Service Monitoring in Integration Server

Version 10.11

October 2021

WEBMETHODS

This document applies to webMethods Integration Server 10.11 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: IS-MON-UG-1011-20230124

Table of Contents

About this Guide

This guide explains how to monitor services and documents that you run on Integration Server, and how to archive or delete the audit data. The guide is intended for developers who know how to create services in Software AG Designer and how to use webMethods Integration Server and messaging brokers.

Service Monitoring in the new Integration Server web user interface is a preview feature that has limited functions and is:

- Not intended for use in a production environment
- Subject to change in the future without deprecation announcements

If you want to provide feedback on this preview feature, go to the Integration Server area in the Software AG TechCommunity.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies service names and locations in the format *folder.subfolder.service*, APIs, Java classes, methods, properties.
Italic	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at https://documentation.softwareag.com.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at https://empower.softwareag.com/.

You can find product information on the Software AG Empower Product Support website at https://empower.softwareag.com.

To submit feature/enhancement requests, get information about product availability, and download products, go to Products.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the Knowledge Center.

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at https://empower.softwareag.com/public_directory.aspx and give us a call.

Software AG Tech Community

You can find documentation and other technical information on the Software AG Tech Community website at https://techcommunity.softwareag.com. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

1 About Service Monitoring

When you run services on Integration Server, you can monitor the following:

- Audit data for flow and coded (for example, Java) services
- Integration Server documents that are in doubt, that have failed, or that have exhausted trigger retries (see *Publish-Subscribe Developer's Guide*)
- Documents that webMethods Broker (deprecated) clients publish or to which they subscribe
- Error details for services and documents

You can use the data you obtain when monitoring a service to track when the service started and completed, and whether a service execution is successful or failed. If you execute a root service (that is invoked directly by a client or by a webMethods Messaging Trigger), you can edit the pipeline of the service and resubmit it. You can also edit and resubmit documents.

To ensure that Service Monitoring is at peak performance, you can archive or delete the monitored data for past periods.

To use Service Monitoring, you log on to the administration user interface of the Integration Server that hosts the WmMonitor package.

2 Requirements for Service Monitoring

Service Monitoring uses the audit data that Integration Server logs into the service log. This service log requires an external database.

To be able to monitor services and documents in Integration Server, you must set up the Integration Server environment as follows:

- Install Integration Server and the WmMonitor package (see *Installing Software AG Products*)
- Configure the Integration Server that hosts the WmMonitor package to connect to an external database (see *Installing Software AG Products*)
- Create the ISCoreAudit database component on the external database (see *Installing Software AG Products*)
- Configure and enable the service logger and the document logger for the Integration Server that hosts WmMonitor (see *webMethods Audit Logging Guide*)
- Enable audit logging for each service (see *webMethods Service Development Help*)
- To monitor services and documents executed on remote Integration Servers, the Integration Server that hosts WmMonitor and the remote Integration Servers must share the same external database.

For detailed information about Integration Server logging, see *webMethods Audit Logging Guide*.

To be able to archive the data from the ISCoreAudit database component, you must:

- Create an Archive database component using the Database Component Configurator (see *Installing Software AG Products*)
- Create a JDBC database connection pool (see Creating a Connection Pool in *webMethods Integration Server Administrator's Guide*)
- Point the Archiving function at the JDBC database connection pool alias (see Pointing Functions at Connection Pools in *webMethods Integration Server Administrator's Guide*).

3 Accessing Service Monitoring

To use service monitoring, you must log on to the Integration Server administration interface as a user that is part of the Administrators group. For more information about adding an administrator user, see *webMethods Integration Server Administrator's Guide*.

To access service monitoring

1. Log on to the Integration Server administration interface as administrator using the following URL:

   ```
   http://localhost:5555/WmAdmin
   ```

2. Click **Monitoring**.

3. On the Monitoring page, select Services, Documents, or Data management.

4 Customizing the Screen Space

To customize the screen space on the Services, Documents, and Data management pages, you can hide or show columns, and switch the Zebra stripes on and off.

