NetIQ® Aegis® 3.4
User Guide

July 2018

Legal Notice

Contents

About this Book and the Library

The *User Guide* provides conceptual information about the NetIQ Aegis product (Aegis). This book defines terminology and various related concepts. This book also provides an overview of the user interfaces and step-by-step guidance for many Process Operator tasks.

Intended Audience

This book provides information for individuals responsible for any of the following tasks:

- Understanding Aegis concepts
- Interacting with processes to handle incidents

Other Information in the Library

The library provides the following information resources:

Help for Configuration Console

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Help for Operations Console

Provides conceptual information and step-by-step guidance for common tasks.

Administrator Guide

Provides conceptual information related to the Configuration Console and step-by-step guidance for many configuration tasks.

Process Authoring Guide

Provides conceptual information related to the Workflow Designer console and step-by-step guidance for many workflow-related tasks.

NetIQ Reporting Center Reporting Guide

Provides conceptual information about the NetIQ Reporting Center product. Intended for individuals responsible for understanding and using Aegis reports.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

.

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introduction

IT operations managers are under increasing pressure to control costs while delivering services at a faster pace than ever before. In the quest to get “more for less,” many IT professionals are exploring ways to automate time-consuming, labor-intensive tasks that increasingly occupy valuable and expensive IT staff resources.

Many enterprises seek to automate routine workflow practices at the level of specific tasks and procedures, sometimes referred to as **run books**. While run books represent proven manual processes, they are subject to human error and can be very expensive by wasting expert staff time on repetitive, menial tasks. Run books can also be abstract, representing “tribal knowledge” that resides with individuals. Tribal knowledge may not be accurately recorded and can be easily lost when individuals leave an organization.

At the same time, IT operations deal with an increasingly diverse and complex IT environment due to highly distributed operations and business acquisitions. Often, these operational environments contain many diverse tools. The lack of integration for these tools can hinder the ability to efficiently respond to events and conduct routine operational activities.

NetIQ designed Aegis from the ground up as an IT workflow automation platform, to enable the automation of IT run books and processes.

What is Aegis?

Aegis is an IT process automation platform that allows you to model, automate, measure, and continuously improve run books and processes. Aegis allows you to:

- Define automated IT processes, using your documented IT processes and run books as the foundation for automation
- Automatically execute process steps on behalf of personnel
- Coordinate work between different IT functions

Integrating with other NetIQ enterprise products, Aegis retrieves normalized information from your operations management systems to provide a cohesive “big picture” view of your IT operation processes.

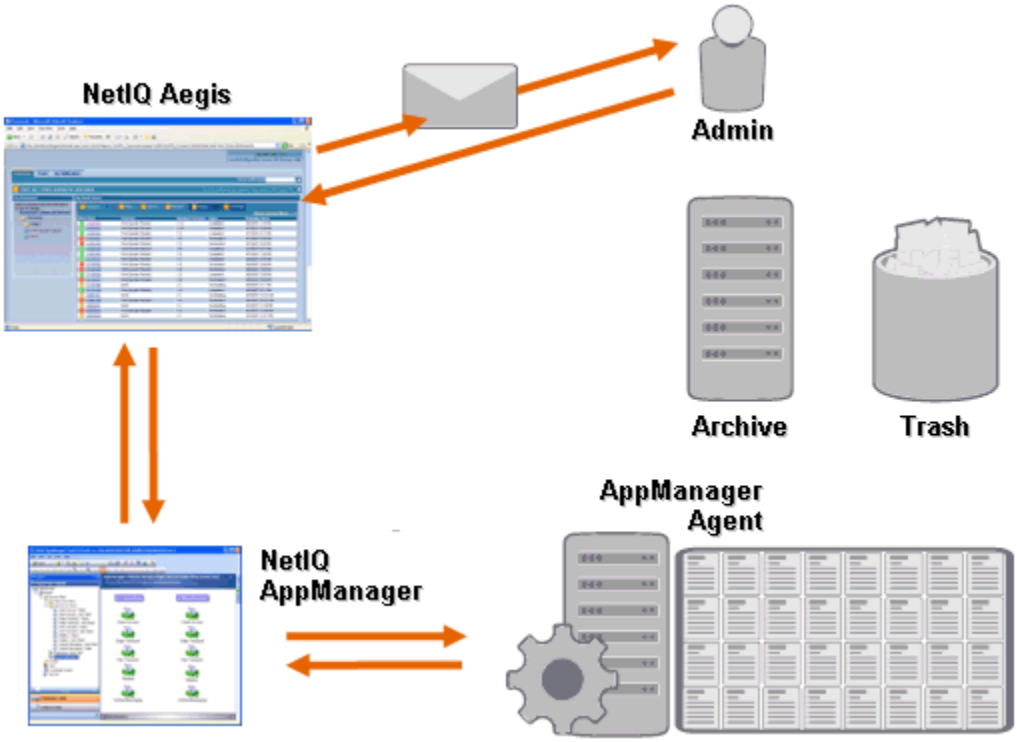
By aggregating this information into a central console, Aegis lets IT operations personnel more easily accomplish the following objectives:

