Adeptia Suite 5.3 Administrator Guide

Version 1.0
Release Date March 19, 2012

Adeptia Inc.
443 North Clark Ave,
Suite 350
Chicago, IL 60610, USA
Phone: (312) 229-1727

DOCUMENT INFORMATION

Adeptia Suite

Administrator Guide

Adeptia Suite Version 5.3

Printed February 2012

Printed in USA

Adeptia Support Information

For support queries, please contact us at *support@adeptia.com*.
Access the Adeptia Web site at the following URL:

www.adeptia.com

Copyright

Trademarks

Confidentiality

Disclaimer

TABLE OF CONTENTS

1

PREFACE

This document provides a detailed description of the Administrative features of Adeptia Suite. It guides you to seamlessly manage the functioning, design and integration of business processes using these administrative features.

The administration of Adeptia Suite involves creation and management of users, groups and business roles. The Administrator's role also involves configuration of system properties, creating database connectors, ensuring system security and monitoring system status.

Target Audience

The Administrative features are used primarily by the Administrator, Sys Admin and Group Admin of organizations.

Pre-requisites

You must have administrative rights to perform administrative tasks. These rights vary based upon the user type..

Other resource materials

The following other resource materials are available.

Title	Description
Installation Guide	This guide is intended for developers. They can use these details to perform all the design features of Adeptia Suite.
Getting Started Guide	This document is intended as a reference for those working with Adeptia Suite for the first time.
Business User Guide	This guide is intended for business users. They can use this guide to perform all the functions of Adeptia Suite.

HOW IS THIS GUIDE ORGANIZED?

This guide is organized into the following sections:

Section	Description
Preface	Introduction to this document
Administering Adeptia Suite	Configuration of system properties, creating database connectors, ensuring system security and monitoring system status
Managing Application and System Settings	System Configuration and updating System Properties of the Adeptia Suite
Creating and Managing User Groups	Creating a user group, viewing properties of a user group, editing properties of a user group and deleting a user group
Creating a User	Creating a user, view properties of a user, editing properties of user, moving objects of a user and deleting a user.
Creating a Business Role	Minimizing the work of a user of *Sys Admin* or *Group Admin* type
Managing Kernel and Scheduler	Understanding Process Flow Status when Kernel or Scheduler is started, paused, or stopped.
Managing Secret Key	Creating, Exporting, and Importing Secret Key, Creating Keystore, Exporting Certificate from the Keystore, Importing Certificate into the Keystore

CONVENTIONS

The following tables list the various conventions used in Adeptia documentation. We follow these conventions to help you quickly and easily identify particular elements, processes, and names that occur frequently in documents.

Typographical conventions

This guide uses the following typographical conventions:

Convention	Description
Bold text	Indicates one of the following: ▪ Screen element ▪ New terminology ▪ A file or folder name ▪ A control in an application's user interface ▪ A registry key ▪ Important information
Italic text	Indicates a reference or the title of a publication.
`Monospaced text`	Indicates code examples or system messages.
`Monospaced bold text`	Indicates system commands that you enter.
Hyperlink	Indicates an Internet link to target material.

Graphical conventions

This guide uses the following graphical conventions:

Convention	Description
	Indicates additional information that may be of interest to the reader.
	Indicates cautions that, if ignored, can result in damage to software or hardware.

CONTACTS/REPORTING PROBLEMS

These sections present contact information for a variety of situations.

Sales

In case of any sales queries, please contact us at *sales@adeptia.com*.

Support

For support queries, please contact us at *support@adeptia.com*.

Latest updates and information

For the latest updates and information, please visit us at *www.adeptia.com*.

Adeptia Web site

Access the Adeptia Web site at the following URL:
www.adeptia.com

2

ADMINISTERING ADEPTIA SUITE

The administration of Adeptia Suite involves creation and management of users, groups and business roles. The Administrator's role also involves configuration of system properties, creating database connectors, ensuring system security and monitoring system status.

Prerequisites

You must have administrative rights to perform administrative tasks. These rights vary based upon the user type

ADMINISTRATIVE RIGHTS OF USERS

Administrative rights vary based on the user type. The *Administrator* is pre-created in Adeptia and is entitled to all administrative tasks. The other users are created by the Administrator.

The Administrator creates the following types of users:

- Sys Admin
- Group Admin
- Business User
- Developer

Sys Admin

A *Sys Admin* user has permissions equivalent to the Administrator. He can create and delete users and groups as well as perform all the tasks of a group admin, business or user developer. However, only Admin and Sys Admin users can update system properties, enable clustering, stop/pause the kernel and restart scheduler.

Group Admin

Each group has one or more "*admin*", who is able to manage the users within that group. A *Group Admin* can create, edit and delete users within its group. He *can* also change the permissions of users and perform all the tasks of a developer.

Business User

A *Business user* has restricted rights. A *Business user* can only execute process flow, complete Human Workflow task and monitor the logs.

Developer

A Developer can create all drivers and connectors. He also has the right to create and manage secret keys and monitor system status.

3

MANAGING APPLICATION AND SYSTEM SETTINGS

Users of *Admin* and *Sys Admin* type can view System Configuration and update System Properties of the Adeptia Suite.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

This chapter describes the following tasks:

- Viewing System Configuration
- Updating System Properties
- Reloading System Configuration

VIEWING SYSTEM CONFIGURATION

The System configuration module displays the Adeptia Suite related information such as Java Classpath, Database Information, Session Time Out and Process Flow Recovery Settings etc. System configurations are non-editable and can be viewed only by the *Admin* for troubleshooting purposes.

Steps to view System Configuration

1. Click **[+] Administer** to expand the tree and then click **[+] Setup**. All items in the **Setup** category are displayed.

2. Click **Application Settings**. The **Application Settings** screen is displayed (see **Error! Reference source not found.**).

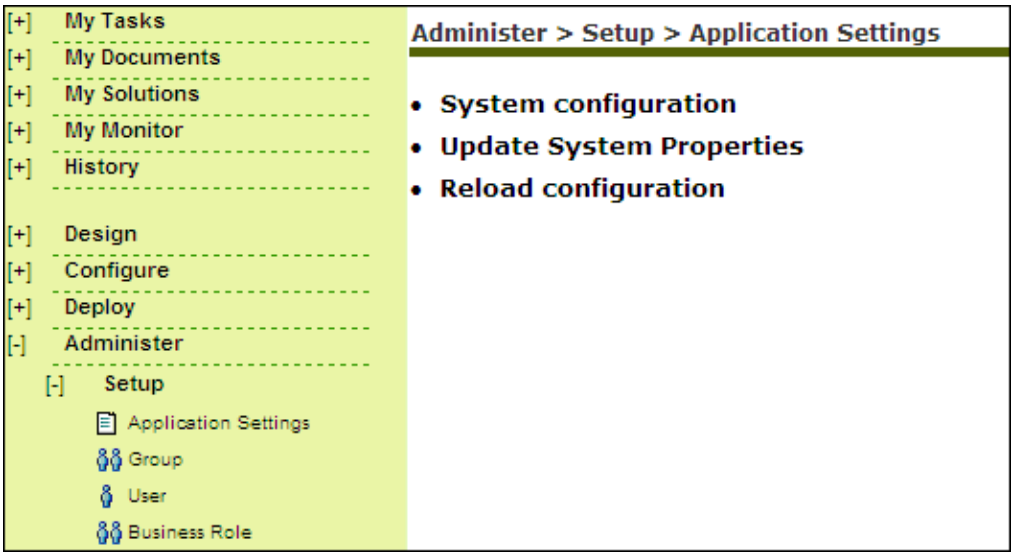


Figure 1: Application Settings

3. Click **System configuration**. The **System configuration** screen is displayed (see Figure 2).

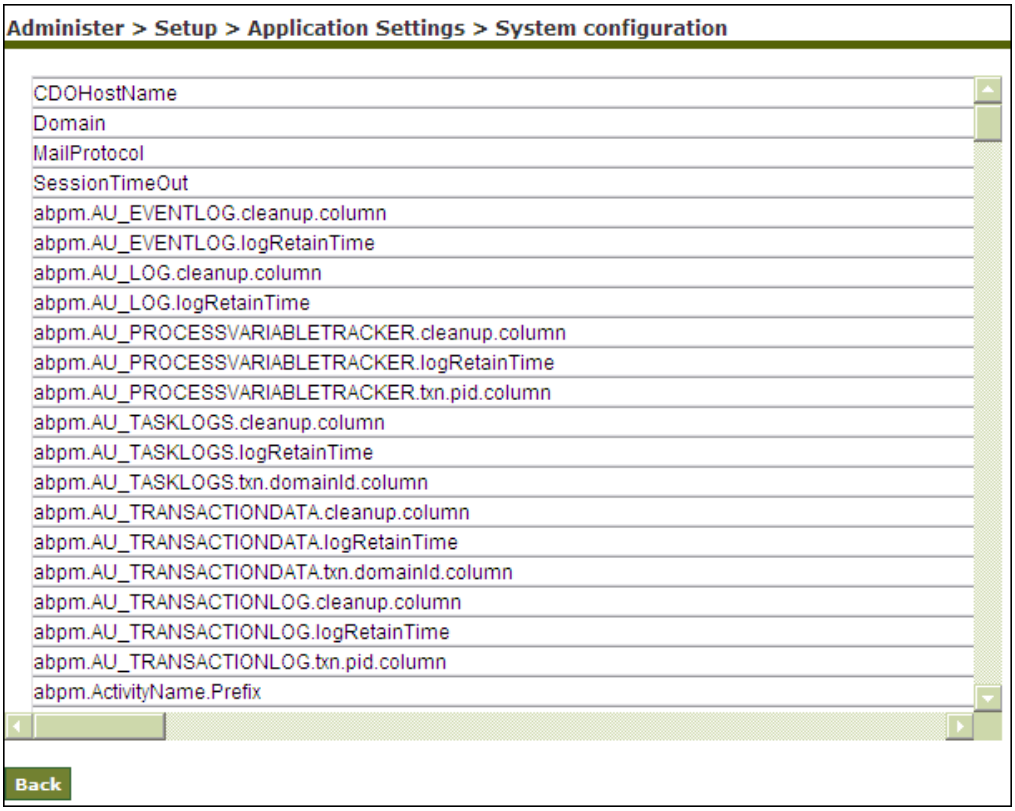


Figure 2: View System Configuration

UPDATING SYSTEM PROPERTIES

The System Properties can be updated to change the properties of the Adeptia Suite. For example, you can change the mail server settings, enable or disable clustering and database settings etc.

> Only the users of *Admin* and *Sys Admin* type can update the System Properties.

Steps to update the system properties of the Adeptia Suite

1. Click **[+] Administer** to expand the tree and then click **[+] Setup**. All the items in the Configure category are displayed.
2. Click **Application Settings**. The **Application Settings** screen is displayed.
3. Click **Update System Properties**. The **Update System Properties** screen is displayed (see Figure 3).

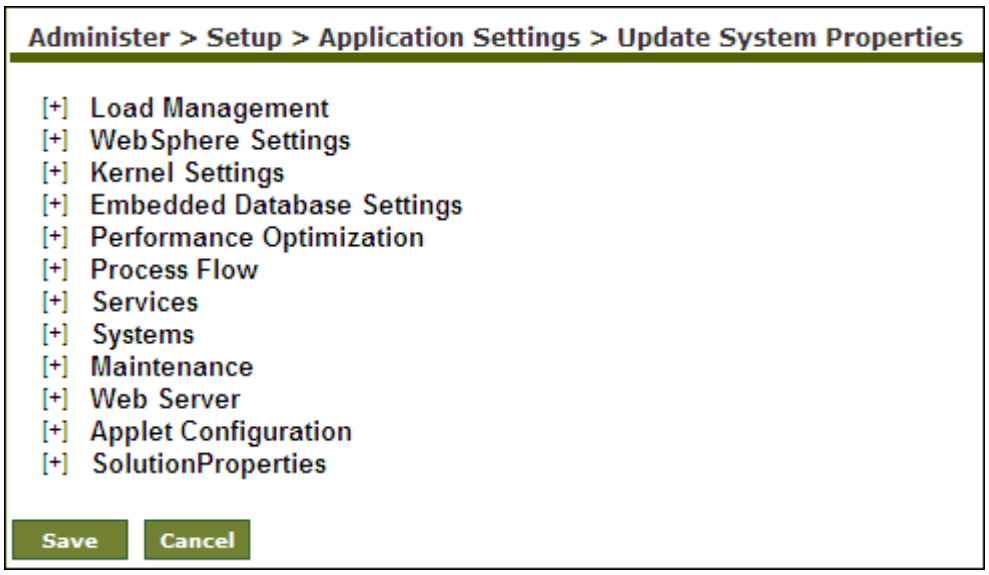


Figure 3: Update System Properties

4. Click **[+]** to expand the required properties (see Figure 4).

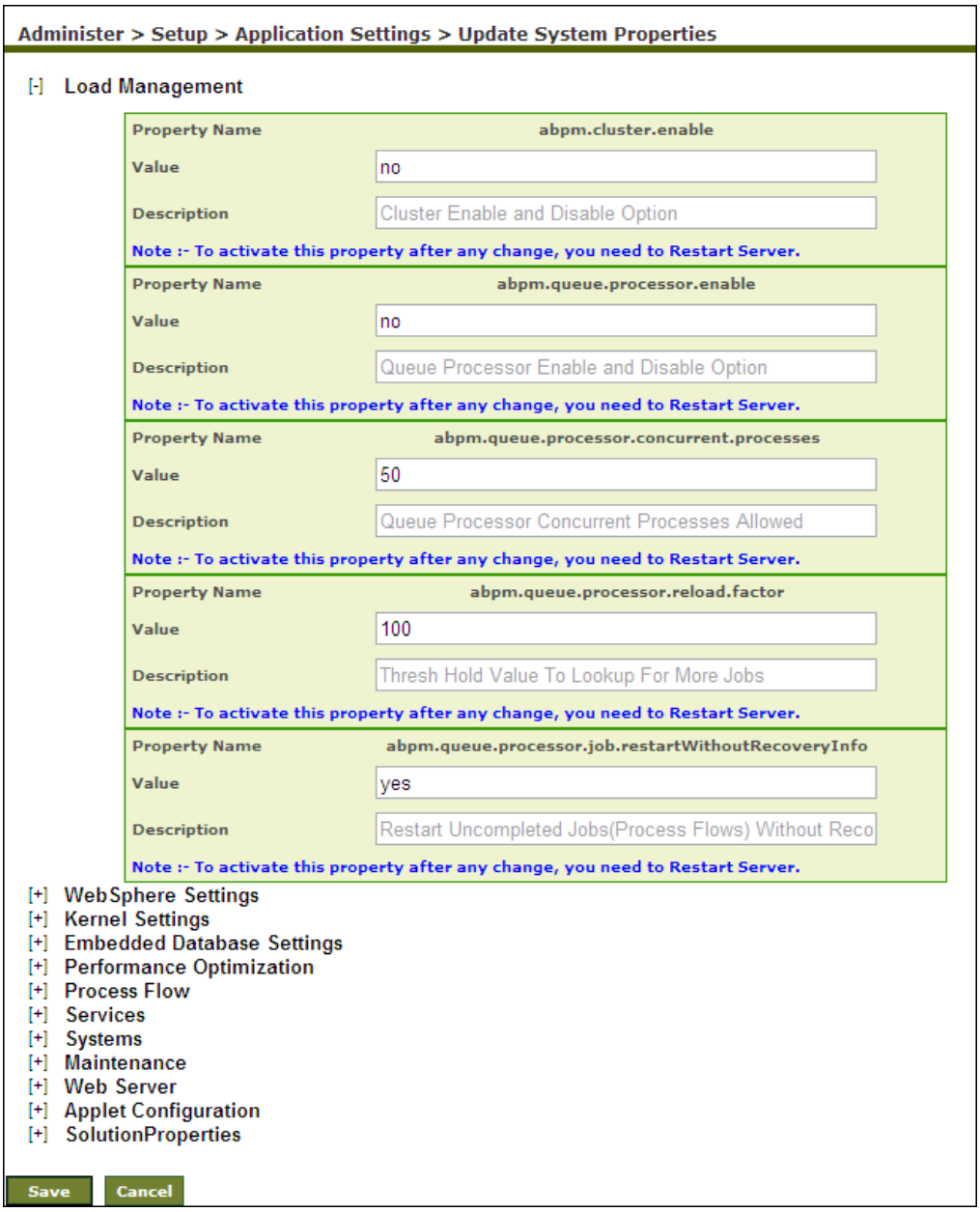


Figure 4: Expand Properties

5. Edit the required properties and click **Save** button. A screen is displayed confirming that System Properties have been saved.

- Changes made in the System Properties do not come into effect until you reload the configuration.
- Value of the properties is not validated while editing. For detailed description of Adeptia Suite System Properties and their Possible Values, refer to Appendix A.

RELOADING SYSTEM CONFIGURATION

Reload 'commits' the changes made to the Adeptia Suite configuration system properties.

Steps to reload the System configuration

1. Click **[+] Administer** to expand the tree and then click **[+] Setup**. All the items in the Configure category are displayed.
2. Click **Application Settings**. The **Application Settings** screen is displayed.
3. Click **Reload Configuration**. A screen is displayed confirming that the configuration has been reloaded.

4

CREATING AND MANAGING USER GROUPS

Groups enable easy organization and management of individual users of the Adeptia Suite. A Group, in essence, is a self-contained entity that can perform all of its work without affecting the work of another User Group. Each group has a *Group Admin*, responsible for creating and managing individual users within the group. The *Group Admin* can perform the same work as any regular user with an additional ability to manage users within its group as well.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

This chapter describes the following tasks:

- Creating a user group
- Viewing properties of a user group
- Editing properties of a user group
- Deleting a user group

CREATING A USER GROUP

Prerequisites

- Only a user of *Admin* or *Sys Admin* type can create a User Group.

Steps to create a user group

1. Click **[+] Administer** to expand the tree and then click **[+] Setup**. All the items in the Configure category are displayed.

2. Click **Group**. The **Manage Group** screen is displayed (see **Error! Reference source not found.**).

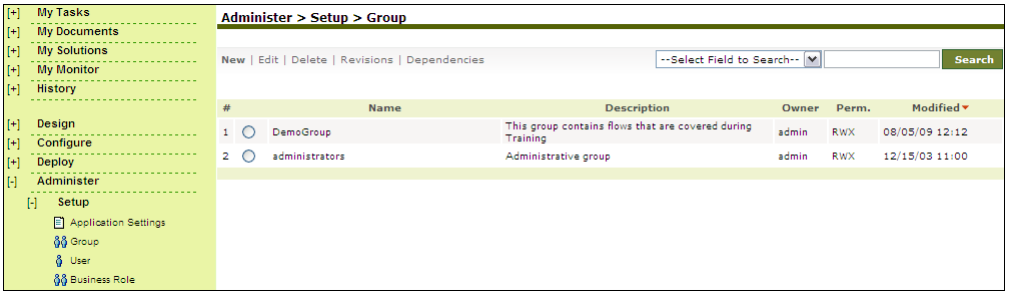


Figure 5: Manage Group

3. Click the **New** link. The **Create Group** screen is displayed (see Figure 6).

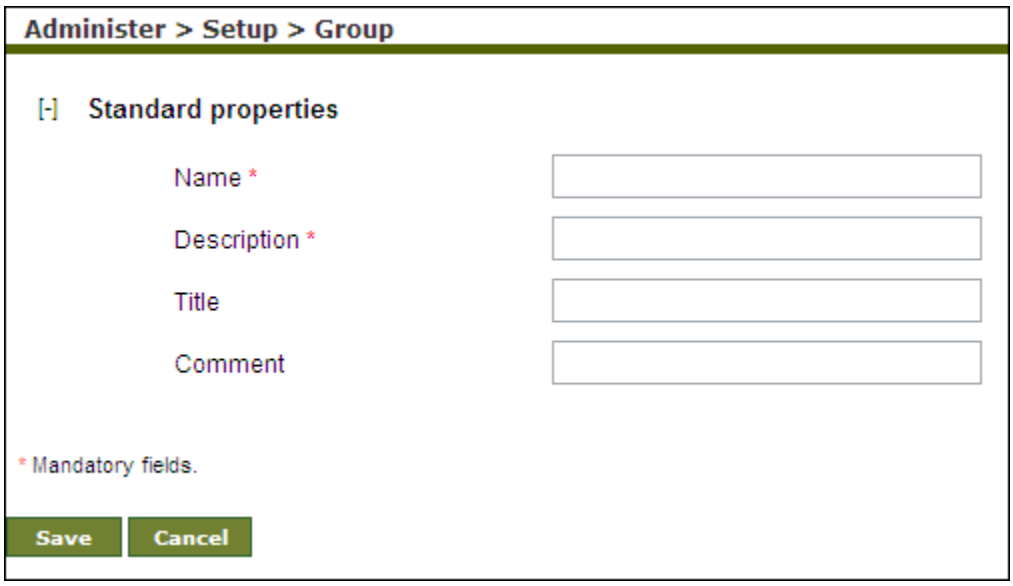


Figure 6: Create Group

4. Enter the name and description of the Group in the **Name** and **Description** respectively.
5. Enter the group title and comments (if any) in the textboxes **Title** and **Comment** respectively.
6. Click the **Save** button. This displays a screen confirming that the User Group has been created successfully. If the **Comments** option is enabled, then clicking **Save** will display a screen, where you need to enter comments related to creating the User Group (see Figure 7).

Figure 7: Enter Comments

7. Enter the comments in the **Add Comments** field.

The Comment should be at least 1 character in length.

8. Click **OK** to save the comments. This displays the screen confirming that the User Group has been created successfully.

By default, the Comments option is disabled. To enable it, refer to the section Updating System Properties.

The Group name must be unique. You cannot create more than one group with the same name.

VIEWING USER GROUP PROPERTIES

Steps to view the properties of a user group

1. In the **Manage Group** screen, click the name the group whose properties you want to view. A screen is displayed showing the properties of the group (see Figure 8).

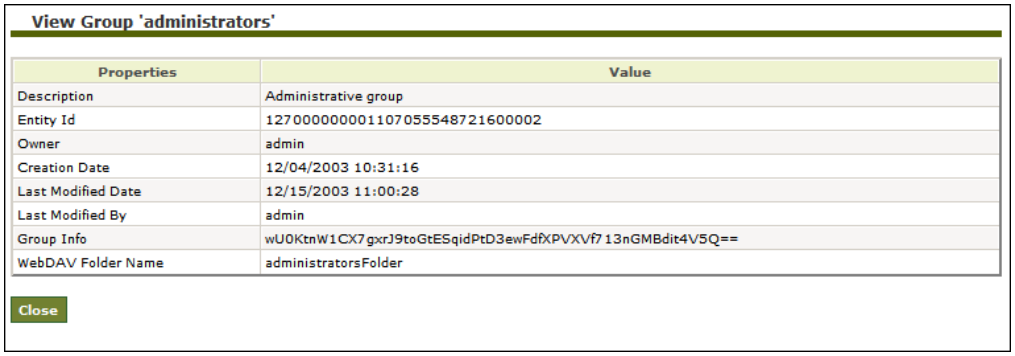


Figure 8: View Group Properties

2. Click **Close** button to close this screen and return to the **Manage Group** screen.

EDITING USER GROUP PROPERTIES

Steps to edit the properties of a user group

1. In the **Manage Group** screen, click the radio button against the group whose properties you want to edit and then click the **Edit** link. A screen is displayed where you can change the name and description of a Group (see Figure 9).

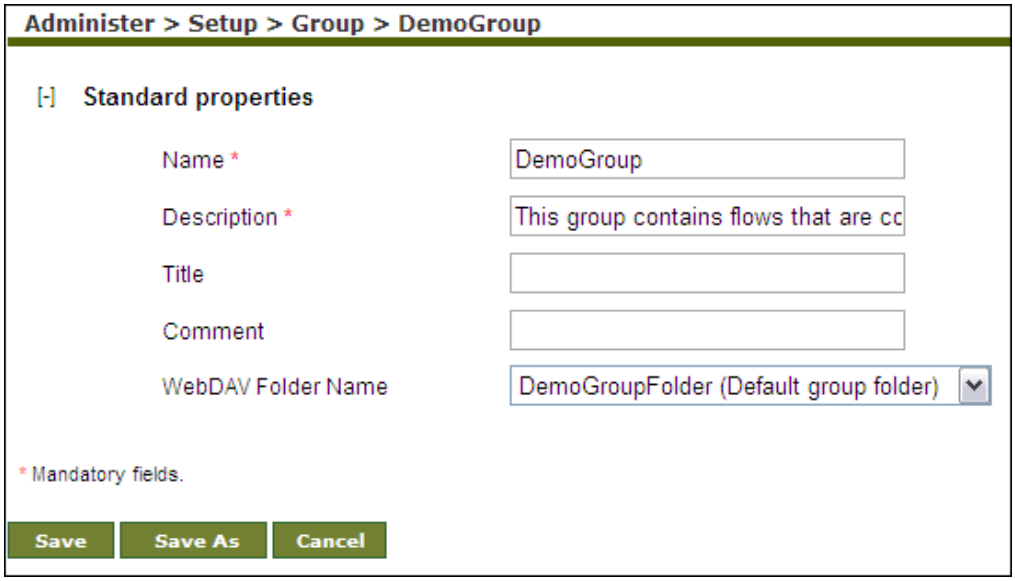


Figure 9: Edit Group

2. After changing the properties, click **Save** button to save the changes. This displays a screen confirming that the User Group has been updated successfully. If the **Comments** option is enabled, then clicking **Save** will display a screen where you need to enter comments related to editing the Group (refer to Figure 7).

3. Enter the comments in the **Add Comments** field.

> The comment should be at least 1 character in length.

4. Click **OK** to save the comments. This displays a screen confirming that the User Group has been updated successfully.

> By default, the Comments option is disabled. To enable it, refer to the section Updating System Properties.

> You cannot edit the Administrator group.
>
> If you want to save a copy of a group, change the name of the group and click Save As button.

DELETING A USER GROUP

Steps to delete a user group

1. In the **Manage Group** screen, click the radio button against the group that you want to delete and then click the **Delete** link. A screen is displayed for a confirmation to delete the Group (see Figure 10).

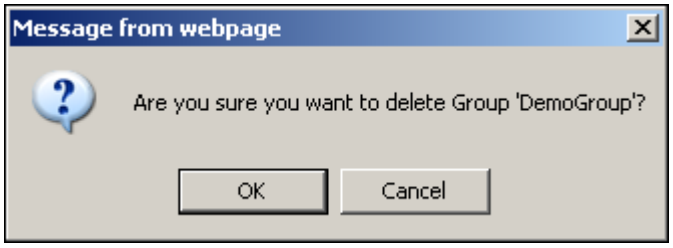


Figure 10: Confirm Deleting a Group

2. Click **OK** button to delete the group, else click **Cancel**.
3. If you click **OK**, a screen is displayed confirming that the group has been deleted successfully. If the *Comments* property is enabled, then clicking **OK** will display a screen where you need to enter comments related to deleting the Group (refer to Figure 7).
4. Enter the comments in the **Add Comments** field.

