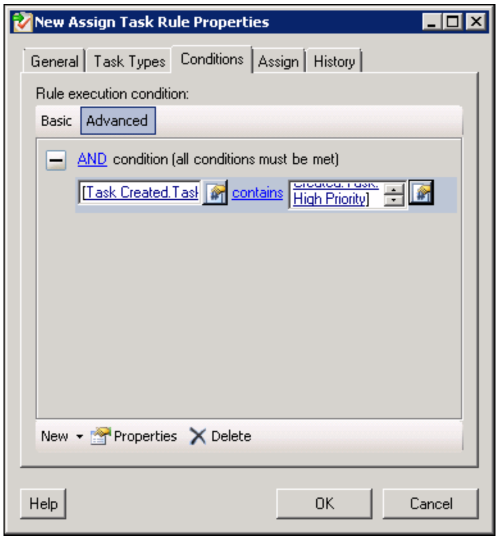
d. Enter the condition description in the text box or click the **Reference** tool to choose a defined variable or reference an object on the Insert Variable Reference dialog box.

e. Click **New** to define additional properties, if necessary.

Defining an Advanced Condition:

a. Click the **Advanced** tab to define a specific type of condition (Compound, Prior Process Instance, Time, or Variable).

Figure 3-7 New Rule Properties Dialog Box—Advanced Condition



Rule execution condition:

AND condition (all conditions must be met)

[Task Created.Tasl contains High Priority]

b. Click the link to modify the option for the condition equation.

Option	Description
AND condition (all conditions must be met)	Click this option if an action is to be taken only when all conditions in the list are *true*.
OR condition (one condition must be met)	Click this option if an action is to be taken when one condition in the list is *true*.

c. Click **New** and choose the type of condition from the drop-down list.

d. Specify the relevant information for the type of condition selected.

Note Click NewClick the **Reference** tool to choose a defined variable or reference an object on the Insert Variable Reference dialog box.

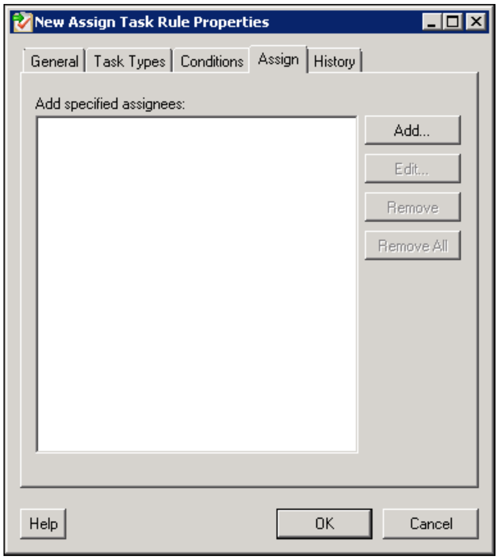
e. Click **New** to define additional properties, if necessary.

Step 7 Click the task rule specific tab (**Assign**, **Notify**, or **Update**) and specify the relevant information for the specific type of rule.

Assign Task Rule

If you are creating an Assign Task Rule, the Assign tab displays on the New Rule Properties dialog box.

Figure 3-8 New Rule Properties Dialog Box—Assign Tab



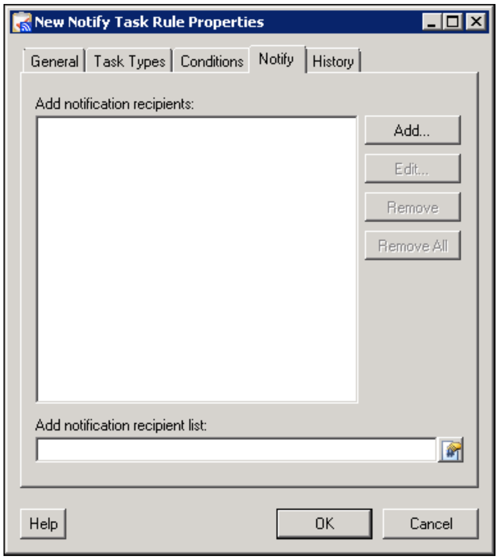
On the Assign tab, specify the assignees for task rule.

Field	Description
Add	Click this button to launch the Select Assignee to Add dialog box to specify the assignees. On the Select Assignee to Add dialog box, use one of the following methods to specify the assignee: • Click the **Reference** tool to select the appropriate variable reference containing the assignee or list of assignees from the Insert Variable Reference dialog box. • Click the **Browse** ... tool to launch the Select User or Group dialog box and add user to the list of assignees.
Edit	Select the appropriate assignee in the list and click this button to view or modify the assignee of the task rule.
Remove	Select the appropriate assignee and click this button to remove the assignee from the list.
Remove All	Click this button to remove all specified assignees from the list.

Notify Task Rule

If you are creating a Notify Task Rule, the Notify tab displays on the New Rule Properties dialog box.

Figure 3-9 New Rule Properties Dialog Box—Notify Tab


New Notify Task Rule Properties
General
Task Types
Conditions
Notify
History
Add notification recipients:
Add...
Edit...
Remove
Remove All
Add notification recipient list:
Help
OK
Cancel

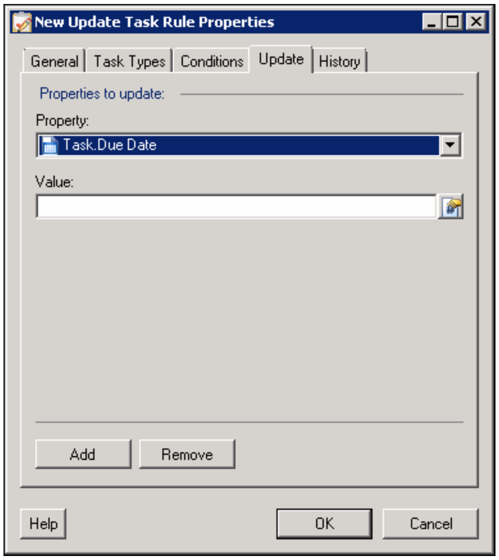
On the Notify tab, specify the recipients of the notification that the task rule has executed. You can add individual recipients or include a notification recipient list.

Field	Description
Add notification recipients	Displays list of users to be notified by the task rule. • Add—Click this button to launch the Select Notification Recipient to Add dialog box to specify the recipients. On the dialog box, enter the email address for the recipient or click the **Reference** tool to select the appropriate variable reference containing the recipient or list of recipients from the Insert Variable Reference dialog box and then click **OK**. • Edit—Select the appropriate recipient in the list and click this button to view or modify the recipient of the task rule. • Remove—Select the appropriate recipient in the list and click this button to remove the recipient from the list. • Remove All—Click this button to remove all specified recipients from the list.
Add notification recipient list	Click the **Reference** tool to select the appropriate variable reference containing list of recipients from the Insert Variable Reference dialog box.

Update Task Rule

If you are creating an Update Task Rule, the Update tab displays on the New Rule Properties dialog box.

Figure 3-10 New Rule Properties Dialog Box—Update Tab



On the Update tab, specify the properties to be updated after the task rule has executed.

Field	Description
Add	Click this button to add a new property to the Properties to update area.
Remove	Click this button to remove the last property added to the Properties to update area.
Property	From the Property drop-down list, choose the item to update within the task. The properties displayed depend on the selected item.
List action	Choose the appropriate item from the drop-down list to determine which action to take with the selected property: • Add Item—Adds item to task. • Remove item—Removes item from task. • Clear—Removes property value from task.
Value	Enter new value for the property.

Step 8 Click **OK** to save the task rule definition and close the dialog box.

Managing Task Rule Definitions

This section provides instructions on modifying task rules in the Definitions—Task Rule view. Only users with administrative rights can modify task rules in TEO.

Note For additional information on managing task rules, see the *Tidal Enterprise Orchestrator Reference Guide*.

Enabling a Task Rule

A task rule is enabled by default. If a task rule is manually disabled, the task rule must be enabled before it is available for execution.

On the Definitions—Task Rules view, select the task rule and then use one of the following methods to enable it:

- On the Results pane, right-click and choose **Enable**.

  -or-

- On the Details pane, select **Click here to enable**.

The Enabled column on the Results pane changes to True. If necessary, click the **Refresh** tool to update the view.

Disabling a Task Rule

Disabling a task rule prevents the item from being available for execution. The disabled task rule is not removed from the list of task rules on the Definitions—Task Rules Results pane.

On the Definitions—Task Rule view, select the task rule and then use one of the following methods to disable it:

- On the Results pane, right-click and choose **Disable**.

  -or-

- On the Details pane, select **Click here to disable**.

The Enabled column on the results pane changes to False. If necessary, click the **Refresh** tool to update the view.

Creating a Copy of a Task Rule

The copy option is used when the user wants to leverage an existing task rule to define a new task rule using existing properties.

Step 1 On the Definitions—Task Rules view, select the appropriate task rule, right-click and choose **Copy**.

Step 2 On the Results pane, right-click and choose **Paste**.

A copy of the defined task rule is pasted onto the Results pane.

Step 3 To rename the copied task rule or other properties, right-click and choose **Properties**.

Step 4 Modify the task rule name, as appropriate, and click **OK** to close the dialog box.

Sorting Task Rules

The task rules are executed according to the order they are listed on the Definitions—Task Rules view. You should sort the task rules based on the order in which you want them to execute.

Note All task rules will execute even if there is more than one task rule assigned for the same condition. For example, if you have two assignment rules for the same incident, both rules will be executed in the order listed in the Task Rules view.

On the Definitions—Task Rules view, select the task rule and use one of the following methods to move it to the desired position in the list:

- Drag and drop the task rule into the appropriate position in the list.
- On the Actions toolbar, click **Move Up** or **Move Down**.
- Click the Actions menu and choose **Move Up** or **Move Down**.
- Right-click and choose **Move Up** or **Move Down**.

The list of task rules are sorted according to the selected action.

Deleting a Task Rule

Use the Definitions—Task Rules view to delete task rules that are no longer used.

Step 1 On the Definitions—Task Rules view, select the task rule, right-click and choose **Delete**.

Step 2 On the Confirm Delete dialog box, click **Yes** to confirm the deletion.

Enabling Notification Based on Assignment Processes

If you want to have emails sent to whoever is assigned to a task but do not want to create notification task rules, you can enable the processes that ship with the Core automation pack that send emails based on assignment.

When these processes are enabled, the user or user group who was assigned to tasks will receive the email notification.

Step 1 In the Definitions workspace, click **Processes**.

Step 2 Click the **Filter by** link and choose **Automation Pack > Core** to filter for the processes that ship with the Core automation pack.

Step 3 Right-click the appropriate **Notification Based on Assignment** process and choose **Enable**.

The following processes are for notification based on assignment:

Process Name	Description
Default Alert Notification Based on Assignment	Sends email when an alert gets assigned.
Default Approval Request Notification Based on Assignment	Sends email when an approval request gets assigned.
Default Change Request Notification Based on Assignment	Sends email when an change requests gets assigned.
Default Guided Operation Request Notification Based on Assignment	Sends email when a guide operation request gets assigned.
Default Incident Notification Based on Assignment	Sends email when an incident gets assigned.
Default Input Request Notification Based on Assignment	Sends email when an input request gets assigned.
Default Review Request Notification Based on Assignment	Send email when a review request gets assigned.

Managing Extended Target Properties

The Incident Analysis for SAP processes use extended target properties to override certain variable properties assigned to targets. For example, extended target properties can be used to specify a different target when certain conditions occur.

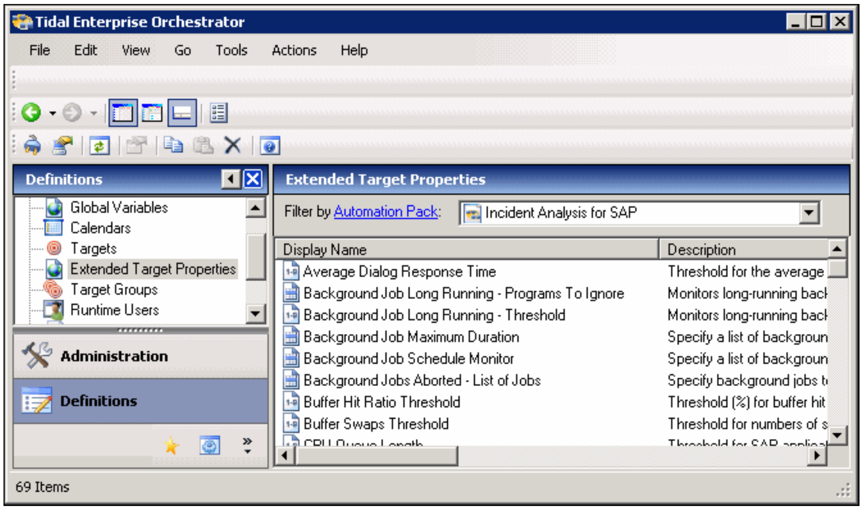
This section provides information on configuring extended target properties.

Accessing Extended Target Properties

The extended target properties that ship with the Incident Analysis for SAP automation pack can be accessed from the Definitions—Extended Target Properties view.

Step 1 On the Console, select the Definitions workspace and click **Extended Target Properties** in the navigation pane. By default, all the properties display in the Extended Target Properties pane.

Figure 3-11 Definitions—Extended Target Properties View



Filter by Automation Pack: Incident Analysis for SAP

Display Name	Description
Average Dialog Response Time	Threshold for the average
Background Job Long Running - Programs To Ignore	Monitors long-running back
Background Job Long Running - Threshold	Monitors long-running back
Background Job Maximum Duration	Specify a list of backgroun
Background Job Schedule Monitor	Specify a list of backgroun
Background Jobs Aborted - List of Jobs	Specify background jobs t
Buffer Hit Ratio Threshold	Threshold (%) for buffer hit
Buffer Swaps Threshold	Threshold for numbers of s

69 Items

The following information about the extended target properties displays by default:

Column	Description
Display Name	Name of the target property.
Description	Text description of the target property.
Value	Value assigned to the target property.
Data Type	Type of value being used for the target property (Boolean, Encrypted String, Identity, Numeric, String, Table).
Automation Pack	Name of the automation pack that provides the target property.
Customizable	Indicates the customization setting for the target property in the automation pack.

Column	Description
Target Types	Indicates the targets associated with the target property.
Last Modified Time	Date and time the variable was last modified.
Last Modified By	Name of the user who last modified the target property.
Id	Unique ID of the target property.
Owner	User name of the owner of the target property. This is typically the person who created the target property.
Created Time	Date and time the target property was created.
Created By	User name of the person who created the target property.

Step 2 Click the **Filter by** link and choose **Automation Pack > Incident Analysis for SAP** to filter for only the extended target properties that ship with the specific automation pack.

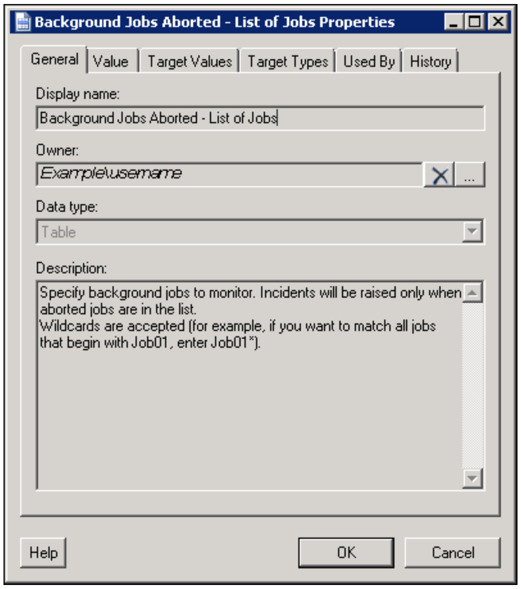
Configuring Extended Target Properties

You use the Extended Target Properties Properties dialog box to view or modify the target property. You access the properties from the Definitions—Extended Target Properties view.

The following section provides information on configuring extended target properties that ship with the Incident Analysis for SAP automation pack.

Step 1 On the Extended Target Properties pane, right-click **[Extended Target Property]** and choose **Properties**.

Figure 3-12 Extended Target Properties—General Tab



Display name: Background Jobs Aborted - List of Jobs

Owner: Example\username

Data type: Table

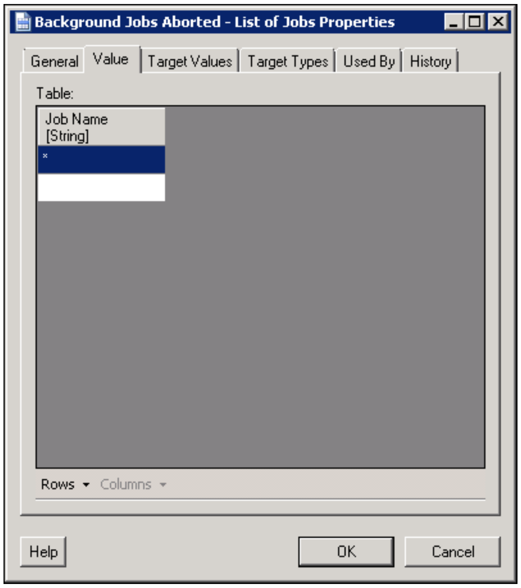
Description:
Specify background jobs to monitor. Incidents will be raised only when aborted jobs are in the list.
Wildcards are accepted (for example, if you want to match all jobs that begin with Job01, enter Job01*).

Step 2 On the General tab, review the information in the Description field to determine the values that need to be specified for the target property.

Step 3 Click the **Value** tab to view or modify the default value for all targets.

Note The tab in the second position will depend on the variable type. *See* the *Tidal Enterprise Orchestrator Reference Guide* for instructions on configuring the different types of target properties.

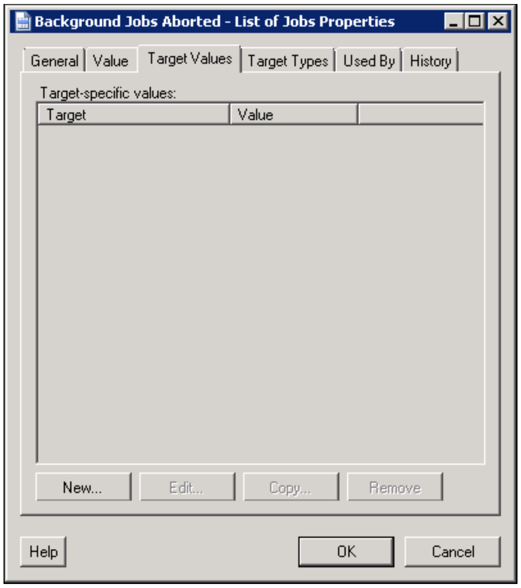
Figure 3-13 Extended Target Properties—Value Tab



Step 4 Click in the cell to specify the default value or change the default value for all SAP targets.