- Automatically initiate standard IT processes to address incidents
- Document all response activities
- Report on adherence to accepted IT policies
- Provide a complete audit history of incident management

By allowing users to quickly identify and automatically group and suppress related events, Aegis reduces the number of false positives users must address and manage.

How Aegis Works

Aegis funnels information from data sources into a central repository, evaluating incoming data against processes that your team defines to match your IT policies. A process runs automatically when event information matches its trigger criteria. If user input is required, the user logs on to the Operations Console to tell the process what to do. For example, if temporary file growth causes disk space to fall below threshold, Aegis can command NetIQ AppManager to perform disk cleanup.



In this example, AppManager detects that available disk space has fallen below threshold and generates an event, which triggers a process in Aegis and creates a **work item** (an instance of a running process). Aegis requests a disk usage analysis from AppManager, identifying the top N culprits by folder, file type, and age, with extra attention paid to known temporary file storage areas. Aegis sends an email with the results of the analysis to the appropriate user, requesting approval to perform disk cleanup. The email includes a link to the Operations Console. The user logs on to the Operations Console and approves partial cleanup. Aegis commands AppManager to delete the approved files and analyze new disk space status. Aegis waits for confirmation of success, which it then sends to the user. Aegis closes the work item.

Aegis processes are flexible. A typical process may automatically complete the following types of steps:

- Check for auxiliary information about the event
- Determine the priority and urgency of the problem
- Allow users to drill down for details about the event stream

2 Understanding Process Components

A **process** consists of the steps taken to respond to an event sent to Aegis by a data source. Aegis evaluates incoming events against the processes your team defines to represent your IT policies. Every process has an associated **workflow**, which is a graphical representation of the steps in the process. These steps define the trigger criteria that execute the process, and then tell the process how to handle the event. When one or more events from a data source match the trigger criteria of a process, Aegis executes the process and initiates a work item.

Understanding Process Terminology

To understand how Aegis uses the processes you define, you need to understand the following terms:

Work Item

A single instance of a process, triggered by either an incoming event or a manual trigger. A process stands idle until a trigger initiates a work item. A single process may have multiple work items running simultaneously. For more information, see Chapter 4, “Managing Work Items,” on page 15.

Activity

A step in a process that performs a specific function, such as starting the workflow, joining multiple flows, waiting for an incoming event, or stopping the workflow.

Trigger

A set of rules associated with a process that determine how to respond to incoming events, such as initiating a new work item or appending an event to an existing work item. A manual trigger requires human intervention to initiate a work item. For more information about triggers, see “Understanding Triggers” on page 12.

Event

An event initiates an action in a process by matching one of the following:

- **Trigger** - Triggers evaluate events to determine whether to start a process or append the event to an existing work item. A single event might trigger multiple processes. A combination of events can trigger a single process.
- **Wait for Event activity** - The Wait for Event activity responds to an event that occurs while a process is running. Typically, each adapter has a customized version of the activity to match events from that adapter. For example, if your Aegis environment has multiple adapters, you might see a Wait for Email Event activity or a Wait for AppManager Event activity.

Scheduled Event

An event that initiates a work item according to a defined schedule, such as nightly backups or monthly maintenance. Scheduled events are not associated with monitored products.

Understanding Triggers

A trigger evaluates incoming events and determines whether to initiate a work item or append one or more events to existing work items.

Automatic Triggers

Automatic triggers respond to matching events based on trigger rules defined by the Process Author.

Manual Triggers

Manual triggers require human intervention to initiate a work item. For more information about manually triggering processes, see “Manually Triggering a Process” on page 19.

Understanding Blocked Events

Aegis can prevent a large number of unnecessary work items by blocking the following types of events:

Repetitive events	A data source may repeatedly send identical events during the course of an outage but the first notice is usually sufficient.
Symptomatic events	One failure may have downstream impacts, each of which generates a symptomatic event. Fix the root cause and many of these events go away.
False warnings	Performance management systems often have static and inexact thresholds that lead to a large number of warnings when there is no real problem.