The comment should be at least 1 character in length.

5. Click **OK** to save the comments. This displays a screen confirming that the Group has been deleted successfully.
6. Click **Group** to return to the screen.

By default, the **Comments** property is disabled. To enable it, refer to the section Updating System Properties.

- The *Administrator* group cannot be deleted.
- A Group having users cannot be deleted. All the users of a group must be deleted before deleting the Group.
- Once a Group is deleted it cannot be recovered.

6

CREATING AND MANAGING USERS

Users are the individual members of a User Group. User can perform common tasks depending on the permission levels granted by the *Admin*.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

This chapter describes the following tasks:

- Creating a User
- Viewing properties of a User
- Editing properties of a User
- Deleting a User
- Moving Objects of a User
- Managing Keystore of a User

CREATING A USER

Prerequisites

You need to have Administrator privileges of Sys Admin or a Group Admin type.

Steps to create a user

1. Click **[+] Administer** to expand the tree and then click **[+] Configure**. All the items in the **Configure** category are displayed.
2. Click **User**. The **Manage User** screen is displayed (see Figure 11).

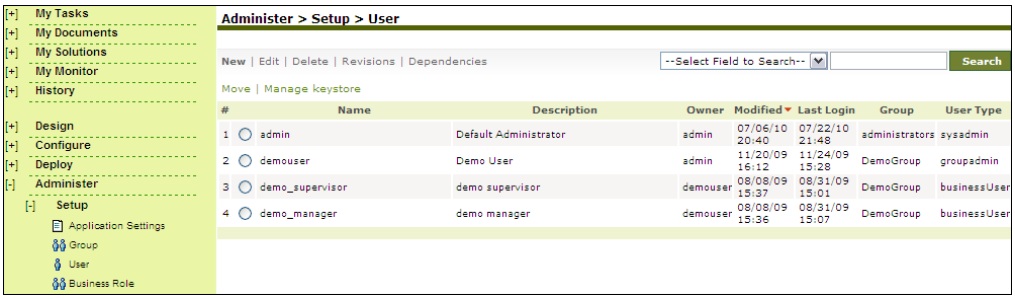


Figure 11: Manage User

3. Click the **New** link. The **Create User** screen is displayed (see Figure 12).

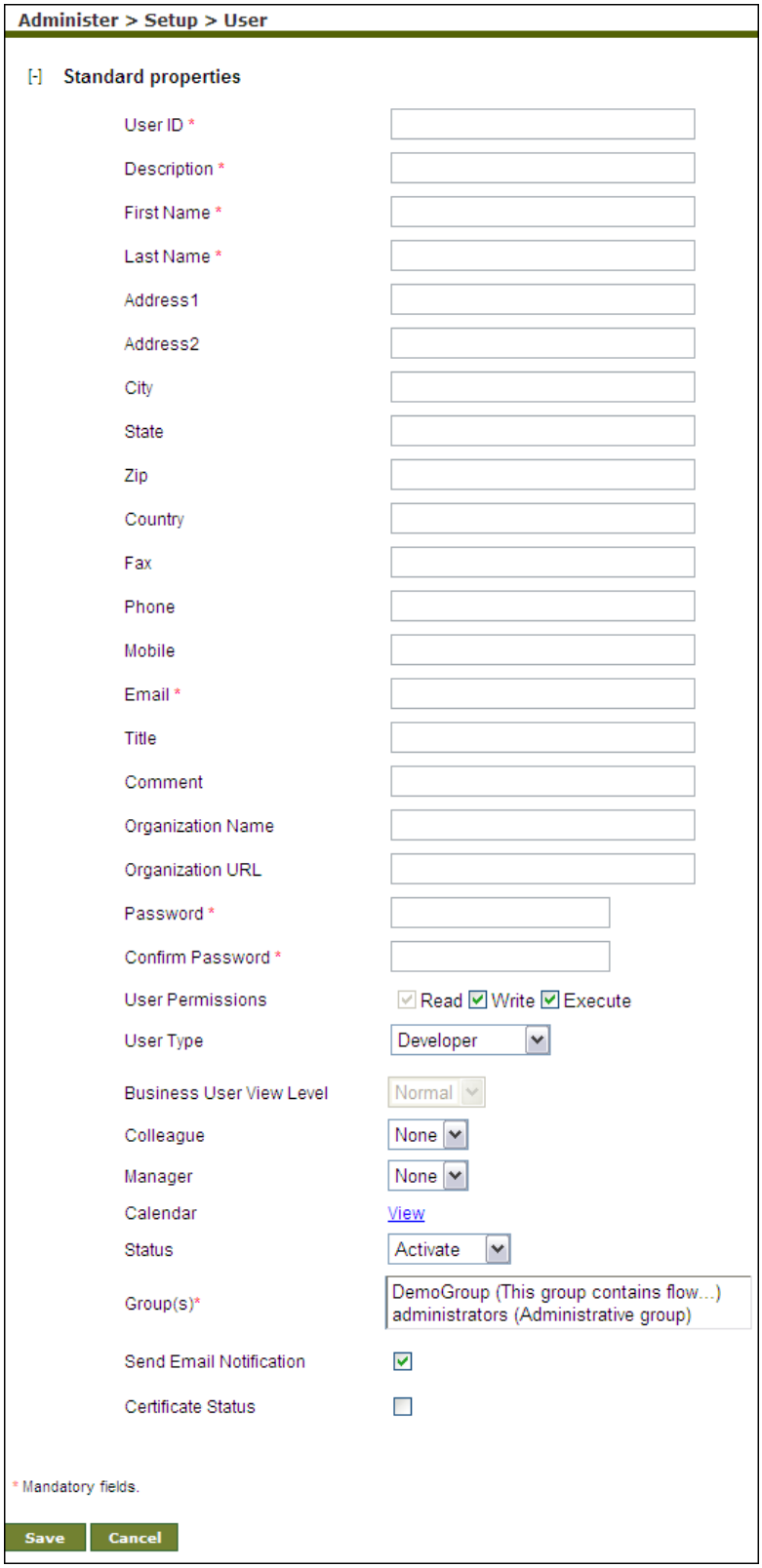


Figure 12: Create a User

4. Enter the User ID, Description, Name, Address, and other related information in their respective fields.
5. To select the User Permissions, check the required checkboxes. The various permissions entitle a user to various rights, as outlined in the table below.

Table 1: User Permissions

Permission	Description
Read	Read permission allows a user to view the Adeptia Suite activities and process flows. The *Read* checkbox is pre-selected and cannot be unchecked.
Write	Click to check the *Write* checkbox to grant the user the permission to create, edit, delete and Save As Adeptia Suite activities and process flows.
Execute	Check the *Execute* checkbox to grant the user permission to execute a process flow.

These user permissions are checked prior to object level permissions so as to allow a user to or restrict a user from performing any task.

6. Select the type of user from the **User Type** drop-down list.
7. If Business User is selected, then select the level of view from the **Business User View Level** drop-down list. There are two types of Business User View Levels, as outlined in the table below.

Table 2: Business User View Levels

Level	Description
Normal	A Business User with Normal view can see Adeptia Suite report and logs. It can execute the process flow, complete the Human Workflow task and monitor the logs.
Limited	A Business User with Limited view can only view Task Manager and execute the assigned task. A Business User with Limited View cannot execute process flows. It cannot see Adeptia Suite reports and logs.

8. You can select colleague of the User from the **Colleague** drop-down list.
9. You can select Manager of the User from the **Manager** drop-down list.

Colleague or Manager can be any other user. A Manager can monitor tasks assigned to its staff. Manager can defer a task to any other user; change the priority, Due date and Expiry Date of the task.

10. Using calendar you can select the days on which user will not be available. To select days, click the **View l**ink in the **Calendar** field (see Figure 13).

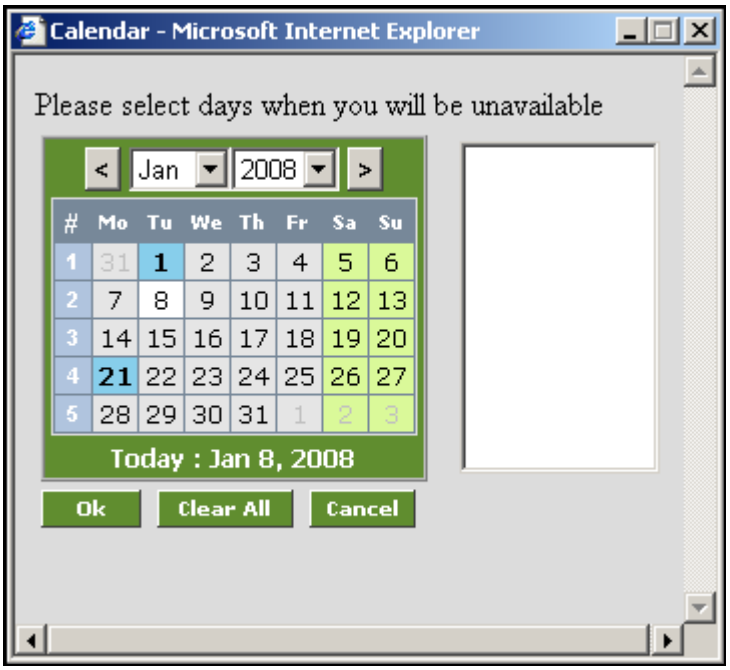


Figure 13: Calendar

11. Click dates, user will not be available and then click **Submit** button.

> While deferring a task of any user to this user, manager can view these dates from his own Home page.

12. In the **Status** drop-down list, select the status of the user. The status of a user can be either Activate or Deactivate. The default status is **Activate**.

> If you select **Deactivate**, the user is disabled and therefore cannot login into the Adeptia Suite.

13. In **Group** drop-down list, select the group to which user is being added. You can add the user to multiple groups. Press and hold the **<Ctrl>** key and select multiple groups.

> A user can be a member of more than one group. But he can login and access objects associated with one group at a time. For example, a user is a member of two groups: Administrators and Executives. Both these groups vary in terms of objects. He can login as a member of either the Administrators or the Executives group at a time.

14. Select the **Send Email Notification** checkbox to automatically send an email to the new user confirming the user creation. It is checked by default. Additionally, if the user changes his password, an email is automatically sent to the user stating that the password has been changed. If you do not want to send these notification emails, disable this checkbox.

15. Select the **Certificate Status** checkbox to attach a digital certificate to the user. Digital Certificate is used to authenticate a user. When you select the **Certificate Status** check box, a digital certificate is attached to the user. A Keystore is also created for the user, which is used as a repository of digital certificates (see Figure 14).

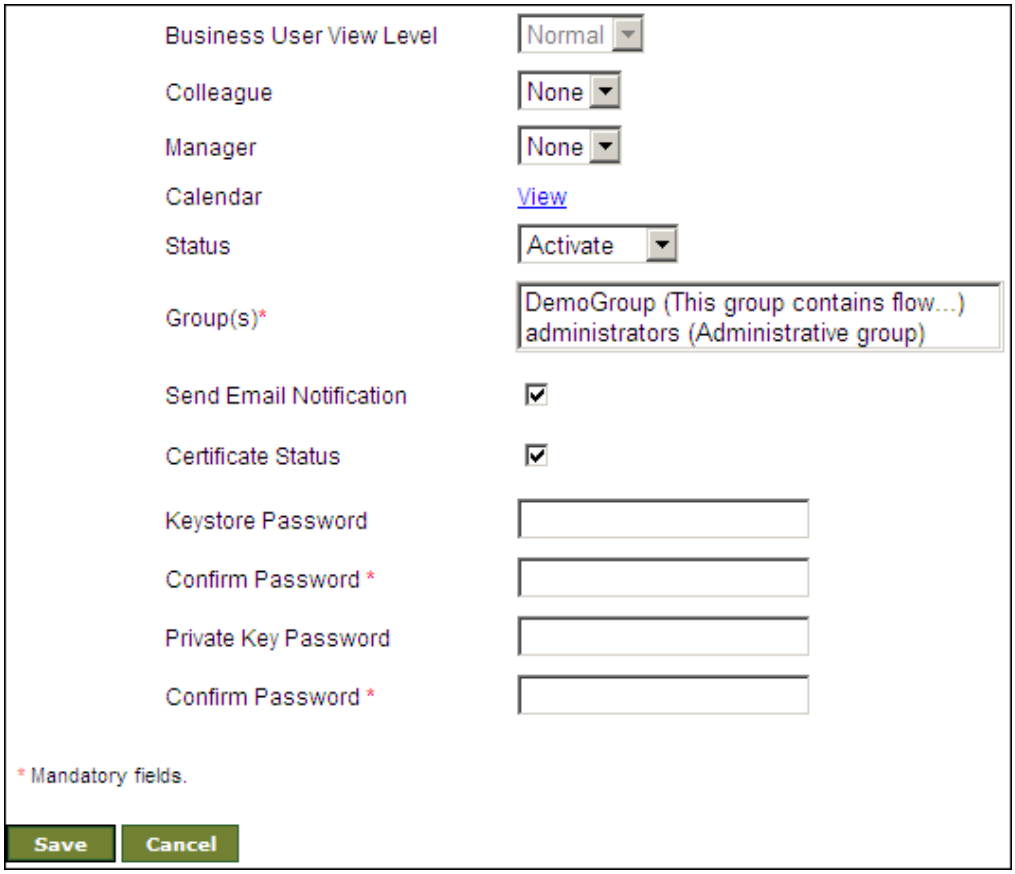


Figure 14: Certificate Status

16. Enter password for Keystore in the textboxes **Keystore Password** and **Confirm Password** respectively. User uses the keystore password to access the keystore.
17. Enter password for the private key in the textboxes **Private Key Password** and **Confirm Password** respectively.
18. Click the **Save** button. This displays a screen confirming that the user has been created successfully. If the **Comments** property is enabled, then clicking **Save** will display a screen where you need to enter comments related to creating the user (refer to Figure 7).
19. Enter the comments in the **Add Comments** field.

> The comment should be at least 1 character in length.

20. Click **OK** to save the comments. This displays a screen confirming that the user has been created successfully.

> By default, the **Comments** option is disabled. To enable it, refer to the section Updating System Properties.

To learn how to manage digital certificates of users refer to section Managing Keystore of Users.

To learn how to use digital certificates to sign outgoing data and how to receive incoming data, which is digitally signed refer to the section Digital Certificate Activity.

VIEWING USER PROPERTIES

Steps to view the properties of a user

1. In the **Manage User** screen, click the user whose properties you want to view. A screen is displayed showing the properties of the User (see Figure 15).

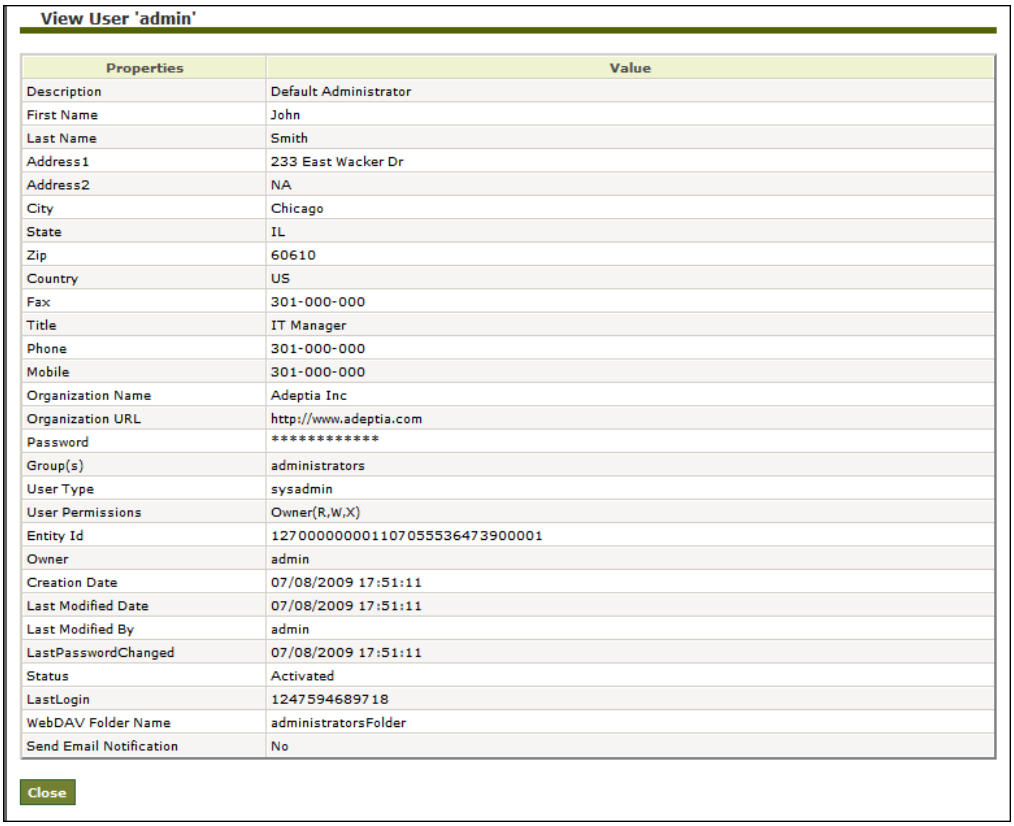


Figure 15: View User Properties

2. Click **Close** button to close this screen and return to the **User** screen.

EDITING USER PROPERTIES

Steps to edit the properties of user

1. In the **Manage User** screen, click the radio button against the user whose properties you want to edit and then click the **Edit** link. A screen is displayed where you can change the properties of a User (see Figure 16).

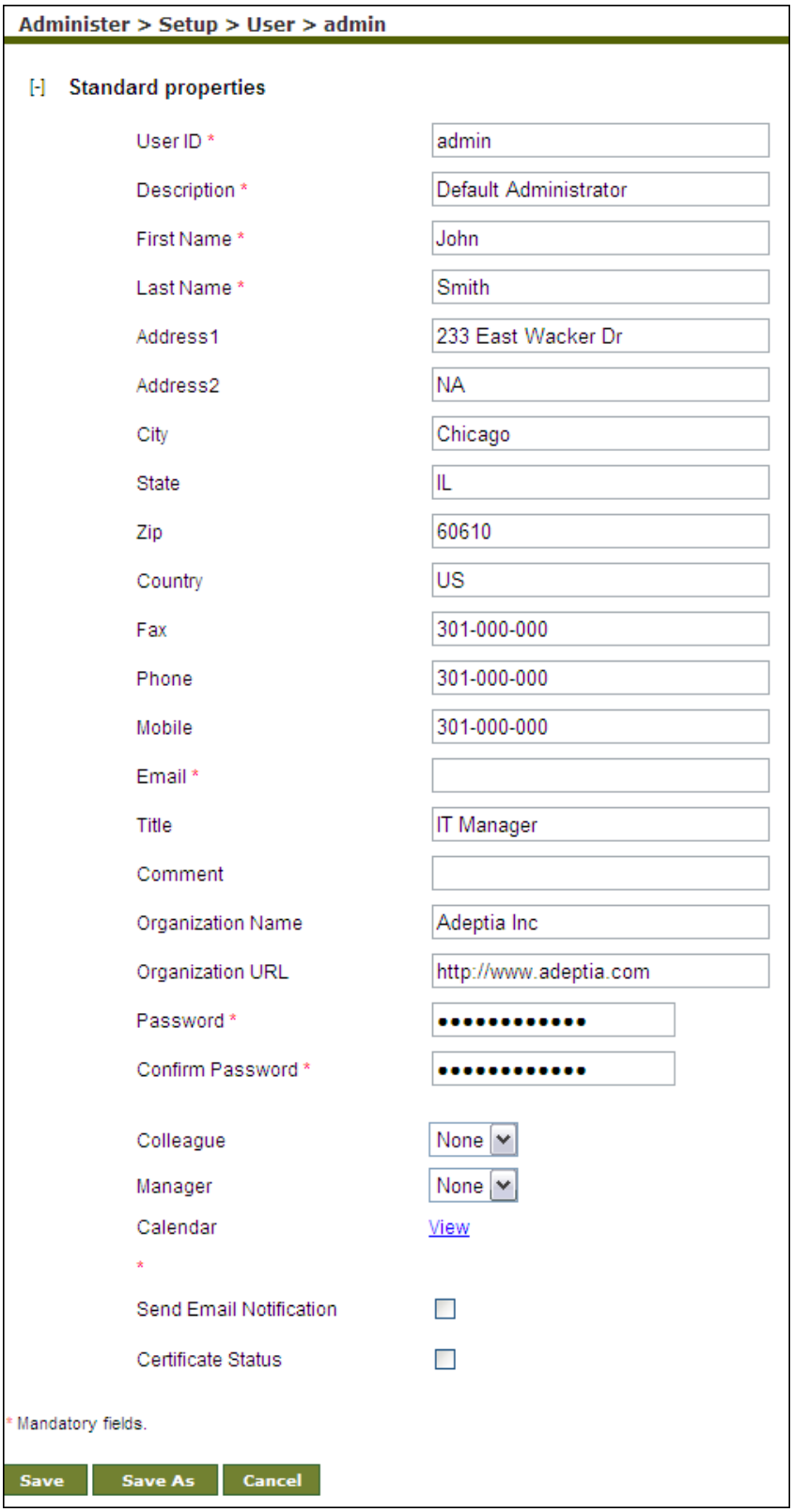


Figure 16: Edit User

3. After changing the properties, click **Save** button to save the changes. This displays a screen confirming that the user has been updated successfully. If the **Comments** option is enabled, then clicking **Save** will display a screen where you need to enter comments related to editing the user (refer to Figure 7).
4. Enter the comments in the **Add Comments** field.

> The comment should be at least 1 character in length.

5. Click **OK** to save the comments. This displays a screen confirming that the user has been updated successfully.

> By default, the **Comments** option is disabled. To enable it, refer to the section Updating System Properties.

DELETING A USER

Steps to delete a user

1. In the Manage User screen, click the radio button against the user that you want to delete and then click the **Delete** link. A screen is displayed for a confirmation to delete the user (see Figure 17).

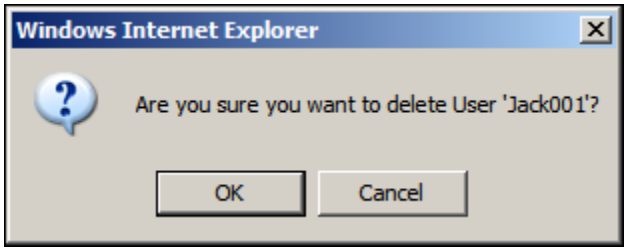


Figure 17: Confirm Deletion

2. Click **OK** to delete the user. Before being deleted, the user needs to transfer his objects to another user. The **Change Ownership** screen is displayed (see Figure 18).

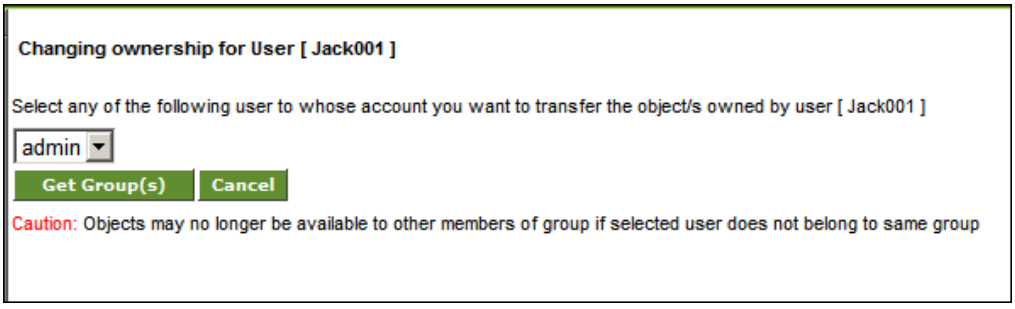


Figure 18: Change Ownership

> Once the user is deleted, his objects cannot be viewed by any other member of his group.

3. Select the user to whom you want to transfer the objects, from the drop-down list. Click **Get Group(s)** button to transfer the objects to the selected user's group. This displays the Select group screen (see Figure 19).

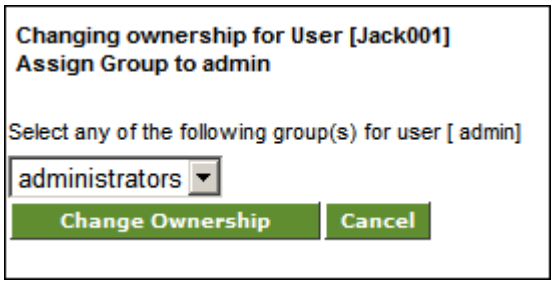


Figure 19: Select Group

4. Select the group to which you want to transfer the objects and click **Change Ownership** button. This displays the **Permanent Delete** screen (see Figure 20).

The Group drop-down list displays only those groups, of which the selected user is a member.

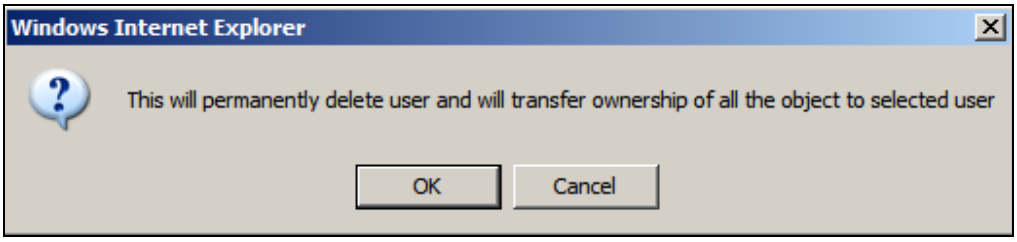


Figure 20: Permanent Delete

5. Click **OK** button to permanently delete the user. A screen is displayed with a message stating "*User activity permanently deleted successfully*." If the **Comments** property is enabled, then clicking **OK** will display a screen where you need to enter comments related to deleting the User (refer to Figure 7).

6. Enter the comments in the **Add Comments** field.

The comment should be at least 1 character in length.

7. Click **OK** to save the comments. This displays a screen confirming that the User has been deleted successfully.

By default, the **Comments** property is disabled. To enable it, refer to the section Updating System Properties.

MOVING USER'S OBJECTS

Objects (activities, process flows etc.) of one user can be moved to another user. When you move objects from one user to another user, ownership of those objects is transferred to new user. If a user belongs to more than one group, it can move its object from one group to another group.