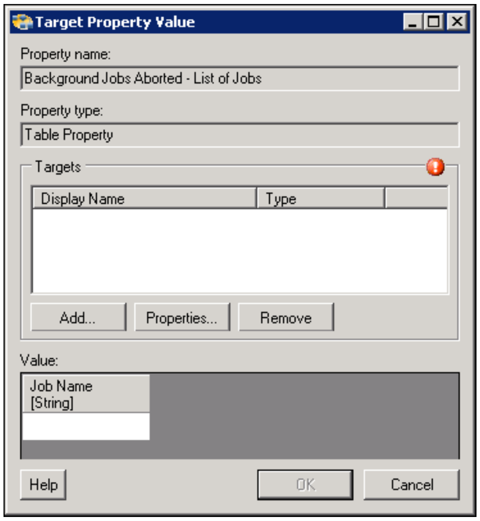
Step 5 Click the **Target Values** tab to specify the targets that should be used to override the default value.

Figure 3-14 Extended Target Properties—Target Values Tab



Step 6 Click **New** to add a new target override.

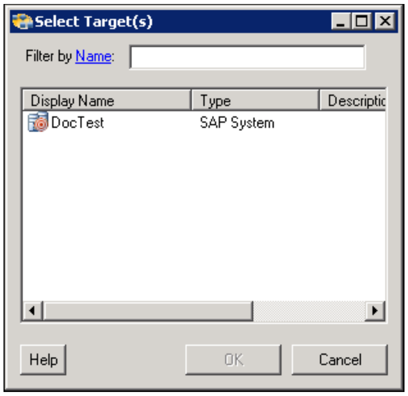
Figure 3-15 Target Property Value Dialog Box


Property name: Background Jobs Aborted - List of Jobs

Property type: Table Property

Step 7 On the Target Property Value dialog box, click **Add** to choose the target (SAP system) to be used for the override value. This is the SAP system that will be monitored for a value other than the default value.

Figure 3-16 Select Target(s) Value Dialog Box

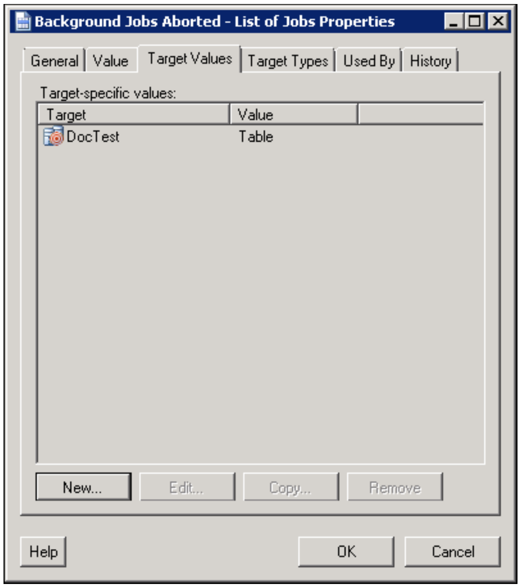


Step 8 Select the SAP system and click **OK**.

Step 9 On the Target Property Value dialog box, enter the information in the Value area to be used for the specified target and then click **OK**.

The target override displays on the Target Values tab.

Figure 3-17 Extended Target Properties—Target Values Tab with Override



Step 10 Click **OK** to close the dialog box and save your changes.

Note The Target Types tab is only available if you have explicit rights to the object. *See* the *Tidal Enterprise Orchestrator Reference Guide* for information on using this property page.

Managing Global Variables

The processes use global variables for information that is used on a regular basis to avoid having to specify the same information in several processes or activities. Some of the variables that ship with the automation packs are configured with default values but can be modified to meet the requirements for your specific environment. Other variables do not have default values defined and must be defined by the user before it can be used in the processes.

The Core Automation for SAP automation pack ships with the global variables that must be configured before they can be used in the processes.

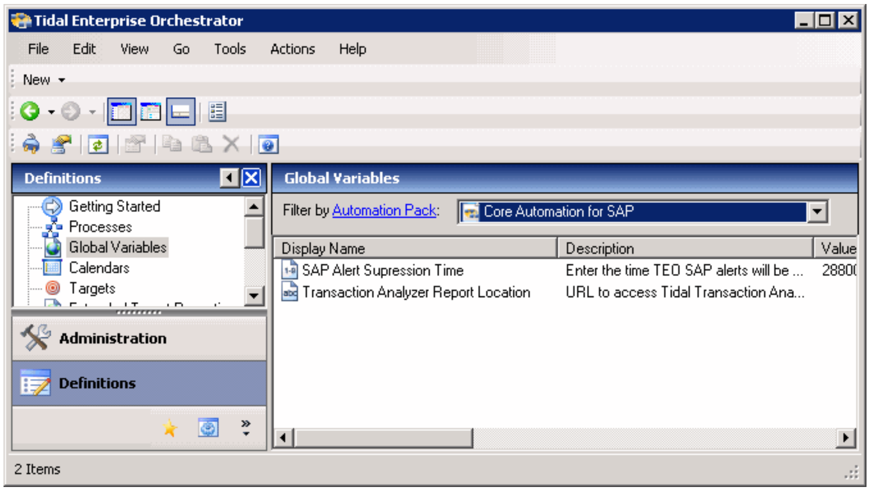
Accessing Global Variables

The global variables that ship with the Core Automation for SAP automation pack can be accessed from the Definitions—Global Variables view.

Step 1 On the Console, select the Definitions workspace and click **Global Variables** in the navigation pane. By default, all the variables display in the Global Variables pane.

Step 2 Click the **Filter by** link and choose **Automation Pack > Core Automation for SAP** to filter for only the global variables that ship with the specific automation pack.

Figure 3-18 Global Variables View



Filter by Automation Pack: Core Automation for SAP

Display Name	Description	Value
SAP Alert Supression Time	Enter the time TEO SAP alerts will be ...	2880(
Transaction Analyzer Report Location	URL to access Tidal Transaction Ana...	

2 Items

The following information about the variables displays by default:

Column	Description
Display Name	Name of the global variable.
Description	Brief overview of the global variable.
Value	Value of the variable.
Data Type	Type of value being used for the variable (Boolean, Encrypted String, Identity, Numeric, String, Table).
Automation Pack	Name of the automation pack that provides the object.

Column	Description
Last Modified Time	Time the global variable was last modified.
Last Modified By	Name of the user who last modified the global variable.

Configuring Global Variables

SAP Alert Suppression Time Properties

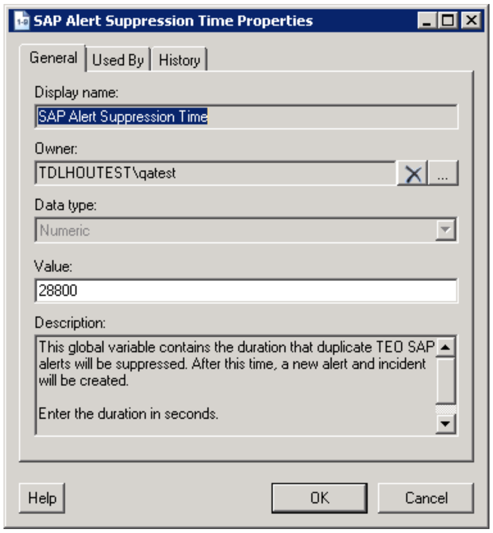
The SAP Alert Suppression Time global variable contains the length of time (in seconds) that TEO SAP alerts will be suppressed when duplicated. After this time, a new alert and incident will be created.

Step 1 In the Definitions view, click **Global Variables** in the navigation pane to display the variables in the Global Variables pane.

Step 2 Click the **Filter by** link and choose **Automation Pack > Core Automation for SAP** to filter for only the global variables that ship with the Core Automation for SAP automation pack.

Step 3 In the Global Variables pane, right-click the **SAP Alert Suppression Time** global variable and choose **Properties**.

Figure 3-19 SAP Alert Suppression Time Properties—General Tab



Display name: SAP Alert Suppression Time

Owner: TDLHOUTEST\qatest

Data type: Numeric

Value: 28800

Description: This global variable contains the duration that duplicate TEO SAP alerts will be suppressed. After this time, a new alert and incident will be created.

Enter the duration in seconds.

Step 4 In the Value text field, enter the number of seconds to suppress duplicate alerts and click **OK**.

Transaction Analyzer Report Location

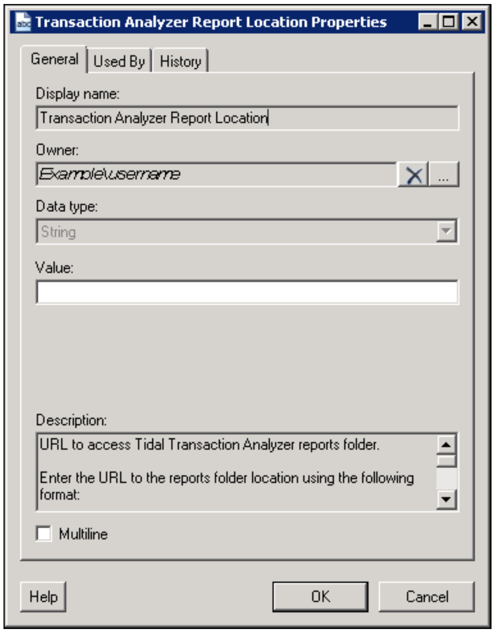
If you have Cisco Tidal Transaction Analyzer installed, you use the Transaction Analyzer Report Location global variable to specify the URL for accessing the Tidal Transaction Analyzer reports folder.

Step 1 In the Definitions view, click **Global Variables** in the navigation pane to display the variables in the Global Variables pane.

Step 2 Click the **Filter by** link and choose **Automation Pack > Core Automation for SAP** to filter for only the global variables that ship with the Core Automation for SAP automation pack.

Step 3 In the Global Variables pane, right-click the **Transaction Analyzer Report Location** global variable and choose **Properties**.

Figure 3-20 Transaction Analyzer Report Location Properties—General Tab



Transaction Analyzer Report Location Properties

Display name: Transaction Analyzer Report Location

Owner: Example\username

Data type: String

Value:

Description: URL to access Tidal Transaction Analyzer reports folder.

Enter the URL to the reports folder location using the following format:

☐ Multiline

Step 4 In the Value text field, enter the URL to access the Tidal Transaction Analyzer reports folder in the following format:

http://<RSServerName>/ReportServer?/Tidal Transaction Analyzer - <TADatabaseServerName>

For example:

http://RSServer01/ReportServer?/Tidal Transaction Analyzer - TADBServer

Step 5 Click **OK** to close the dialog box.

CHAPTER 4

Managing Incident Analysis for SAP Processes

This chapter provides information on using the product, specific to the Incident Analysis for SAP automation pack. It includes information on accessing the Incident Analysis for SAP processes and filtering for specific processes, managing the SAP processes, starting a process, and viewing a running process, its results, and the automation summary generated by the process.

It includes the following sections:

- Accessing Incident Analysis for SAP Processes, page 4-2
- Managing SAP Processes, page 4-4
- Running Processes, page 4-9
- Viewing Process Results, page 4-13
- Viewing Automation Summary, page 4-17

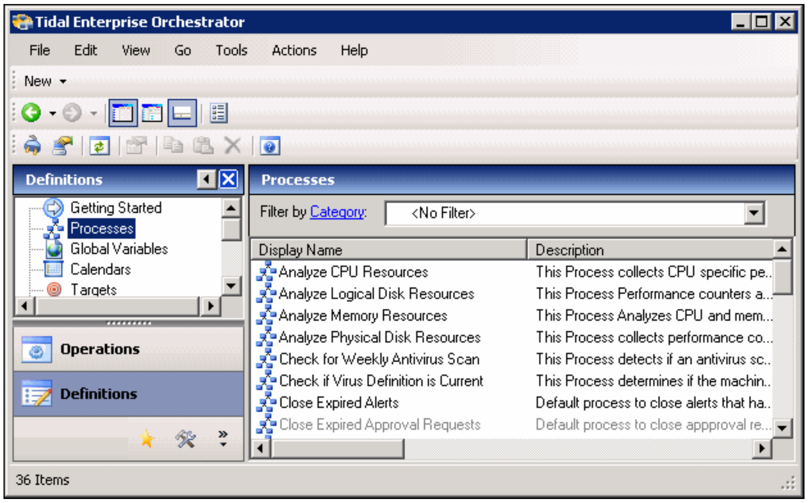
Note Before you can run the Incident Analysis for SAP processes, you must configure the objects that are referenced by the processes and activities. *See* Chapter 3, "Getting Started Using the Automation Pack" for information on configuring the SAP-related objects in TEO.

Accessing Incident Analysis for SAP Processes

The processes that ship with the product can be accessed from the Definitions—Processes view.

Step 1 On the Console, select the Definitions workspace and click **Processes** in the navigation pane. By default, all the processes display in the Processes pane.

Figure 4-1 Processes View



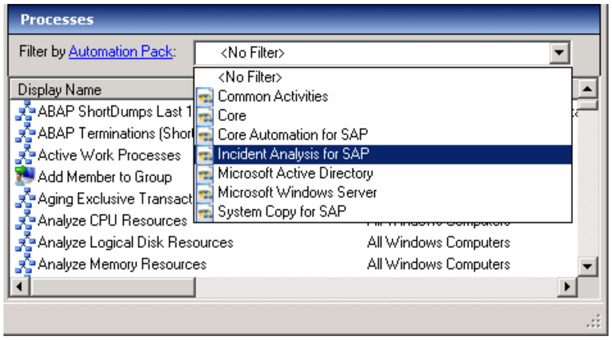
Display Name	Description
Analyze CPU Resources	This Process collects CPU specific pe...
Analyze Logical Disk Resources	This Process Performance counters a...
Analyze Memory Resources	This Process Analyzes CPU and mem...
Analyze Physical Disk Resources	This Process collects performance co...
Check for Weekly Antivirus Scan	This Process detects if an antivirus sc...
Check if Virus Definition is Current	This Process determines if the machin...
Close Expired Alerts	Default process to close alerts that ha...
Close Expired Approval Requests	Default process to close appproval re...

If you have multiple automation packs installed, you can filter the processes to display the processes specific to the automation pack.

Step 2 In the upper portion of the Processes pane, click the **Filter by** link and choose **Automation Pack**.

Step 3 In the drop-down list, choose **Incident Analysis for SAP**.

Figure 4-2 Filtering Processes by Automation Pack



Display Name	
ABAP ShortDumps Last 1	
ABAP Terminations (Short	
Active Work Processes	
Add Member to Group	
Aging Exclusive Transact	
Analyze CPU Resources	
Analyze Logical Disk Resources	All Windows Computers
Analyze Memory Resources	All Windows Computers

The processes display in the Processes pane.

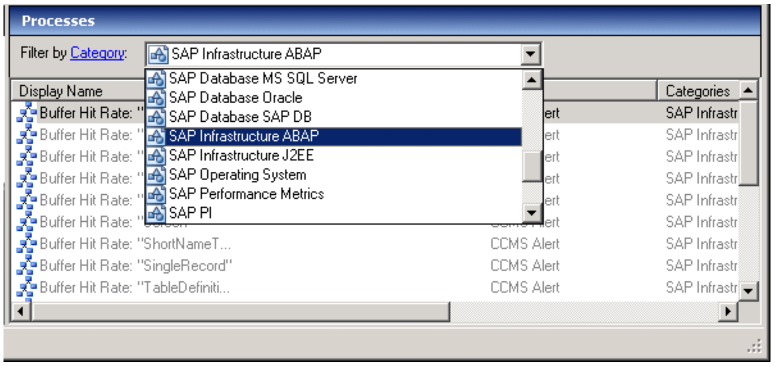
Filtering Processes by Category

You can also filter the processes by category to find a specific process.

Step 1 In the upper portion of the Processes pane, click the **Filter by** link and choose **Category**.

Step 2 In the drop-down list, choose the category.

Figure 4-3 Filtering for SAP Infrastructure ABAP Processes



Filter by Category: SAP Infrastructure ABAP

Step 3 Scroll to the process.

Managing SAP Processes

This section provides information on managing the SAP processes, including:

- Enabling and disabling processes
- Enabling and disabling the process archival feature
- Modifying a process schedule
- Creating an automation pack for new processes

Enabling a Process

Some of the processes that ship with the automation packs are disabled by default to reduce the load on the server. These processes must be enabled before they can execute.

Perform the following steps to enable a process.

Step 1 In the Processes view, navigate to the process that you want to enable (disabled processes appear dimmed).

Step 2 Use one of the following methods to enable the process:

- Right-click the process and choose **Enable** from the submenu.
- In the Process Editor, click the **General** tab and then checke the **Enabled** check box. Click the **Save** 💾 tool to save your changes to the process and close the Process Editor.

Disabling a Process

Disabling a process prevents the process from executing. You may want to disable some processes to reduce the load on your server or while you are modifying the process definition.

Perform the following steps to disable a process.

Step 1 In the Processes view, navigate to the process that you want to disable.

Step 2 Use one of the following methods to disable the process:

- Right-click the process and choose **Disable** from the submenu.
- In the Process Editor, click the **General** tab and then uncheck the **Enabled** check box. Click the **Save** 💾 tool to save your changes to the process and close the Process Editor.

Modifying Process Instance Archival

TEO provides an option in the process definition that allows you choose whether or not to archive process and activity execution in the TEOProcess database. Disabling the **Archive completed instances** option helps improve performance and minimize the size of the database. It is also useful when debugging the execution of processes.

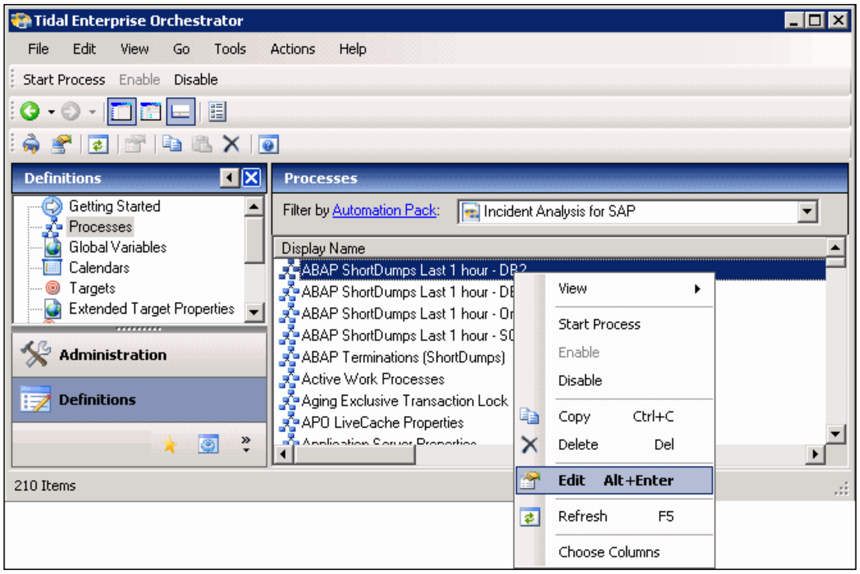
The automation packs shipped by Cisco normally have the archival functionality disabled by default for the Incident Analysis for SAP processes. If you want to view the execution of a process and its activities, or view the process instances after a process has completed, you must enable the archival functionality in the process definition.

Perform the following steps to enable or disable the archival feature.

Step 1 In the Processes view, navigate to the process you want to flag for archival.