Process Authors can configure triggers to prevent new work items by blocking events. For example, after an event matches the conditions to generate the work item, the trigger blocks subsequent matching events.

A trigger blocks matching events only while the work item is running. Once the work item is complete, new matching events initiate a new work item.

Process Authors can also define work item-level blocks when designing a workflow. A work item block terminates a running work item if it meets pre-defined conditions. For example, a conditional connector can take the workflow to an End of Workflow activity.

For more information about related events, see “Viewing a Work Item’s Related Events” on page 17.

Understanding Appended Events

Process Authors can configure triggers to append events to an existing work item. For example, after an event matches the conditions to generate the work item, the trigger appends subsequent matching events to the work item as related events.

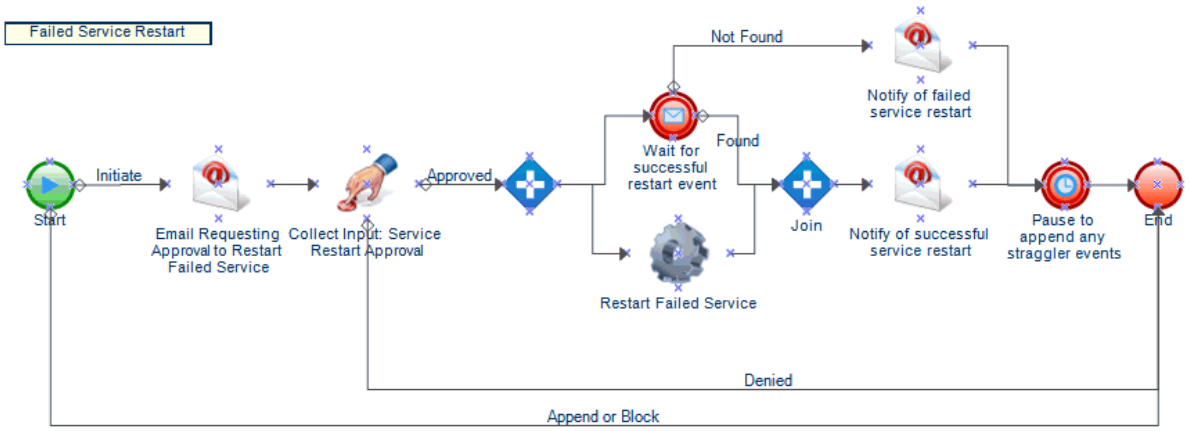
A trigger appends matching events to a work item only while the work item is running. When the work item is complete or the trigger’s time window expires, new matching events initiate a new work item.

A single event can trigger or be appended to multiple work items.

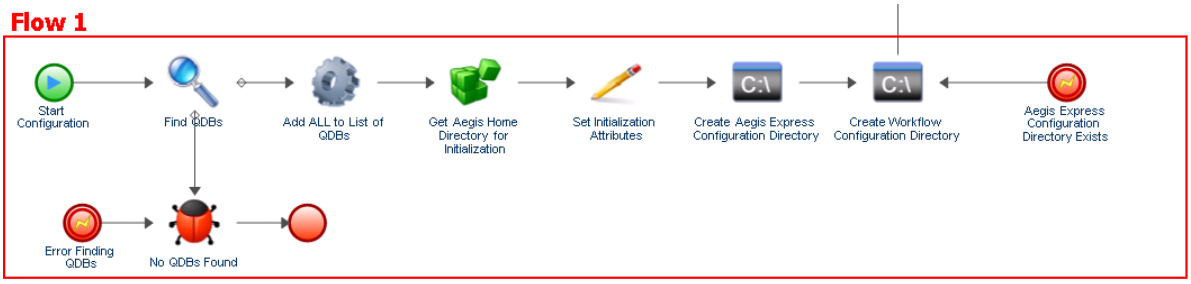
For more information about related events, see “Viewing a Work Item’s Related Events” on page 17.