Steps to move object from one user to another User

1. In the **Manage User** screen, click the radio button against the user that you want to move and then click the **Move** link. The **Select Activities** screen is displayed with the list of activities belongs to the user (see Figure 21).

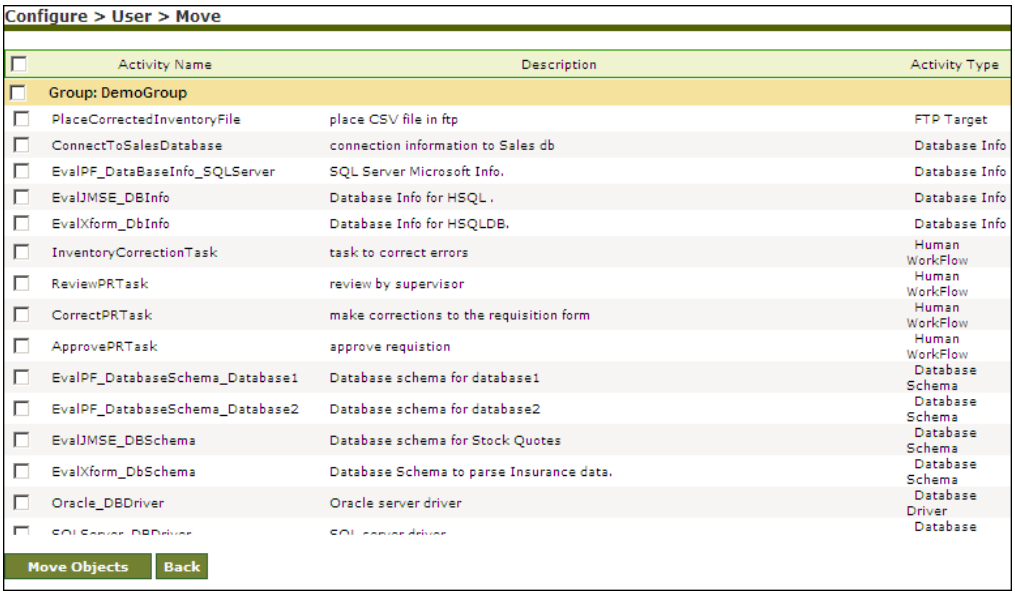


Figure 21: Select Objects

2. Select the required object(s) and click **Move Objects** button. The **Change Ownership** screen is displayed (refer to Figure 18).
3. Select the user to whom the objects will be moved, from the drop-down list and then click **Get Group(s)** button. The **Select Group** screen is displayed with Group(s), the selected User belongs (refer to Figure 19).
4. Select the group, the user belong to and click **Change Ownership** button. A confirmation screen is displayed that the ownership of selected objects has been changed successfully.

MANAGING KEYSTORE OF USER

Keystore of a user is a protected repository that holds digital certificates owned by the user. Keystore is created during creation of the user. Access to a keystore is guarded by a password defined at the time of creation of user. Keystore is created only for those users whose certificate status is enabled during their creation.

Digital Certificate Activity

A Digital Certificate is an attachment to an electronic message that is used to maintain its integrity. The most common use of a digital certificate is to authenticate a user.

Admin and *Group Admin* can export the digital certificates of a user into a digital certificate directory and then import that digital certificate into the keystore of another user. The *Admin* also has the right to delete the digital certificate of a user.

Exporting Digital Certificate

Steps to export the digital certificate of a user

1. In the **Manage User** screen, click the radio button adjacent to the user for whom you want to export digital certificate and then click the **Manage Keystore** link. The **Keystore Management** screen is displayed (see Figure 22).

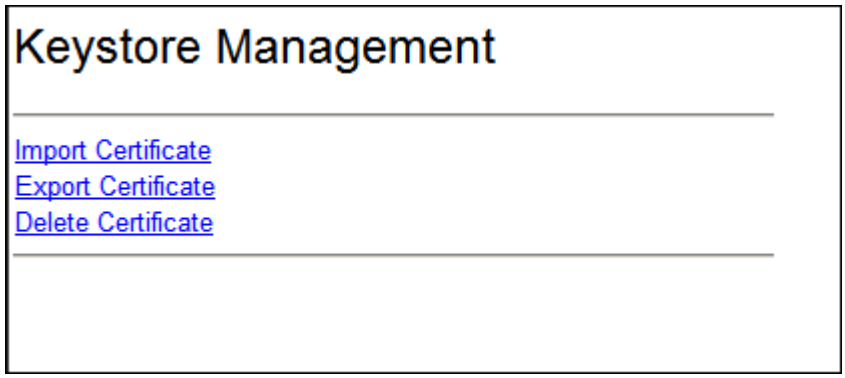


Figure 22: Keystore Management

2. Select **Export Certificate**. A screen is displayed confirming that the Digital Certificate has been exported successfully.

> Once the digital certificate of a user is exported, Admin can import it for any other user.

Importing Digital Certificate

Steps to import digital certificate

1. In the **Manage User** screen, click the radio button adjacent to the user for whom you want to import the digital certificate and then click the **Manage Keystore**. The **Keystore Management** screen is displayed.
2. Click **Import Certificate**. The **Import Certificate for user** screen is displayed (see Figure 23).

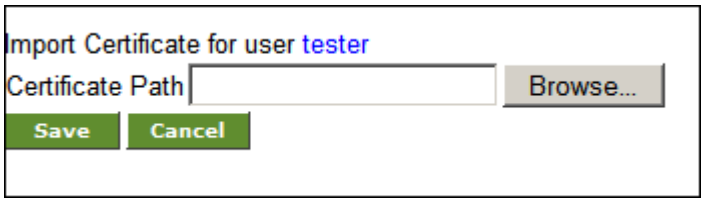


Figure 23: Import Certificate

3. Click the **Browse** button and select the Digital Certificate file (.cer) from *Digital Certificate* folder.

> All exported digital certificates are stored in the ../../AdeptiaServer-5.3/ServerKernel/etc/security/digitalcertificate
>
> where first two dots (..) represent drive letter and next two dots (..) represent base directory where Adeptia Suite is installed.

4. Select the certificate you want to import and then click **Open**. The selected certificate file with the file path is displayed in the **Certificate Path** field.

The extension of certificate file is .cer. For example if you are importing the certificate of *User1*, name of the certificate file will be *user1.cer*.

5. Click **Save** button. A screen is displayed confirming that the certificate has been added successfully.

The Digital Certificates that has been imported is stored in Keystore of the user.

Deleting Digital Certificate

Steps to delete any of the certificates of a user from its Keystore

1. In the Manage User screen, click **Manage Keystore**. The **Keystore Management** screen is displayed.
2. Click **Delete Certificate**. The **Delete Certificate** screen is displayed (see Figure 24).

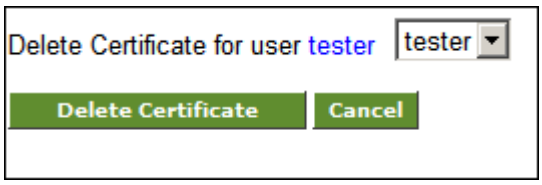


Figure 24: Delete Certificate

3. Select the certificate you want to delete from the **Delete Certificate** *for* user drop-down list. Then click **Delete Certificate** button. A confirmation screen for deleting the certificate is displayed (see Figure 25).

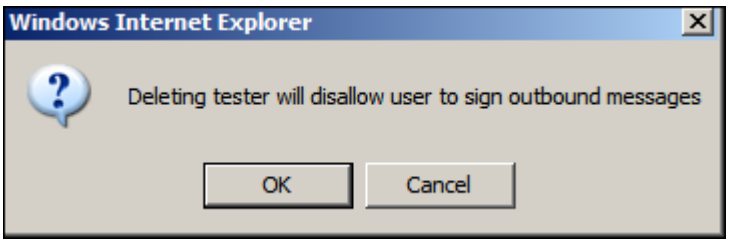


Figure 25: Confirm Deletion

4. Click **OK** button to delete the digital certificate. A screen is displayed confirming that the certificate has been deleted successfully from the keystore of the user.

7

CREATING A BUSINESS ROLE

In any business operation, it is required that a task can be assigned to all the users of a department. One way is to select all the users of the department one by one while assigning the task in the workflow. Another way is to make a group of users and assign the task to a group rather than assigning it to all the users. This group of users is called a Business Role. Task assigned to a Business Role is listed in the Task Manager of every user of the Business Role. Any one user of the Business Role can complete this task.

It should be noted that the Business Role is different than a User Group. The purpose of the User Group is to minimize the work of a user of *Sys Admin* or *Group Admin* type while giving access permissions on Adeptia Suite objects. On the other hand, the purpose of Business Role is to assign the task to a group of users.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√		

Steps to create a Business Role

1. Click **[+] Administer** to expand the tree and then click **[+] Setup**. All the items in the **Setup** category are displayed.
2. Click **Business Role**. The **Manage Business Role** screen is displayed (see Figure 26).

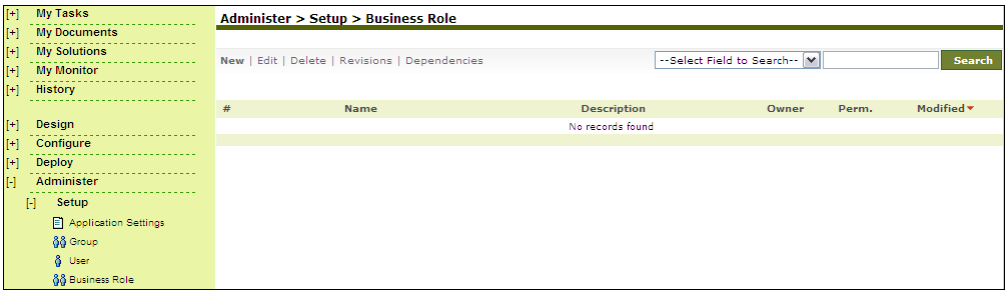


Figure 26: Manage Business Role

3. Click the **New** link. The **Create Business Role** screen is displayed (see Figure 27).

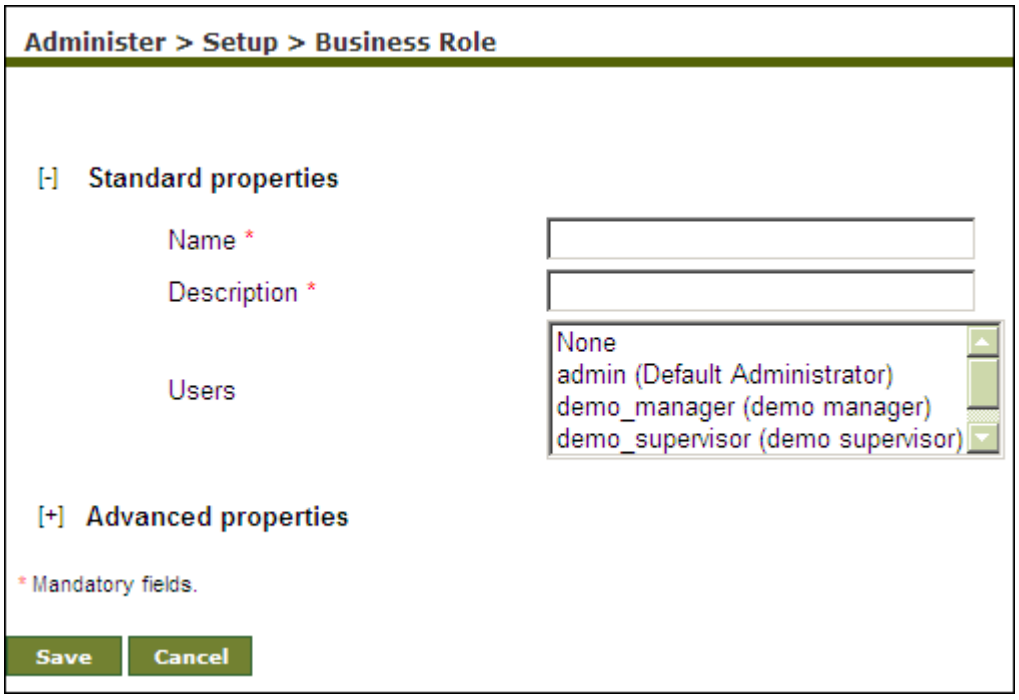


Figure 27: Create Business Role

4. Enter the name and description of the Business Role in the *Name* and *Description* fields respectively.
5. To select the users, press **<CTRL>** key and click users. The selected users are highlighted.
6. Click **Save** button. This displays a screen confirming that the Business Role has been created successfully. If the *Comments* property is enabled, then clicking **Save** will display a screen where you need to enter comments related to creating the Business Role (refer to Figure 7).
7. Enter the comments in the *Add Comments* field.

> The comment should be at least 1 character in length.

8. Click **OK** to save the comments. This displays a screen confirming that the Business Role has been created successfully.

> By default, the **Comments** property is disabled. To enable it, refer to the section Updating System Properties.

8

MANAGING KERNEL AND SCHEDULER

At times, you may want to stop or pause the kernel without stopping it as a service (if the kernel is running as a service) or stopping it by pressing **<Ctrl> + <C>** from the console. In such cases you can stop or even pause the kernel from the GUI. When the kernel is stopped or paused, no requests for new process flows are executed.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

Process Flow Status when Kernel is Stopped

When the kernel is stopped, the system does not accept any new process flow requests for triggering. It just completes the existing process flows that are running, and then shuts down the kernel.

Process Flow Status when Kernel is Paused

When the kernel is paused, the system just completes the existing process flows that are running. However, it does not accept any new process flow requests for triggering. Additionally, it does not accept any waiting process flows which could be manual execution requests or those in the *Queue Processor*. When the kernel is paused, the *Queue Processor* is also paused. It does not activate any process flows or escalate them from the waiting queue to ready queue. It just maintains them in the queue list.

The pausing of the kernel pauses the scheduler too. It does not allow triggering of any process flows through any events except JMS and HTTP events. The pausing/resuming/stopping of scheduler synchronizes with the pausing/resuming/stopping of the kernel.

If sub processes are being executed with **Call** action when the kernel is paused or stopped, then they need to made recoverable with the **Call** action, when the process flow shuts down, as the parent process flow will not stop unless all child process flows are executed.

This chapter describes the following tasks:

- Managing Kernel
- Managing Scheduler

MANAGING KERNEL

Steps to manage the kernel

1. Click **[+] Administer** to expand the tree and then click **[+] Maintenance**. All the items in the **Maintenance** category are displayed.

2. Click **Kernel.** The **Change Kernel State** screen is displayed showing the status of kernel (see Figure 28).

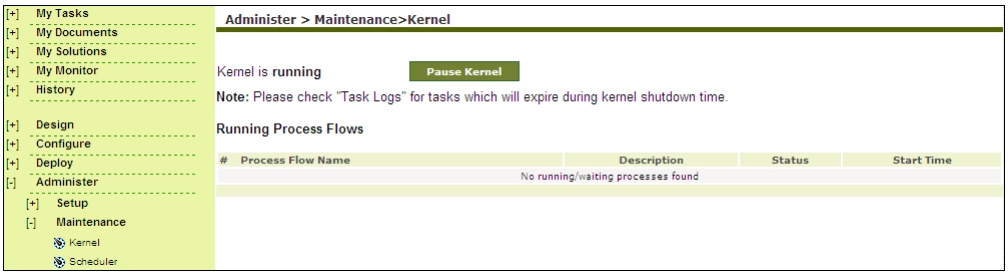


Figure 28: Change Kernel State

3. This screen is divided into two parts. The first part displays the status of the kernel and allows you to change the status as and when required. The second part displays a list of process flows that are running (if kernel is running).

4. To pause the Kernel, click **Pause Kernel** button on the Change Kernel State screen. A confirmation screen is displayed. Click **OK** to pause the Kernel. This pauses the Kernel and displays a screen with the message that the Kernel has been paused.

> The **Pause Kernel** button changes to **Resume Kernel**, once the Kernel is paused.
>
> When the Kernel is Paused, the list of running process flows is not displayed.

5. To resume the Kernel, click **Resume Kernel** button. This resumes the Kernel and displays the Change Kernel State screen. Once the Kernel is resumed, it starts accepting new process flow requests for execution. The Queue Processor also activates and escalates process flows in queue, and the Scheduler resumes triggering of events.

MANAGING SCHEDULER

Scheduler is a component of Adeptia Suite that manages events and triggers process flows based on the occurrence of events. The normal state of the Scheduler is *Running*. However, it may be required to pause or stop occasionally for system performance or maintenance reasons. When the scheduler is Paused or Stopped, no scheduler supported Event will be fired.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√		

Events managed by the scheduler (time based events) are:

- File Event
- FTP Event
- Mail Event
- Database Event
- Timer Event
- Calendar Event

Self-driven events i.e. events that are not managed by the scheduler (action based events) are:

- JMS Event
- HTTP Event

Misfire Event Handling

An event may not be fired at the scheduled time due to multiple reasons. These are outlined as:

No thread is available (refer to org.quartz.threadPool.threadCount property)

System is busy

When the event is not fired at the scheduled time, it is considered as a delayed event. The delayed event will be fired, when the thread becomes available or the system is not too busy. This will happen as long as delay is not more than misfire threshold. If delay is more than misfire threshold, event is considered as a misfired event. The misfire threshold is specified by following parameter defined in quartz.properties file:

org.quartz.jobStore.misfireThreshold = 60000

60000 = 60 Seconds

60 seconds is the default value of misfire threshold, which can be changed, based on your requirements.

Misfired events are handled based on two factors:

- Smart Misfire Policy
- Repeat Count

The Smart Misfire Policy is dependent on the Repeat Count value. In case of all events except Timer event, the Repeat Count value is Infinity. However, in case of a Timer event, the Repeat Count value is based on the Expiry Criteria value. This is described in the table below.

Table 3: Repeat Count Value of Timer Event and Misfire Policy

Expiry Criteria	Repeat Count	Misfire Policy
Timer Event- Run only Once	0	The misfired event will be triggered only once
Timer Event-Repeat Count specified value e.g. 10	Specified value e.g. 10	All misfired events and the remaining events will be triggered. The number of misfired event triggered at a time is controlled by org.quartz.jobStore.maxMisfiresToHandleAtATime properties defined the quartz.properties file.
Timer Event-Expiry by Date/time or All other Events	Infinity	Only the remaining events will be triggered. All misfired events will be lost.

Firing of Events when Scheduler is Stopped

The events that are scheduled to fire while the scheduler is stopped will be fired upon restarting of the scheduler based on the Repeat Count value as described in Table 3 .

When the scheduler is stopped, events cannot be activated or deactivated.

Firing of Events when Scheduler is Paused

When the scheduler is paused, the events that are scheduled to be fired will not be triggered. When the scheduler is resumed, only the remaining events will be triggered. The misfired events will be lost.

When the scheduler is paused, events can be activated, but they will not trigger.

Scheduler Related Properties

For scheduler related properties, you can refer to the quartz.properties file that is located in the *../../AdeptiaServer-5.3/ServerKerne*l directory. These include:

org.quartz.jobStore.maxMisfiresToHandleAtATime

Description	**This property is used to define the maximum number of misfired triggers that the jobstore can handle at a given time**
Default Value	5
Possible Values	1-100
Selection Criteria	NA
Comments	If the jobstore handles many triggers at once then the database tables could get locked, thus hampering the performance of other triggers. This property limits the maximum number of misfired events that can be fired at a time. If there are numerous misfired events, then they are fired in batches.

org.quartz.jobStore.misfireThreshold

Description	**This property is used to define the number of milliseconds that the scheduler will retain a trigger, before passing it to the next firing time, before it is considered as misfired**
Default Value	60000
Possible Values	Any positive integer
Selection Criteria	
Comments	

org.quartz.threadPool.threadCount

Description	**This property is used to define the number of threads available for concurrent execution of jobs (for firing of events)**
Default Value	15

Possible Values	1-100
Selection Criteria	NA
Comments	If only few jobs are fired a few times in a day, then 1 thread is sufficient. If thousands of jobs are fired every minute, then 50 or 100 threads are required, based on the jobs count and system resources.

Steps to manage the scheduler

1. Click **[+] Administer** to expand the tree and then click **[+] Maintenance**. All the items in the Configure category are displayed.
2. Click **Scheduler**. The **Change Scheduler** State screen is displayed showing the status of scheduler (see Figure 29).

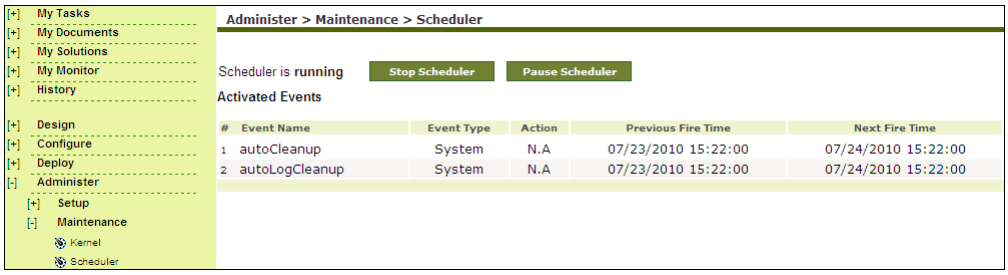


Figure 29: Change Scheduler State

3. This screen is divided into two parts. The first part displays the status of the scheduler and allows you to change the status as and when required. The second part displays a list of events that are activated (only if scheduler is running). You can deactivate an event by clicking **Deactivate** against the event. This will deactivate the event and remove it from the list.

> The autoCleanup and autoLogCleanup events cannot be deactivated as they are generated by the system.

4. To view an event, click the **View** link against the required event. The properties of the event are displayed.
5. To stop the Scheduler, click **Stop Scheduler** button. A screen is displayed showing that scheduler stopped successfully.
6. To start the scheduler, in the Change Scheduler State screen, click **Start Scheduler**. A screen is displayed showing that the scheduler started successfully.
7. To pause the Scheduler, click **Pause Scheduler** button. A screen is displayed showing that scheduler stopped successfully.

> The **Pause Scheduler** button changes to **Resume Scheduler**, once the scheduler is paused.
> When the scheduler is Stopped or Paused, the list of activated events is not displayed.

8. To resume the scheduler, click **Resume Scheduler** button. This resumes the scheduler and displays the scheduler screen.

9

MANAGING SECRET KEY

A secret key helps you to create encryption or decryption activity. Encryption and decryption activities are required to encrypt outgoing data and decrypt incoming data respectively.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

This chapter describes the following tasks:

- Creating Secret Key
- Exporting Secret Key
- Importing Secret Key
- Creating Keystore
- Exporting Certificate from the Keystore
- Importing Certificate into the Keystore

CREATING SECRET KEY

Steps to create a Secret Key activity

1. Click **[+] Administer** to expand the tree and then click **[+] Security**. All items in the Security category are displayed.
2. Click **Secret Key**. The **Manage Secret Key** screen is displayed (see Figure 30).

Figure 30: Manage Secret Key

3. Click the **New** link. The **Create Secret Key Activity** screen is displayed (see Figure 31).

Figure 31: Create Secret Key Activity

4. Enter the name and description of the new Secret Key in the textboxes **Name** and **Description** fields respectively.
5. Enter the password in the textboxes **Secret Key Password** and **Confirm Password** respectively.

> To learn about Advanced Properties refer to Developer Guide.

6. Click **Save** button. This displays a screen confirming that the Secret Key activity has been created successfully. If the **Comments** property is enabled, then clicking **Save** will display a screen where you need to enter comments related to creating the Secret Key (refer to Figure 7).
7. Enter the comments in the **Add Comments** field.

> The comment should be at least 1 character in length.

8. Click **OK** to save the comments. This displays a screen confirming that the Secret Key activity has been created successfully.

> By default, the Comments property is disabled. To enable it, refer to the section Updating System Properties.

EXPORTING SECRET KEY

Steps to export a Secret Key

1. Click **[+] Administer** to expand the tree and then click **[+] Security**. All the items in the Security category are displayed.
2. Click **Secret Key**. The Manage Secret Key screen is displayed (refer to Figure 30).
3. Select the radio button adjacent to required secret key activity that you want to export and then click **Export** link. A screen is displayed confirming that the Secret Key has been exported successfully.

> The exported Secret Key is stored in ../../AdeptiaServer-5.3/ServerKernel/etc/security/secret keys folder.

IMPORTING SECRET KEY

Steps to import a Secret Key

1. Click **[+] Administer** to expand the tree and then click **[+] Security**. All the items in the **Security** category are displayed.
2. Click **Secret Key**. The **Manage Secret Key** screen is displayed (refer to Figure 30).
3. Click **Import Secret Key** link. The **Import Secret Key** screen is displayed (see Figure 32).

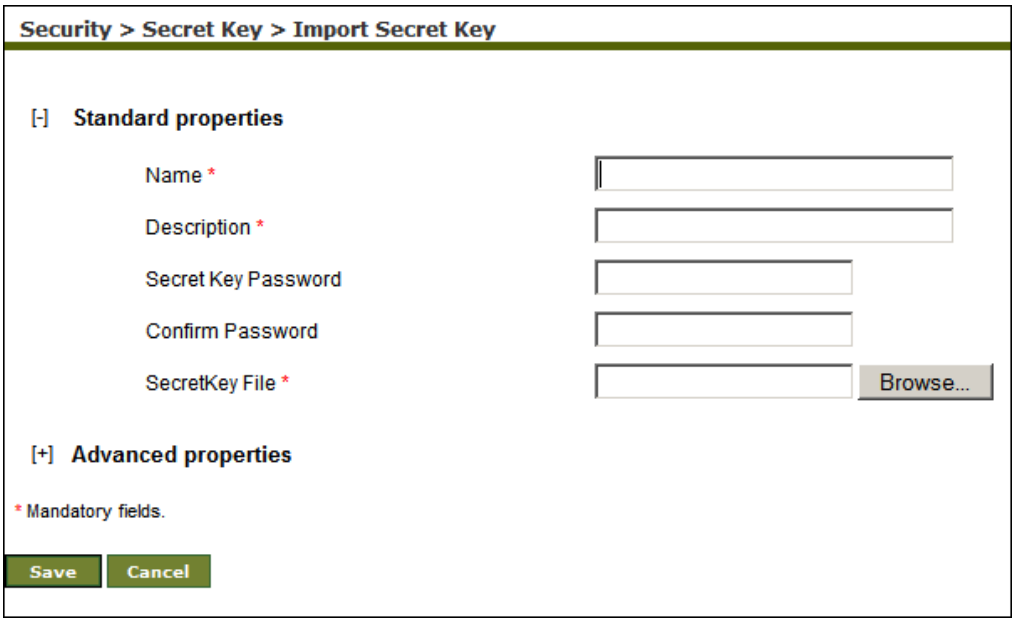


Figure 32: Import Secret Key

4. Enter the name and description for the Import Secret Key activity in the textboxes **Name** and **Description** respectively.
5. Enter the Secret Key to be used for encryption and decryption in textboxes **Secret Key Password** and **Confirm Password** fields respectively.