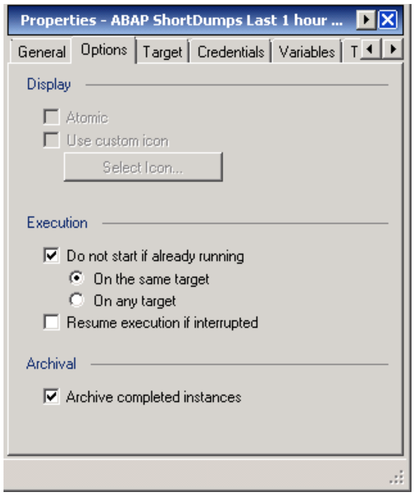
Step 2 Right-click the process and choose **Edit** from the submenu.

Figure 4-4 Opening a Process to Edit Properties


Tidal Enterprise Orchestrator
File Edit View Go Tools Actions Help
Start Process Enable Disable
Definitions
Getting Started
Processes
Global Variables
Calendars
Targets
Extended Target Properties
Administration
Definitions
210 Items
Processes
Filter by Automation Pack: Incident Analysis for SAP
Display Name
ABAP ShortDumps Last 1 hour - DB2
ABAP ShortDumps Last 1 hour - DE
ABAP ShortDumps Last 1 hour - Or
ABAP ShortDumps Last 1 hour - SC
ABAP Terminations (ShortDumps)
Active Work Processes
Aging Exclusive Transaction Lock
APO LiveCache Properties
View
Start Process
Enable
Disable
Copy Ctrl+C
Delete Del
Edit Alt+Enter
Refresh F5
Choose Columns

Step 3 On the process Properties dialog box, click the **Options** tab.

Figure 4-5 Process Properties—Options Tab



Display

□ Atomic

□ Use custom icon

Select Icon...

Execution

☑ Do not start if already running

● On the same target

○ On any target

□ Resume execution if interrupted

Archival

☑ Archive completed instances

Step 4 On the Options tab, check the **Archive completed instances** check box to enable process instance archival.

If the process is already flagged for archival and you no longer want to save the process instances for this process, uncheck the check box.

Step 5 Click the **Save** tool to save your changes to the process and close the process Editor.

Modifying a Process Schedule

Many of the processes that ship with the automation packs are triggered by a schedule. You can modify when the process will be executed by disabling the existing schedule and then creating a new schedule for the process. You use the process Properties dialog box to modify the process schedule.

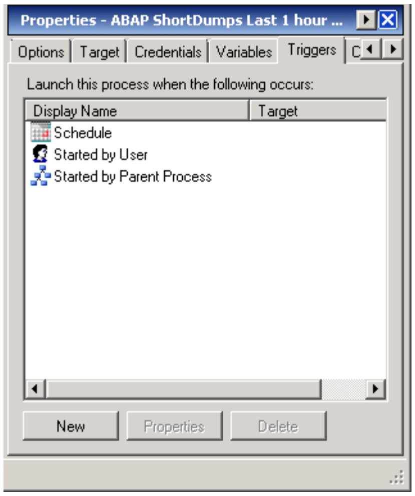
Perform the following steps to assign a new schedule to a process.

Step 1 In the Processes view, navigate to the process for which you want to modify.

Step 2 Right-click the process and choose **Edit** from the submenu (see Figure 4-4 on page 4-5).

Step 3 On the process Properties dialog box, click the **Triggers** tab.

Figure 4-6 Process Properties—Triggers Tab



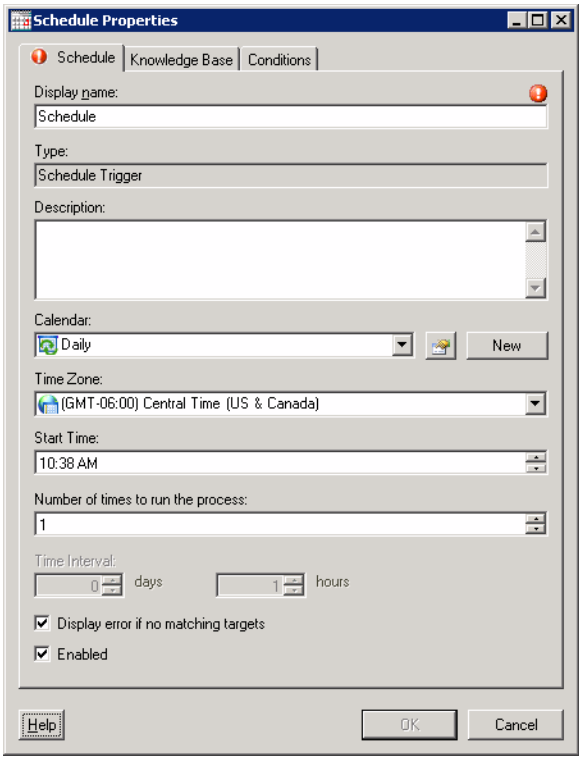
Launch this process when the following occurs:

Display Name	Target
Schedule	
Started by User	
Started by Parent Process	

Step 4 On the Triggers tab, right-click the current **Schedule** and choose **Disable** from the submenu.

Step 5 Click **New > Schedule** to open the Schedule Properties dialog box to create a new schedule for this process.

Figure 4-7 Schedule Properties



Display name: Schedule

Type: Schedule Trigger

Description:

Calendar: Daily

Time Zone: (GMT-06:00) Central Time (US & Canada)

Start Time: 10:38 AM

Number of times to run the process: 1

Time Interval: 0 days 1 hours

☑ Display error if no matching targets

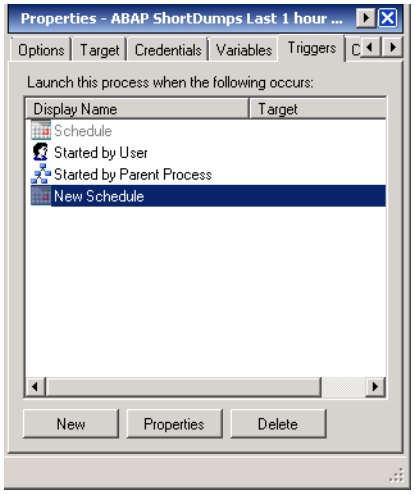
☑ Enabled

Step 6 On the Schedule Properties dialog box, specify the criteria for the new schedule and click **OK**.

Note For information on creating schedules, *see* “Managing Triggers” in the *Tidal Enterprise Orchestrator Reference Guide*.

The newly created schedule displays on the Triggers tab and is enabled.

Figure 4-8 Process Properties—Triggers Tab with Newly Created Schedule



Properties - ABAP ShortDumps Last 1 hour ...

Launch this process when the following occurs:

Display Name	Target
Schedule	
Started by User	
Started by Parent Process	
New Schedule	

Step 7 Click the **Save** 💾 tool to save your changes to the process and close the process Editor.

Running Processes

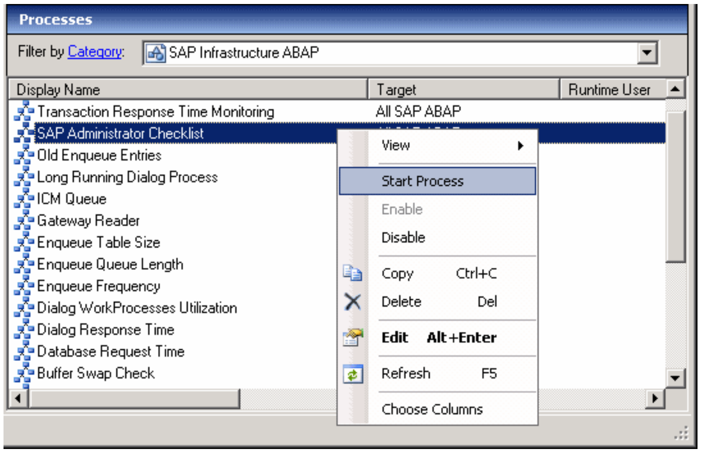
The processes that ship with the product will run based on the trigger that was defined in the process definition. For processes that are triggered by a schedule, you can also manually start a process at any time (adhoc). This section guides you through starting a process and viewing its progress as it runs.

Note You can only view a running process and the process instances for processes that have the Archive completed instances feature enabled. See Modifying Process Instance Archival, page 4-5 for information on enabling the archival feature on a specific process.

Starting a Process

Step 1 In the Processes view, right-click the process and choose **Start Process** from the submenu.

Figure 4-9 Starting a Process



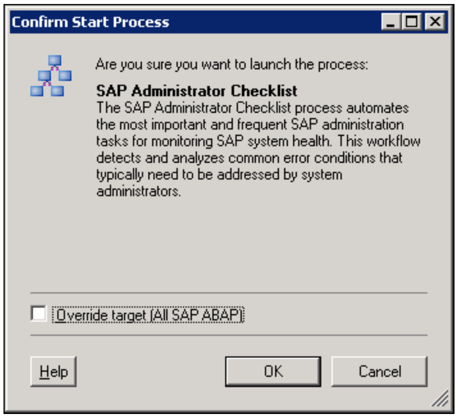
Processes

Filter by Category: SAP Infrastructure ABAP

Display Name	Target	Runtime User
Transaction Response Time Monitoring	All SAP ABAP	
SAP Administrator Checklist		
Old Enqueue Entries		
Long Running Dialog Process		
ICM Queue		
Gateway Reader		
Enqueue Table Size		
Enqueue Queue Length		
Enqueue Frequency		
Dialog WorkProcesses Utilization		
Dialog Response Time		
Database Request Time		
Buffer Swap Check		

The Confirm Start Process dialog box displays.

Figure 4-10 Confirm Start Process



Confirm Start Process

Are you sure you want to launch the process:

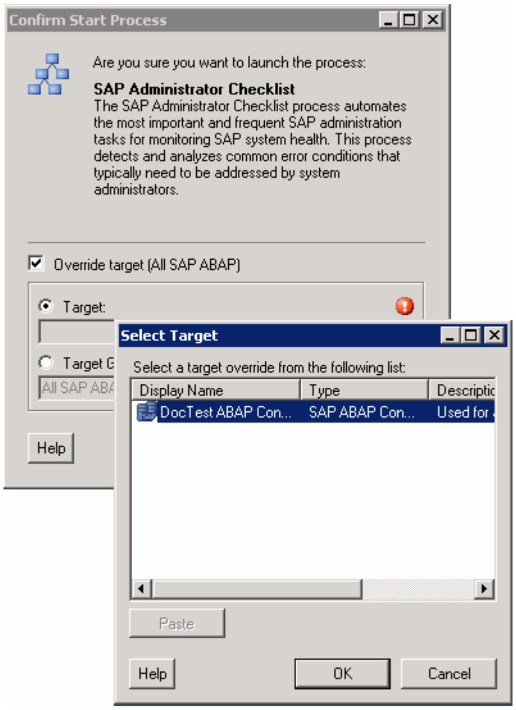
SAP Administrator Checklist
The SAP Administrator Checklist process automates the most important and frequent SAP administration tasks for monitoring SAP system health. This workflow detects and analyzes common error conditions that typically need to be addressed by system administrators.

☐ Override target (All SAP ABAP)

This process is defined to run on systems in the All SAP ABAP target group. In this example, we will override the default target and choose a specific system on which to run the process.

Step 2 On the Confirm Start Process dialog box, check the **Override target (All SAP ABAP)** check box to expand the fields on the dialog box.

Figure 4-11 Specifying Target Override



Confirm Start Process

Are you sure you want to launch the process:

SAP Administrator Checklist
The SAP Administrator Checklist process automates the most important and frequent SAP administration tasks for monitoring SAP system health. This process detects and analyzes common error conditions that typically need to be addressed by system administrators.

☑ Override target (All SAP ABAP)

● Target:

○ Target G

All SAP ABA

Select Target

Select a target override from the following list:

Display Name	Type	Descriptic
DocTest ABAP Con...	SAP ABAP Con...	Used for

Step 3 Click the **Target** radio button and then click the **Browse** ... tool to open the Select Target dialog box.

Step 4 Select the target in the list and then click **OK**.

Step 5 On the Confirm Start Process dialog box, click **OK** to start the process.

The Start Process Results dialog box displays. Proceed to Viewing Running Process, page 4-11.

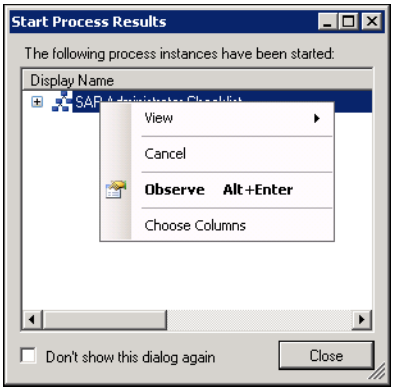
Viewing Running Process

After starting the process, you can use the Process Viewer to view the process as it runs through each activity.

Note You can only view a running process and the process instances for processes that have the Archive completed instances feature enabled. See Modifying Process Instance Archival, page 4-5 for information on enabling the archival feature on a specific process.

Step 1 On the Start Process Results dialog box, right-click the process and choose **Observe**.

Figure 4-12 Start Process Results—Observe Submenu

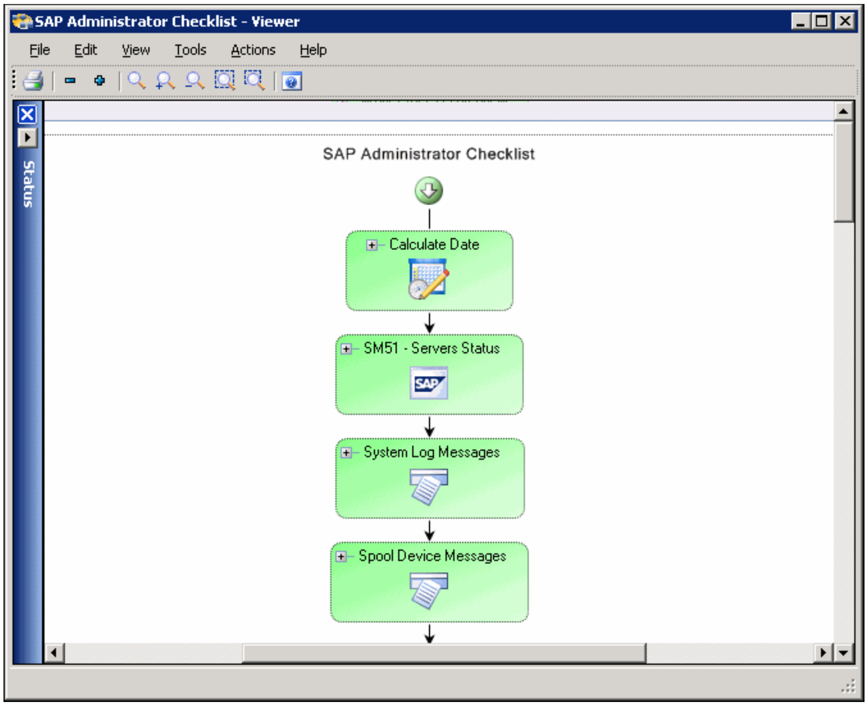


Start Process Results

The following process instances have been started:

The Process Viewer displays the process workflow.

Figure 4-13 Process Viewer—Viewing SAP Administrator Checklist Process Running



Step 2 View the process as it proceeds through the workflow.

The activities within the process workflow will change to green as they complete (succeed). If an activity fails, an incident is created.

Step 3 When the process completes, close the Process Viewer and proceed to Viewing Process Results, page 4-13.

Viewing Process Results

After a process completes, you can view the results in the Operations workspace. This section guides you through viewing the results from running the SAP Administrator Checklist process.

Note You can only view a running process and the process instances for processes that have the Archive completed instances feature enabled. See Modifying Process Instance Archival, page 4-5 for information on enabling the archival feature on a specific process.

Accessing Process View

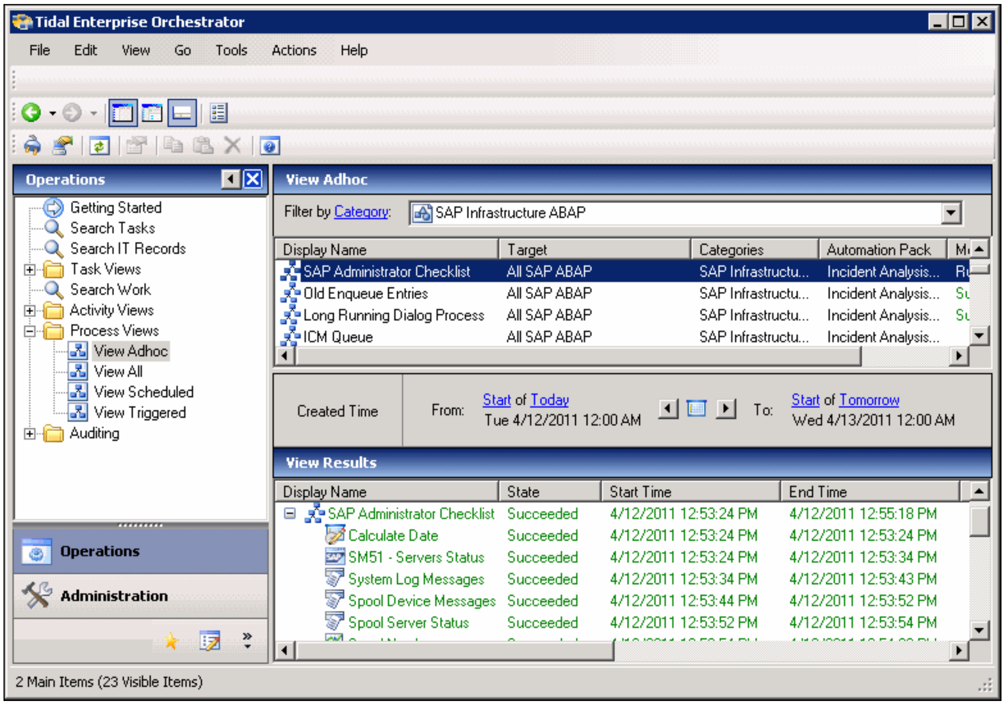
Step 1 On the Operations workspace, expand expand **Process Views** in the navigation pane and click **View Adhoc** (since the SAP Administrator Checklist process was manually executed).

Step 2 Using the **Filter by** link, choose **Category** and then choose **SAP Infrastructure ABAP** from the drop-down list.

Step 3 Scroll to the **SAP Administrator Checklist** process and select it.

Step 4 In the View Results pane, expand the **SAP Administrator Checklist** process to view each activity in the process workflow.

Figure 4-14 Operations Workspace—Viewing Process Results



Filter by Category: SAP Infrastructure ABAP

Display Name	Target	Categories	Automation Pack	M
SAP Administrator Checklist	All SAP ABAP	SAP Infrastructu...	Incident Analysis...	Ru
Old Enqueue Entries	All SAP ABAP	SAP Infrastructu...	Incident Analysis...	Su
Long Running Dialog Process	All SAP ABAP	SAP Infrastructu...	Incident Analysis...	Su
ICM Queue	All SAP ABAP	SAP Infrastructu...	Incident Analysis...	