To customize the screen space

1. Click the **Table settings** icon on the page you want to customize.
2. Switch on or off the Zebra stripes.
3. Click **Show columns**.
4. Select the columns that you want to show on the page, or click **Restore defaults** to use the default column settings.
5. Click **Save**.
6. To enter full screen and hide the charts on the screen, click **Show full screen**.
7. To exit full screen and view the charts on the screen, click **Exit full screen**.

5 Changing the Locale Settings

When you first log on to the Integration Server administrator interface, Service Monitoring takes the locale settings of the web browser and sets the browser's time zone, date format, and time format as the default ones for the Monitoring pages.

The locale settings are stored in the local storage of the web browser, which means that if you switch the web browser on the same machine, or you use a different machine, you might have entirely different locale settings. If different users log on the same machine, each user can have different locale settings. Also, each Integration Server instance that you access through the Integration Server administrator interface has its own locale settings.

You can change the format that Service Monitoring uses to display dates and times on the Monitoring pages.

To modify the locale settings

1. Click the **Profile** icon.
2. Click **My profile**.
3. Click **Edit**.
4. Select the locale settings in the fields, described in the following table.

Field	Description
Time zone	The time zone in which to display the time.
Date format	The format in which to display the date (day, month, and year).
Time format	The format in which to display the time (in seconds, minutes, and hours).

5. Click **Save**.

6 Service Monitoring

Filtering Services by Service Name

You can search for a specific service by full name or part of the name.

You can filter services by Service name using the Basic or Advanced filters. In the Advanced filter, you can combine Service name with other search criteria to narrow down your search results.

Note:
Whether a search is case-sensitive or case-insensitive depends on the way the underlying database (for example, Oracle, DB2, or SQL Server) handles the queries that service monitoring issues to obtain data.

To find services by service name

1. On the Services page, click **Basic** or **Advanced**.

2. In the **Service name** field, type a part of the service name or the full service name of the service that you want to find. For example:

   - The fully-qualified name of a service, such as, OrderPartner.Services:processOrder, to list all executed instances of the service.
   - A partial service name, such as processOrder, to list all services that have "processOrder" in the name.

   Tip:
   You can search for a service by name and status. If you select specific statuses in the Status field, the search results will list all executed instances of the service that match the specified status(es).

3. Click **Apply**.

   The services on the page are filtered based on the search criteria. For more information about the service execution details that you can view on the Services page, see " Viewing Service Execution Details" on page 23.

   Tip:
   Each search filter that you apply is saved and used in subsequent searches until you delete its label. You can clear all saved filters by clicking **Clear all**.

Filtering Services by Status

In the Service executions doughnut chart you can view the total number of service executions, and the total number of service executions by status. Each status is represented by a color as described in the chart legend. When you click on a colored slice of the doughnut chart, the services are filtered by the status represented by the color. For example, clicking the red slice of the chart lists all Failed services.

You can also filter services by Status using the Basic or Advanced filters. In the Advanced filter, you can combine Status with other search criteria to narrow down your search results.

To find services by status

1. On the Services page, click **Basic** or **Advanced**.

2. In the **Status** check-box, select the status(es) that you are interested in.

Status	Description
Started	The service is currently running.
Completed	The service completed successfully.
Failed	An error occurred during the service execution and the service did not complete successfully.
Resubmitted	The service was resubmitted.

3. Click **Apply**.

   The services on the page are filtered based on the search criteria. For more information about the service execution details that you can view on the Services page, see " Viewing Service Execution Details" on page 23.

   Tip:
   Each search filter that you apply is saved and used in subsequent searches until you delete its label. You can clear all saved filters by clicking **Clear all**.

Filtering Services Using Advanced Search Criteria

You use an advanced search criteria, in combination with other criteria or on their own.

To find services with advanced search

1. On the Services page, click **Advanced**.

2. In the Search area, specify search criteria in the fields. To combine several search criteria from the list, click +. For example, to search by Service name and Server ID, click + to add a search field with Server ID.

The following table provides more information about the search criteria.