6. Click **Browse** button and select the Secret Key file to be imported from **../../AdeptiaServer-5.3/ServerKernel/etc/security/keystore** folder. The path of Secret Key file is displayed in **SecretKey File** textbox (see Figure 33).

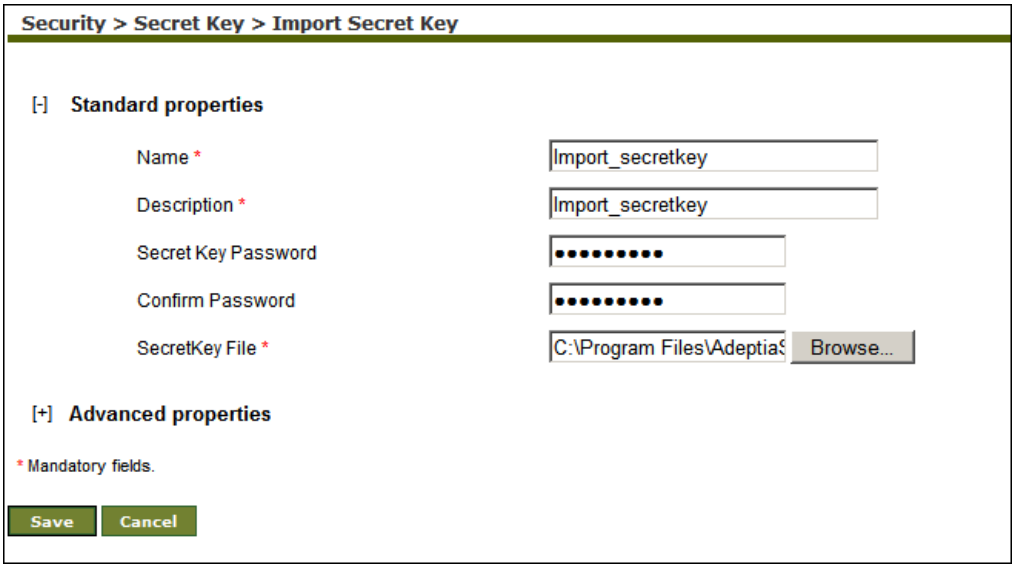


Figure 33: Select Secret Key File

To learn about Advanced Properties refer to the Developer Guide.

7. Click **Save** button. A screen is displayed confirming that the Secret Key activity has been imported successfully.

CREATING KEYSTORE

Steps to create Keystore

1. Click **[+] Administer** to expand the tree and then click **[+] Security**. All the items in the Security category are displayed.
2. Click **Keystore**. The **Manage Keystore** screen is displayed (see Figure 34).

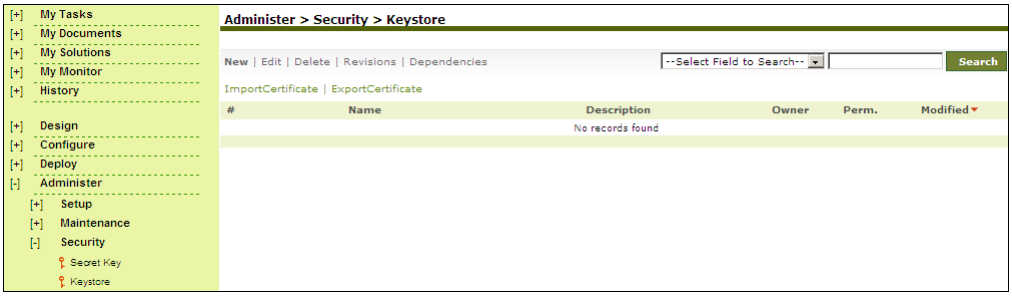


Figure 34: Manage Keystore

3. Click **New** link. The **Create Keystore** screen is displayed (see Figure 35).

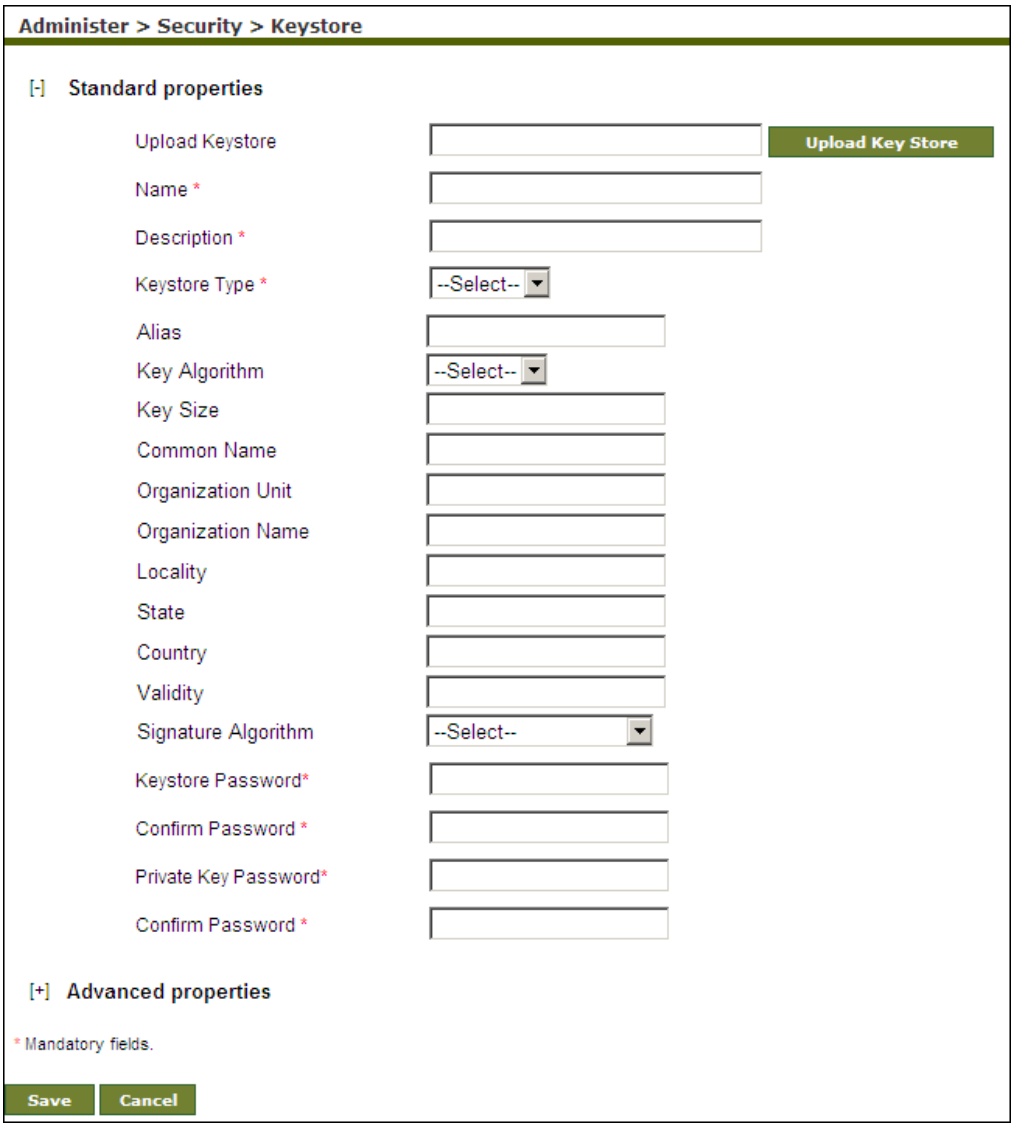


Figure 35: Create Keystore

4. To create a new keystore enter the name and description of the keystore activity in textboxes **Name** and **Description** respectively.
5. Enter values in all the fields and click **Save**. It creates a keystore and the private public key pair inside the keystore.
6. Alternately you can define a keystore by uploading the existing keystore.

To upload the keystore:

7. Enter the name and description in the textboxes **Name** and **Description**.
8. Select the keystore type from the drop-down list **Keystore**.
9. Enter the keystore password in **Keystore Password** and **Confirmed Password** field.
10. Click the **Upload Keystore** button and select the keystore.
11. After uploading the keystore, select the alias from the drop-down list **Alias**.

Rest of the fields is populated automatically.

12. Click **Save**.

Keystore with multiple key entries is not supported.

EXPORTING CERTIFICATE FROM KEYSTORE

Steps to export certificate from the Keystore

1. Click **[+] Administer** to expand the tree and then click **[+] Security**. All the items in the **Security** category are displayed.
2. Click **Keystore**. The **Manage Keystore** screen is displayed (see Figure 36).

Figure 36: Manage Keystore

3. Select the keystore from which you want to export the certificate, and click the **export** link. **Export Certificate** screen is displayed (see Figure 37).

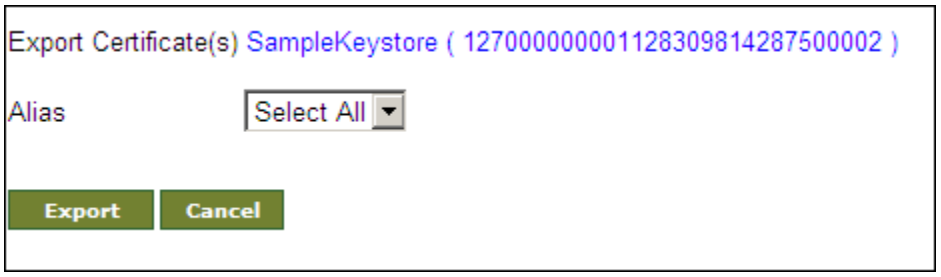


Figure 37: Export Certificate

4. Select the **Alias** name of the certificate, which you want to export and click **the Export** button. The selected certificate is exported in **/ServerKernel/ etc/security/WSdigitalcertificate** folder (see Figure 38).

Figure 38: Download Certificate

5. To view or download, the certificate click the **View/Download** link.

IMPORTING CERTIFICATE INTO KEYSTORE

Steps to import certificate into Keystore

1. Click **[+] Administer** to expand the tree and then click **[+] Security**. All items in the **Security** category are displayed.
2. Click **Keystore**. The **Manage Keystore** screen is displayed (see Figure 39).

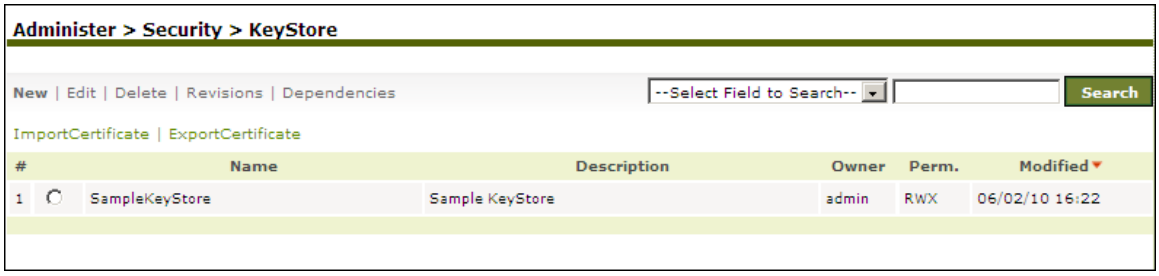


Figure 39: Manage Keystore

3. Select the keystore into which you want to import the certificate, and click the *Import* link. The **Import Certificate** screen is displayed (see Figure 40).

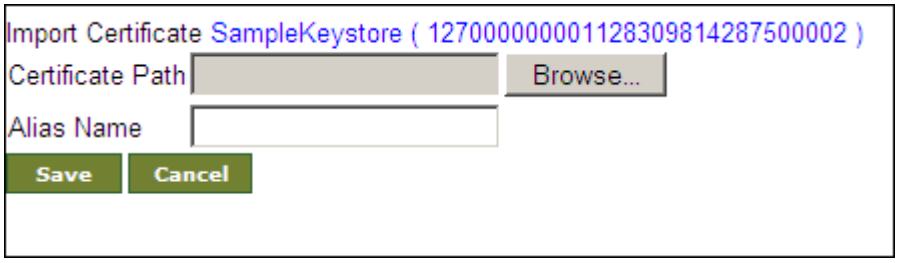


Figure 40: Import Certificate

4. Click the **Browse** button and select the select the certificate that you want to import.
5. Enter the alias name in the **Alias** *Name* field.
6. Click **Save**. The selected certificate is imported in the selected keystore.

10

MONITORING RUNNING PROCESS FLOWS AND LOGGED IN USERS

The Monitoring applet of the Adeptia Suite allows you to view running activities and memory usage of the system. It displays information about the nodes that are part of cluster, details of each node in the cluster and the Process Flow Execution Report. It provides information about the following:

- System Load Analysis (Process Flow Execution History of the Cluster)
- Cluster Nodes (Nodes of the Cluster)
- Details of each Node
- System Activities at each node
- Current Users logged in
- Kernel Memory usage
- Process Flow Status
- Node Load Analysis
- Configuring Refresh Time

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

This chapter describes the following tasks:

- Monitoring Adeptia Suite Cluster System
- Monitoring System Status of Node
- Monitoring Process Flows on Node
- Viewing Process Flow Execution History of Node
- Configuring Monitoring Properties

MONITORING ADEPTIA SUITE CLUSTER SYSTEM

Prerequisites

- The *Pop-up Blocker* needs to be disabled in the web browser, to open the Monitoring applet. By default, the *Pop-up Blocker* is enabled.

Steps to monitor Adeptia Suite Cluster

1. Click **[+] Administer** to expand the tree and then click **System Status**. All items in the **System Status** category are displayed.
2. Click **System Monitor**. This loads the **Monitoring** applet and displays Adeptia Suite cluster status (see Figure 41).

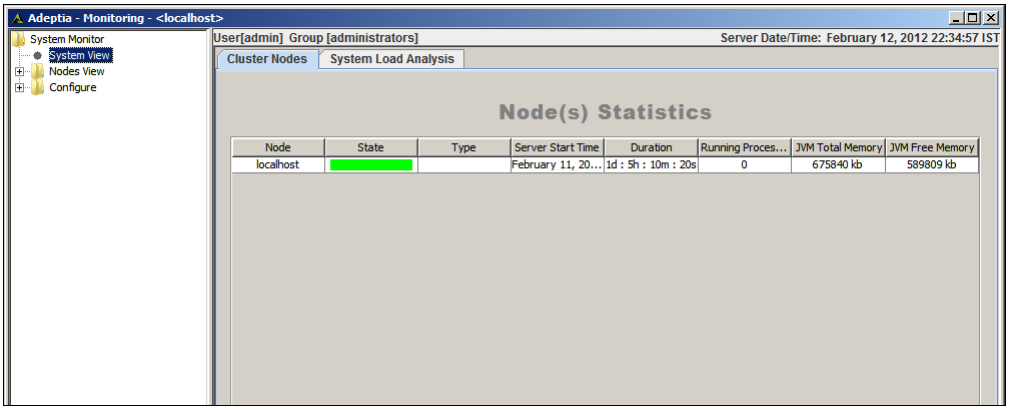


Figure 41: Adeptia Suite Cluster Status

3. The **Monitoring** applet is divided into two parts. The left pane displays the list of components that can be monitored or configured. The right pane displays the details of the components selected in the left pane. The right pane is further divided into two parts. The **Cluster Nodes** tab displays the Node statistics of the Adeptia Suite. The **System Load Analysis** tab displays the Process Flow execution history of the Adeptia Suite Cluster. The **Cluster Nodes** tab is selected by default.
4. The **Cluster Nodes** tab displays a list of nodes of the cluster (refer to Figure 41). There are various cluster nodes listed under the Cluster Nodes tab. These are listed in the table below.

Table 4: Node Statistics

Node	Name of each Node
Node	Name of the Node
State	State of the Node whether Active or Inactive.
Type	Type of the node whether the node is Server or member
Server Start Time	Starting time of Adeptia Suite Kernel on the selected Node
Duration	Time elapsed since the Adeptia Suite Kernel has started
Running Processes	Number of process flows that are currently in running state
JVM Total Memory	Memory allocated to Adeptia Suite Kernel
JVM Free Memory	Available memory of Adeptia Server Kernel

5. Click the **System Load Analysis** tab. This displays **Process Flow Execution History** (see Figure 42).

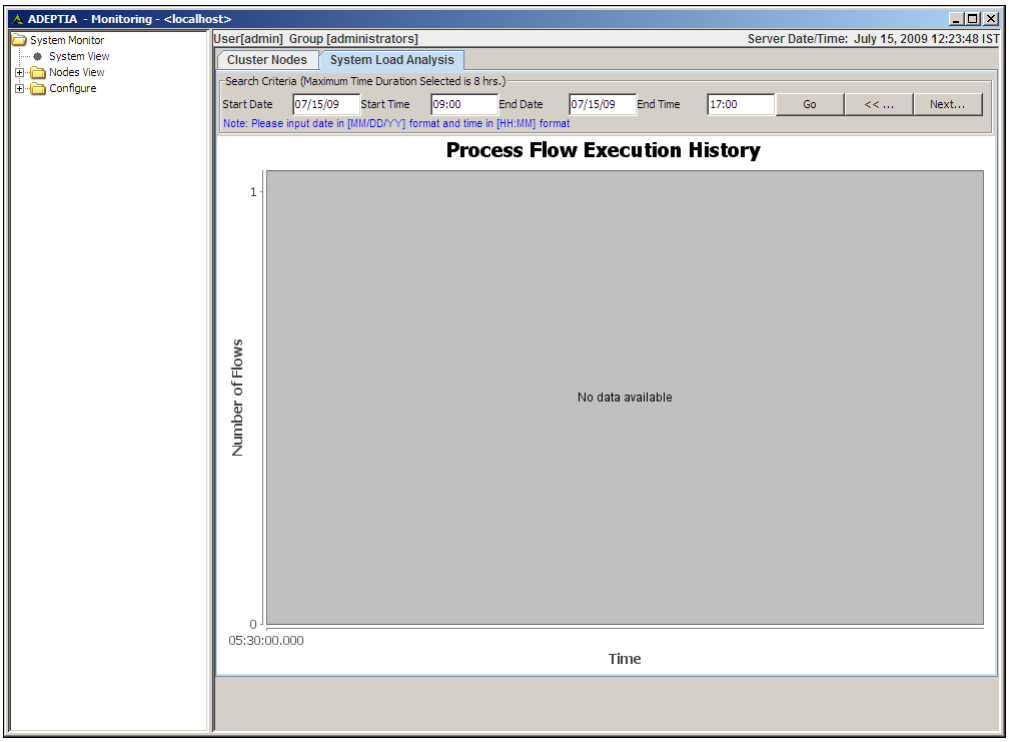


Figure 42: Process Flow Execution History

6. Enter the date range and the time interval for which you want view the Process Flow execution history and click **Go** button. This displays the process flow history for the specified time interval (see Figure 43).

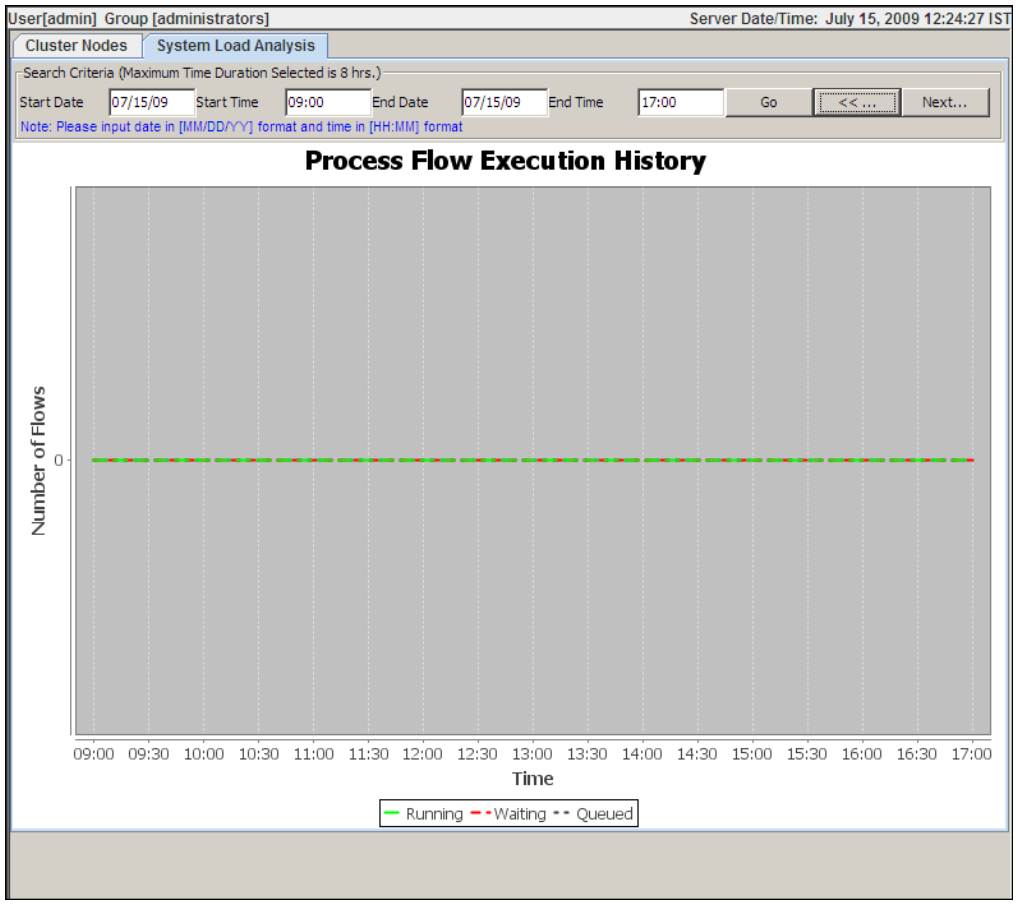


Figure 43: Process Flow Execution History

MONITORING SYSTEM STATUS OF NODE

Steps to view all system activities of a node

1. Click **[+] Node View** on the **Node(s) Statistics** screen to expand the tree and then click required node. This displays the system status of the selected node (see Figure 44).

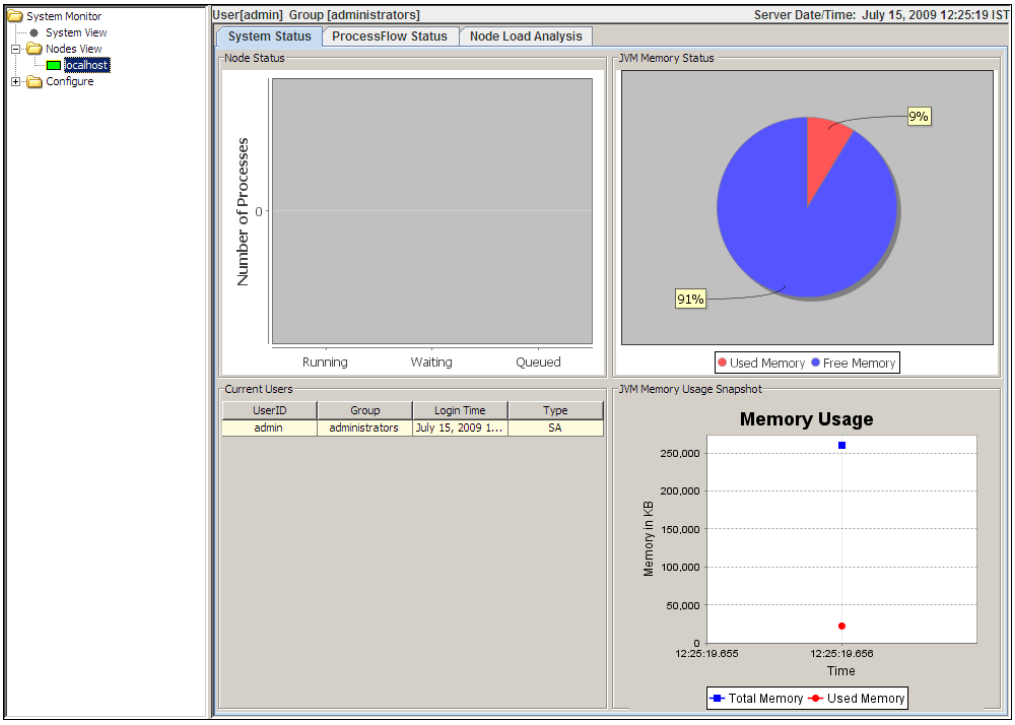


Figure 44: View System Status

2. This screen has three tabs: **System Status**, **Process Flow Status** and **Node Load Analysis**. By default, the **System Status** tab is selected and shows the following information:

   - **Node Status** bar chart displays the number of Process Flows that are *Running, Waiting* and *Queued*.
   - **JVM Memory Status** pie chart displays *Used Memory* and *Free Memory*.
   - **JVM Memory Usage** snapshot shows a graph of *Memory Usage* (in KB) against *Time*.
   - **Current Users** shows the list of users currently logged in, group to which they belong, their login time and the user type.

MONITORING PROCESS FLOWS ON NODE

Steps to view status of process flows on a node

1. Click **Process Flow Status** tab on the screen displayed in Figure 44. This tab displays the **Process Flow Status** screen (see Figure 45).