Created Time From: Start of Today Tue 4/12/2011 12:00 AM To: Start of Tomorrow Wed 4/13/2011 12:00 AM

Display Name	State	Start Time	End Time
SAP Administrator Checklist	Succeeded	4/12/2011 12:53:24 PM	4/12/2011 12:55:18 PM
Calculate Date	Succeeded	4/12/2011 12:53:24 PM	4/12/2011 12:53:24 PM
SM51 - Servers Status	Succeeded	4/12/2011 12:53:24 PM	4/12/2011 12:53:34 PM
System Log Messages	Succeeded	4/12/2011 12:53:34 PM	4/12/2011 12:53:43 PM
Spool Device Messages	Succeeded	4/12/2011 12:53:44 PM	4/12/2011 12:53:52 PM
Spool Server Status	Succeeded	4/12/2011 12:53:52 PM	4/12/2011 12:53:54 PM

2 Main Items (23 Visible Items)

Step 5 Review the status of the process and each activity within the process to verify that it has succeeded.

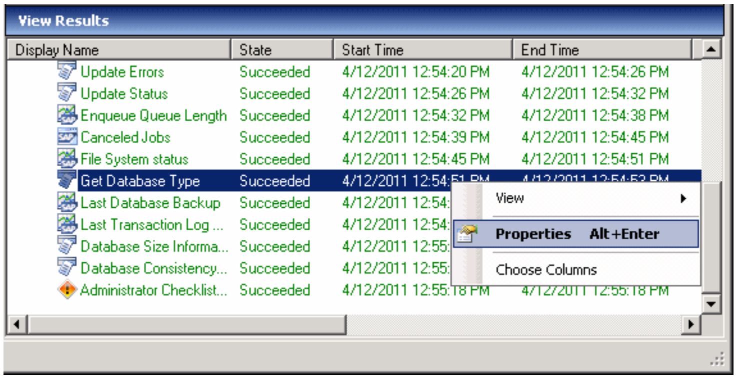
Viewing Activity Results

You can view the results of a specific activity within the process using the Activity Instance Properties dialog box. In this example, we will view the results of the Get Database Type activity, which retrieves information about the SAP database associated with the SAP system.

Step 1 In the View Results pane, scroll to the **Get Database Type** activity.

Step 2 Right-click **Get Database Type** and choose **Properties**.

Figure 4-15 Activity Properties Submenu

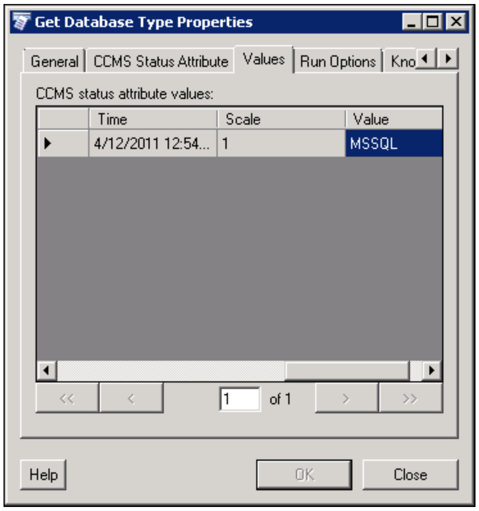


View Results

Display Name	State	Start Time	End Time
Update Errors	Succeeded	4/12/2011 12:54:20 PM	4/12/2011 12:54:26 PM
Update Status	Succeeded	4/12/2011 12:54:26 PM	4/12/2011 12:54:32 PM
Enqueue Queue Length	Succeeded	4/12/2011 12:54:32 PM	4/12/2011 12:54:38 PM
Canceled Jobs	Succeeded	4/12/2011 12:54:39 PM	4/12/2011 12:54:45 PM
File System status	Succeeded	4/12/2011 12:54:45 PM	4/12/2011 12:54:51 PM
Get Database Type	Succeeded	4/12/2011 12:54:51 PM	4/12/2011 12:54:53 PM
Last Database Backup	Succeeded	4/12/2011 12:54:	
Last Transaction Log ...	Succeeded	4/12/2011 12:54:	
Database Size Informa...	Succeeded	4/12/2011 12:55:	
Database Consistency...	Succeeded	4/12/2011 12:55:	
Administrator Checklist...	Succeeded	4/12/2011 12:55:18 PM	4/12/2011 12:55:18 PM

Step 3 On the Get Database Type Properties dialog box, click the **Values** tab.

Figure 4-16 Get Database Type Properties—Values Tab



Get Database Type Properties

CCMS status attribute values:

Time	Scale	Value
4/12/2011 12:54...	1	MSSQL

Step 4 For each system, scroll to the Value column to view the database type (MSSQL).

Step 5 When you have completed reviewing the results, click **Close** to close the dialog box.

Viewing Incidents

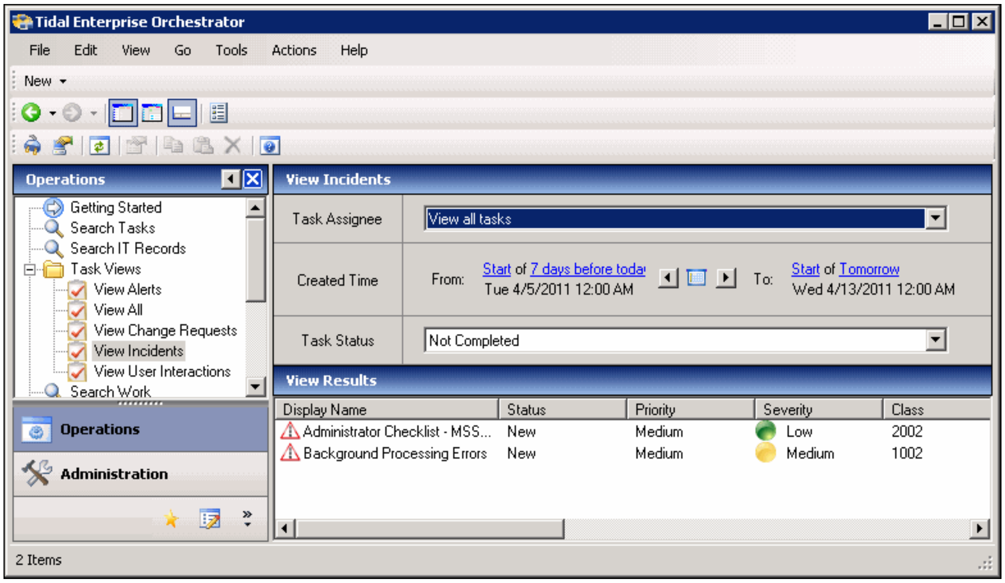
When a process detects an issue that requires action, an incident is generated. If you have configured the product to send notifications to a specific person in your organization, that person will receive an email notification whenever an incident is generated. You can also view these incidents in the Task Views on the Operations workspace.

In this example, we will view the incidents that were generated from the SAP Administrator Checklist process.

Step 1 On the Operations workspace, expand **Task Views** in the navigation pane and click **View Incidents**.

Step 2 In the View Incidents pane, choose **View all tasks** from the Task Assignee drop-down list to display all the incidents in the View Results pane.

Figure 4-17 Viewing Incidents



Task Assignee: View all tasks

Created Time: From: Start of 7 days before toda Tue 4/5/2011 12:00 AM To: Start of Tomorrow Wed 4/13/2011 12:00 AM

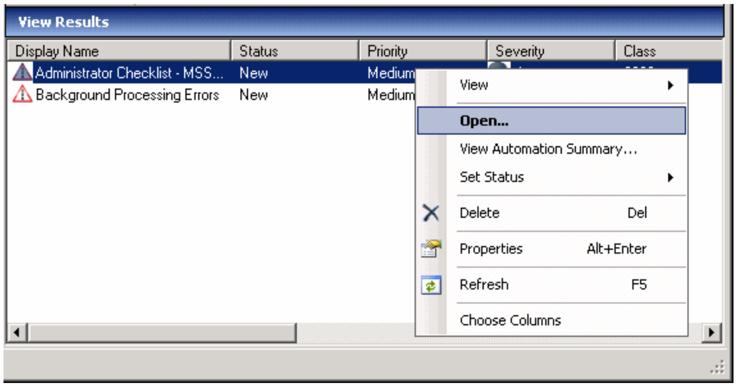
Task Status: Not Completed

Display Name	Status	Priority	Severity	Class
Administrator Checklist - MSS...	New	Medium	Low	2002
Background Processing Errors	New	Medium	Medium	1002

2 Items

Step 3 To view a specific incident, right-click the incident and choose **Open**.

Figure 4-18 Incident Open Submenu

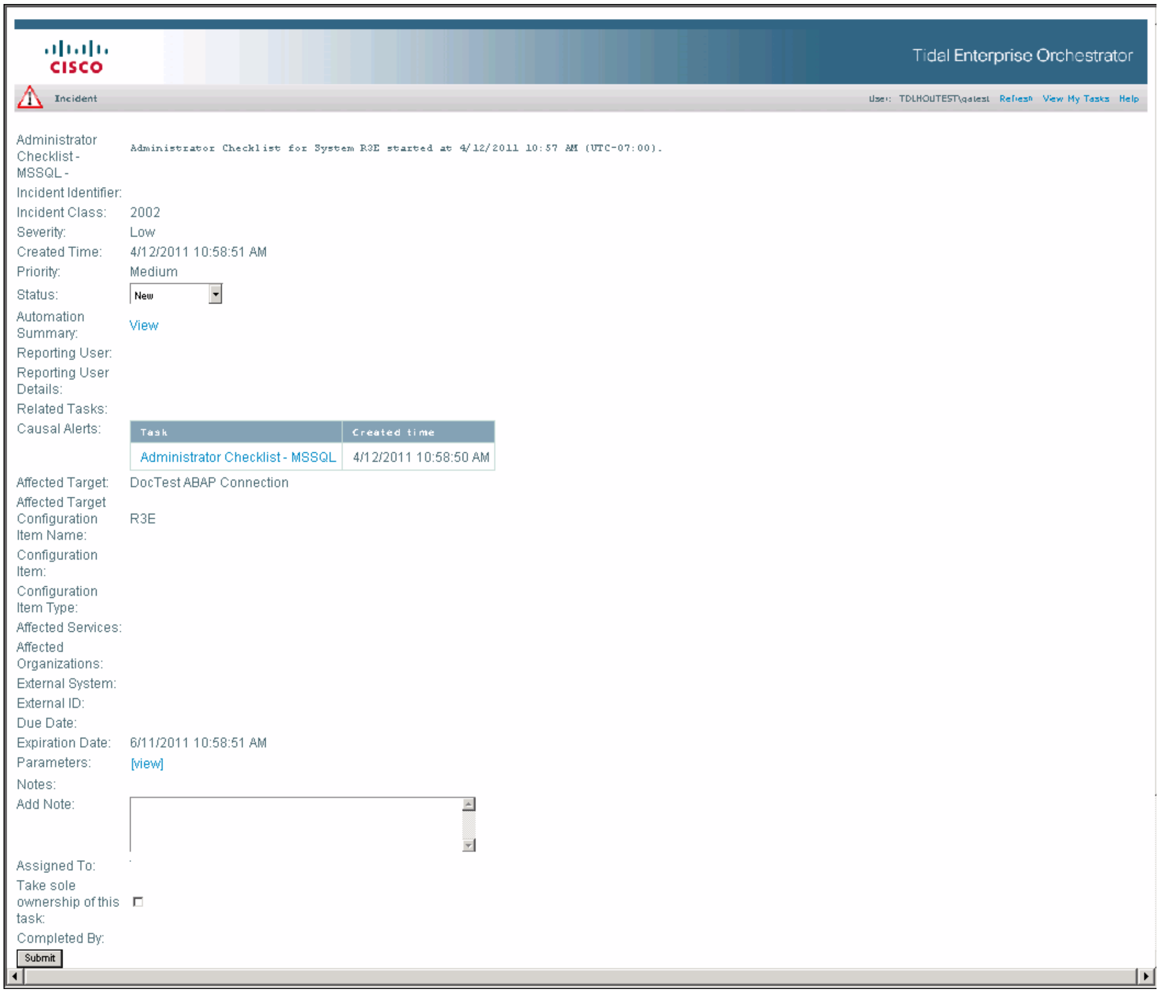


View Results

Display Name	Status	Priority	Severity	Class
Administrator Checklist - MSS...	New	Medium		
Background Processing Errors	New	Medium		

The Incident Report displays in your web browser.

Figure 4-19 Tidal Enterprise Orchestrator Incident Report



Administrator Checklist - MSSQL -	Administrator Checklist for System R3E started at 4/12/2011 10:57 AM (UTC-07:00).
Incident Identifier:	
Incident Class:	2002
Severity:	Low
Created Time:	4/12/2011 10:58:51 AM
Priority:	Medium
Status:	New
Automation Summary:	View
Reporting User:	
Reporting User Details:	
Related Tasks:	
Causal Alerts:	
Affected Target:	DocTest ABAP Connection
Affected Target Configuration Item Name:	R3E
Configuration Item:	
Configuration Item Type:	
Affected Services:	
Affected Organizations:	
External System:	
External ID:	
Due Date:	
Expiration Date:	6/11/2011 10:58:51 AM
Parameters:	[view]
Notes:	
Add Note:	
Assigned To:	
Take sole ownership of this task:	□
Completed By:	

Task	Created time
Administrator Checklist - MSSQL	4/12/2011 10:58:50 AM

Viewing Automation Summary

When incidents are generated, TEO delivers an online Automation Summary that details the analysis that was performed to identify a situation that may require action. It also shows relevant diagnostic and state information captured while performing the situation analysis, and provides a recommended resolution for the situation.

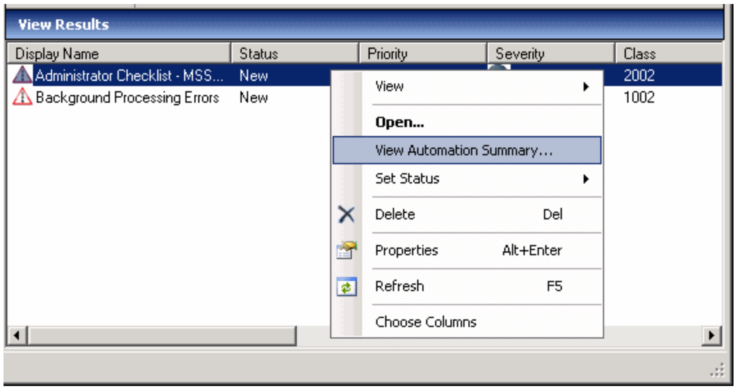
You can access the Automation Summary from the Tasks View on the Operations workspace.

Step 1 On the Operations workspace, expand **Task Views** in the navigation pane and click **View Incidents**.

Step 2 In the View Incidents pane, click the **View all tasks** radio button to display the incidents in the View Results pane.

Step 3 Right-click **Administrator Checklist** and choose **View Automation Summary**.

Figure 4-20 View Automation Summary Submenu

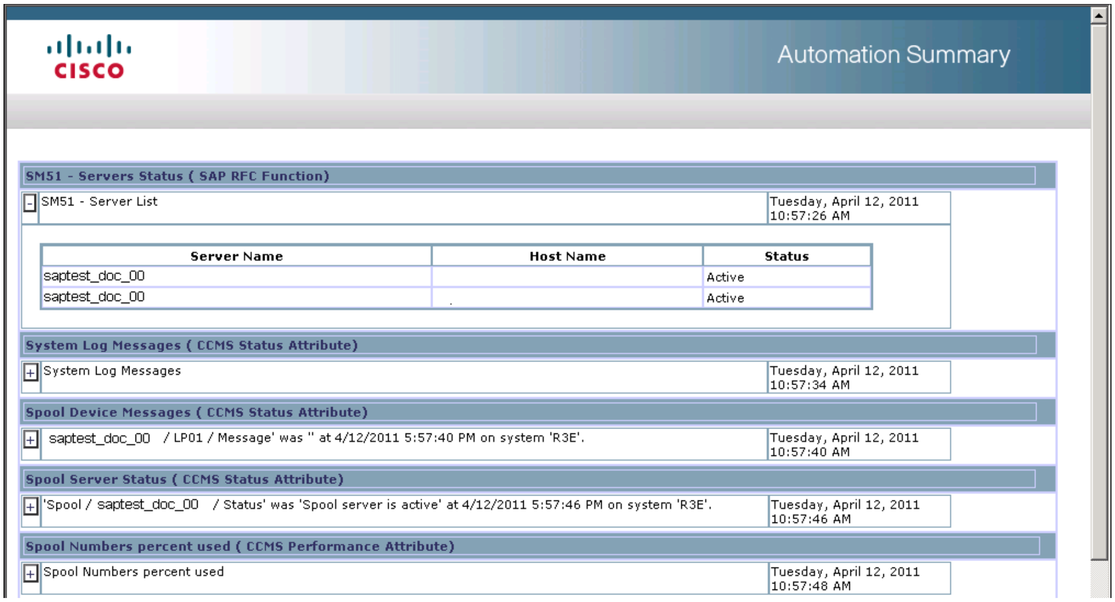


View Results

Display Name	Status	Priority	Severity	Class
Administrator Checklist - MSS...	New			2002
Background Processing Errors	New			1002

The Automation Summary displays in your web browser.

Figure 4-21 Automation Summary



Automation Summary

SM51 - Servers Status (SAP RFC Function)

SM51 - Server List — Tuesday, April 12, 2011 10:57:26 AM

Server Name	Host Name	Status
saptest_doc_00		Active
saptest_doc_00	.	Active

System Log Messages (CCMS Status Attribute)

System Log Messages — Tuesday, April 12, 2011 10:57:34 AM

Spool Device Messages (CCMS Status Attribute)

saptest_doc_00 / LP01 / Message' was '' at 4/12/2011 5:57:40 PM on system 'R3E'. — Tuesday, April 12, 2011 10:57:40 AM

Spool Server Status (CCMS Status Attribute)

'Spool / saptest_doc_00 / Status' was 'Spool server is active' at 4/12/2011 5:57:46 PM on system 'R3E'. — Tuesday, April 12, 2011 10:57:46 AM

Spool Numbers percent used (CCMS Performance Attribute)

Spool Numbers percent used — Tuesday, April 12, 2011 10:57:48 AM

CHAPTER A

Installing TEO SAP Monitoring Management Pack In SCOM

Tidal Enterprise Orchestrator (TEO) can be installed on the Microsoft System Center Operations Manager 2007 (SCOM) management framework if you are using this framework to monitor all incidents from a central location in your environment.

This appendix guides you through configuring your SCOM environment and importing the TEO SAP Monitoring management pack. It includes the following sections:

- Prerequisites, page A-1
- Configuring the SCOM Environment, page A-2
- Importing Management Pack, page A-9
- Enabling SAP Alerts on Windows Event Log Process, page A-16

Prerequisites

The following prerequisites should be met to successfully run TEO automation packs with the SCOM management framework:

Prerequisite	Description
Software Requirements	
Microsoft System Center Operations Manager 2007 SP1 or R2	A SCOM agent should be installed on the TEO server prior to importing the management packs.
Windows Powershell v1.0 or later	Must be installed on the TEO server
SCOM Server Requirements	
Security settings	The SCOM agent on the TEO server must be configured to allow the agent to act as a proxy.
Run As Account	A *Run As Account* should be created for the server where the TEO Process database resides and then distributed to the TEO server.