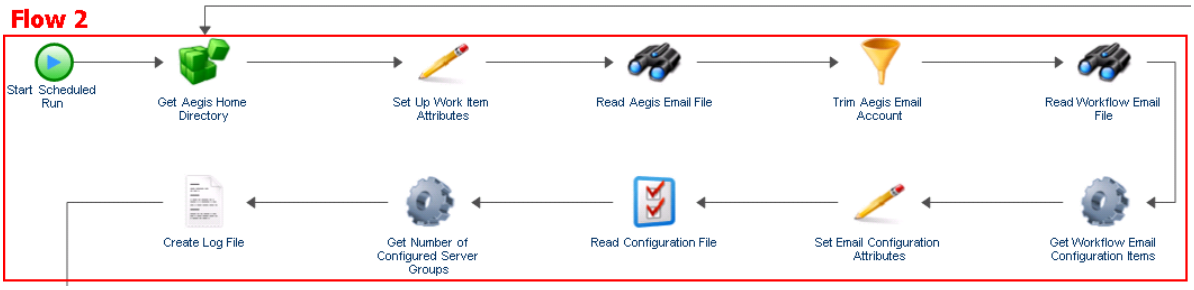
3 Understanding Workflows

A **workflow** is a graphical representation of the steps in a process, made up of activities and connectors, designed to reflect a specific IT policy, as shown in the following figure. When one or more events from a data source match the trigger criteria of a process, Aegis executes the process and initiates a work item.



During execution, a workflow visits activities and traverses connectors in a specific order (called a **flow**). The Start of Workflow activity is the first activity the workflow executes. If the workflow contains multiple Start of Workflow activities, the workflow can have multiple simultaneous flows, as shown in the following figure.





The workflow can also create multiple flows when it traverses more than one connector from an activity or when the trigger appends a new event to the work item. When there are no more active flows, execution terminates.

NOTE: Multiple flows with the same termination point can terminate at different times.

Understanding Workflow Activities

The following table provides information about the symbols used in the Operations Console. For more information about viewing a work item's workflow, see "Viewing a Work Item's Workflow" on page 16.

The Workflow Designer provides the following basic activity types Process Authors use to build workflows. The icons for each activity are defined by the Business Process Management Initiative. For more information about the Business Process Management Initiative, see www.bpmi.org.

	Start of Workflow	Starts the workflow when its associated triggers match incoming events from a data source. A workflow can have multiple Start of Workflow activities that create more than one flow at the same time.
	Task	Performs a specific task, such as collecting user input or sending an email, before proceeding. An associated piece of code, or module, performs the task. Aegis provides several activity libraries that group Task activities according to function. Each Aegis adapter, such as the AppManager adapter or the Secure Configuration Manager adapter, provides its own library of product-specific activities. Task activities in an Aegis or adapter library have an icon that represents their functions, such as the Send Email activity.
	Join	Allows the process to split into multiple parallel flows or combine two or more parallel flows into one.
	Wait for New Email Message	Waits for an incoming message that matches the defined filter. If a matching message does not arrive in the specified time frame, the process continues.
	Pause for Specified Time	Waits for a specified period of time or until a specified time before continuing.
	Capture Workflow Errors	Waits for errors to occur in the workflow. This activity sits outside the main flow. When an error occurs, the flow "jumps" to this activity and proceeds down an alternate flow that handles the error before rejoining the main flow.
	End of Workflow	Marks the end of the process. A workflow can have multiple End of Workflow activities, depending on the number of sub-flows. If the workflow has multiple flows but only one End of Workflow activity, a Completed icon displays when the first flow terminates, even if other flows are still active.

4 Managing Work Items

Using the Operations Console, you can view all of the work items assigned to you. A work item is a single instance of a process. The Operations Console records the activities performed by work items and Process Operators, and collects work item resolution metrics.

Aegis saves the state of all work items so that in the case of an interruption in service (such as a power outage), it will start back up in its previous state with all existing work items.

Understanding Work Item Properties

Using the Operations Console, you can view detailed information about a work item. Work item properties are divided into the following categories:

General Attributes

Displays basic information about the work item, such as its name, description, and current status.

Custom Attributes

Displays any custom attributes the Process Author created specifically for the work item.

Resources

Specifies the clusters, computers, and business services associated with the work item.

People

Specifies the work item's owner and stakeholders.

To view a work item's properties:

1. ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.
2. Under **Work Items**, select the work item.
3. On the **View** menu, click **Properties**.
4. Click the appropriate tab to see the work item's properties.

Working with Supporting Analysis Results

These topics provide step-by-step guidance for accessing and viewing Supporting Analysis results.

When designing a workflow, the Process Author can configure one or more data source-specific activities to collect information related to the process, either in the initial stages of investigation or after the work item has been closed. Process Operators can view supporting analysis results in the Operations Console.

In the initial stages of investigation, supporting analysis activities can collect information from all data sources related to a work item to ensure that a Process Operator has as much information as possible to identify the root cause.

After a work item completes, supporting analysis activities can collect information from all related data sources to verify the incident has been correctly resolved.

If a Process Operator views supporting analysis results before all supporting analysis steps are complete, the Operations Console displays the completed results (if any) and indicates which steps are still running.