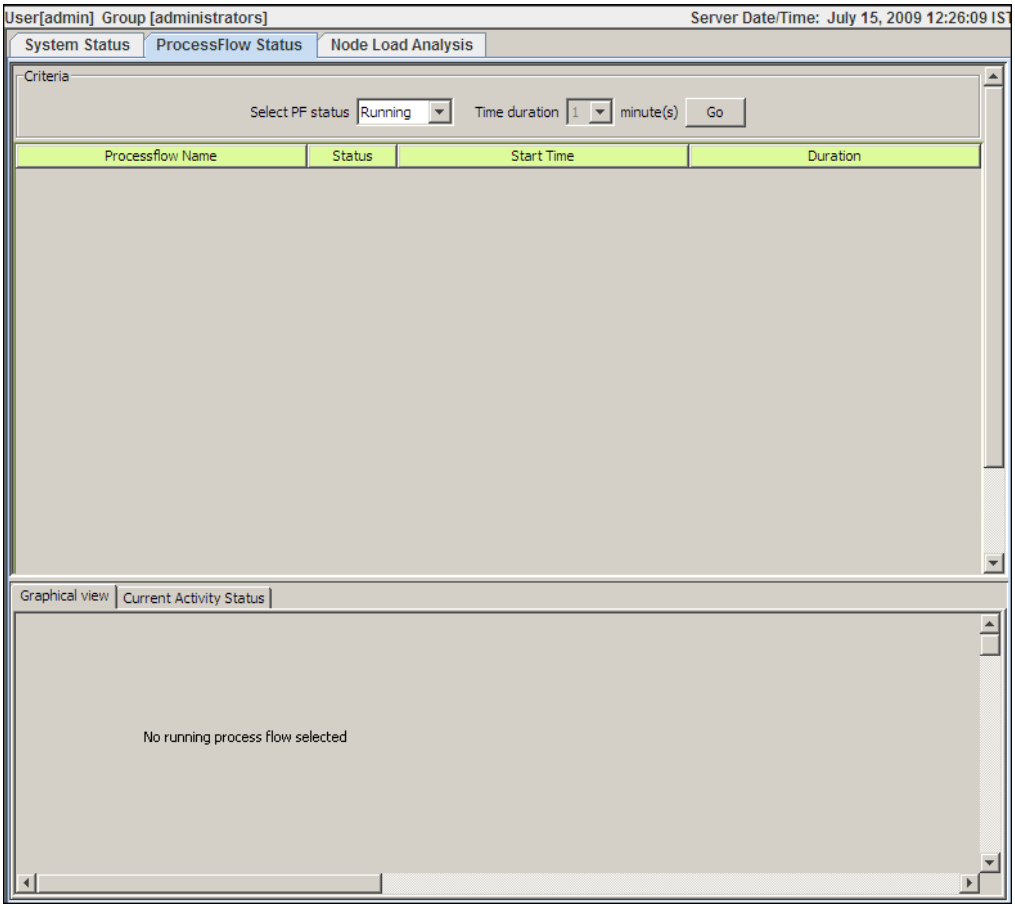


Figure 45: Process Flow Status

This screen is divided into two parts. The first part displays the statistical graph of the process flow with respect to the time elapsed. By default it shows the currently running Process Flows. It further enables you to view this graph based on specified search criteria. The second part displays details and a graphical view of the selected process flow.

2. Enter the criteria to view the statistical graph of the process flow in the first part of the screen. Select the status of the process flow that you wish to view, from the **Select PF Status** drop-down menu. By default, **Running** is selected.

3. Select the time duration elapsed (in minutes) for which you wish to view the statistical graph, from the **Time Duration** drop-down menu. By default, 1 is selected. This time duration is considered from the time when last process flow is executed. For example, if you select 15 minutes and the last process flow is executed before half an hour from now, the process flows which are executed within 45 minutes from now, are shown.

4. Click **Go** button. This displays a list of the process flows based on the entered criteria, in a tabular format (see Figure 46).

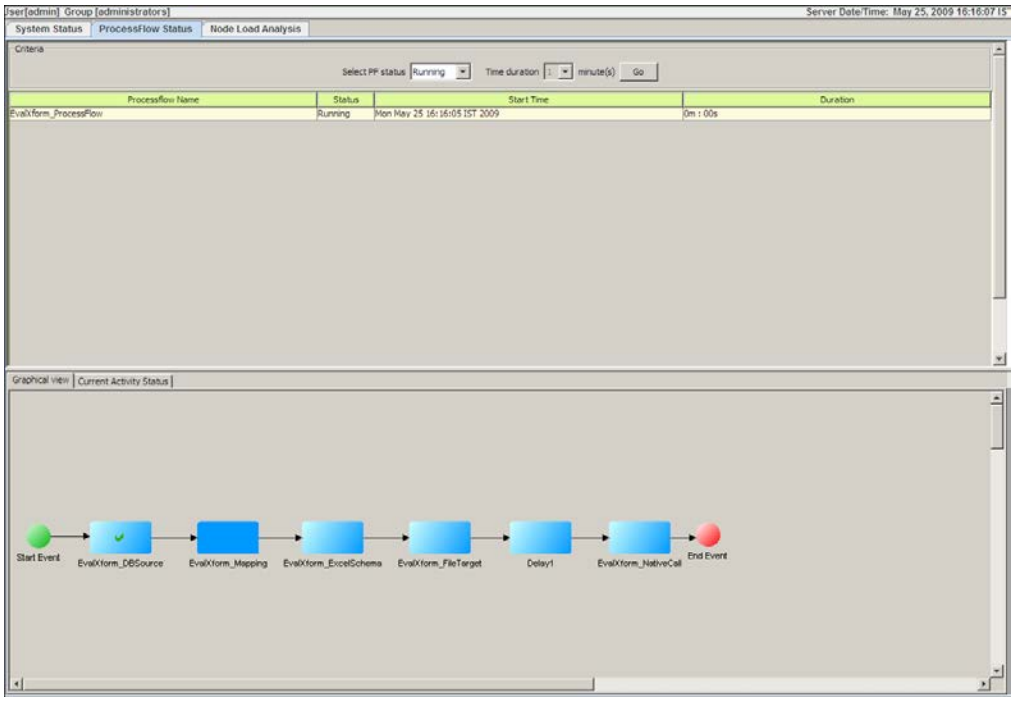


Figure 46: Process Flow Status

5. Click the required Process Flow, from the first part of the screen to view the details of the Process Flow. Details of the selected Process Flow are displayed in the second part of the screen. By default first process flow is selected (refer to Figure 46).

6. The second part of the screen has two tabs: **Graphical View** and **Current Activity Status**. By default, **Graphical View** is selected. This tab displays a graphical presentation of the selected process flow.

- The activity that is currently running on the Adeptia Suite is indicated as blinking.
- If the activity has been executed successfully, then a check sign (✔) is displayed on the activity field.
- If the activity has been aborted or failed due to some reason, then a cross sign (✘) is displayed on the activity field.

7. Click the **Current Activity Status** tab (see Figure 47).

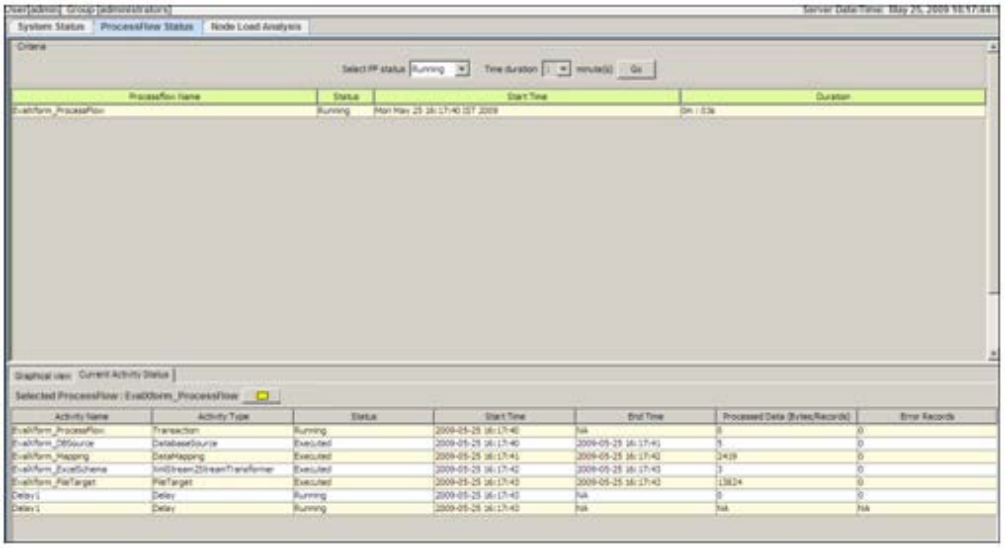


Figure 47: Current Activity Status

8. This screen displays the following details of all activities in the currently running process flow:

   - Name of the Process Flow
   - Activity Type
   - Current status of each activity of the process flow
   - Start and end time of the execution of activity
   - Processed data
   - Number of Error records

> Processed Data shows the data of a particular activity that is processed. Processed data is shown either in bytes or as records depending on the type of activity. For example, processed data is shown in bytes for a source activity and as records for mapping activity.

9. To abort a running process flow, click kill  button.

VIEWING PROCESS FLOW EXECUTION HISTORY OF NODE

Steps to view Execution History of Process Flows of a node

1. Click **Node Load Analysis** tab on the screen displayed in Figure 44. This displays the **Process Flow Execution History** screen (see Figure 48).

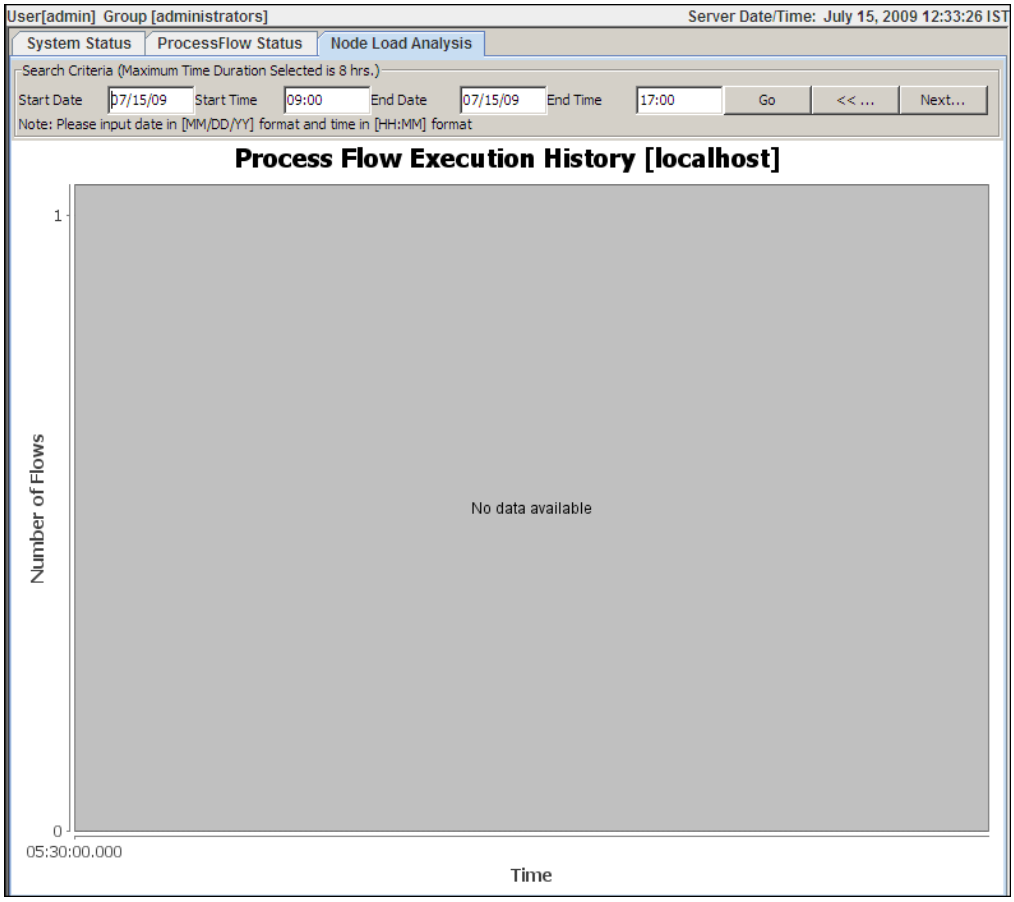


Figure 48: Node Load Analysis

2. Enter the time interval for which you want view the Process Flow execution history and click **Go** button. This displays the Process Flow History for the specified time interval (see Figure 49).

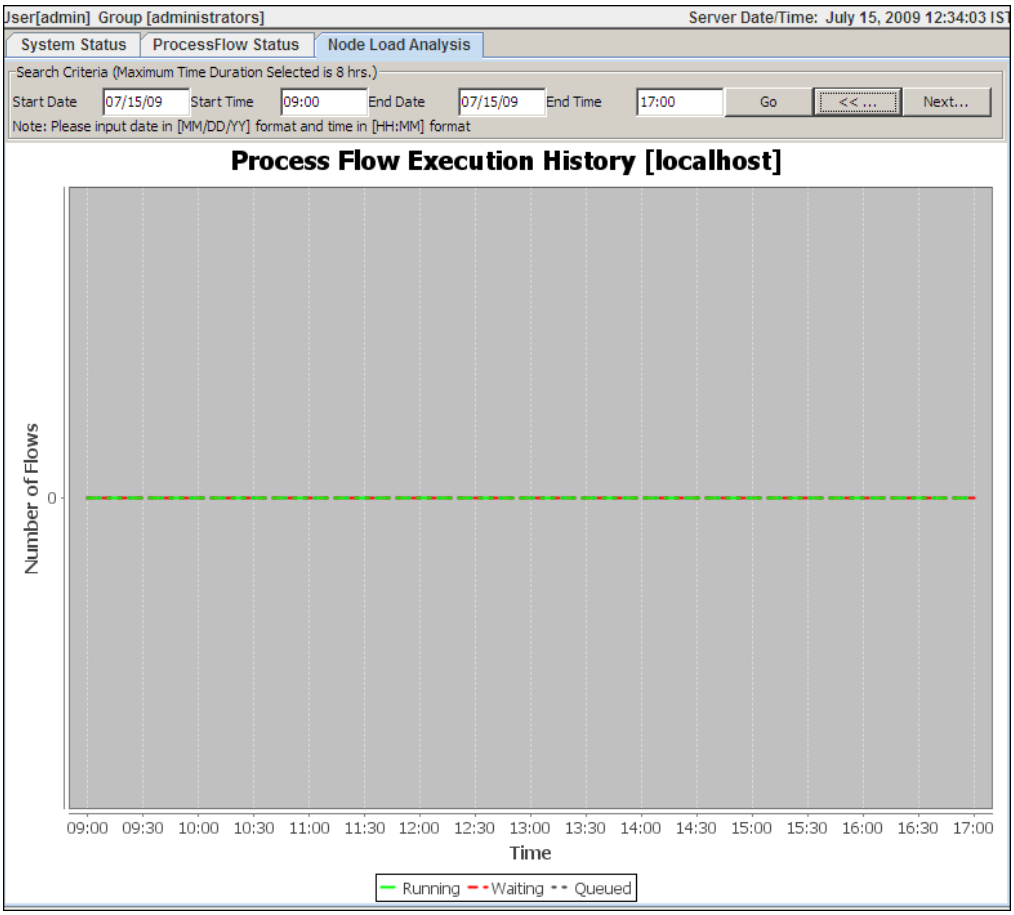


Figure 49: Process Flow Execution History

3. This screen displays a statistical view of all process flows that are *running*, *waiting* or *queued* at various time intervals on the selected node.

Process Flows are identified based on their status color.

CONFIGURING MONITORING PROPERTIES

Steps to configure monitoring related properties

1. Click **[+] Configure** on the Node(s) Statistics screen to expand the tree and then click **Properties**. This displays the **Configure Properties** screen (see Figure 50).

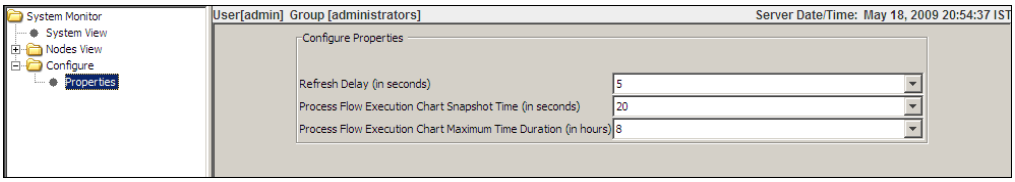


Figure 50: Configure Monitoring Properties

2. This screen displays options to configure following properties:

   - **Refresh Delay**: Time duration (in seconds) after which monitoring statistics are refreshed
   - **Historical Chart Snapshot Time**: Time interval (in seconds) between two successive snapshots taken to show system load in the Historical Chart. For example if this is set to 60 second (1 Minute), Historical Chart will take snapshot at every 1 minute interval (e.g. 12.00.00, 12.01.00). If a process flow starts and stops within snapshot interval, it will not be displayed in Historical chart.
   - **Historical Chart Maximum Time Duration**: Maximum time duration (in hours) for which process flow execution history can be viewed.

11

DEPLOYING CLUSETRING

Adeptia Suite provides integrated clustering services to deliver higher levels of service and availability. A cluster is a group of independent Adeptia Suites working collectively as a single system. Clustering provides high-availability, scalability, and manageability for resources and applications by grouping multiple servers running Adeptia Suite.

Clustering is used for:

- Load Balancing: This is used to distribute the execution of process flows evenly between the members of the cluster so that no single Adeptia Suite is overloaded. Load balancing is especially important for networks where it is difficult to predict the number of requests that is issued to a server. Adeptia Suite supports Round- Robin method for load balancing.
- Fail Over Capability: When one of the Adeptia Suites in a cluster environment fails then other Adeptia Suites detect this failure and automatically handle any new process flow execution request.
- Scalability: Cluster services can grow to meet rising demands. When the overall load exceeds the capabilities of the cluster, additional nodes can be added.

The first Adeptia Suite to start in a cluster is designated as a server Node and all subsequent Adeptia Suites are designated as member nodes in that cluster. The Server node regularly checks the member nodes for their status to determine their availability for process flow execution. In case of a server node failure, one of the member nodes (node with maximum up time) automatically takes over the responsibility of the server node for managing load distribution in the cluster.

In the Adeptia Suite this feature is available in:

EBIS Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

This chapter describes the following tasks:

- Enabling Clustering service
- Starting Adeptia Suite in Clustering mode
- Viewing Clustering status

ENABLING CLUSTERING SERVICE

Clustering service, by default, is disabled. To enable clustering, you need to enable clustering, as described below, in each of the node of the cluster.

Prerequisites

- Adeptia Suite must be installed on each node of the cluster.
- All the nodes of the cluster should use common backend and log database defined in server-configure.properties file in the **../../AdeptiaServer-5.3/ServerKernel/etc** folder.

When you install Adeptia Suite, no option is displayed to select the backend database You can only configure the log database.

By default HSQLDB, which is an embedded database, is used as backend.

To use a common database as backend, you need to run the installer from the command prompt with an additional argument. as shown below:

install.exe -DConfigureBackendDatabase=true

When you use the above command to start the execution, an additional screen is displayed, where you can select the database to be used as backend. Enter the required configuration of database, which will be used as backend. In all subsequent installation select the same database as backend. In this way the same database will us used as backend.

- Date and time of all the nodes must be same.
- Nodes of the cluster should be started in sequence. It means Kernel and WebRunner of one node must be started completely before starting them on other node.

Steps to enable Clustering service

1. Click **[+] Administer** to expand the tree and then click **[+] Setup**. All the items in the **Configure** category are displayed.
2. Click **Application Settings**. The **Application Settings** screen is displayed (see Figure 51).

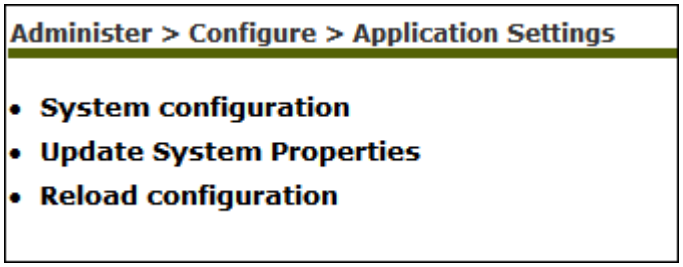


Figure 51: Application Settings

3. Click **Update System Properties**. The **Update System Properties** screen is displayed (see Figure 52).

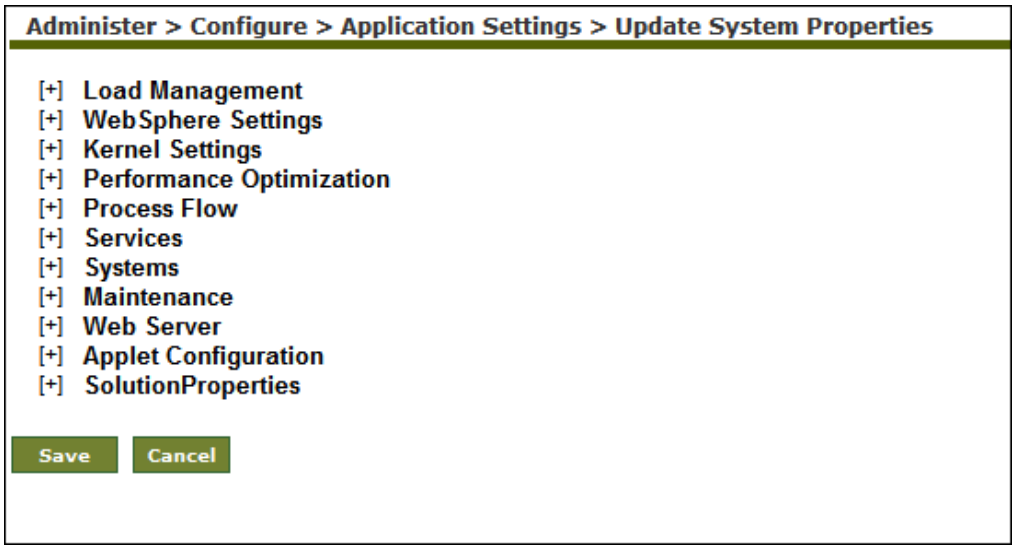


Figure 52: Update System Properties

4. Click **[+]** to expand **Load Management** (see Figure 53).

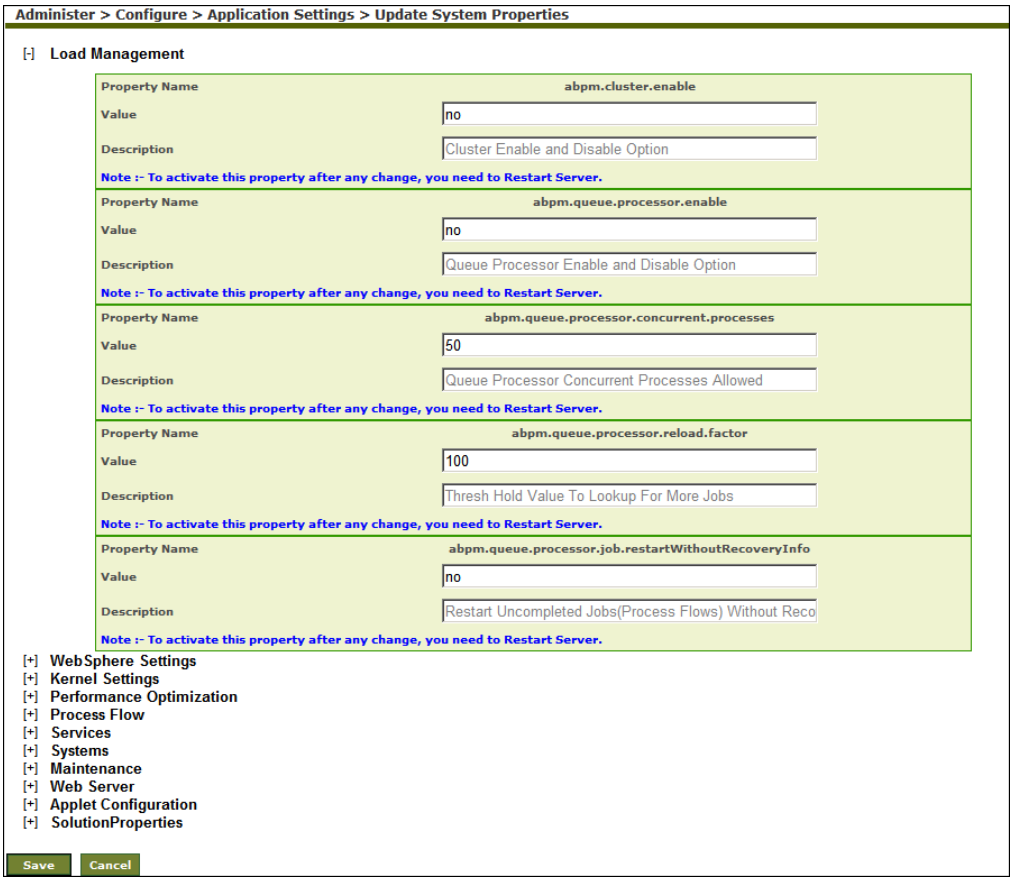


Figure 53: Expand Load Management Properties

5. In **Value** field of the property *abpm.cluster.enable*, replace *no* with *yes* (see Figure 54).

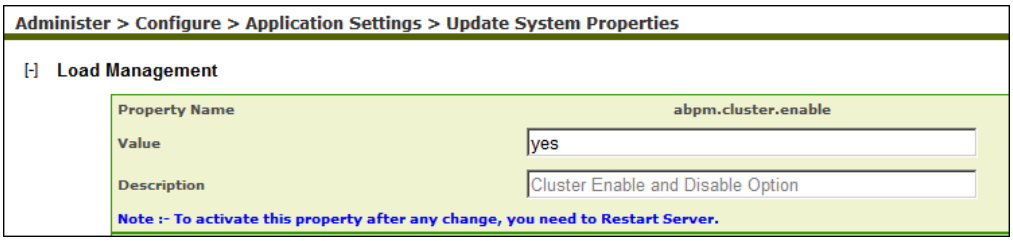


Figure 54: Edit Load Management Properties

6. Click **[+]** to expand **Kernel Settings** (see Figure 55).

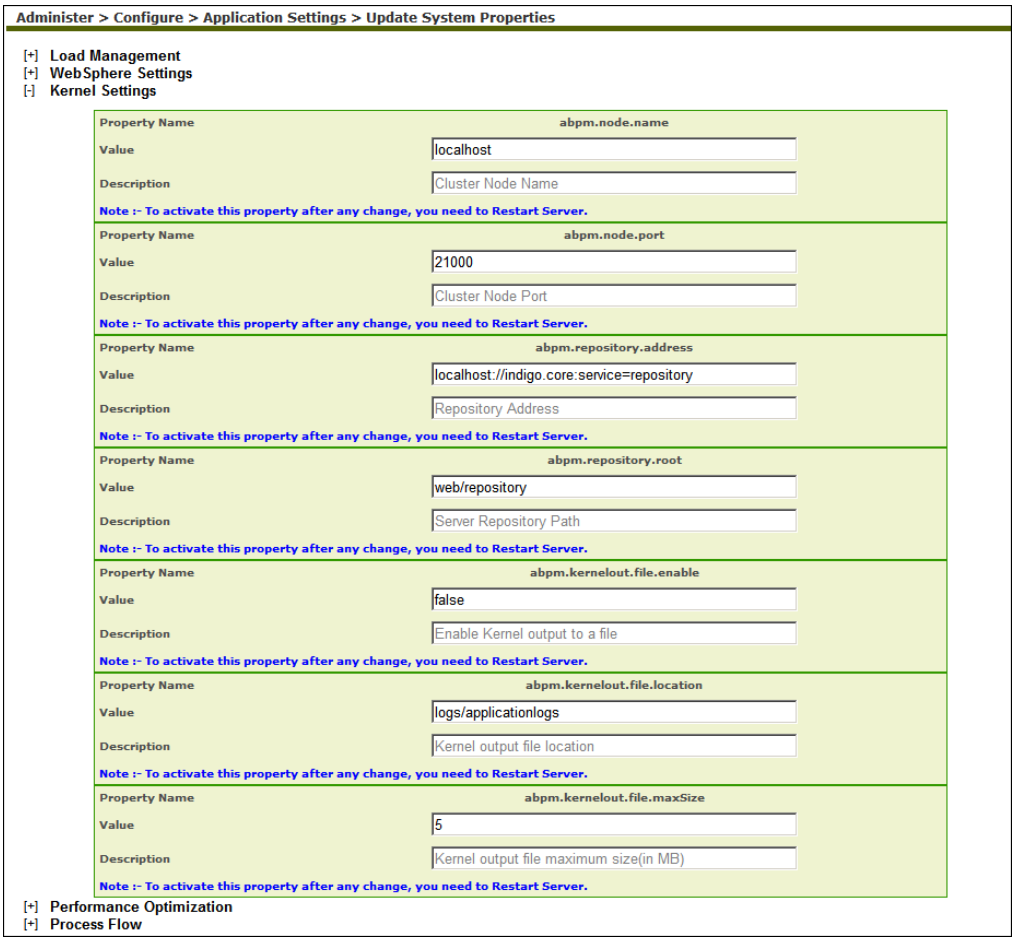


Figure 55: Edit Kernel Settings Properties

7. In **Value** column of the property *abpm.node.name*, replace localhost with the IP address of the server on which the Adeptia Suite is installed.