Note The procedures in this chapter are for System Center Operations Manager 2007 R2. If you have an earlier version (OM 2007 SP1) installed, the procedures and screenshots will be slightly different.

Configuring the SCOM Environment

It is recommended that you perform some setup tasks prior to importing the management packs. This section guides you through configuring the security settings to allow the agent to act as a proxy, creating a *Run As Account* for the TEO Process database, and associating the *Run As Account* with a *Run As Profile* in the SCOM Administration view.

Configuring Security Settings

When TEO is installed on a SCOM agent, the agent security settings need to be configured to allow the agent to act as a proxy so that the SAP class instances can be discovered.

Step 1 In the Operations Console Administration view, navigate to **Device Management** and click the **Agent Managed** node.

Step 2 In the results pane pane, right-click the management server and choose **Properties**.

Step 3 On the Agent Managed Server Properties dialog box, click the **Security** tab.

Step 4 Under Server Proxy, check the check box to allow this server to act as a proxy.

Step 5 Click **OK** to close the dialog box.

Step 6 Restart the agent HealthService to implement the changes.

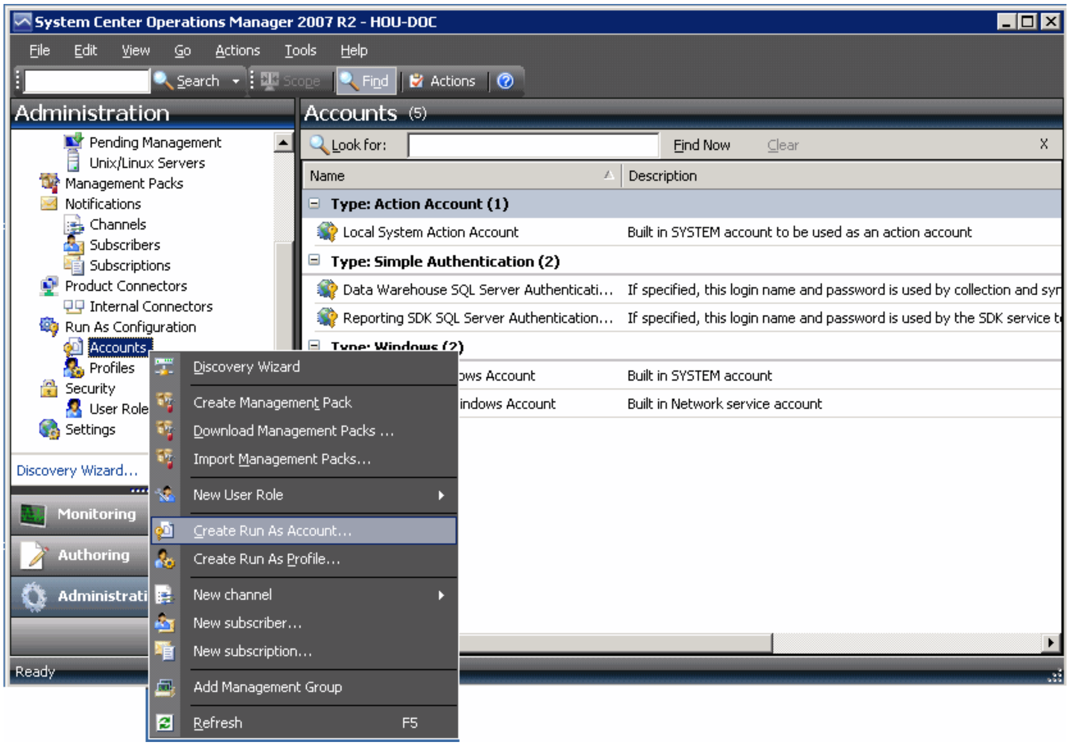
Creating A Run As Account

It is recommended that you create a *Run As Account* for the server where the TEO Process database resides prior to installing the management pack. The account must have *Read* permissions on the TEO Process database.

Step 1 In the Administration view, navigate to the **Run As Configuration** node.

Step 2 Right-click **Accounts** and choose **Create Run As Account**.

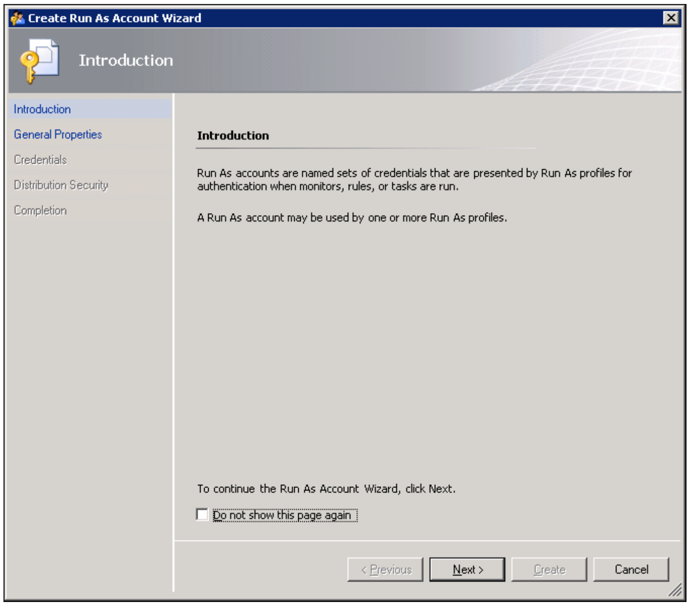
Figure A-1 Create Run As Account Submenu



Name	Description
Type: Action Account (1)	
Local System Action Account	Built in SYSTEM account to be used as an action account
Type: Simple Authentication (2)	
Data Warehouse SQL Server Authenticati...	If specified, this login name and password is used by collection and syr
Reporting SDK SQL Server Authentication...	If specified, this login name and password is used by the SDK service t
Type: Windows (2)	
ows Account	Built in SYSTEM account
indows Account	Built in Network service account

The Create Run As Account wizard Introduction panel displays.

Figure A-2 Create Run As Account—Introduction



Introduction

Run As accounts are named sets of credentials that are presented by Run As profiles for authentication when monitors, rules, or tasks are run.

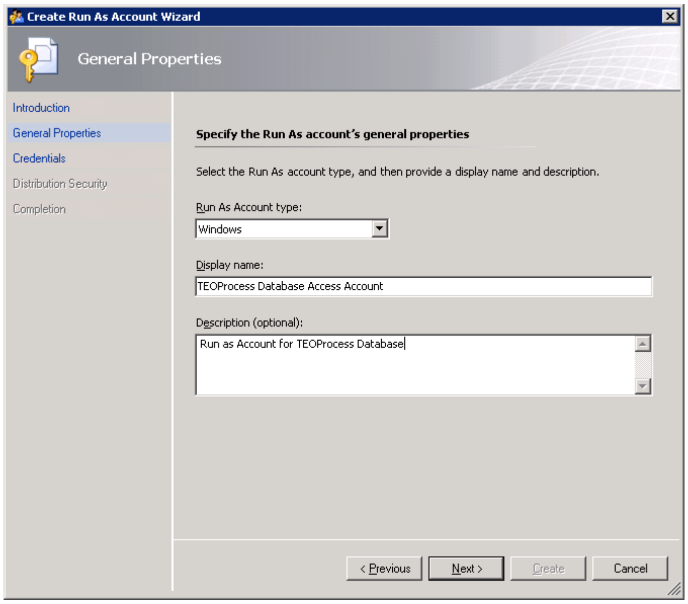
A Run As account may be used by one or more Run As profiles.

To continue the Run As Account Wizard, click Next.

☐ Do not show this page again

Step 3 Click **Next** to display the General Properties panel.

Figure A-3 Create Run As Account—General Properties



Specify the Run As account's general properties

Select the Run As account type, and then provide a display name and description.

Run As Account type: Windows

Display name: TEOProcess Database Access Account

Description (optional): Run as Account for TEOProcess Database

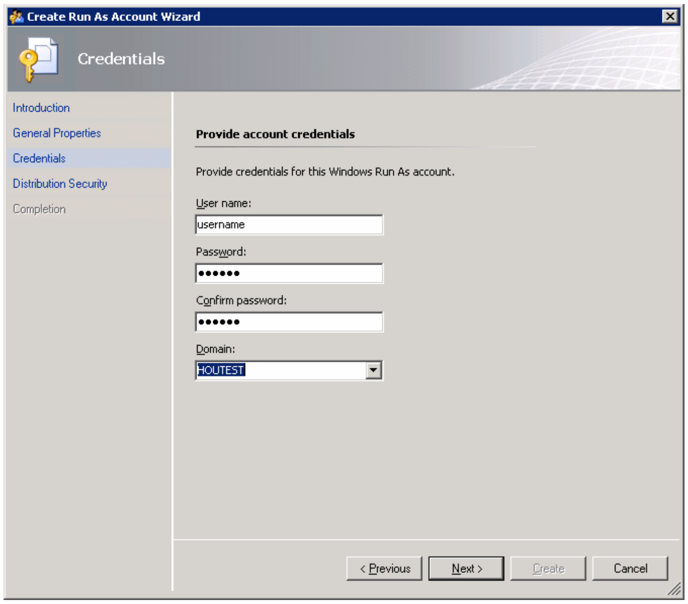
Use this panel to specify the *Run As Account* type, name for the account and an optional description for the account.

Step 4 Specify the information in the following fields:

Field	Description
Run As Account type	Indicates the type of authentication that the account provides. Choose **Windows** from the drop-down list.
Display name	Enter a name for the account.
Description	*Optional*. Enter a text description of the account.

Step 5 Click **Next** to display the Credentials panel.

Figure A-4 Create Run As Account—Credentials



Provide account credentials

Provide credentials for this Windows Run As account.

User name: username

Password: ••••••

Confirm password: ••••••

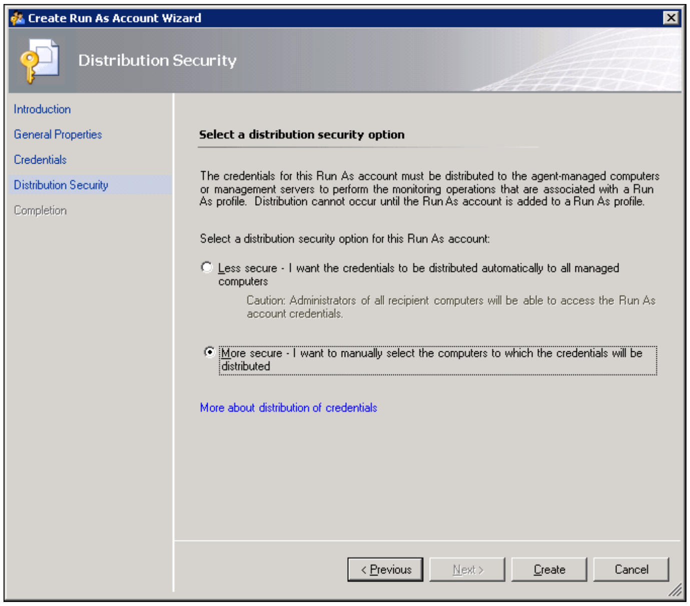
Domain: HOUTEST

Step 6 Use the Credentials panel to specify attributes of the account that you are creating:

Field	Description
User name	Enter the name of the domain or local user account.
Password	Enter the password for the user account.
Confirm password	Re-enter the user account password to confirm it.
Domain	Choose the domain of the user account from the drop-down list.

Step 7 Click **Next** to display the Distribution Security panel.

Figure A-5 Create Run As Account—Distribution Security



Select a distribution security option

The credentials for this Run As account must be distributed to the agent-managed computers or management servers to perform the monitoring operations that are associated with a Run As profile. Distribution cannot occur until the Run As account is added to a Run As profile.

Select a distribution security option for this Run As account:

○ Less secure - I want the credentials to be distributed automatically to all managed computers

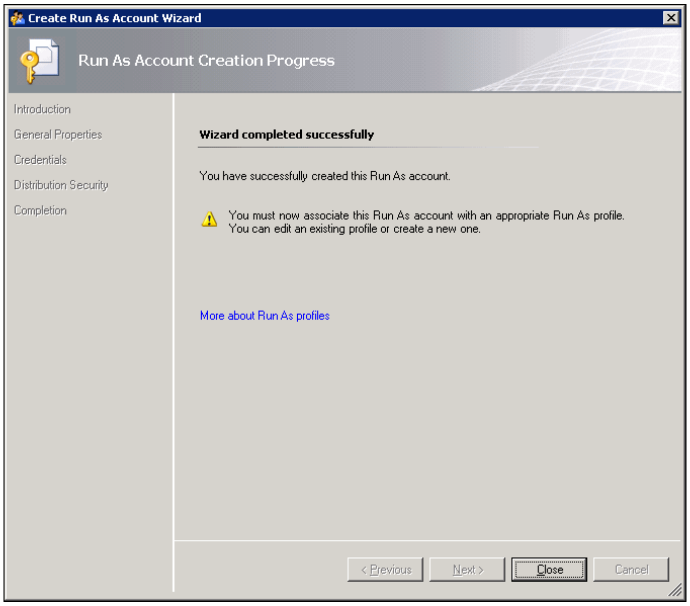
Caution: Administrators of all recipient computers will be able to access the Run As account credentials.

● More secure - I want to manually select the computers to which the credentials will be distributed

More about distribution of credentials

Step 8 Click the **More secure** radio button and then click **Create**.

Figure A-6 Create Run As Account—Completion



Wizard completed successfully

You have successfully created this Run As account.

You must now associate this Run As account with an appropriate Run As profile. You can edit an existing profile or create a new one.

More about Run As profiles

Step 9 On the Completion panel, click **Close** to exit the wizard.

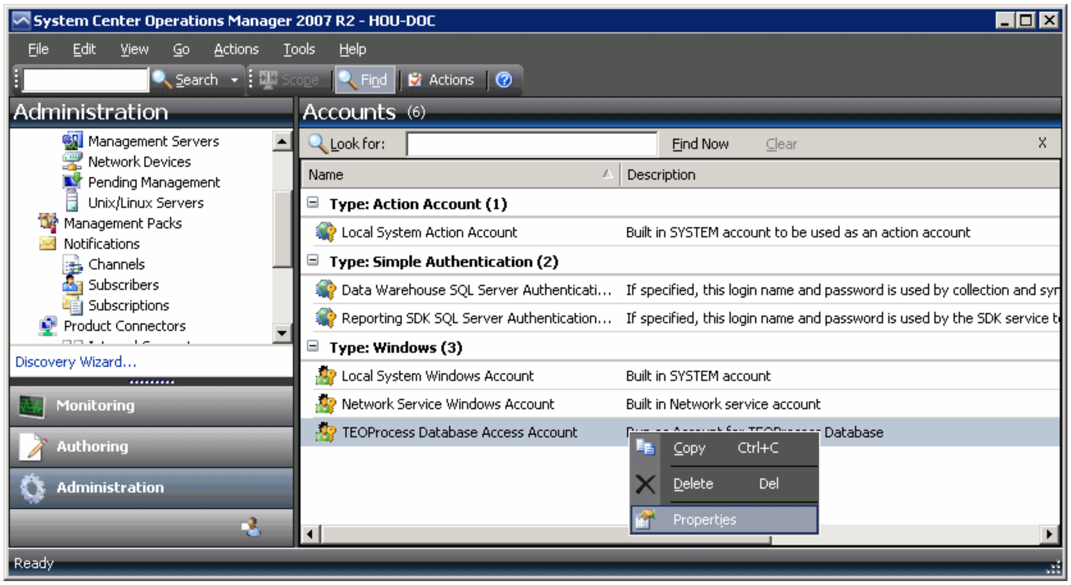
Distributing Run As Account

You must now distribute the *Run As Account* to the TEO server.

Step 1 In the Administration view, expand the **Run As Configuration** node and click **Accounts**.

Step 2 In the Accounts pane, right-click **TEOProcess Database Access Account** and choose **Properties**.

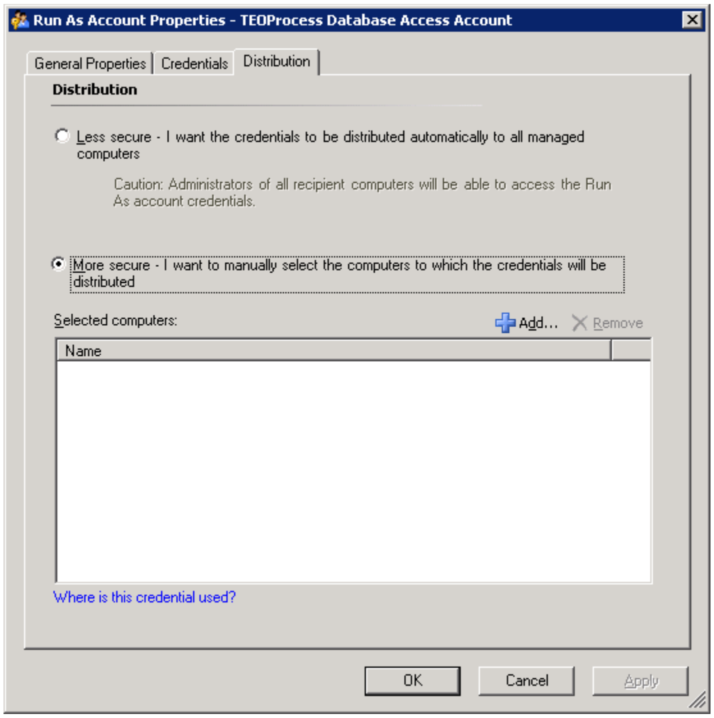
Figure A-7 Run As Account Properties Submenu



Name	Description
Type: Action Account (1)	
Local System Action Account	Built in SYSTEM account to be used as an action account
Type: Simple Authentication (2)	
Data Warehouse SQL Server Authenticati...	If specified, this login name and password is used by collection and syr
Reporting SDK SQL Server Authentication...	If specified, this login name and password is used by the SDK service t
Type: Windows (3)	
Local System Windows Account	Built in SYSTEM account
Network Service Windows Account	Built in Network service account
TEOProcess Database Access Account	Run as Account for TEOProcess Database

Step 3 On the Run As Account Properties dialog box, click the **Distribution** tab.

Figure A-8 Run As Account Properties—Distribution Tab



Run As Account Properties - TEOProcess Database Access Account

Distribution

○ Less secure - I want the credentials to be distributed automatically to all managed computers

Caution: Administrators of all recipient computers will be able to access the Run As account credentials.