Viewing Supporting Analysis Results

Using the Operations Console, you can view the results of a work item's supporting analysis activities.

To view a work item's supporting analysis results:

1. ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.
2. Under **Work Items**, select the work item.
3. On the **View** menu, click **Supporting Analysis**.
4. In the tree, expand the appropriate folder to locate assistance activities.
5. In the tree, click each assistance activity you want to view.

Accessing Supporting Analysis Results from External Web Sites

External Web sites may link to the Operations Console to view supporting analysis results through a URL as long as they have the work item ID.

Understanding Work Item Comments

Using the Operations Console, you can view any comments currently associated with a work item. As a Process Operator, you can add comments to a work item. These comments are visible to other Process Operators, who can respond with comments of their own.

To view comments associated with a work item:

1. ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.
2. Under **Work Items**, select the work item.
3. On the **View** menu, click **Comments**.

Viewing a Work Item's Workflow

Using the Operations Console, you can view the current state of a work item's workflow. For more information about workflows, see Chapter 3, "Understanding Workflows," on page 13.

To view the state of the work item's workflow in the Operations Console:

1. ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.
2. Under **Work Items**, select the work item.

3 On the View menu, click **Workflow**.

For more information about workflows, see Chapter 3, “Understanding Workflows,” on page 13.

4 ***If you want to see details about an activity or connector***, click the item in the workflow, and then click **View Execution Results**.

Viewing a Work Item’s Related Events

You can view a list of all events related to a work item. An event can have one of the following relationships with the work item:

- **Initiated** - Event that matched the initiate conditions on the process trigger.
- **Appended** - Event that matched the append conditions on the process trigger after the trigger has initiated a work item.
- **Blocked** - Event that matched the block conditions on process trigger.
- **Late Matched** - Event that matched the initiate conditions on the process trigger after the trigger has initiated a work item. A late matched event is similar to an appended event.
- **Awaited** - Event that matched an activity that waits for incoming events during the course of the workflow, such as the Wait for New Email Message activity or the Wait for Scheduled Event activity.

To view a work item’s related events in the Operations Console:

1 ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.

2 Under **Work Items**, select the work item.

3 On the **View** menu, click **Related Events**.

Viewing a Work Item’s Related Work Items

You can view a list of all work items related to a work item. A related work item can have one of the following relationships with the current work item:

- **Parent** - Work item that launched the current work item using either the Execute Process activity or the Execute Process with Context activity.
- **Child** - Work item the current work item launched.

To view a work item’s related work items in the Operations Console:

1 ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.

2 Under **Work Items**, select the work item.

3 On the **View** menu, click **Related Work Items**.

Terminating Work Items

Using the Operations Console, you can terminate one or more running work items. If an activity in the work item initiated an external task on a remote computer in your environment, the external task continues to run. For example, if the Execute SQL Commands & Scripts activity executes a stored procedure, and you terminate the work item, the stored procedure continues to run until it completes its task.

To terminate a running work item in the Operations Console:

1. ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.
2. Under **Work Items**, select the work items you want to terminate.
3. Click **Terminate**, and then click **Yes**.

Deleting Work Items

Using the Operations Console, you can delete one or more work items. You must terminate a running work item before deleting it

To delete a work item in the Operations Console:

1. ***If you want to see work items associated with a specific process,*** under **Processes**, click the appropriate process.
2. Under **Work Items**, select the work items you want to delete.
3. Click **Delete**, and then click **Yes**.

Viewing Event Details

Using the Operations Console, you can view a complete list of events in Aegis. You can drill down to see granular details for any event in the list.

To view event details:

1. In the Operations Console, click the **Events** tab.
2. Select the event you want to view, and then click **View Event Details**.

Providing Input to a Work Item

Process Authors can configure a workflow to send an email with a link to an Input window. When you click the link, Aegis opens the Input window, where you can provide the necessary input to a workflow activity waiting for user feedback, such as setting priority or starting a job. The link does not open the Operations Console. When you close the Input window, Aegis closes your browser.

You can also use the Operations Console to view all work items waiting for input.

To use the Operations Console to provide input to work items waiting for user input:

1. In the Operations Console, click the **Work Items Waiting for Input** tab.
2. In the list, click the work item for which you want to provide input.

3 Click **Submit Input Form**.

4 On the Input window, provide the appropriate information.

Manually Triggering a Process

You can manually trigger a process that has a manual trigger attached to it. For more information about manual triggers, see “Understanding Triggers” on page 12.

To manually trigger a process:

1 Under **Processes**, click the process you want to start manually.

2 Click **Start Process**.