For example, if the IP address of the server where Adeptia Suite is installed is '192.168.1.1' the value should be 192.168.1.1 .

8. In **Value** column of the property *abpm.repository.address*, replace the localhost with the IP address of the Server on which the Adeptia Suite is installed (see Figure 56).

For example, if the name of the Server where Adeptia Suite is installed is '192.168.1.1' the value should be 192.168.1.1://indigo.core:service=repository.

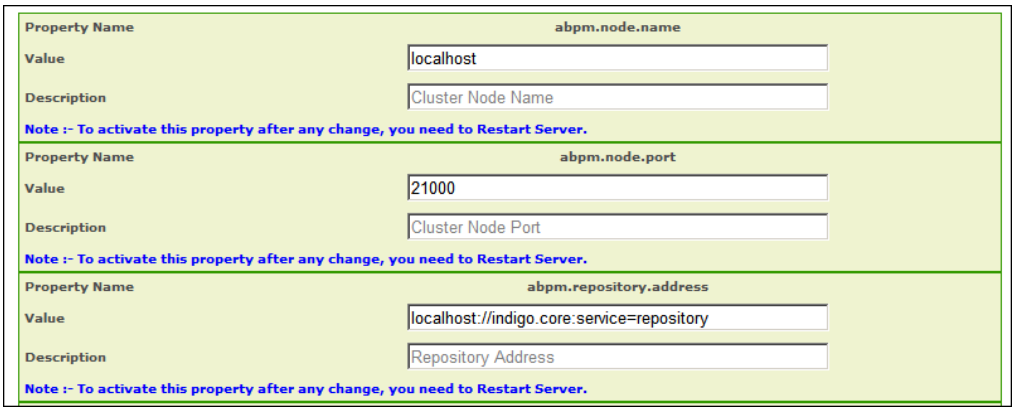


Figure 56: Enable Clustering

9. The value of property *abpm.repository.root* must be same for all nodes of the cluster. This property defines a location where intermediate data files are stored for each of the nodes. Preferably this should be a shared folder in the network, which can be accessed by all the nodes of the cluster, for example \\192.168.1.1\Repository. Here 192.168.1.1 is the IP address and Repository is the shared folder. There should not be any username/password required to connect to this folder. In case the shared folder, which you will use for repository, resides on linux OS, you should mount this shared folder as local drive on all the nodes of the cluster and define the absolute path in the *abpm.repository.root* folder.

10. Click **Save** button to save the changes. A screen is displayed confirming that system properties have been saved.

> Changes made in the System properties do not come into effect until you restart the Kernel and WebRunner. So restart the Kernel and WebRunner.

11. Go to the folder **../../AdeptiaServer-5.3/ServerKernel/etc/Cluster** on the server where Adeptia Suite is installed.

12. Open the clustering-service.xml file in text editor. The contents of the file are as displayed in Figure 57.

```
<?xml version="1.0" encoding="UTF-8"?>
<mbeans-descriptors>
 <mbean
  descriptor="com.adeptia.indigo.cluster.ClusterMember"
name="bpm.core.cluster:name=BPMCluster,node=node1" port="21000">
 </mbean>
</mbeans-descriptors>
```

Figure 57: XML File in Text Editor

13. Replace the word *node1* with the IP adress of the server where Adeptia Suite is installed and will be a part of the cluster. When a Adeptia Suite starts in cluster environment, it looks for the IP address of server, where it has been installed in clustering-service.xml

14. To add more nodes in the cluster, for each node, add the following lines in the clustering-service.xml file and replace the node1 with the IP adress of the server.

```
<mbean
descriptor="com.adeptia.indigo.cluster.ClusterMember"
```

```
name="bpm.core.cluster:name=BPMCluster,node=node1" port="21000">
</mbean>
```

15. For example, if there are three Servers (192.168.1.1, 192.168.1.2 and 192.168.1.3) in the cluster, the clustering-service.xml file will be as displayed below (see Figure 58)

```
<?xml version="1.0" encoding="UTF-8"?>
<mbeans-descriptors>
 <mbean
   descriptor="com.adeptia.indigo.cluster.ClusterMember"
name="bpm.core.cluster:name=BPMCluster,node=192.168.1.1" port="21000">
</mbean>
<mbean
descriptor="com.adeptia.indigo.cluster.ClusterMember"
name="bpm.core.cluster:name=BPMCluster,node=192.168.1.2" port="21000">
</mbean>
<mbean
descriptor="com.adeptia.indigo.cluster.ClusterMember"
name="bpm.core.cluster:name=BPMCluster,node=192.168.1.3" port="21000">
 </mbean>
</mbeans-descriptors>
```

Figure 58: Edited XML File

16. Save the file and close it.

Step 1 to 16 must be performed on all the servers that will be part of Cluster.

Instead of making same changes in clustering-service.xml file of all servers, you can make changes in only one server and copy the file on other servers

STARTING ADEPTIA SUITE IN CLUSTERING MODE

Adeptia Suite version 5.3 onwards no additional steps are needed to start the kernel and WebRunner in clustering mode. Only you need to make sure that Kernel and Webrunner on one node must be completely started before you start them on another node.

This section explains:

- Starting Adeptia suite in Clustering Mode on Windows
- Starting Adeptia Suite in Clustering Mode on Linux

Starting Clustering on Windows

Steps to start Adeptia Suite in Clustering Mode on Windows

1. Go to **../AdeptiaSuite/bin** folder.
2. To start the Kernel and WebRunner, double click the **Kernel.exe** and **WebRunner.exe** respectively.
3. Wait until the Kernel and WebRunner on this node is completely started.

4. Now repeat above steps to start the Kernel and WebRunner on each node of the cluster.

> To learn how to login into the Adeptia Suite, refer to section *Login into Adeptia Suite* in the *Getting Started* guide**.**

Starting Clustering on Linux

Steps to start Adeptia Suite in Clustering Mode on Linux

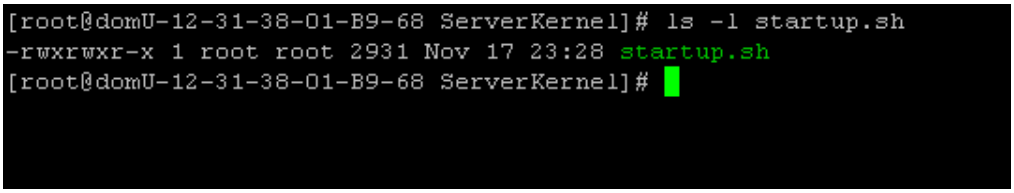
1. Change directory where Adeptia Suite is installed using following command:

   ```
   cd /usr/local/bin/AdeptiaSuite/AdeptiaServer-5.3/ServerKernel/
   ```

2. Ensure the ***startup.sh*** file has **Execute** permission using following command:

   ```
   ls –l startup.sh
   ```

   Example:



3. Execute ***startup.sh*** using following command:

   ```
   ./startup.sh
   ```

> This command starts both Kernel and Webrunner.

4. Wait until the Kernel and WebRunner on this node is completely started.
5. Now repeat above steps to start the Kernel and WebRunner on each node of the cluster.

VIEWING CLUSTERING STATUS

The Clustering status shows a list of the member servers and their status whether available or not.

Steps to view clustering status

1. Click **[+] Administer** to expand the tree and then click **[+] System Status**. All the items in the **System Status** category are displayed.

2. Click **System Monitor**. The Monitoring applet is displayed with the list of nodes of the cluster (see Figure 59).

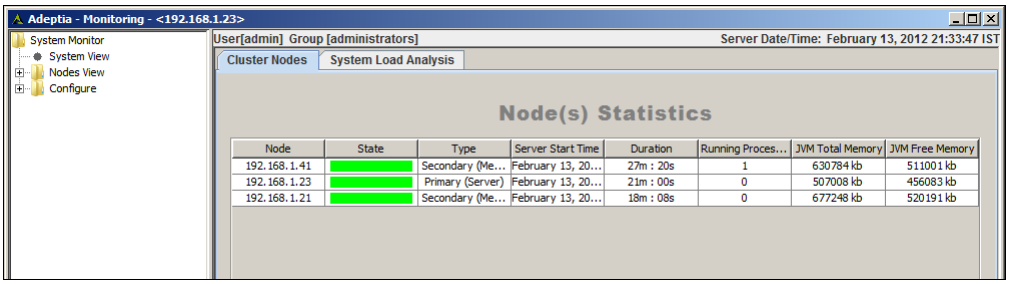


Figure 59: Node(s) Statistics

The green color in the State column denotes that the node is in active state and the part of the cluster.

The red color in the State column denotes that the node is not available.

The yellow color in the state column denotes that the node is active but not the part of cluster.

To know, how to view the details of each node of a cluster, refer to the section Monitoring System Status of Node

RECOMMENDED SETTING

This section describes the recommended setting, while using clustering.

The following table lists the properties, there recommended value and the description.

Property Category/Property Name	Recommended Value	Description
Load Management > abpm.queue.processor.enable	yes	Queue Processor should be enabled.
Load Management > abpm.queue.processor.job.restart WithoutRecoveryInfo	yes	Recovery through Queue Processor should be enabled. When this property is set to *yes,* all the running process flow get recovered from the beginning in case the kernel is restated.
Process flow > abpm.transaction.recovery.enable	No.	When this property is set to *yes,* partial recovery of running process flows are done. In this case following process flows are not recovered: • Child flows executed through *Call* • Child flows executed through *spawn* and *wait for child* is set to *true.*

		Partial recovery is not recommended and hence this property should be set to *no.*

12

MONITORING ADEPTIA SUITE PERFORMANCE

To ensure efficient management and high availability of the Adeptia Suite for various business requirements, you may need to monitor the status and performance of Adeptia Suite. For this, you need to understand the usage of various resources such as memory, log database and repository database etc.

Adeptia Suite enables you to monitor the performance of the Adeptia server with the help of various parameters. To monitor various parameters of Adeptia Suite, you need to give your request in the form of a HTTP request. The current values of these parameters are retuned in the XML data.

This chapter enables you to understand that how can you monitor the performance of the Adeptia server and which parameters are displayed. In addition, it also explains how this information is presented to the user.

In the Adeptia Suite this feature is available in:

EBIM Suite	BPM Suite	ESB Suite	ETL Suite
√	√	√	√

Prerequisites

- You must start the Kernel and the WebRunner before monitoring the Adeptia server.

Adeptia Suite enables you to monitor the performance of the Kernel and WebRunner separately. In addition, you can also monitor the performance of the complete cluster as well.

To monitor the Adeptia Suite, you need to send a request as a HTTP URL. The format for the HTTP URL is:

http://<hostname>:<port>/adeptia/control/monitorMatrix?monitorFlag=<monitorflag>&matrixFlag=<matrixflag>

Here,

<**hostname**> in the address is the name of the Server on which Adeptia Suite is running.

<**port**> is the Web server HTTP port number i.e. on which HTTP Adeptia Suite WebRunner is running. By default, Adeptia Suite WebRunner runs at 8080 port.

<**monitorflag**> is used to define the JVM for which you want to monitor the performance. <monitorflag> can have any of the following three values:

- kernel
- webrunner
- cluster

- When you set *kernel* as the monitorflag, then parameters of kernel JVM are displayed.
- When you set *webrunner* as the monitorflag, the parameters of webrunner JVM are displayed.
- When you set *cluster* as the monitorflag, status of all nodes of the cluster are displayed.
- When you set <monitorflag> to cluster then you need not provide any value for the <matrixflag>. Then the format for the HTTP URL is:

  http://<hostname>:<port>/adeptia/control/monitorMatrix?monitorFlag=<cluster>

<**matrixflag**> is used to define the category of parameters for which you want to monitor. Each category of parameters has a set of properties. The <**matrixflag**> can have any of the following values:

- memory
- gc
- thread
- repositoryDB
- logDB
- all
- default

Error! Reference source not found. lists these categories and the parameters displayed in each category.

Table 5

Category	Parameter	Description
memory	UP-TIME OF JVM	Up-time of the JVM shows how long the JVM has been running.
	HEAP MEMORY	Heap Memory is the storage for Java objects. Heap memory is the run-time data area from which the JVM allocates memory for all class instances and arrays.
	MAX MEMORY	MAX Memory is the maximum amount of memory to which heap can grow.
	USED MEMORY	USED Memory is the amount of heap memory in use.
	COMMITTED MEMORY	Committed Memory is the amount of memory allocated to heap.
	INIT MEMORY	Init Memory is the amount of memory, which JVM initially requests from Operating System for memory management.
	NON-HEAP MEMORY	Non-heap memory includes a method area shared among all threads and memory required for the internal processing or optimization for the JVM. Non-heap Memory is used by Java to

		store loaded classes and other meta-data.
	MAX MEMORY	MAX Memory is the maximum amount of memory that can be used for memory management.
	USED MEMORY	USED Memory is the amount of memory currently used. Memory used includes the memory occupied by all objects.
	COMMITTED MEMORY	Committed Memory is the amount of memory guaranteed to be available for use by the JVM.
	INIT MEMORY	Init Memory is the amount of memory, which JVM initially requests from Operating System for memory management.
gc	GARBAGE COLLECTION	Garbage Collection (GC) is how the JVM frees memory occupied by objects that are no longer referenced. It is the process of releasing memory used by the dead objects.
	GARBAGE COLLECTOR NAME	Garbage Collector Name is the name of the memory manager.
	GARBAGE COLLECTIONS	Garbage Collections are the total number of collections that have occurred.
	TOTAL TIME SPENT	Total Time Spent is the approximate accumulated collection elapsed time.
thread	PEAK THREAD	Highest number of live threads since JVM started.
	PEAK THREAD COUNT	Counts the peak live thread since the JVM started or peak was reset.
	LIVE THREAD	Current number of live daemon threads plus non-daemon threads
	LIVE THREAD COUNT	Counts the current number of live threads including both daemon and non-daemon threads.
	DAEMON THREAD	Threads that work in the background to support the runtime environment are called daemon threads.
	THREAD DEADLOCK COUNT	Counts the number of threads that are in deadlock waiting to acquire object monitors or synchronizers that can be owned.
logDB/ repositoryDB	DATABASE MATRIX TYPE	It shows the type of database. The database can be log database and repository database.
	STATUS	It shows whether the connection to database is active or not. Its values are UP/DOWN.
	ACTIVE CONNECTION COUNT	Counts the current number of active connections that have been allocated from the data source.

	IDLE CONNECTION COUNT	Counts the current number of idle connections that are waiting to be allocated from the data source.
	QUERY RESPONSE TIME	It describes the response time of SQL statement issued to database. By default Query Response Time is not displayed. To know how to view Query Response Time, refer to section Monitoring Query Response Time.
cluster	CLUSTER NODE MATRIX	A cluster is a group of independent Adeptia Suites working collectively as a single system.
	NODE NAME	It shows the IP address of the nodes that are a part of cluster.
	TYPE	It specifies the type of node that is PRIMAY (SERVER) or SECONDARY (MEMBER).
	STATUS	It **s**pecifies if a node is up (running) or not. Its values can be UP/DOWN.
	NETWORK LINK	It **s**pecifies if network link to this node is UP/DOWN.
all	It displays every parameter of all categories.	
default	It displays set of default parameter. To know how to define default parameters, refer to Configuring Default Monitoring Parameters.	

The performance of Adeptia Server is presented in the XML format. In response to the request sent to Adeptia Suite in the form of URL, an XML page is displayed. This XML page displays the information with respect to the flags passed in the URL.

For example, if Adeptia Suite is running on your local machine and if you hit the following URL:
http://localhost:8080/adeptia/monitorMatrix?monitorFlag=kernel&matrixFlag=memory

The following XML response is returned. This page displays values of different *memory* parameters of *kernel* (see Figure 60)).

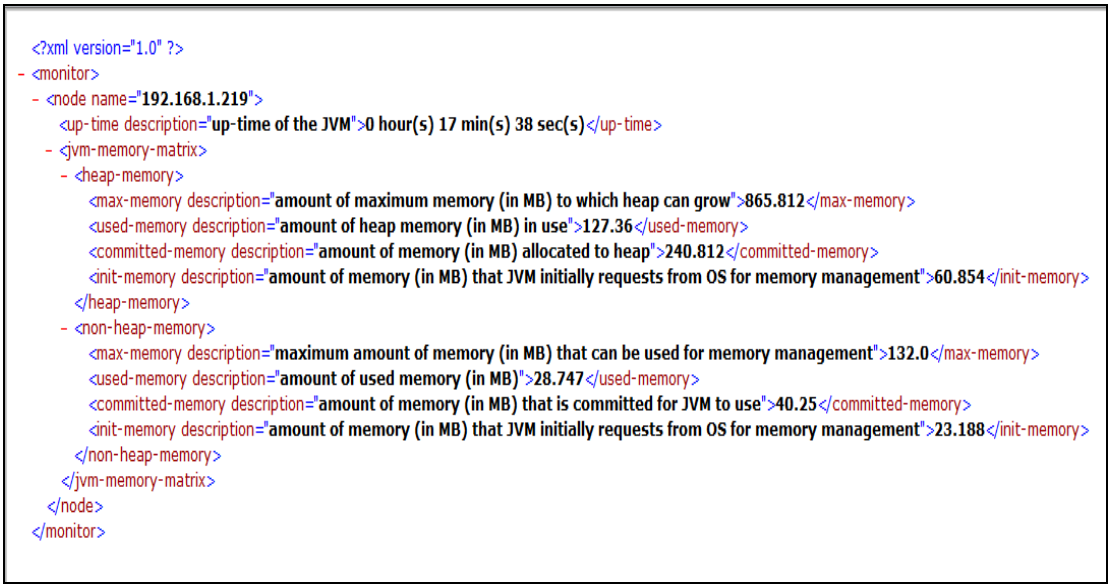


Figure 60: The Performance Matrix XML page

Values for parameters are displayed in the default units. For example value of memory is displayed in MB. To change this unit, open the monitoring-matrix.properties file and change the required properties.

CONFIGURING DEFAULT MONITORING PARAMETERS

This section describes how you can configure the parameters which shall be displayed when you use *default* as matrix flag.

Steps to configure default monitoring parameters

1. Go to **../Serverkernel/etc** folder.
2. Open the *monitoring-matrix.properties* file (see Figure 61).

```
# ms for milli-seconds, sec for seconds, min for minutes, hr for hours
abpm.monitoring.time.unit = min
# Bytes for bytes, KB for kilobytes, MB for megabytes, GB for gigabytes
abpm.monitoring.memory.unit = MB
# Comma separated values for default monitoring matrix, options are as follows:
# memory for JVM Memory Matrix, gc for JVM garbage collection matrix, thread for JVM
Thread information, repositoryDB for repository database information, logDB for log
database information
abpm.monitoring.matrix.default = memory,repositoryDB,logDB
# SQL Query for repository database
abpm.monitoring.repository.sql =
# SQL Query for log database
abpm.monitoring.log.sql =
# time unit for SQL statement response time (nano-sec for nano-seconds, micro-sec for
micro-seconds, ms for milli-seconds, sec for seconds, min for minutes)
abpm.monitoring.sql.response.time.unit = micro-sec
# enable basic authentication
abpm.monitoring.authentication.enable = yes
# user credential required for basic authentication
abpm.monitoring.authentication.user = admin
```

Figure 61: Default Monitoring Parameters XML page

3. Change the value if abpm.monitoring.matrix.default.

By default, parameters of memory, repositoryDb and logDb categories are displayed. To add another category, add the name of category. Names of categories must be separated by comma.

4. Save the file and restart the Kernel and WebRunner.

MONITORING QUERY RESPONSE TIME

This section describes how you check the query response time. Query response time is total time which is taken when you run any select query on Adeptia Suite repository or log database.

By default, query response time is not displayed. To view the query response time first of all you need to define the query through which you want to measure the query response time. You can define the query to run on repository database as well as on log database.

Steps to configure SQL Query

1. Go to ../Serverkernel/etc folder.
2. Open monitoring-matrix.properties file (see Figure 62).

```
# ms for milli-seconds, sec for seconds, min for minutes, hr for hours
abpm.monitoring.time.unit = min
# Bytes for bytes, KB for kilobytes, MB for megabytes, GB for gigabytes
abpm.monitoring.memory.unit = MB
# Comma separated values for default monitoring matrix, options are as follows:
# memory for JVM Memory Matrix, gc for JVM garbage collection matrix, thread for JVM
Thread information, repositoryDB for repository database information, logDB for log
database information
abpm.monitoring.matrix.default = memory,repositoryDB,logDB
# SQL Query for repository database
abpm.monitoring.repository.sql =
# SQL Query for log database
abpm.monitoring.log.sql =
# time unit for SQL statement response time (nano-sec for nano-seconds, micro-sec for
micro-seconds, ms for milli-seconds, sec for seconds, min for minutes)
abpm.monitoring.sql.response.time.unit = micro-sec
# enable basic authentication
abpm.monitoring.authentication.enable = yes
# user credential required for basic authentication
abpm.monitoring.authentication.user = admin
```

Figure 62: Default Monitoring Parameters XML page

3. To define the query to run on Adeptia Suite's repository database, change the value of *abpm.monitoring.repository.sql* property

   For example: select * from AU_FileSource

   Whenever you use *repositoryDB* as matrix flag in request URL, this query will run on the repository database and the response time will be displayed in the result.

   In SQL query you can use any table name of the backend database

4. To define the query to run on Adeptia Suite's log database, change the value of *abpm.monitoring.log.sql* property.

   For example: select * from AU_TransactionData

   Whenever you give *logDB* as matrix flag in request URL, this query will run on the log database.

   In this SQL query you can use any table of backend database.

5. Save the file and restart the Kernel and WebRunner.

ENABLING AUTHENTICATION

This section describes how to enable authentication. If you want that only the authorized users or the administrators are able to check the monitoring performance parameters and their values, you need to enable authentication. For this, you need to authorize users by setting credentials.

When authentication is enabled, you will be required to use a HTTP tool that can pass basic authentication parameters.

By default, authentication is disabled. You need to manually enable the basic authentication by setting the property *abpm.monitoring.authentication.enable to yes*. To enable the credentials, you need set the property *abpm.monitoring.authentication.enable* to *admin* or any other user.

Steps to enable authentication

1. Go to ../Serverkernel/etc folder.
2. Open monitoring-matrix.properties file (see Figure 63).

```
# ms for milli-seconds, sec for seconds, min for minutes, hr for hours
abpm.monitoring.time.unit = min
# Bytes for bytes, KB for kilobytes, MB for megabytes, GB for gigabytes
abpm.monitoring.memory.unit = MB
# Comma separated values for default monitoring matrix, options are as follows:
# memory for JVM Memory Matrix, gc for JVM garbage collection matrix, thread for JVM
Thread information, repositoryDB for repository database information, logDB for log
database information
abpm.monitoring.matrix.default = memory,repositoryDB,logDB
# SQL Query for repository database
abpm.monitoring.repository.sql =
# SQL Query for log database
abpm.monitoring.log.sql =
# time unit for SQL statement response time (nano-sec for nano-seconds, micro-sec for
micro-seconds, ms for milli-seconds, sec for seconds, min for minutes)
abpm.monitoring.sql.response.time.unit = micro-sec
# enable basic authentication
abpm.monitoring.authentication.enable = yes
# user credential required for basic authentication
abpm.monitoring.authentication.user = admin
```

Figure 63: Default Monitoring Parameters XML page

3. To enable authentication, change the value of the property *abpm.monitoring.authentication.enable to yes*.
4. To enable the credentials, set the value of the property *abpm.monitoring.authentication.user to admin* or any other user.
5. Save the file and restart the Kernel and WebRunner.

Now, when you send the HTTP request to monitor the Adeptia server performance, along with HTTP request URL, you need to send the basic authentication parameters as shown below.

Where:

Name: Authorization

Value: Basic *username*: *password*

Here, *username* is a valid user name that exists in the Adeptia Suite repository and *password* is above user's password (in plain text)

13

ACCESSING PID OF KERNEL AND WEBRUNNER

Whenever you start the Kernel and WebRunner on Linux OS, a Process ID (PID) is assigned to both the Kernel and WebRunner. These PIDs are stored in the separate PID files for Kernel and WebRunner. The PID file for Kernel is **kernel.pid** and the PID file for WebRunner is **webrunner.pid**.

These files can be accessed from the following location:

<AdeptiaSuiteInstalledFolder>/ServerKernel/

The Linux users can use these PID files to read the PID assigned to the Kernel or the WebRunner. These PIDs can be further used to monitoring resources used such as memory and CPU usage etc.

Whenever you stop the Kernel or the WebRunner, these PID files are automatically deleted by the OS. However, in case of unexpected system shutdown or in case the Kernel and WebRunner are stopped unexpectedly, you need to manually delete these PID files. In case, you do not delete these PID files, the following error message is displayed:

"PID file already exists."

14

LOAD MANAGEMENT

Load Management is an advanced feature of Adeptia BPM Server. Adeptia BPM Server uses Queue Processor to manage the load. Queue Processor is used to limit the number of process flows executing simultaneously to improve the performance of the system. It also helps in minimizing process flow execution failures due to lack of system resources such as CPU and Memory. All the process flows, which are to be executed, are submitted to the Queue Processor. Queue Processor allows only specified number of process flows to be executed at a time. Rest of the process flows are queued with the Queue Processor and are stored in the database.