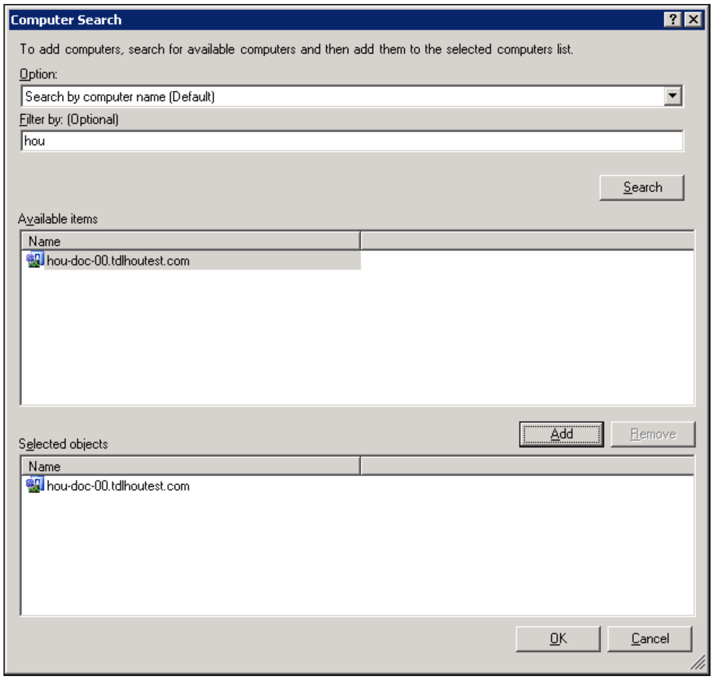
● More secure - I want to manually select the computers to which the credentials will be distributed

Selected computers:

Where is this credential used?

Step 4 Click **Add** to add the computer where the TEOProcess database resides.

Figure A-9 Computer Search



Computer Search

To add computers, search for available computers and then add them to the selected computers list.

Option: Search by computer name (Default)

Filter by: (Optional) hou

Available items: hou-doc-00.tdlhoutest.com

Selected objects: hou-doc-00.tdlhoutest.com

Step 5 Enter the appropriate search options and then click **Search** to find the computer where the TEO service is installed.

Step 6 In the Available items pane, select the computer that you want to add to the Selected objects list and then click **OK**.

The computer displays on the Distribution tab of the Run As Account Properties dialog box.

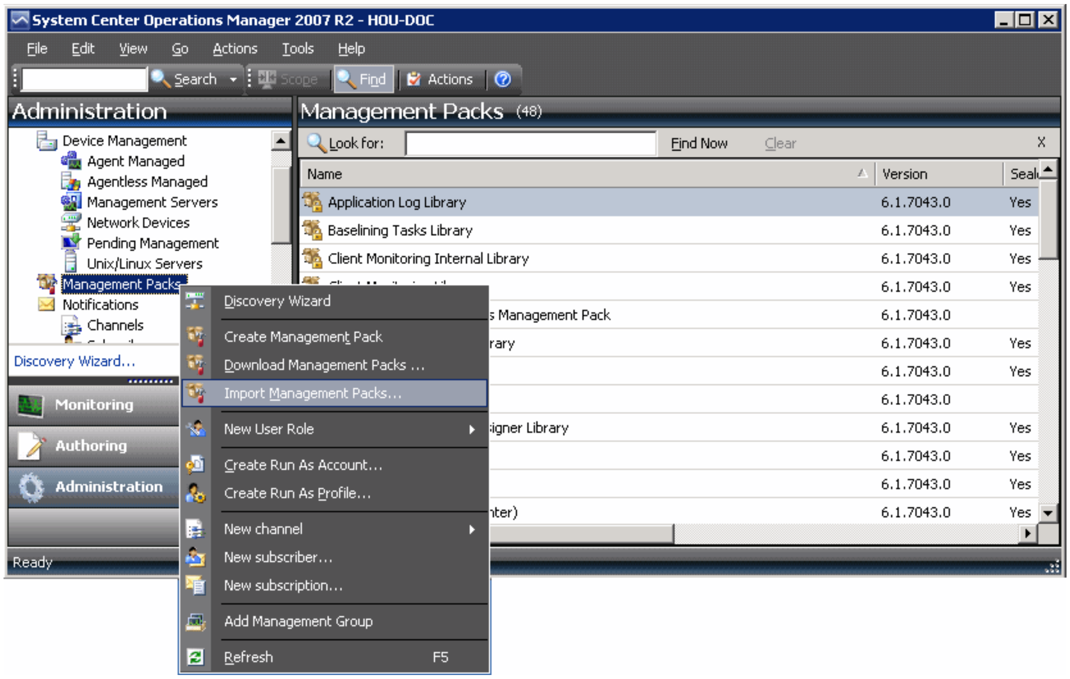
Step 7 Click **OK** to complete the procedure.

Importing Management Pack

You are now ready to import the management pack for SAP monitoring.

Step 1 In the Administration view, right-click **Management Packs** and choose **Import Management Packs**.

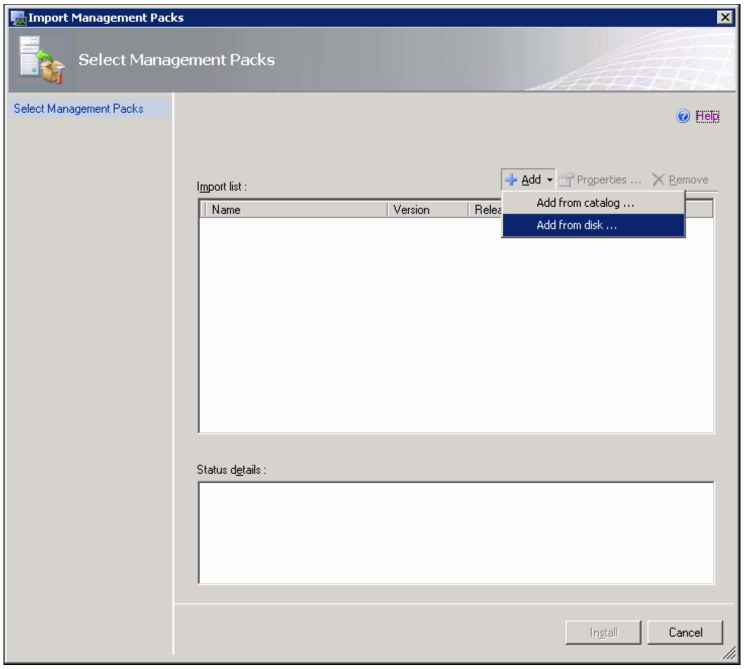
Figure A-10 Import Management Packs Submenu



Name	Version	Seal
Application Log Library	6.1.7043.0	Yes
Baselining Tasks Library	6.1.7043.0	Yes
Client Monitoring Internal Library	6.1.7043.0	Yes
	6.1.7043.0	Yes
s Management Pack	6.1.7043.0	
rary	6.1.7043.0	Yes
	6.1.7043.0	Yes
	6.1.7043.0	
igner Library	6.1.7043.0	Yes
	6.1.7043.0	Yes
	6.1.7043.0	Yes
nter)	6.1.7043.0	Yes

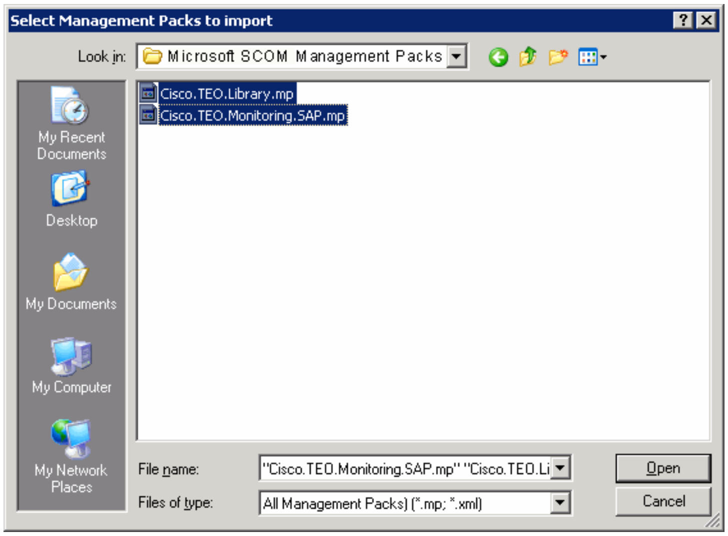
The Import Management Packs wizard opens.

Figure A-11 Import Management Packs—Select Management Packs



Step 2 On the Select Management Packs panel, click **Add** and choose **Add from disk**.

Figure A-12 Select Management Packs to Import



Cisco.TEO.Library.mp
Cisco.TEO.Monitoring.SAP.mp

File name: "Cisco.TEO.Monitoring.SAP.mp" "Cisco.TEO.Li

Files of type: All Management Packs) (*.mp; *.xml)

Step 3 On the Select Management Packs to import dialog box, navigate to the folder where the managment packs were extracted during the Automation Pack Import process. By default, the files are stored in the following directory:

C:\Documents and Settings\User\My Documents\Cisco\Tidal Enterprise Orchestrator\Management Packs

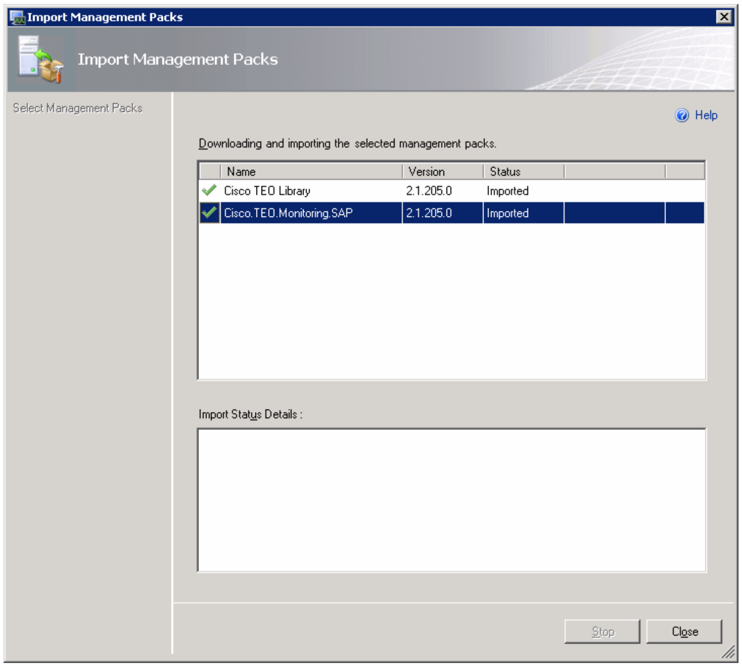
Step 4 Select the following management pack files and click **Open**:

- Cisco.TEO.Library.mp
- Cisco.TEO.Monitoring.SAP.mp

Note The wizard will inform you if additional management packs are required to complete the import. Locate these management packs on your SCOM installation media or SCOM install directory (%ProgramFiles%\System Center Operations Manager 2007).

Step 5 On the Import Management Packs panel, click **Install**.

Figure A-13 Import Management Packs—Import Management Packs



Downloading and importing the selected management packs.

Name	Version	Status
✓ Cisco TEO Library	2.1.205.0	Imported
✓ Cisco.TEO.Monitoring.SAP	2.1.205.0	Imported

Import Status Details :

Step 6 Once the management packs are imported and the Status column displays *Imported*, click **Close** to exit the wizard.

You must now configure the profile for the TEOProcess Database Access Account. Proceed to Creating a Profile for TEOProcess Database Run As Account, page A-12.

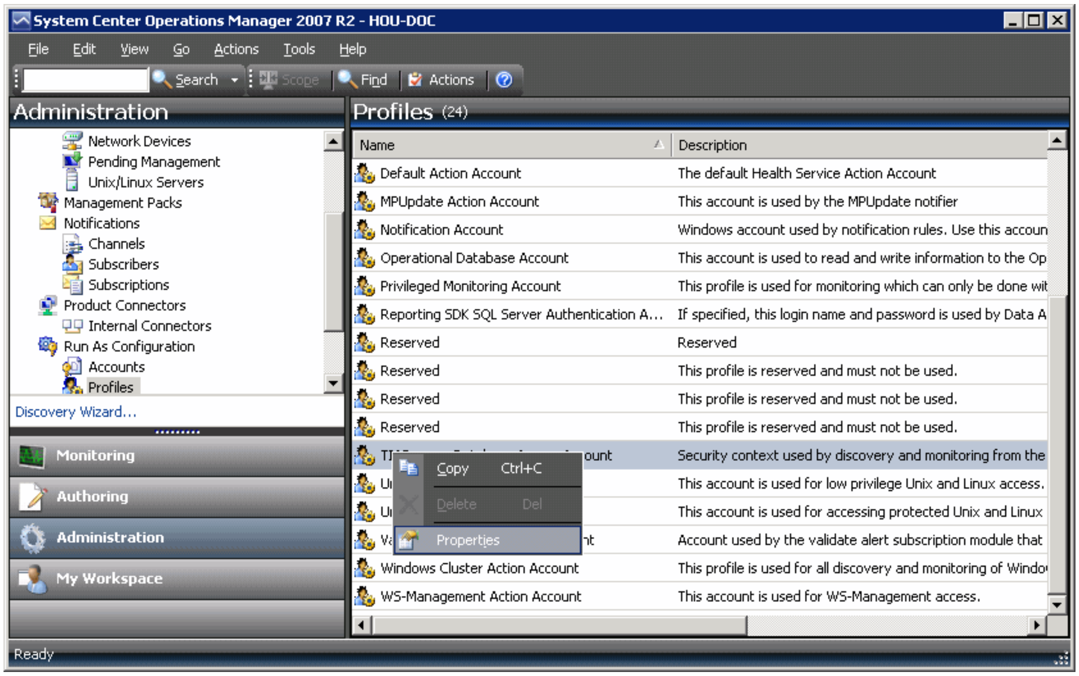
Creating a Profile for TEOProcess Database Run As Account

After the management packs are imported, you must associate the *Run As Profile* with the *Run As Account* created earlier for the TEOProcess database.

Step 1 In the Administration view, expand the **Run As Configuration** node and click **Profiles**.

Step 2 In the Profiles pane, right-click the profile for the TEOProcess Database (**TEOProcess Database Access Account**) and choose **Properties**.

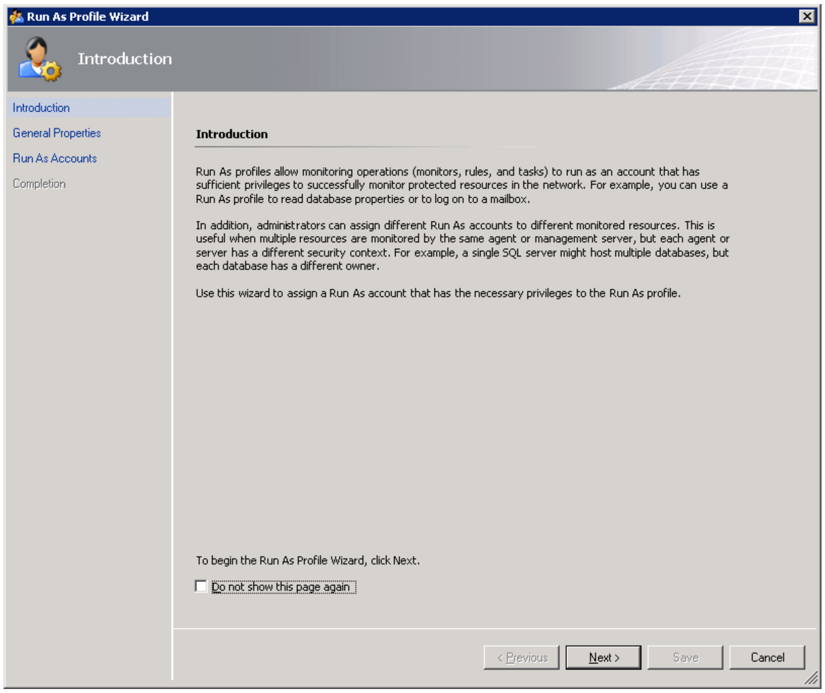
Figure A-14 Accessing TEOProcess Database Profile Properties



Name	Description
Default Action Account	The default Health Service Action Account
MPUpdate Action Account	This account is used by the MPUpdate notifier
Notification Account	Windows account used by notification rules. Use this accoun
Operational Database Account	This account is used to read and write information to the Op
Privileged Monitoring Account	This profile is used for monitoring which can only be done wit
Reporting SDK SQL Server Authentication A...	If specified, this login name and password is used by Data A
Reserved	Reserved
Reserved	This profile is reserved and must not be used.
Reserved	This profile is reserved and must not be used.
Reserved	This profile is reserved and must not be used.
TI ount	Security context used by discovery and monitoring from the
Ui	This account is used for low privilege Unix and Linux access.
Ui	This account is used for accessing protected Unix and Linux
Vi nt	Account used by the validate alert subscription module that
Windows Cluster Action Account	This profile is used for all discovery and monitoring of Windo
WS-Management Action Account	This account is used for WS-Management access.

The Run As Profile wizard opens. You use this wizard to assign a *Run As Account* that has the necessary privileges for the *Run As Profile*.

Figure A-15 Run As Profile—Introduction



Introduction

Run As profiles allow monitoring operations (monitors, rules, and tasks) to run as an account that has sufficient privileges to successfully monitor protected resources in the network. For example, you can use a Run As profile to read database properties or to log on to a mailbox.

In addition, administrators can assign different Run As accounts to different monitored resources. This is useful when multiple resources are monitored by the same agent or management server, but each agent or server has a different security context. For example, a single SQL server might host multiple databases, but each database has a different owner.

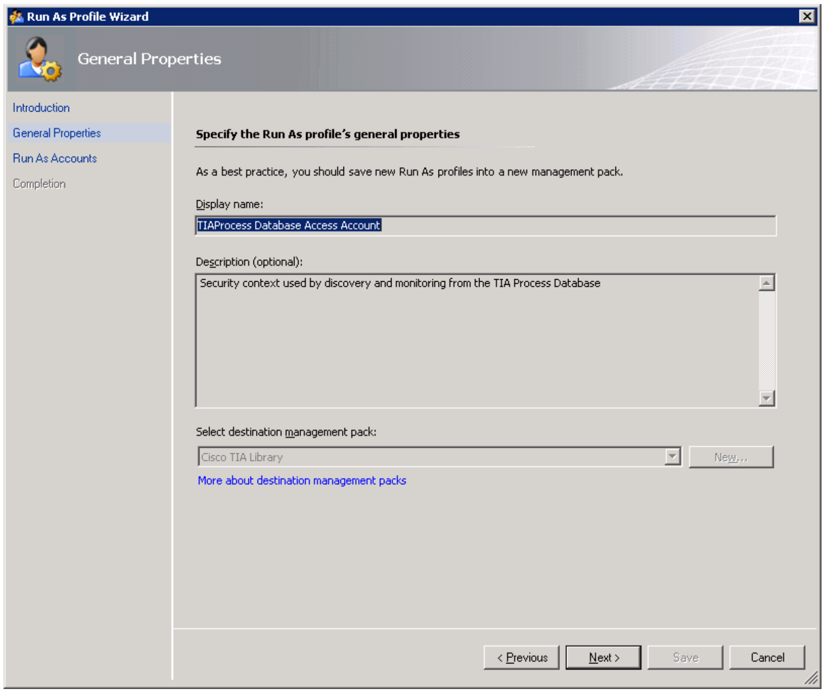
Use this wizard to assign a Run As account that has the necessary privileges to the Run As profile.

To begin the Run As Profile Wizard, click Next.

□ Do not show this page again

Step 3 On the Introduction panel, click **Next**.

Figure A-16 Run As Profile—General Properties



Specify the Run As profile's general properties

As a best practice, you should save new Run As profiles into a new management pack.