In clustering mode, only the Queue Processor of primary node is used to fire the jobs (request for execution of process flows). If primary node goes down, any other node from the clusters becomes the primary node. So it is recommended to enable the Queue Processor on all the nodes of the cluster. The queuing of jobs (request for execution of process flows) can be done by any node in cluster mode.

ENABLING QUEUE PROCESSOR

By default Queue Processor is disabled. To enable the Queue Processor, change the value of the property *abpm.queue.processor.enable* from no to yes. To know how to change the property, refer to the section Updating Adeptia Suite Properties.

After Queue Processor is enabled, you need to specify the following properties:

abpm.queue.processor.Concurrent.processes

Concurrent Process Size is the maximum number of process flows, queue processor allows to be executed simultaneously.

abpm.queue.processor.reload.factor

Reload Factor specifies the threshold of number of process flows, which can be queued into Queue Processor memory. Once the number of process flows queued in to Queue Processor memory becomes less than Reload Factor, the Queue Processor looks for other process flows from database.

By Default Concurrent Processes Size is set to 50 and Reload Factor is set to 100. To change the Concurrent Processes Size and Reload Factor, refer to the section Updating Adeptia Suite Properties.

15

MAINTENANCE

When you-use Adeptia Suite for day to day data processing, it creates some temporary files. These files keep filling the disk space. Similarly run time logs are also written in the log database. Adeptia Suite provides the Data Cleanup and Log Cleanup feature, which is used to clean these data, This section describes how Data and Log Cleanup works and how you can optimize it. This section describes:

- Data Cleanup
- Log Cleanup

DATA CLEANUP

When Adeptia Suite process flows are executed, process flow creates temporary files to store intermediate data called repository files. For each instance of the Process flow execution a unique repository folder is created that contains Source, intermediate XML data files and target formatted data. By default repository files are being stored in the **../../AdeptiaServer-5.3/ServerKernel/web/repository** folder.

These files can cause disk space problem if they are accumulated over a long period of time. To make sure Adeptia Suite runs without disk space issue Adeptia Suite has Data Cleanup task that is scheduled to run at a specified time to cleanup repository files older than specified number of days. This cleans unnecessary files from server's hard disk.

By default, Data Cleanup is *enabled* and runs implicitly along with log cleanup. By default the log cleanup is set to run automatically at 8:00 P.M daily. To run data cleanup explicitly (not along with the log cleanup), you need to set the value of abpm.appmanagement.cleanupCronExpression property. You need to define this value in form of cron expression.

Also, by default, Data Cleanup deletes repository files older than 5 days. Again, to change this time, you need to set the value of abpm.appmanagement.retainTime property.

- To know how to change the Adeptia Suite Properties, refer to section Updating System Properties.
- Data Cleanup does not delete the repository of the process flows that are in running / waiting state. It means that if a process flow is in running / waiting state for more days than specified in abpm.appmanagement.retainTime property, then, the Data Cleanup does not deletes the repository files of this particular process flow.

LOG CLEANUP

Adeptia Suite keeps application logs/errors in log files and/or database based on the logging properties. These logs are used for viewing Process flow logs and for debugging and troubleshooting.

Adeptia Suite keeps Process flow reports in log database tables. These data is used by Monitoring GUI.

These logs can cause database issues if they accumulate over a long period of time. Adeptia Suite has Log Cleanup task that is scheduled to run at a specified time to cleanup repository logs older than specified number of days. This cleans unnecessary logs from server's hard disk.

By default, Log Cleanup is *enabled* and runs automatically at 8:00 P.M. daily. To change this time, you need to set the value of abpm.appmanagement.logCleanupCronExpression property. You need to define this value in form for cron expression.

By default, the logs older than 5 days are deleted during the Log Cleanup process. You can change the retain time for various logs such as Event Logs, Process Flow Logs etc. To change the retain time for various logs, open ***../../AdeptiaServer-5.3/ServerKernel/etc/*log-cleanup.properties file** and change the retain time of the property associated to that particular log. The properties associated to various logs are as follows:

Property Name	Logs
abpm.AU_LOG.logRetainTime	System Logs, Audit Trail Logs and Process Flow Logs
abpm.AU_TRANSACTIONDATA.logRetainTime	Process Flow Logs
abpm.AU_EVENTLOG.logRetainTime	Event Logs
abpm.AU_TASKLOGS.logRetainTime	Task History
abpm.AU_PROCESSVARIABLETRACKER.logRetainTime	Solution Dashboard

- To know how to change the Adeptia Suite Properties, refer to section Updating System Properties.
- Log Cleanup does not delete logs of those process flows that are in running / waiting state. It means that if a process flow is in running / waiting state for more days than specified in retain time properties of logs, then, the Log Cleanup does not deletes the logs of this particular process flow.

16

BACKUP AND RESTORE

It is always recommended to take the backup of Adeptia Suite on a certain interval so that you can restore the objects incase drive on which Adeptia Suite is running gets damaged.

This section explains the steps to take the backup of objects. (activities, process flows, User, Groups and configuration file etc.).

BACKUP

Using Migration Utility can be used to take the backup of all objects of Adeptia Server.

createbackup.bat (for windows) and **createbackup.sh** (for linux and solaris) is provided in the **<InstallFolder>\ServerKernel** folder. When you execute this file, it creates a zip file, which contains the backup of objects. Name of the zip file will be **backup_<Date>_<Time>.zip**.

A file *backup.properties* is provided in **<InstallFolder>\ServerKernel\MigrationUtility**. This file is used to define following parameters:

- Folder where zip file is created
- Whether to back up the optional file or not

KernelApplication.log and WebrunnerApplication.log are the optional files. These file contains logs of Kernel and WebRunner.

Default backup.properties is given in Figure 64

```
#folder where backup zips will be stored
backup.folder = ../
optional.files = no
```

Figure 64: Sample backup.properties file

By default the zip file is created in the folder where Adeptia Suite is installed. For example if Adeptia Suite is installed in **C:\Program Files\AdeptiaSuite\AdeptiaServer-5.0** then the backup is created in **C:\Program Files\AdeptiaSuite\AdeptiaServer-5.0**.

If you want to create the backup file in any other folder, then edit the **<InstallFolder>\ServerKernel\MigrationUtility\backup.properties** file and specify the path where you want to create the backup zip. You can specify any absolute patch.

Use only forward slash (/) in the path.

By default optional files are not included in the backup. If you want to include optional files in the backup then edit the **backup.properties** file and change the value of **optional.files** from no to yes.

Steps to backup the objects:

1. Make sure that the Kernel is running.
2. In case you want to create the backup in folder other than the default folder, edit the **backup.properties** file and specify the path where you want to create the backup zip.
3. Go to **<InstallFolder>\ServerKernel** folder in execute the createbackup.bat file.

On Linux or Solaris, execute **createbackup.sh** file using following command.

```
./createbackup.sh
```

RESTORE

To restore the backup you need to use Migration Utility's *Offline Migration* option. For detailed information, refer to *Import/Restore* section of this *Migration Utility* guide.

17

APPENDIX A: ADEPTIA SUITE PROPERTIES

This appendix describes Adeptia Suite Properties, their default values and other Possible Valuess. Adeptia Suite properties are grouped into following categories:

Possible Values of the properties are case sensitive. So use the exact case mentioned in the Possible Values of the properties.

LOAD MANAGEMENT

abpm.cluster.enable

Description	Enable Adeptia Suite Clustering
Default Value	no
Possible Values	yes/no
Selection Criteria	If *yes* Adeptia Suite clustering will be enabled. If *no* Adeptia Suite clustering will not be enabled.

abpm.queue.processor.enable

Description	Enable Adeptia Suite's Queue Processor Server
Default Value	no

Possible Values	yes/no
Selection Criteria	To limit the number of process flows executing concurrently, set this attribute value to yes

abpm.queue.processor.concurrent.processes

Description	**Maximum number of Process Flows, Queue Processor should allow to execute**
Default Value	50
Possible Values	Any Integer value
Selection Criteria	Depends upon the configuration of the server, where Adeptia Suite is running

abpm.queue.processor.reload.factor

Description	**Reload Factor specifies the threshold of number of process flows, which can be queued into Queue Processor memory. Once the number of process flows queued in to Queue Processor memory becomes less than Reload Factor, the Queue Processor loads more queued process flows from its database into queue processor memory to execute them.**
Default Value	100
Possible Values	Any number between 1 to 1000
Selection Criteria	Depends upon the configuration of the server, where Adeptia Suite is running

abpm.queue.processor.job.restartwithoutRecoveryInfo

Description	**Specifies whether to restart the execution of incomplete Process Flow, even if recovery information for that Process Flow is not available.**
Default Value	No
Possible Values	Yes/no
Selection Criteria	If Yes, Queue Processor will restart the execution incomplete Process Flow right from the beginning. If no, Queue Processor will not restart the execution incomplete Process Flow.

To know more about Queue Processor, refer to the section Load Management.

WEBSPHERE SETTINGS

abpm.websphere.workingDir

Description	This contains files that are required by Adeptia Suite for runtime operations.
Default Value	Copy Adeptia folder inside WebSphere installation directory (*/WebSphere/AppServer/profiles/AppSrv01*) where *AppSrv01* is an instance of server on which Adeptia Suite is deployed
Possible Values	To change location of this folder, specify path in this property, for example, to change path in Working Directory folder, enter */WorkingDir/adeptia* as the path.
Selection Criteria	

KERNEL SETTINGS

abpm.node.name

Description	Name of machine where Adeptia Suite runs
Default Value	localhost
Possible Values	localhost/machine name
Selection Criteria	Use localhost only if Adeptia Suite is running in a single node configuration. In clustering environment use machine name
Comments	NA

abpm.node.port

Description	Port used by Adeptia Suite Kernel
Default Value	21000
Possible Values	Any port number which is free i.e. no other application is using that port
Selection Criteria	
Comments	NA

abpm.repository.address

Description	Address of the repository used by Adeptia Suite
Default Value	localhost://indigo.core:service=repository
Possible Values	localhost/machine name
Selection Criteria	Use localhost only if Adeptia Suite is running in a single node configuration. In clustering environment use machine name

abpm.repository.root

Description	Directory path to store intermediate files to be created during process flow execution
Default Value	./web/ repository
Possible Values	Any valid directory path
Selection Criteria	Always a directory path
Comments	By default the repository directory is 'repository' present under the ../../AdeptiaServer-5.3/ServerKernel/ .

abpm.kernelout.file.enable

Description	Specifies whether the output of kernel is logged in a file or not
Default Value	false
Possible Values	true/false
Selection Criteria	If you want to log the output of kernel in a file, then select true, otherwise select false.
Comments	NA

abpm.kernelout.file.location

Description	Specifies the location, where the log file is generated
Default Value	logs\applicationlogs
Possible Values	Any absolute path or relative path from server kernel folder.
Selection Criteria	This property specifies the path, where output log file of kernel is created.
Comments	This property is applicable, only when the abpm.kernelout.file.enable is set to true. Do not specify the file name in the value of this property. By default the file name is KernelApplication.log.

abpm.kernelout.file.maxSize

Description	Specifies the maximum size of the log file
Default Value	20
Possible Values	Any positive integer
Selection Criteria	NA
Comments	This property specifies the maximum size of the log file. Once the log file reaches the specified maximum size, it is renamed to KernelApplication-[Date].log. Where Date specifies the current date in yyyy-MM-dd hh-mm-ss format.

	This property is applicable, only when the abpm.kernelout.file.enable is set to true.

EMBEDDED DATABASE

These properties are related to tuning backend and log databases.

abpm.embedded.db.names

Description	Name of the embedded backend and log databases.
Default Value	indigo,logs
Possible Values	
Selection Criteria	It is not recommended to change these values.
Comments	**indigo** is the name of the backend database and **logs** is the name of the log database.

abpm.embedded.indigo.port

Description	Port used by the embedded backend database
Default Value	2476
Possible Values	Any available port.
Selection Criteria	The port specified here should not be used by another application.
Comments	NA

abpm.embedded.indigo.memory

Description	Minimum and Maximum JVM memory used by embedded backend database
Default Value	-Xms128M -Xmx256M -Xrs
Possible Values	
Selection Criteria	Minimum and memory can be increased based on the objects stored in the backend database and the memory available in the system.
Comments	-Xms represents the minimum memory and –Xmx represents the maximum memory.

abpm.embedded.logs.port

Description	Port used by the embedded log database
Default Value	2477
Possible Values	Any available port.
Selection Criteria	Port specified here should not be used by another application.

Comments	NA

abpm.embedded.logs.memory

Description	Minimum and Maximum JVM memory used by embedded log database
Default Value	-Xms128M -Xmx256M -Xrs
Possible Values	
Selection Criteria	Minimum and memory can be increased based on the logs being stored in the logs database and the memory available in the system.
Comments	-Xms represents the minimum memory and –Xmx represents the maximum memory.

PERFORMANCE OPTIMIZATION

These properties are related to tuning of Adeptia Suite performance.

IO

abpm.internals.tuning.io.buffer.size

Description	Buffer size in bytes used by data stream in process flow
Default Value	16384
Possible Values	Any integer non zero, non negative integer value
Selection Criteria	It should be multiple of 1024.
Comments	Default value is 16*1024. It is tuning parameter data stream to copy from source to target.

abpm.internals.tuning.io.pool.enabled

Description	IO Pool Enable and Disable Option
Default Value	no
Possible Values	yes/no
Selection Criteria	If pooling is required to pass pooled objects from source to target, in case of transformer type services, in process flow, then this parameter is set to yes. This parameter is internal to process flow.

abpm.internals.tuning.io.gc.limit

Description	It defines the limit of garbage collection explicitly done by Adeptia Suite. After writing these many records into a pool Adeptia Suite call garbage collector to free all the records, which are already read. This property is applicable when IO Pool is enabled.
Default Value	75000
Possible Values	NA
Selection Criteria	There should be a positive integer value.
Comments	This limit is used internally by process flow when it has transformer type services.

CACHING

abpm.dataMapper.dblookup.cache.limit

Description	Number of Data Mapper Select Query and result string pair to be cached
Default Value	10000
Possible Values	Any integer
Selection Criteria	NA
Comments	Number of Data Mapper Select Query and result string pair to be cached. This limit applies on whole Adeptia Suite not on individual Data Mapper applet.

JMX

abpm.mbeanServer.connection.retry.count

Description	Number of retries if mbean server connection is down
Default Value	3
Possible Values	Any integer
Selection Criteria	NA
Comments	Number of retries to connect to the mbean server, if it is down

abpm.mbeanServer.connection.lookup.time

Description	The lookup time between two retries of connecting to the mbean Server
Default Value	2000
Possible Values	Any integer
Selection Criteria	NA
Comments	

BACKEND DATABASE

Backend Connection Failure

abpm.jdo.connection.retryCount

Description	Number of retries to connect to the backend database if it is down
Default Value	-1
Possible Values	Any integer
Selection Criteria	NA
Comments	Number of retries to connect to the backend database, if it is down. By default, it the set to infinite retries, as if the backend database is down, then all GUI operations are at a standstill.

abpm.jdo.connection.retryTimeInterval

Description	The time interval (in seconds), between two retries of connecting to the backend server
Default Value	60
Possible Values	Any integer
Selection Criteria	NA
Comments	The time interval between two retries of connecting to the backend server.

Cluster Connection Pooling

abpm.cluster.maxActive

Description	Maximum number of active connections that can be allocated from this pool at the same time.
Default Value	50
Possible Values	Any positive integer
Selection Criteria	NA
Comments	

abpm.cluster.maxIdle

Description	Maximum number of connections that can remain idle in the pool, without extra ones being released.
Default Value	10
Possible Values	Any integer
Selection Criteria	NA

Comments	

abpm.cluster.minIdle

Description	**Minimum number of connections that can remain idle in the pool, without extra ones being created.**
Default Value	0
Possible Values	Any positive integer
Selection Criteria	NA
Comments	

abpm.cluster.maxWait

Description	**Maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception.**
Default Value	-1
Possible Values	Any positive integer
Selection Criteria	NA
Comments	Put -1 to wait indefinitely.

abpm.cluster.timeBetweenEvictionRunsMillis

Description	**The number of milliseconds to sleep between runs of the idle object evictor thread.**
Default Value	60000
Possible Values	Any positive integer
Selection Criteria	NA
Comments	When non-positive, no idle object evictor thread will be run.

abpm.cluster.numTestsPerEvictionRun

Description	**The number of objects to examine during each run of the idle object evictor thread.**
Default Value	3
Possible Values	Any positive integer
Selection Criteria	NA

Comments	

abpm.cluster.minEvictableIdleTimeMillis

Description	**The minimum amount of time an object may sit idle in the pool before it is eligible for eviction by the idle object evictor.**
Default Value	1800000
Possible Values	?
Selection Criteria	?
Comments	?

abpm.cluster.removeAbandoned

Description	**Flag to remove abandoned connections if they exceed the removeAbandonedTimout.**
Default Value	false
Possible Values	true/false
Selection Criteria	?
Comments	If set to true a connection is considered abandoned and eligible for removal if it has been idle longer than the removeAbandonedTimeout. Setting this to true can recover db connections from poorly written applications which fail to close a connection.

abpm.cluster.removeAbandonedTimeout

Description	**Timeout in seconds before an abandoned connection can be removed.**
Default Value	300
Possible Values	?
Selection Criteria	?
Comments	?

abpm.cluster.logAbandoned

Description	**Flag to log stack traces for application code which abandoned a Statement or Connection.**
Default Value	false
Possible Values	true/false
Selection Criteria	?

Comments	Logging of abandoned Statements and Connections adds overhead for every Connection open or new Statement because a stack trace has to be generated.

abpm.clusterdb.isolation.level

Description	**This is used for identify transaction Isolation Level for the connections in the pool.**
Default Value	1
Possible Values	1/2
Selection Criteria	?
Comments	Specify 1 for READ UNCOMMITTED and 2 for READ COMMITTED.

Backend Connection Pooling

abpm.jdo.connection.pooling.enable

Description	**Enable pooling for connection to backend database**
Default Value	yes
Possible Values	yes/no
Selection Criteria	NA
Comments	

LOG DATABASE

Log Connection Failure

abpm.log.connection.retryCount

Description	**Number of retries to connect to the log database server if it is down**
Default Value	-1
Possible Values	Any integer
Selection Criteria	NA
Comments	Number of retries to connect to the log database, if it is down. By default, it the set to infinite retries, as if the log database is down, then logs are not entered into the database, but stored into a file.

abpm.log.connection.retryTimeInterval

Description	**The time interval (in seconds), between two retries of connection to log database server is lost**
Default Value	60
Possible Values	Any integer
Selection Criteria	NA

Comments	The time interval between two retries of connection to log database server is lost.

abpm.log.recovery.log4jfile

Description	**The log file that contains data for table AU_LOG when connection to log database server is lost.**
Default Value	KernelWebRunner.log
Possible Values	
Selection Criteria	NA
Comments	The log file that contains data for the table AU_LOG when connection to log database server is lost.

abpm.log.recovery.transactionDataFile

Description	**The log file that contains data for table AU_TRANSACTIONDATA when connection to log database server is lost**
Default Value	transaction.log
Possible Values	
Selection Criteria	NA
Comments	The log file that contains data for the table AU_TRANSACTIONDATA when connection to log database server is lost.

abpm.log.recovery.taskLogFile

Description	**The log file that contains data for table AU_TASKLOGS when connection to log database server is lost**
Default Value	Tasklog.log
Possible Values	
Selection Criteria	NA
Comments	The log file that contains data for the table AU_TASKLOGS when connection to log database server is lost.

abpm.log.recovery.processVariableTrackerFile

Description	**The log file that contains data for table AU_PROCESSVARIABLETRACKER when connection to log database server is lost**
Default Value	processVariableTracker.log
Possible Values	
Selection Criteria	NA

Comments	The log file that contains data for the table AU_ PROCESSVARIABLETRACKER when connection to log database server is lost.

Log Connection Pooling

abpm.logdb.pool.enable

Description	Enable pooling for connection to log database
Default Value	yes
Possible Values	yes/no
Selection Criteria	NA
Comments	

abpm.logdb.pool.maxActive

Description	Maximum number of active connections that can be allocated from this pool at the same time.
Default Value	100
Possible Values	Any positive integer/ -1 for no limit
Selection Criteria	Depends on the maximum number of connection allowed by log database server.
Comments	

abpm.logdb.pool.maxIdle

Description	Maximum number of connections that can remain idle in the pool, without extra ones being released
Default Value	10
Possible Values	Any positive integer/ -1 for no limit
Selection Criteria	
Comments	

abpm.logdb.pool.minIdle

Description	Minimum number of connections that can remain idle in the pool, without extra ones being created
Default Value	10
Possible Values	Any positive integer/ 0 to create none
Selection Criteria	

Comments	

abpm.logdb.pool.maxWait

Description	**Maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception**
Default Value	10
Possible Values	Any positive integer/ -1 to wait indefinitely
Selection Criteria	
Comments	

PROCESS FLOW

RECOVERY

These properties are related to the recovery of the process flow, which are not completed due to system crash. Process flow is only recoverable if it has some checkpoints defined in it. On reaching each of the checkpoints, state (data, context variables) of process flow is written to a file in recovery directory. When system restarted after failure, it checks the recovery directory and find out the recoverable process flow and restart the process flow execution from the last successful checkpoint saved. The recovery information saved in the recovery folder remains there unless the process flow is recovered and completed. After the process flow is executed, this information is deleted. There is one file for each process flow. If the recovery option is set to NO the recovery information are saved but recovery is not done. If you enable the recovery property, the failed process flows are recovered.

abpm.transaction.recovery.enable

Description	**This property is used to enable or disable recovery of process flow after system failure**
Default Value	yes
Possible Values	yes/no
Selection Criteria	NA
Comments	If queue processor is enabled then queue processor will do recovery.

abpm.recovery.repository.root

Description	**This is a folder, where recovery information of process flow is saved**
Default Value	recovery
Possible Values	Any valid directory path
Selection Criteria	There should be valid directory path
Comments	By default the path to recovery directory is ‘recovery’. This directory is present under Adeptia Suite directory.

ARCHIVAL

abpm.transaction.repository.archive.server

Description	Specifies where to archive the process flow repository files
Default Value	default
Possible Values	Webdav/default
Selection Criteria	Select webdav if you want to archive repository files in webdav repository. If webdav is selected, repository files are archived into the default folder of the group, executor of Process Flow belongs to. Select default if want to archive repository files into a folder specified in abpm.transaction.repository.archive.path property.
Comments	NA

abpm.transaction.repository.archive.path

Description	This is a folder where process flow repository files are archived
Default Value	C:/Repo
Possible Values	Any valid directory path
Selection Criteria	NA
Comments	This property is not applicable if the value of abpm.transaction.repository.archive.server property is set to webdav.

SERVICES

PROXY SETTINGS

abpm.transportProxy

Description	Transport Proxy Enable and Disable Option
Default Value	false
Possible Values	true/false
Selection Criteria	true - If Adeptia Suite is behind the proxy server. false- If Adeptia Suite is not behind the proxy server

abpm.transportProxyHost

Description	Transport Proxy Host IP Address
Default Value	192.168.1.129
Possible Values	Depends on proxy server configuration.
Selection Criteria	IP Address of the proxy server.

abpm.transportProxyHttpPort

Description	HTTP port used by proxy server
Default Value	8082
Possible Values	Depends on proxy server configuration.
Selection Criteria	HTTP port of the proxy server.

abpm.transportProxyFtpPort

Description	FTP port used by proxy server
Default Value	21
Possible Values	Depends on proxy server configuration.
Selection Criteria	FTP Port of the proxy server

WEB SERVICE CONFIGURATION

abpm.webservice.uddisearch.maxrowsreturn

Description	This property defines Maximum Rows returned, when doing UDDI search
Default Value	50
Possible Values	Any positive integer (maximum value depends on browser used).
Selection Criteria	Maximum number of rows a browser can display smoothly
Comments	Suppose if user has given 2000 then the number of rows returned will depend upon the browser.

abpm.webservice.host

Description	The machine name where web service is running
Default Value	localhost
Possible Values	localhost/machine name
Selection Criteria	Always use machine name in production environment
Comments	localhost indicates the web service is running in local machine, machine name indicates that the web service is running in remote machine.

abpm.webservice.port

Description	The Web service port number i.e. on which port web service is running
Default Value	8080
Possible Values	Any value, which can be used as port for web service
Selection Criteria	It should be same as web server port
Comments	First set the web server port then use same value as web service port

abpm.webservice.sPort

Description	The Web service secure port number i.e. on which secure port web service is running
Default Value	8443
Possible Values	Any value, which can be used as secure port for web server
Selection Criteria	It should be same as web server secure port (Https port)
Comments	

abpm.webservice.wsdlDeployPath

Description	Web service wsdlDeployPath
Default Value	wsdl
Possible Values	Any absolute path on the local system/ relative path from 'ServerKernel' directory location
Selection Criteria	Any directory where user want to save WSDL created for published process flow
Comments	

abpm.webservice.serverKeyStorePath

Description	Key store path used by web server for web service SSL configuration
Default Value	../etc/truststore/cacerts
Possible Values	Any accessible location on local system
Selection Criteria	Depends which directory key store has been created into.
Comments	Use the default value. It has pre-created key store. In case you want to generate key store just copy that into default location. If you have pre created key store just use the absolute path of this key store as property value

BUSINESS CALENDAR

org.quartz.scheduler.bCalendar

Description	Specifies list of holidays of year
Default Value	NA
Possible Values	Any date in mm/dd/yyyy format
Selection Criteria	NA
Comments	These days are assumed as holidays in Adeptia Suite calendar. If a process flow is scheduled to be fired on Business Days, the process will not be fired on days specified in this property.