Display name:
TIAProcess Database Access Account

Description (optional):
Security context used by discovery and monitoring from the TIA Process Database

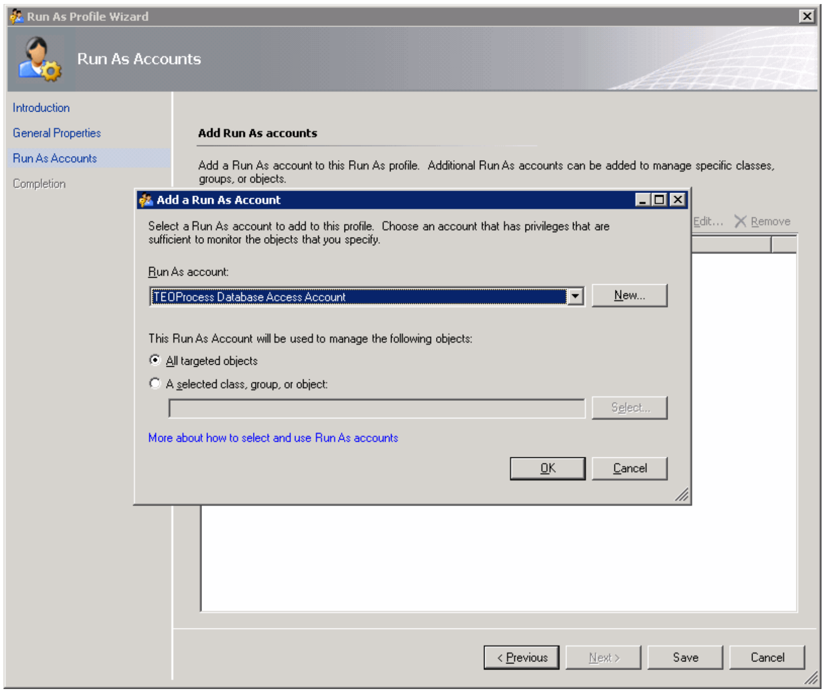
Select destination management pack:
Cisco TIA Library

Step 4 On the General Properties panel, click **Next**.

The Run As Accounts panel displays. Use this panel to add the TEO Process Database *Run As Account* to this *Run As Profile*.

Step 5 Click **Add** to open the Add a Run As Account dialog box.

Figure A-17 Run As Profile—Run As Accounts—Adding a Run As Account



Add Run As accounts

Add a Run As account to this Run As profile. Additional Run As accounts can be added to manage specific classes, groups, or objects.

Select a Run As account to add to this profile. Choose an account that has privileges that are sufficient to monitor the objects that you specify.

Run As account: TEOProcess Database Access Account

This Run As Account will be used to manage the following objects:

● All targeted objects

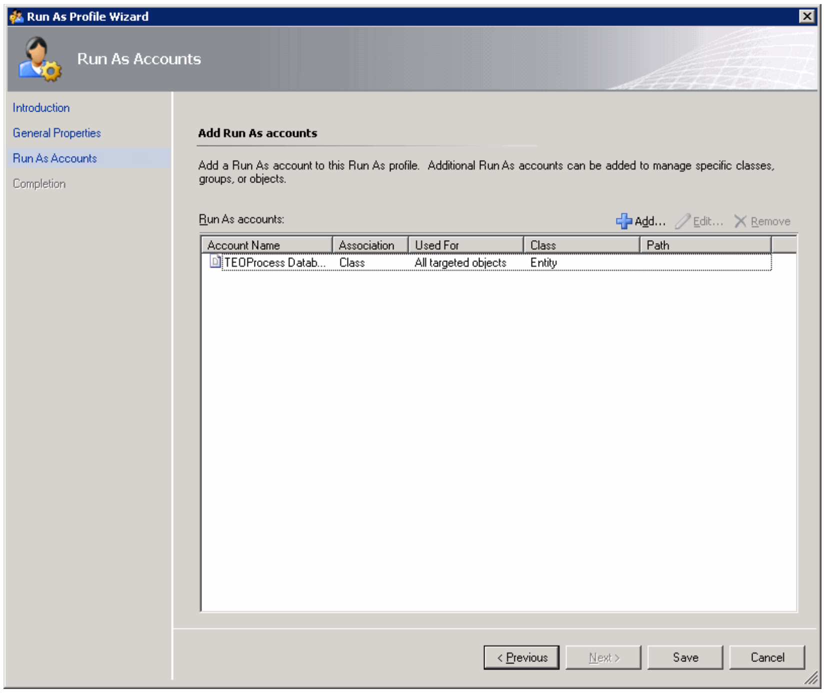
○ A selected class, group, or object:

More about how to select and use Run As accounts

Step 6 On the Add a Run As Account dialog box, choose **TEO Process Database Access Account** from the drop-down list.

Step 7 Click the **All targeted objects** radio button and then click **OK**.

Figure A-18 Run As Profile—Run As Accounts with Account Added



Add Run As accounts

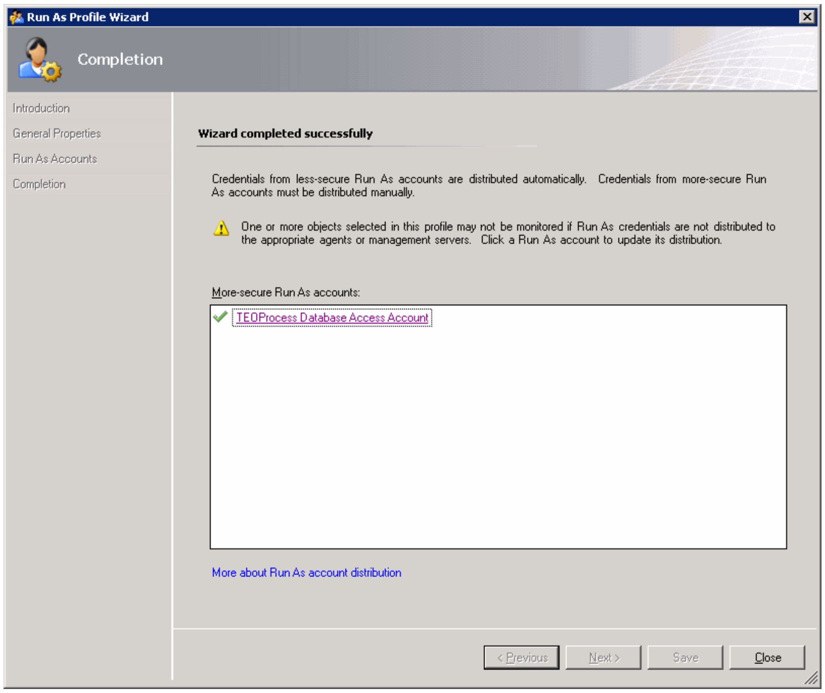
Add a Run As account to this Run As profile. Additional Run As accounts can be added to manage specific classes, groups, or objects.

Run As accounts:

Account Name	Association	Used For	Class	Path
TEOProcess Datab...	Class	All targeted objects	Entity	

Step 8 On the Run As Accounts panel, click **Save**.

Figure A-19 Run As Profile—Completion



Wizard completed successfully

Credentials from less-secure Run As accounts are distributed automatically. Credentials from more-secure Run As accounts must be distributed manually.

⚠ One or more objects selected in this profile may not be monitored if Run As credentials are not distributed to the appropriate agents or management servers. Click a Run As account to update its distribution.

More-secure Run As accounts:

✓ TEOProcess Database Access Account

More about Run As account distribution

Step 9 On the Completion panel, click the **TEO Process Database Access Account** link in the More-secure Run As accounts pane to update the distribution of the credentials. When distribution has been verified, the warning symbol changes to a green checkmark.

Step 10 Click **Close** to exit the wizard and complete the procedure.

Enabling SAP Alerts on Windows Event Log Process

The SAP Alerts on Windows Event Log process is disabled by default in TEO. To receive alerts in SCOM, you must enable this process in TEO.

Step 1 On the Console Definitions workspace, click **Processes** in the navigation pane.

Step 2 Click the **Filter by** link and choose **Automation Pack > Core Automation for SAP** to display the processes.

Step 3 Right-click the **Publish SAP Alerts on Windows Event Log** process and choose **Enable**.

CHAPTER B

Installing the SPI for HP OpenView

Tidal Enterprise Orchestrator (TEO) can be integrated with HP Openview (HPOV) if you are using this framework to monitor all alerts from a central location in your environment.

This appendix guides you through installing the TEO modules for HPOV, configuring the HPOV services and deploying the policies. It includes the following sections:

- Prerequisites, page B-1
- Installing TEO HP OpenView SPI, page B-2
- Configuring HP OpenView, page B-5
- Enabling SAP Alerts on Windows Event Log Process, page B-9

Prerequisites

The following prerequisites should be met to successfully run TEO automation packs with the HPOV management framework:

Prerequisite	Description
HP OpenView Operations for Windows® Version 7.x or later	To integrate with HP Open View, you must have the HP OpenView agent installed and configured prior to installing TEO. For information on installing HP OpenView, refer to the documentation that shipped with the product or visit the HP web site at www.hp.com. A should be installed on the TEO server prior to importing the management packs.

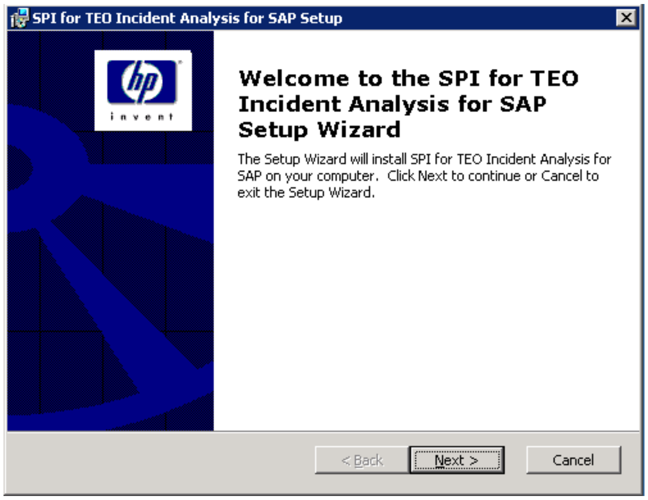
Installing TEO HP OpenView SPI

Note The procedures in this chapter are for HP OpenView v7.2. If you have an earlier version installed, the procedures and screenshots may be different.

If you are using HP OpenView to monitor alerts in your environment, you must install the SPI for TEO Incident Analysis for SAP on the HP OpenView management framework using the SPI for TEO Incident Analysis Setup wizard.

Step 1 On the Tidal Enterprise Orchestrator installation CD, navigate to the **ManagementFramework > HPOV** folder and double-click **TEASAPSPI.msi** to open the SPI for TEO Incident Analysis for SAP Setup wizard.

Figure B-1 Welcome to the SPI for TEO Incident Analysis for SAP Setup Wizard

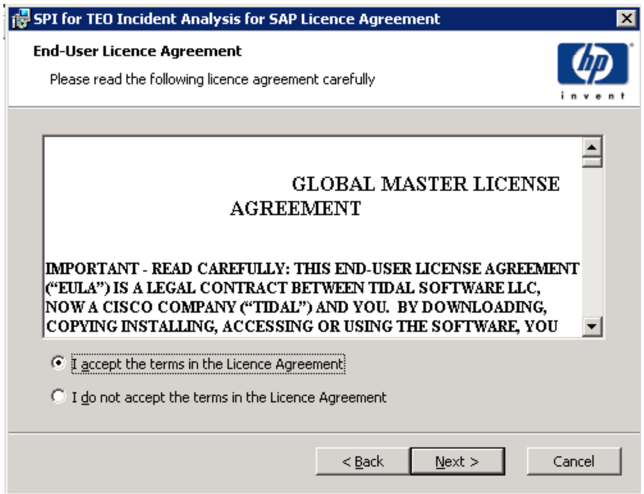


Welcome to the SPI for TEO Incident Analysis for SAP Setup Wizard

The Setup Wizard will install SPI for TEO Incident Analysis for SAP on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Step 2 On the Welcome panel, click **Next**.

Figure B-2 End-User License Agreement



SPI for TEO Incident Analysis for SAP Licence Agreement

End-User Licence Agreement

Please read the following licence agreement carefully

GLOBAL MASTER LICENSE AGREEMENT

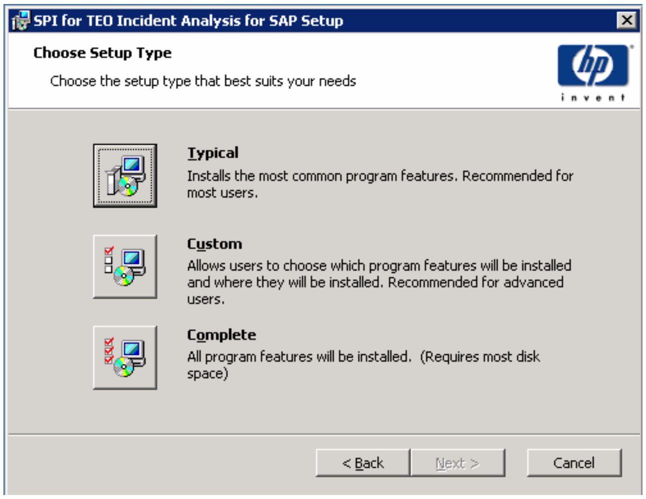
IMPORTANT - READ CAREFULLY: THIS END-USER LICENSE AGREEMENT ("EULA") IS A LEGAL CONTRACT BETWEEN TIDAL SOFTWARE LLC, NOW A CISCO COMPANY ("TIDAL") AND YOU. BY DOWNLOADING, COPYING INSTALLING, ACCESSING OR USING THE SOFTWARE, YOU

● I accept the terms in the Licence Agreement

○ I do not accept the terms in the Licence Agreement

Step 3 On the End-User License Agreement panel, click the **I accept the terms in the License Agreement** radio button and then click **Next**.

Figure B-3 Choose Setup Type



SPI for TEO Incident Analysis for SAP Setup

Choose Setup Type

Choose the setup type that best suits your needs

Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

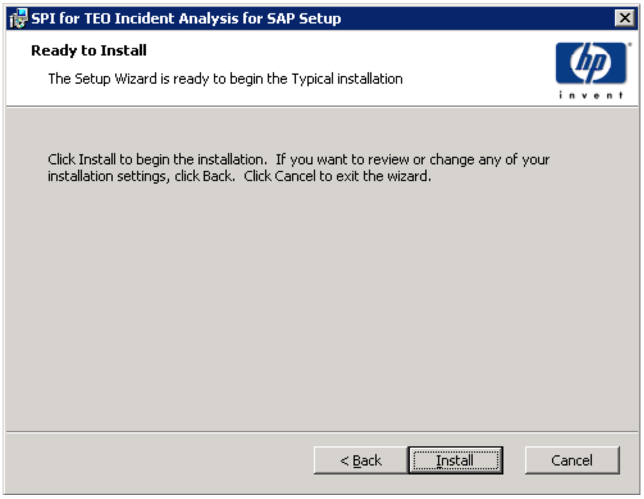
Complete
All program features will be installed. (Requires most disk space)

Step 4 On the Choose Setup Type panel, click one of the following setup options:

- Typical—Installs the most common program features (recommended for most users).
- Custom—Allows you to choose which program features will be installed and where they will be installed (recommended for advanced users.
- Complete—All program features will be installed (requires the most disk space).

Note The following steps are for a Typical setup.

Figure B-4 Ready to Install



SPI for TEO Incident Analysis for SAP Setup

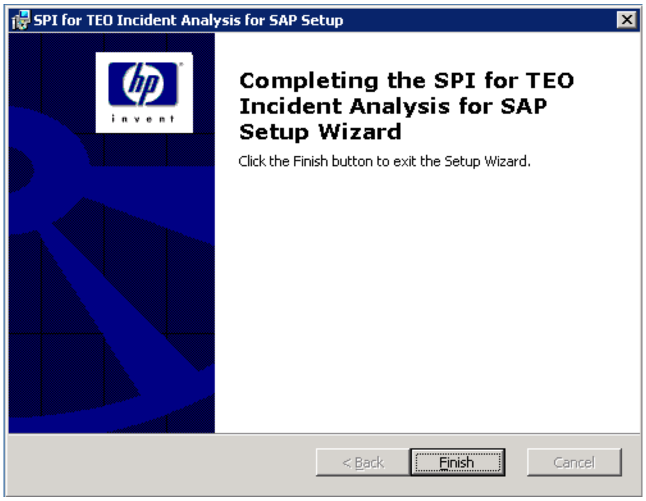
Ready to Install

The Setup Wizard is ready to begin the Typical installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 5 On the Ready to Install panel, click **Install** to begin the installation.

Figure B-5 Completing SPI for TEO Incident Analysis for SAP Setup Wizard



SPI for TEO Incident Analysis for SAP Setup

Completing the SPI for TEO Incident Analysis for SAP Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 6 On the Completing panel, click **Finish**.

Configuring HP OpenView

You must now configure the services and deploy the policies in HP OpenView.

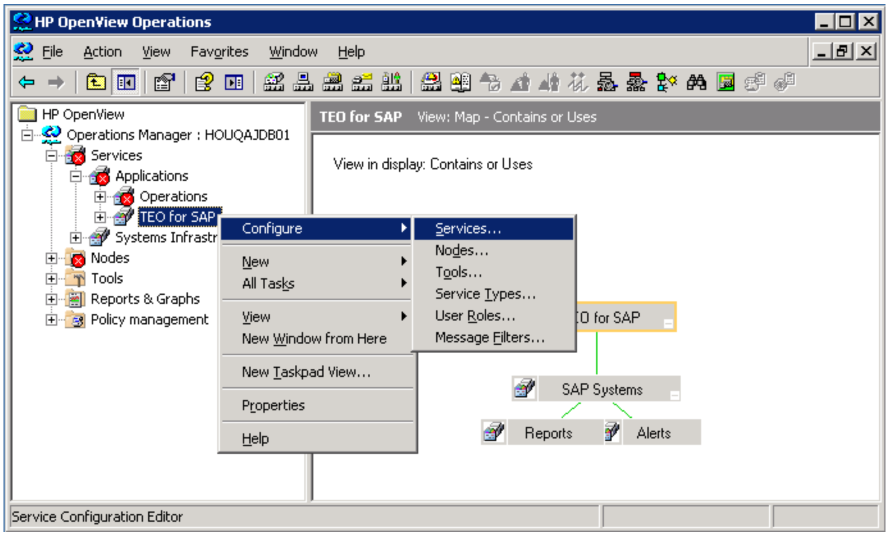
Configuring Services

You must configure the Services in the HP OpenView Operations Console with your system information. This enables you to view incidents for individual systems instead of a combined view of all incidents.

Step 1 Open the HP OpenView Operations Console and navigate to the **Services > Applications** container.