WORKFLOW

abpm.hi.polling.frequency

Description	Time interval (in seconds) a waiting process flow, checks the status of workflow activity listed in task manager
Default Value	30
Possible Values	Time in seconds
Selection Criteria	NA
Comments	NA

abpm. hi.repository.type

Description	Repository type, where files, attached with Human Work Flow activity is saved during execution of Process Flow
Default Value	WebDav
Possible ValuesPossible Valuess	WebDav/default
Selection Criteria	Select WebDav, if you want to save HumanWorkflow files into WebDav folder. Select default, if you want to save HumanWorkflow files into Process Flow Repository.
Comments	NA

abpm. hi.chainedHW.timeout

Description	Total time (in seconds) for which the active screen will wait for the next task to come after the first task is completed, and the next task is assigned to the same user.
Default Value	50
Possible ValuesPossible Valuess	Integer
Selection Criteria	NA
Comments	This property is for screen flow support in workflow task and is applicable only if screen flow support is on for that task. It is recommended that this property should be 4-5 times higher than the *waitTime* property.

abpm. hi.chainedHW.waitTime

Description	Total time (in seconds) for which the active screen will poll (look) for the next task to come after the first task is completed, and the next task is assigned to the same user.
Default Value	10
Possible Values	Integer
Selection Criteria	NA
Comments	This property is for screen flow support in workflow task and is applicable only if screen flow support is on for that task. It is recommended that this property should be 4-5 times lesser than the *timeout* property.

abpm.hi.chainedHW.waitTime

Description	Max limit of file size that can be uploaded in any Human Workflow task.
Default Value	1024
Possible ValuesPossible Valuess	Integer
Selection Criteria	NA
Comments	

WEBDAV SERVER

abpm.webdav.servername

Description	The machine name where WebDAV server is running
Default Value	localhost
Possible Values	localhost/machine name
Selection Criteria	Same as the value of abpm.node.name
Comments	If machine name is used in abpm.node.name property use machine name in this property also.

abpm.webdav.port

Description	Port on which WebDAV server is running
Default Value	8080
Possible Values	Any value, which can be used as port for WebDAV server
Selection Criteria	It should be same as web server port
Comments	First set the web server port then use same value as web service port

abpm.webdav.dirbaselocation

Description	Folder which is used a base location for WebDAV repository
Default Value	/slides/files
Possible Values	Any valid directory (absolute or relative)
Selection Criteria	NA
Comments	NA

abpm.webdav.userenabled

Description	Folder which is created when a new user is created
Default Value	true
Possible Values	True/False
Selection Criteria	NA
Comments	Used to add/remove the creation of WebDAV folder for user

REPORTS LIBRARY

abpm.reporting.repository

Description	Folder where jasper files are stored
Default Value	/web/Jasper Report
Possible Values	Path of any valid folder
Selection Criteria	NA
Comments	Adeptia Suite looks for jasper file in this folder to generate custom reports

DATABASE TARGET

abpm.database.errorcodes

Description	This property is used to configure error code returned by database server to abort the process flow.
Default Value	942,208
Possible Values	NA
Selection Criteria	NA
Comments	NA

DATABASE CONNECTION

abpm.database.connectionWaitTime

Description	This property is used to configure the time (in seconds) that the driver will wait to connect to the database.
Default Value	60
Possible Values	NA
Selection Criteria	NA
Comments	NA

SCHEMA PROPERTY

abpm.schemashowfieldcount

Description	This property is used to configure the maximum number of fields to be displayed in Advance Positional and EDI schemas
Default Value	200
Possible Values	NA
Selection Criteria	NA
Comments	If field count exceeds 200, then no records are displayed. In such a case, Definition File option is used.

MAIL EVENT PROPERTY

abpm.mailEvent.mailProcessConcurrency

Description	This is used to set the maximum number of concurrent emails that can be processed by a mail event at a time
Default Value	0
Possible Values	Any positive integer
Selection Criteria	Should be based on the mail server that you are using
Comments	Enter the maximum number of concurrent emails that can be processed at a time by mail event. By default, this value is 0 which means there is no limit to the number of mails that can be processed by a mail event. This property is applicable for all mail events that you have in your Adeptia Suite. If want to define this number specifically on one mail event, you can define it in Advanced properties of mail event.

abpm.mailEvent.retry

Description	This is used to set the number of retries when a 'MailBox in Use' error occurs
Default Value	0
Possible Values	Any positive integer

Selection Criteria	Should be based on the mail server that you are using
Comments	This specifies the number of times a mail source, mail event and mail polling activity will retry on 'Mailbox in Use' error before it aborts. By default, this value is 0, which means there are no retries.

abpm.mailEvent.sleepTime

Description	**This is used to set the sleep time (in milliseconds) before a retry takes place, when a 'Mailbox in Use' error occurs**
Default Value	0
Possible Values	Any positive integer
Selection Criteria	Should be based on the mail server that you are using
Comments	This specifies the time interval (in milliseconds) between two retries for 'Mailbox in Use' error. By default, this value is 0, which implies that the time interval is 2 seconds. This property is applicable if the abpm.mailEvent.retry property is greater than 0.

SYSTEMS

LOGGING

Adeptia Suite uses Log4J for logging. Log4j has three main components: loggers, appenders and layouts. These three types of components work together to log messages according to message type and level, and to control at runtime how these messages are formatted and where they are reported.

The logging level controls the type of messages that are logged. Adeptia Suite supports following logging levels:

- **DEBUG**: The DEBUG Level designates fine-grained informational events that are most useful to debug an application.
- **INFO**: The INFO level designates informational messages that highlight the progress of the application at coarse-grained level.
- **ERROR**: The ERROR level designates error events that might still allow the application to continue running.

The behavior of the logger is hierarchical. This is illustrated in the figure below.

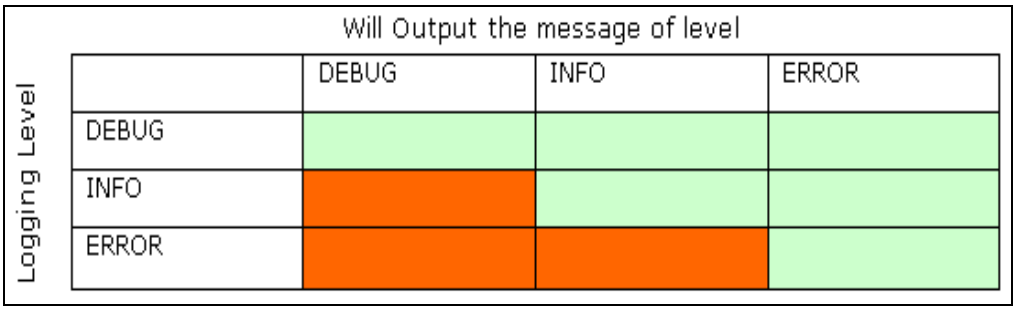


Figure 65: Logging Level Behavior

DEBUG is the highest logging level and it logs messages of DEBUG, INFO and ERROR level. ERROR is the lowest logging level and it only logs message of ERROR level.

Adeptia Suite supports following appenders:

- **jdbc**: It appends log to a database.

- **console**: It appends log events to system.out or system.err using layout specified by the user. The default target is system.out.
- **file** : It appends log to a file.

All the appenders are case-sensitive and must be defined in lower case.

For more details on log4j refer to http://logging.apache.org/log4j/docs/index.html.

log4j.rootLogger

Description	System and Process Flow Logging Level and appenders
Default Value	INFO,console,jdbc
Possible Values	A combination of valid log level along with the Appenders
Selection Criteria	NA
Comments	For example INFO,console, jdbc: INFO indicates the logging level and console and jdbc indicate appender. The data can go to console, jdbc or file.

Console appender

log4j.appender.console

Description	This Log4j console Appender class
Default Value	org.apache.log4j.consoleAppender
Possible Values	Any implementation of console Appender
Selection Criteria	NA
Comments	ConsoleAppender appends log events to System.out or System.err using a layout specified by the user. The default target is System.out.

Database appender

log4j.appender.jdbc

Description	This is Log4j jdbc Appender class.
Default Value	org.apache.log4j.jdbcplus.jdbcAppender
Possible Values	Any implementation of jdbc Appender
Selection Criteria	NA
Comments	The JDBCAppender writes messages into a database via JDBC. Multiple configuration options and parameters are supported

log4j.appender.jdbc.url

Description	This is URL of the database where logs are appended
Default Value	As specified during installation
Possible Values	Any valid jdbc url
Selection Criteria	NA
Comments	

log4j.appender.jdbc.dbclass

Description	Database driver to connect to the database specified in log4j.appender.jdbc.url
Default Value	net.sourceforge.jtds.jdbc.Driver
Possible Values	This value is provided by the JDBC driver used and the default value depends on the database selected during installation
Selection Criteria	NA
Comments	

log4j.appender.jdbc.username

Description	Username to access the database specified in log4j.appender.jdbc.url
Default Value	As specified during installation
Possible Values	NA
Selection Criteria	NA
Comments	Username specified here must have write permission to the specified database

log4j.appender.jdbc.password

Description	Password of the username specified in log4j.appender.jdbc.username property
Default Value	As specified during installation
Possible Values	NA
Selection Criteria	NA
Comments	NA

log4j.appender.jdbc.connector

Description	The connector used for log4j JDBC Appender
Default Value	com.adeptia.indigo.logging.DbcpPoolConnectionHandler
Possible Values	NA
Selection Criteria	NA

Comments	Connector used to establish connection with log4j JDBC Appender

File logging

log4j.appender.file

Description	This is Log4j Rolling File Appender class
Default Value	org.apache.log4j.RollingFileAppender
Possible Values	Any implementation of FileAppender
Selection Criteria	NA
Comments	RollingFileAppender is used to backup the log files when they reach a certain size

log4j.appender.file.Webrunner.file

Description	Name and path of the file where Webrunner log is appended
Default Value	adeptia_webrunner.Log
Possible Values	Any absolute path on the local system and the file name or Relative path from 'ServerKernel' directory and the file name
Selection Criteria	Any location where you want to save the Webrunner log.
Comments	

log4j.appender.file.Kernel.file

Description	Name and path of the file where Kernel log is appended
Default Value	adeptia_kernel.Log
Possible Values	Any absolute path on the local system and the file name or Relative path from 'ServerKernel' directory and the file name
Selection Criteria	Any location where you want to save the kernel log.
Comments	

log4j.appender.file. MaxBackupIndex

Description	Number of backup log file
Default Value	10
Possible Values	Any positive integer
Selection Criteria	NA
Comments	

log4j.appender.file. MaxFileSize

Description	Maximum size of the log file

Default Value	1 MB
Possible Values	Size of file in MB
Selection Criteria	NA
Comments	After the log file reaches this size another log file is created.

SECURITY

abpm.security.secretkeystorename

Description	Adeptia Suite Secretkeystorename
Default Value	SecretKeys.Keystore
Possible Values	Any valid JCEKS Keystore
Selection Criteria	SecretKeys.Keystore is a protected database that holds keys which are generated when user creates Secret Key entity. These keys are used by Encryption, Decryption activity and Schema services. Access to a keystore is guarded by a password defined in the abpm.security.secretkeypassword.encrypt property. This password is not changeable. In addition, each private key in a keystore can be guarded by its own password.

abpm.security.repository

Description	**Folder where secret keys and keystore are stored**
Default Value	etc/security
Possible Values	Any valid directory path
Selection Criteria	NA
Comments	This property represents the folder path where security related folders are stored viz. Keystore, secret keys etc.

abpm.security.passwordExpiryDays

Description	**Number of days after which the password expires**
Default Value	0
Possible Values	
Selection Criteria	NA
Comments	This property represents the number of days after which the password expires. If it has a value of 0, then the password does not expire.

abpm.security.passwordExpiryMessageDisplayDays

Description	**Number of days before the password expiry for prompting expiry warning**
Default Value	5
Possible Values	

Selection Criteria	NA
Comments	This property represents the number of days before the password expiry, the expiry warning is to be displayed. This warning is displayed at login.

abpm.security.activitycomments.enable

Description	Add comments before saving or editing an activity.
Default Value	No
Possible Values	Yes
Selection Criteria	NA
Comments	This property represents the comment that is added after an activity is saved or edited. You can enter the reason for the add or edit action.

If you enable/disable comments property in the middle of a process flow or a mapping activity, you need to restart the respective applet.

AUTHENTICATION AND AUTHORIZATION

java.security.auth.login.config

Description	This is a file where the JVM looks for security JAAS configuration
Default Value	etc/jaas.config
Possible Values	Any file containing the login module configurations
Selection Criteria	Valid login modules
Comments	This Configuration specifies which Login Modules should be used for Adeptia Suite application, and in what order the Login Modules should be invoked

SERVER MAIL SERVER PARAMETERS

These properties are used when any mail notification generated by Adeptia Suite is send. Adeptia Suite generates mail notifications when:

- You click on the Forgot Password link in the login page
- Any Mail Notification activity is executed

MailProtocol

Description	Specifies the protocol used by outgoing mail server
Default Value	smtp
Possible Values	Smtp/mapi
Selection Criteria	Select smtp if the outgoing mail server is using SMTP protocol. Select mapi if outgoing mail is using MAPI protocol. For Example Exchange Server

mailServer

Description	IP address or host name of Outgoing (SMTP) mail server
Default Value	Whatever value is given during Adeptia Suite installation
Possible Values	NA
Selection Criteria	This property is applicable only when the mailProtocol is smtp

Domian

Description	Specifies the domain name
Default Value	Adeptia
Possible Values	NA
Selection Criteria	Enter the domain name, on which the Exchange server is running. This property is applicable, only when mailProtocol is mapi.

CDOHostName

Description	Name of the CDOHost machine
Default Value	CDOHOSTMachine
Possible Values	NA
Selection Criteria	CDOHOST allows Adeptia Suite to communicate with Exchange server.

systemAdminEmailId

Description	Email Address of the person who is responsible for the administration of the Adeptia Suite
Default Value	Whatever value is given during Adeptia Suite installation
Possible Values	NA
Selection Criteria	NA

mailServerUserId

Description	User ID used to access the mailbox of the Adeptia Suite administrator
Default Value	Whatever value is given during Adeptia Suite installation
Possible Values	NA
Selection Criteria	NA

mailServerPassword

Description	Adeptia Suite administrator mail server password.
Default Value	Whatever value is given during Adeptia Suite installation
Possible Values	NA
Selection Criteria	NA

mailsubject

Description	Subject of the mail to be sent.
Default Value	
Possible Values	Subject string with which mail notification will be send
Selection Criteria	Any string which user can identify

abpm.notification.mailNotification.sslEnabled

Description	Specifies Whether mail server is ssl enabled or not
Default Value	no
Possible Values	yes/no
Selection Criteria	Select yes if the specified mail server requires a secure connection. Select no if the specified mail server doesn't require a secure connection.

abpm.notification.mailNotification.port

Description	Port of the outgoing mail server
Default Value	25
Possible Values	NA
Selection Criteria	NA

abpm.changePasswordNotification.sendNewPassword

Description	Specifies whether you want to send the new password, whenever user's password is changed
Default Value	Yes
Possible Values	Yes/no
Selection Criteria	Select yes if you want the new password to be sent in the notification mail, whenever a user password is changed. Select no if you want the notification mail to be sent without new password.

ACTIVITY NAMING CONVENTION

abpm.ActivityName.Prefix

Description	This is the prefix that is appended to an activity name
Default Value	
Possible Values	
Selection Criteria	NA
Comments	Prefix appended to an activity name

MULTITENANT ENVIRONMENT

abpm.multitentant.environment.enable

Description	This is an option to enable or disable a multitenant environment
Default Value	no
Possible Values	Yes/no
Selection Criteria	NA
Comments	This option is used to enable or disable a multitenant environment.

PAGINATION

abpm.pagination.enable

Description	This is an option to enable or disable the pagination feature
Default Value	yes
Possible Values	Yes/no
Selection Criteria	NA
Comments	This option is used to enable or disable pagination feature Limitation: This feature does not work for SQL 2000 Server

abpm.pagination.page.size

Description	This is an option to set the maximum number of records to be displayed in one page
Default Value	10
Possible Values	Positive Integer
Selection Criteria	NA
Comments	This option is used to set the number of records to be displayed in one page

MAINTENANCE

DATA CLEANUP PROPERTIES

abpm.appmanagement.cleanupCronExpression

Description	Cron Expression to schedule data cleanup time
Default Value	0 0 20 * * ?
Possible Values	Any valid Cron Expression
Selection Criteria	When and how often user wants intermediate data to be cleaned up. By default it is set to 8 P.M. daily.
Comments	To know more about Cron expression, refer to http://www.opensymphony.com/quartz. Also look into quartz scheduler document

abpm.appmanagement.retainTime

Description	Intermediate file retain Time (in days)
Default Value	14
Possible Values	Any positive integer
Selection Criteria	Based on how old (days) data, user wants to retain in case Data Clean up is called. By default two days old data is retained.
Comments	Value given is in days. For example- default value 14 days

LOG CLEANUP PROPERTIES

abpm.appmanagement.logCleanupCronExpression

Description	Cron Expression to schedule log cleanup time
Default Value	0 0 20 * * ?
Possible Values	Any valid Cron Expression
Selection Criteria	When and how often user wants log data to be cleaned up
Comments	To know more about Cron expression, refer to http://www.opensymphony.com/quartz. Also look into quartz scheduler document

abpm.appmanagement.logCleanupPropertiesFile

Description	Name and Path of file which contains retain time for logs
Default Value	Log-cleanup.properties
Possible Values	Path of file which contains logs retain time properties.
Selection Criteria	
Comments	

WEB SERVER

abpm.webserver.address

Description	The machine name where web Server is running
Default Value	localhost
Possible Values	localhost/machine name
Selection Criteria	Always use machine name in production environment
Comments	localhost indicates the web server is running in local machine, machine name indicates that the web service is running in remote machine.

abpm.webserver.public.address

Description	The public IP address used to access the Adeptia Suite behind a firewall
Default Value	
Possible Values	
Selection Criteria	
Comments	Enter the public IP address that allows you to access the Adeptia Suite behind a firewall.

abpm.webserver.http.port

Description	The Web server HTTP port number i.e. on which HTTP port web server is running.
Default Value	8080
Possible Values	Any value, which can be used as HTTP port for web server
Selection Criteria	
Comments	

abpm.webserver.https.port

Description	The Web server secure port number i.e. on which secure port web server is running.
Default Value	8443
Possible Values	Any value, which can be used as secure port for web server
Selection Criteria	The port specified here must not be used any other application
Comments	

abpm.transactionmonitor.ActivityStatusRefreshTime

Description	Time interval (in seconds) at which status of activity in monitoring applet refreshes
Default Value	10
Possible Values	Time in seconds
Selection Criteria	NA
Comments	NA

SessionTimeOut

Description	Maximum time (in minutes) for which user can remain logged in Adeptia Suite in idle state
Default Value	1440
Possible Values	Time in minute
Selection Criteria	NA
Comments	For unlimited duration enter negative value.

abpm.webrunnerout.file.enable

Description	Specifies whether the output of WebRunner is logged in a file or not
Default Value	false
Possible Values	true/false
Selection Criteria	If you want to log the output of WebRunner in a file, then select true, otherwise select false.
Comments	NA

abpm.webrunnerout.file.location

Description	Specifies the location, where the log file is generated
Default Value	logs\applicationlogs
Possible Values	Any absolute path or relative path from server kernel folder.
Selection Criteria	This property specifies the path, where output log file of webrunner is created.
Comments	This property is applicable, only when the abpm.webrunnerout.file.enable is set to true. Do not specify the file name in the value of this property. By default the file name is WebRunnerApplication.log.

abpm.webrunnerout.file.maxSize

Description	Specifies the maximum size of the log file
Default Value	5
Possible Values	Any positive integer
Selection Criteria	NA
Comments	This property specifies the maximum size of the log file. Once the log file reaches the specified maximum size, it is renamed to WebrunnerApplication-[Date].log. Where Date specifies the current date in yyyy-MM-dd hh-mm-ss format. This property is applicable, only when the abpmwebrunnerout.file.enable is set to true.

APPLET CONFIGURATION

DATA MAPPER

abpm.dataMapper.minHeapsize

Description	The minimum memory required for the data Mapper applet
Default Value	128M
Possible Values	
Selection Criteria	NA
Comments	This indicates the minimum amount of memory required to run the Data Mapper applet.

abpm.dataMapper.maxHeapsize

Description	The maximum memory possible for the data Mapper applet
Default Value	256M
Possible Values	
Selection Criteria	NA
Comments	This indicates the maximum amount of memory required to run the Data Mapper applet.

abpm.dataMapper.readTimeOut

Description	The maximum time (in seconds) for which the data mapper applet waits, before throwing an error message, in case of a problem such as backend database server being down

Default Value	720
Possible Values	Any positive integer
Selection Criteria	NA
Comments	The maximum time for which the data mapper applet waits, before throwing an error message in case of a problem such as backend database server being down

MONITORING

abpm.monitoring.minHeapsize

Description	**The minimum memory required for the Monitoring applet**
Default Value	128M
Possible Values	
Selection Criteria	NA
Comments	This indicates the minimum amount of memory required to run the Monitoring applet.

abpm.Monitoring.maxHeapsize

Description	**The maximum memory possible for the Monitoring applet**
Default Value	256M
Possible Values	
Selection Criteria	NA
Comments	This indicates the maximum amount of memory required to run the Monitoring applet.

abpm.Monitoring.readTimeOut

Description	**The maximum time (in seconds) for which the monitoring applet waits, before throwing an error message, in case of a problem such as backend database server being down**
Default Value	720
Possible Values	Any positive integer
Selection Criteria	NA
Comments	The maximum time for which the monitoring applet waits, before throwing an error message in case of a problem such as backend database server being down

PROCESS DESIGNER

abpm.Process Designer.minHeapsize

Description	**The minimum memory required for the Process Designer applet**

Default Value	128M
Possible Values	
Selection Criteria	NA
Comments	This indicates the minimum amount of memory required to run the Process Designer applet.

abpm.Process Designer.maxHeapsize

Description	**The maximum memory possible for the Process Designer applet**
Default Value	256M
Possible Values	
Selection Criteria	NA
Comments	This indicates the maximum amount of memory required to run the Process Designer applet.

abpm.Process Designer.readTimeOut

Description	**The maximum time (in seconds) for which the Process Designer applet waits, before throwing an error message, in case of a problem such as backend database server being down**
Default Value	720
Possible Values	Any positive integer
Selection Criteria	NA
Comments	The maximum time for which the process designer applet waits, before throwing an error message in case of a problem such as backend database server being down

SOLUTION PROPERTIES

SALESFORCE INTEGRATION ACCELERATOR PARAMETERS

abpm.Salesforce.UserId

Description	**The UserId to access the Salesforce Accelerator solution**
Default Value	
Possible Values	
Selection Criteria	
Comments	Enter the UserId to login into the Salesforce Accelerator solution.

abpm.Salesforce.Password

Description	**The password used to access the Salesforce Accelerator solution**

Default Value	
Possible Values	
Selection Criteria	
Comments	Enter the password to login into the Salesforce Accelerator solution.

NETSUITE INTEGRATION ACCELERATOR PARAMETERS

abpm.solution.netsuite.emailID

Description	The LoginID used to login into the NetSuite Accelerator solution
Default Value	
Possible Values	
Selection Criteria	
Comments	Enter the emailID to login into the NetSuite Accelerator solution.

abpm.solution.netsuite.accountID

Description	The account ID of the NetSuite Accelerator solution
Default Value	
Possible Values	
Selection Criteria	
Comments	Enter the account ID of the NetSuite Accelerator solution.

abpm.solution.netsuite.password

Description	The password used to login into the NetSuite Accelerator solution
Default Value	
Possible Values	
Selection Criteria	
Comments	Enter the password used for logging into the NetSuite Accelerator solution.

abpm.solution.netsuite.accountType

Description	The type of account of the NetSuite Accelerator solution
Default Value	
Possible Values	
Selection Criteria	

Comments	Enter the type of account of the NetSuite Accelerator solution.

2

ADEPTIA SUITE APPENDIX B: CRON EXPRESSION

A "Cron-Expression" is a string comprised of 6 or 7 fields separated by white space. The 6 mandatory and 1 optional fields are as follows:

Field Names	Allowed Values	Allowed special Character
Seconds	0-59	, - * /
Minutes	0-59	, - * /
Hours	0-23	, - * /
Day-of-month	1-31	, - * ? / L W C
Month	1-12 or JAN-DEC	, - * /
Day-of-Week	1-7 or SUN-SAT	, - * ? / L C #
Year (Optional)	empty, 1970-2099	, - * /

- The '*' character is used to specify all values. For example, "*" in the minute field means "every minute".
- The '?' character is allowed for the day-of-month and day-of-week fields. It is used to specify 'no specific value'. This is useful when you need to specify something in one of the two fields, but not the other. See the examples below for clarification.
- The '-' character is used to specify ranges For example "10-12" in the hour field means "the hours 10, 11 and 12".
- The ',' character is used to specify additional values. For example "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".
- The '/' character is used to specify increments. For example "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". You can also specify '/' after the '*' character - in this case '*' is equivalent to having '0' before the '/'.
- The 'L' character is allowed for the day-of-month and day-of-week fields. This character is shorthand for "last", but it has different meaning in each of the two fields. For example, the value "L" in the day-of-month field means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means "7" or "SAT". But if used in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last Friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing results.
- The 'W' character is allowed for the day-of-month field. This character is used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However if you specify "1W" as the

value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.

- The 'L' and 'W' characters can also be combined for the day-of-month expression to yield 'LW', which translates to "last weekday of the month".
- The '#' character is allowed for the day-of-week field. This character is used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means the third Friday of the month (day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given day-of-week in the month, then no firing will occur that month.
- The 'C' character is allowed for the day-of-month and day-of-week fields. This character is shorthand for "calendar". This means values are calculated against the associated calendar, if any. If no calendar is associated, then it is equivalent to having an all-inclusive calendar. A value of "5C" in the day-of-month field means "the first day included by the calendar on or after the 5th". A value of "1C" in the day-of-week field means "the first day included by the calendar on or after Sunday".
- The legal characters and the names of months and days of the week are not case sensitive.

Here are some full examples:

Expression	Meaning
0 0 12 * * ?	12pm (noon) every day
0 15 10 ? * *	10:15am every day
0 15 10 * * ?	10:15am every day
0 15 10 * * ? *	10:15am every day
0 15 10 * * ? 2005	10:15am every day during the year 2005
0 * 14 * * ?	Every minute starting at 2pm and ending at 2:59pm, every day
0 0/5 14 * * ?	Every 5 minutes starting at 2pm and ending at 2:55pm, every day
0 0/5 14,18 * * ?	Every 5 minutes starting at 2pm and ending at 2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day
0 0-5 14 * * ?	Every minute starting at 2pm and ending at 2:05pm, every day
0 10,44 14 ? 3 WED	2:10pm and at 2:44pm every Wednesday in the month of March.
0 15 10 ? * MON-FRI	10:15am every Monday, Tuesday, Wednesday, Thursday and Friday
0 15 10 15 * ?	10:15am on the 15th day of every month
0 15 10 L * ?	10:15am on the last day of every month
0 15 10 ? * 6L	10:15am on the last Friday of every month
0 15 10 ? * 6L 2002-2005	10:15am on every last friday of every month during the years 2002, 2003, 2004 and 2005
0 15 10 ? * 6#3	10:15am on the third Friday of every month

TABLE OF FIGURES

INDEX