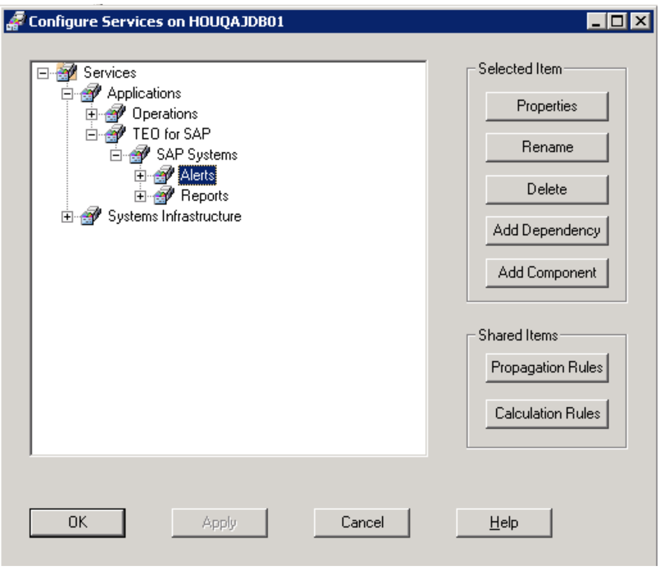
Step 2 Right-click **TEO for SAP** and choose **Configure > Services** from the submenus.

Figure B-6 Configure Services Submenus



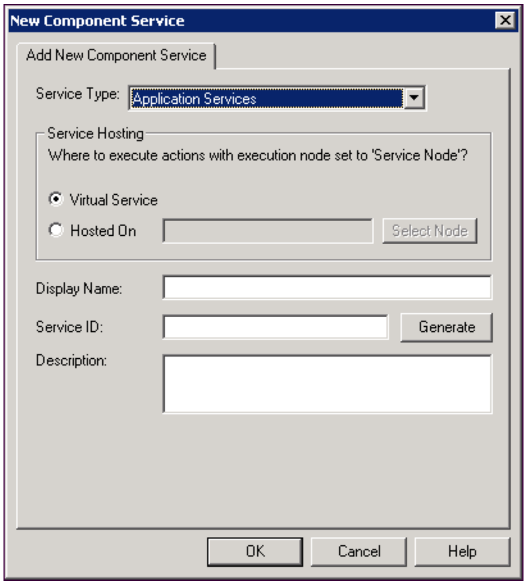
Step 3 On the Configure Services dialog box, expand the **Applications > TEO for SAP > SAP Systems** containers.

Figure B-7 Configure Services



Step 4 Click the **Alerts** container and then click **Add Component**.

Figure B-8 New Component Service



Step 5 From the Service Type drop-down list, choose **Application Services**.

Step 6 In the Display Name text field, enter the name of the system.

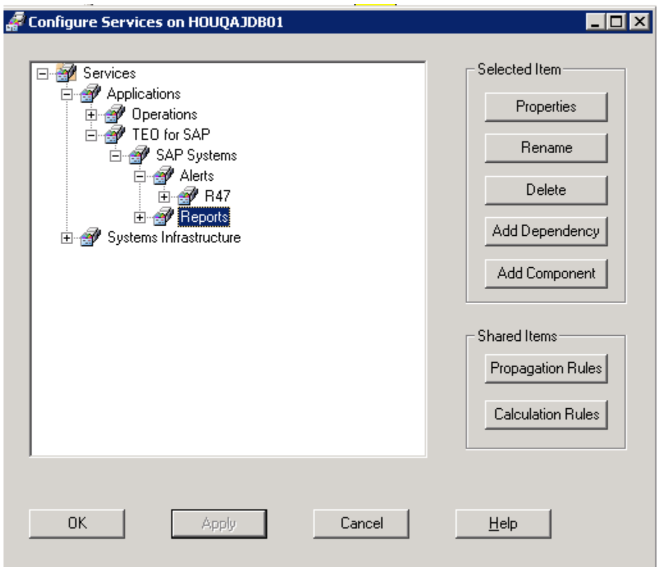
Step 7 In the ServiceID text field, enter **TEOSAPAlerts<space>SAP system name** (for example, enter *TEOSAPAlerts R47*) and then click **OK**.

The newly added component displays on the Configure Services dialog box under Alerts.

Step 8 Click **Apply**.

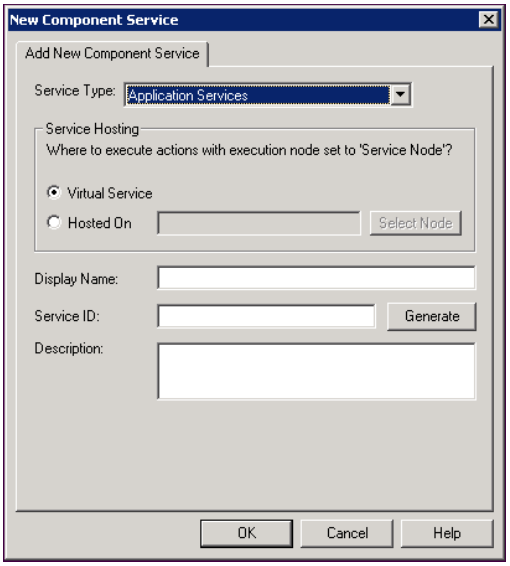
Step 9 On the Configure Services dialog box, click **Reports**.

Figure B-9 Configure Services—Reports



Step 10 Click **Add Component**.

Figure B-10 New Component Service



Service Type: Application Services

Service Hosting
Where to execute actions with execution node set to 'Service Node'?

● Virtual Service
○ Hosted On

Step 11 On the New Component Service dialog box, choose **Application Services** from the Service Type drop-down list.

Step 12 In the Display Name text field, enter the name of the system.

Step 13 In the ServiceID text field, enter **TEOSAPReports<space>SAP system name** (for example, enter *TEOSAPReports R47*) and then click **OK**.

The newly added component displays on the Configure Services dialog box under Reports.

Step 14 Click **Apply**.

Step 15 Click **OK** to to close the dialog box and complete the procedure.

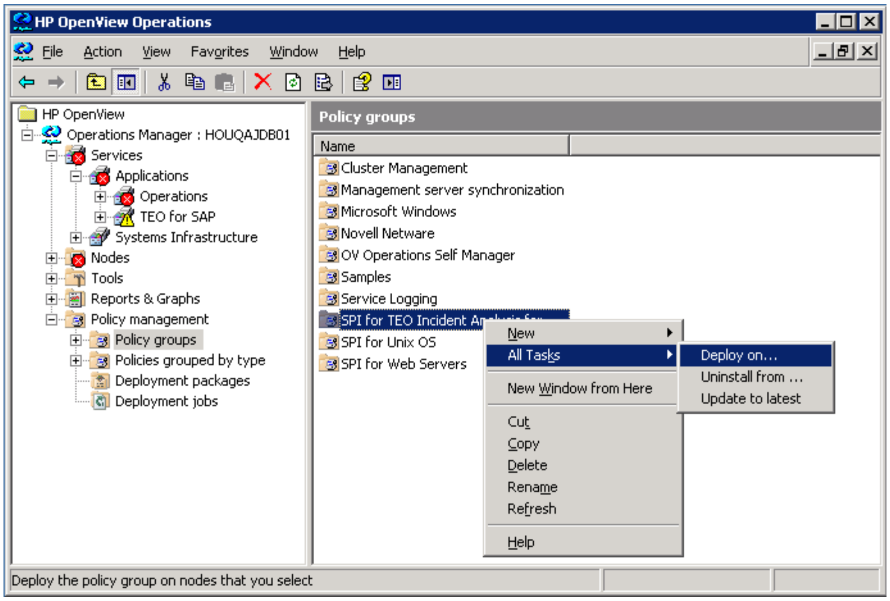
Deploying TEO Policies

You must now deploy the TEO policies on the node where TEO is installed.

Step 1 In the HP OpenView Operator Console, navigate to the **Policy management** node and click **Policy groups**.

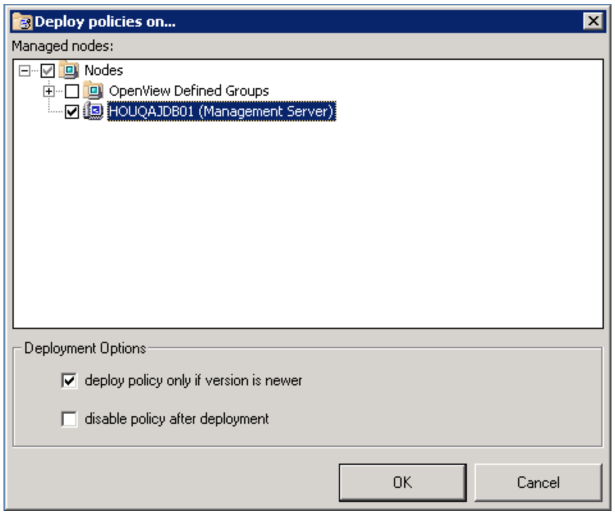
Step 2 In the details pane, right-click **SPI for TEO Incident Analysis for SAP** and choose **All Tasks > Deploy on**.

Figure B-11 Deploying Policies



The Deploy policies on dialog box displays.

Figure B-12 Deploy Policies On



☑ deploy policy only if version is newer

□ disable policy after deployment

Step 3 Check the checkbox for the HPOV agent that is installed on the TEO server.

Step 4 Under Deployment Options, check the **deploy policy only if version is newer** check box and click **OK** to complete the procedure.

Enabling SAP Alerts on Windows Event Log Process

The SAP Alerts on Windows Event Log process is disabled by default in TEO. To receive alerts in HPOV, you must enable this process in TEO.

Step 1 On the TEO Console Definition workspace, click **Processes** in the navigation pane.

Step 2 Using the **Filter by** link, choose **Automation Pack > Core Automation for SAP** to display the processes.

Step 3 Right-click the **Publish SAP Alerts on Windows Event Log** process and choose **Enable**.

APPENDIX C

Understanding the Core Automation for SAP Content

The Cisco TEO Automation Pack for Core Automation for SAP contains content that is used in the other SAP-related automation packs.

This appendix contains the content included in the Core Automation for SAP automation pack. It contains the following sections:

- Automation Pack Content, page C-1
- Automation Pack Dependencies, page C-4

Automation Pack Content

Use the automation pack Properties dialog box to view the content (objects) included in the automation pack. For instructions on accessing the automation pack properties, see the Accessing Automation Pack Properties, page 2-2.

Core Automation for SAP Task Rules

The following table contains the task rule that is imported by the Core Automation for SAP automation pack.

Task Rule	Description
SAP Default Assignment	Default user or group who will be assigned all SAP-related incidents.

For information on configuring Task Rules, *see* Using Task Rules for Assignments and Notifications, page 3-8.

Core Automation for SAP Global Variables

The following table contains the global variables that are imported by the Core Automation for SAP automation pack.

Global Variable Name	Description
SAP Alert Suppression Time	Used to specify the time TEO SAP alerts will be suppressed when duplicated. After this time, a new alert and incident will be created. Enter the time in seconds.
Transaction Analyzer Report Location	If you have Cisco Tidal Transaction Analyzer installed, you use this URL to access Tidal Transaction Analyzer reports folder.

For instructions on configuring global variables, *see* Managing Global Variables, page 3-27.

Core Automation for SAP Processes

The Core Automation for SAP automation pack contains support processes that may be triggered by alerts and incidents from processes in the other SAP automation packs. You must enable the processes that will be used in your environment before the other processes can be successfully executed.

For instructions on enabling processes, *see* Managing Incident Analysis for SAP Processes, page 4-1.

The following table contains the processes that are imported by the Core Automation for SAP automation pack.

Process Name	Description
Disable SAP System Monitoring	Allows users to disable the SAP system in TEO. This process can be used as an example to create custom processes to disable/enable SAP system monitoring during scheduled downtime.
Enable SAP System Monitoring	Allows users to enable the SAP system in TEO. This process can be used as an example to create custom processes to disable/enable SAP system monitoring during scheduled downtime.
Example – Transaction Analyzer Link	Example process for linking to Transaction Analyzer.
Publish SAP Alerts on Windows Event Log	Alerts created by processes in the Automation for SAP BW and BWA automation pack will create events in the Windows event log in the TEO server. This is necessary for integration with management frameworks such as Microsoft SCOM 2007 and HP OpenView for Windows. **Note** This process must be enabled if you have integrated TEO with SCOM 2007 or HP OpenView.
Reset SAP System Alerts and Incidents	Closes all the alerts and incidents for the selected SAP system in TEO.

Process Name	Description
SAP Adapter Connection Issue	Monitors the health of TEO connection to SAP systems.
SAP Process Execution Error	Raises an incident when there are errors in activities executed in SAP processes.

Core Automation for SAP Target Groups

The Core Automation for SAP automation pack provides the target groups that are used by the SAP processes. Most of the target groups are automatically populated with members when the targets are configured. For those that are not automatically populated, you must manually add the members. For information on adding members to target groups, *see* the *Tidal Enterprise Orchestrator Reference Guide*.

The following table contains the target groups that are imported by the Core Automation for SAP automation pack.

Target Group Name	Description	Automatically Populated with Members
All Cisco UCS Managers (SAP)	All UCS Managers.	Yes
All SAP ABAP	All SAP systems configured with component ABAP.	Yes
All SAP ABAP 46C	All SAP systems configured with component ABAP and version 46C.	Yes
All SAP ABAP non 46C	All SAP systems configured with component ABAP and not version 46C.	Yes
All SAP BI Warehouse	All SAP BI Warehouse targets.	Yes
All SAP Java	All SAP systems configured with component Java.	Yes
All SAP Systems	All SAP systems.	Yes
All SAP Systems – DB2 Mainframe	All SAP systems configured with database DB2 Mainframe.	Yes
All SAP Systems – DB2 UDB	All SAP systems configured with database DB2 UDB.	Yes
All SAP Systems – Oracle	All SAP systems configured with database Oracle.	Yes
All SAP Systems – SQL Server Database	All SAP systems configured with database SQL Server.	Yes
All Unix Servers (SAP)	All Unix servers.	Yes
All Windows Computers (SAP)	All Windows server.	Yes
Location Availability Monitors	Windows computers that have Tidal Availability Monitor Utility installed. Tidal Availability Monitor is used to monitor location availability. Contact Cisco Systems support to download the utility.	No

Core Automation for SAP Categories

The Core Automation for SAP automation pack ships with categories that are used by the SAP processes. The following categories are imported by the Core Automation for SAP automation pack.

- SAP
- SAP APO
- SAP Application Layer
- SAP Availability
- SAP Background Processing
- SAP BW
- SAP Communication
- SAP Configuration
- SAP Database DB2
- SAP Database DB2 Mainframe
- SAP Database Informix
- SAP Database MS SQL Server
- SAP Database Oracle
- SAP Database SAP DB
- SAP Infrastructure ABAP
- SAP Infrastructure J2EE
- SAP Operating System
- SAP Performance Metrics
- SAP PI
- SAP Spool System
- SAP System Errors
- SAP Update
- TEO SAP Examples
- TEO SAP Operations
- TEO SAP Self Monitoring

Automation Pack Dependencies

Use the Dependencies tab on the automation pack Properties dialog box to view the automation packs and adapters referenced by the objects in the automation pack. These objects must be installed prior to importing the Core Automation for SAP automation pack.

For instructions on accessing the automation pack properties, see the Accessing Automation Pack Properties, page 2-2.

Object Type	Dependency
Automation Packs	• Core
Adapters	• Core Functions Adapter • Microsoft Windows Adapter

INDEX

A

ABAP application server 3-4

ABAP system connection information 3-4

about

- installing TEO on SCOM A-1

accessing

- extended target properties 3-22
- global variables 3-27
- task rules 3-8

adding assignees 3-10

approver for SAP incidents, specifying 1-5

assignments and notifications 3-8

Assign Task Rule, creating 3-11, 3-16

automation pack content C-1

Automation Pack Import Wizard

- launching 1-2

C

categories

- Core Automation for SAP C-4

configuring

- global variables 3-28
- HP OpenView B-2
- HP OpenView Services B-5
- security settings, SCOM A-2

configuring task rules 3-9

connection information

- SAP ABAP system, specifying 3-4

connection string 3-6

copying task rules 3-20

Core Automation for SAP automation pack

- importing 1-1, 1-4

creating

- Assign Task Rule 3-11, 3-16
- Notify Task Rule 3-17
- runtime user 3-2
- Update Task Rule 3-18

credentials

- SAP ABAP system, specifying 3-4
- SAP User 3-2, 3-3

D

default

- recipient for SAP incidents, specifying 1-5
- runtime user, specifying 3-5

deleting task rules 3-20

deploy

- TEO policies in HP OpenView B-8

disabling task rule 3-19

distributing Run As account in SCOM A-7

E

email notifications 3-8

enabling

- notification based on assignment processes 3-21
- task rule 3-19

extended target properties

- accessing 3-22
- managing 3-22

F

filtering
- global variables 3-27

G

global variables 3-27
- accessing 3-27
- Core Automation for SAP C-2
- filtering 3-27
- properties 3-28

H

HP OpenView
- configuring B-2
- operations console B-5
- services, configuring B-5
- specifying service B-6

I

importing
- Core Automation for SAP automation pack 1-1, 1-4
- Core SAP Automation automation pack 1-2
- SAP management pack in SCOM A-9
- TEO modules in HP OpenView B-2

Incident Analysis for SAP reports, location 1-9

J

Java monitoring 3-7

M

management framework
- HP OpenView, configuring B-2

management server
- properties, SCOM A-2

managing
- extended target properties 3-22
- global variables 3-27
- task rules 3-19

modifying
- global variable 3-28

monitoring
- SAP ABAP application server 3-4
- server availability 3-6

N

New SAP System Wizard 3-4

Notify Task Rule, creating 3-17

O

objects, viewing 2-3

P

policies, deploy in HP OpenView B-8

policy management node B-8

processes
- Core Automation for SAP C-2
- notification based on assignment 3-21

properties
- automation packs 2-3
- global variable 3-28

R

reports
- specifying location 1-9

Run As account, creating in SCOM A-2

runtime user

creating 3-2

S

SAP database 3-6

SAP incidents and approvals

specifying default 1-5

SAP User

credentials, specifying 3-2, 3-3

SCOM

creating profile for TEOProcess database A-12

creating Run As account A-2

distributing Run As account A-7

importing management packs A-9

installing TEO A-1

prerequisites for management pack A-1, B-1

security settings, configuring A-2

setup tasks A-2

server availability

specifying servers 3-6

server proxy, configuring in SCOM A-2

services, HP Openview B-5

sorting task rules 3-20

specifying

availability monitoring 3-6

default runtime user 3-5

Incident Analysis for SAP reports location 1-9

Java application server 3-7

SAP incidents approver 1-5

SAP incidents recipient 1-5

SAP User credentials 3-2, 3-3

T

target groups

Core Automation for SAP C-3

task rules 3-8, 3-10

accessing 3-8

assign 3-11

conditions 3-13

configuring 3-9

copying 3-20

deleting 3-20

disabling 3-19

enabling 3-19

General properties 3-12

managing 3-19

sorting 3-20

task types 3-12

TEO

modules, importing in HP OpenView B-2

policies, deploying in HP OpenView B-8

U

Update Task Rule, creating 3-18

V

viewing

automation pack content C-1

automation pack properties 2-3

Core Automation for SAP categories C-4

Core Automation for SAP global variables C-2

Core Automation for SAP processes C-2

Core Automation for SAP target groups C-3