Search criteria	Description
Service name	Fully qualified or partial name of the services (such as OrderPartner.Services:processOrder or processOrder).
Server ID	Integration Server on which the services are executed. Type the Integration Server's DNS name and port (such as `integration.east.rubicon.com:5555`) or partial DNS name or port (such as `rubicon`). **Note:** To monitor services on a remote Integration Server host, the local and remote Integration Server must share the same database.
Context ID	Full service context ID of the service.
Root context ID	Full root context ID, to find all services that were invoked one after another starting with the specified root service.
Parent context ID	Full parent service context ID, to find all services invoked by the specified parent service.
Custom context ID	Full custom context ID of the service.
User	Full or partial name of the user that invoked the service.
Status	Status of the services (**Started**, **Completed**, **Failed**, or **Resubmitted**). Select the check-boxes of the statuses to include in the search filter.

3. If you want to search for services based on custom logged fields, use **Log field name**.

The following table provides more information about how to use the field.

Field	Description
Log field name	Full name of a custom logged field to use for the search. The field name is case-insensitive. Wildcard characters are not supported.
Operator	Select the operator to use: Equals, Contains, Not contains, Not equals, >, >=, <, <=.
Value	Specify the value to use for comparison. Click **Add a condition** to specify additional fields.

4. Select the **Show root level services only** check-box if you want to limit the search to root services.

5. In the **Search condition** switch, select **AND** to find services that match all search criteria. Select **OR** to find services that match any search criteria.

   Note:
   The **OR** condition also applies to the pre-selected monitoring time period.

6. Click **Apply**.

   The services on the page are filtered based on the search criteria. For more information about the service execution details that you can view on the Services page, see " Viewing Service Execution Details" on page 23.

   Tip:
   Each search filter that you apply is saved and used in subsequent searches until you delete its label. You can clear all saved filters by clicking **Clear all**.

Changing the Service Monitoring Time Period

You can change the time range for which service monitoring lists the services on the Services page. The default time range is 1 hour. You can select one of the pre-defined time periods in the time-range picker. You can also specify a custom time period, which starts/ends at a specific time and date.

In the History bar chart you can monitor the number of service executions by status and time.

- If the time period that you want to select corresponds to one of the predefined values, click the value in the time-range picker.
- If you want to select a custom time period, follow the steps below.

  1. Click **Custom**.
  2. Select start date and time.
  3. Select end date and time.
  4. Click **Apply**.

  The services on the page are filtered based on the selected time period. For more information about the service execution details that you can view on the Services page, see " Viewing Service Execution Details" on page 23.

  Tip:
  The time period that you select is saved and used in subsequent searches until you change it.

Viewing Service Execution Details

Use the details about the services listed in the search results to track which services are executed and what is the current status of an executed service. You can view the following details about an executed service instance:

Column	Description
Service name	Fully-qualified name of the service.
Status	Current status of the service.
Context ID	Context ID of the service. Each time a service is resubmitted, the Integration Server assigns that service a new context ID.
Start time	Date and time when the service started.
Last updated	Date and time on which the activity indicated by the **Status** (for example, **Failed**) is logged.
Duration	Duration of the service. The interval in ms from the time the service was started until the time the service was completed
Server ID	DNS name and port number of the Integration Server on which the service runs.
User	Name of the user that ran the service.
Custom context ID	Custom value that you can define for the Context ID of an executed service by using the pub.flow:setCustomContextID service. You can click the filter icon next to a particular service to display all services that have the same Custom context ID.

Viewing Details about a Service

You can view the details of each service in the search results.

If you are monitoring a root service with child services, you see the details of the root service and links to the details of the child services.

If you are monitoring a child service, you see the details of the child service and links to the parent, root, and all other child services of the root service.

To view the details of a service

1. In the search results on the Services page, find the service that you want to inspect.
2. Click the service name.

   On the Service detail page you can view the following details about the service:

Field	Description
Status	Current status of the service.

Field	Description
Duration	Duration of the service execution. The interval in ms from the time the service was started until the time the service was completed.
Last updated	Date and time on which the activity indicated by the **Status** (for example, **Failed**) is logged. In this box you will also have links to the details of the root, parent, last audited parent, and child services.
Service name	Fully-qualified name of the service.
Custom context ID	Custom value that you can define for the Context ID of an executed service by using the pub.flow:setCustomContextID service.
Root context ID	Context information that service monitoring uses to connect related entries from different logs. Context ID of the root-level service.
Parent context ID	Context ID of the service that invoked the service, which is referred to as the parent service. The parent context ID can be the same as the root context ID.
Context ID	Context ID of the service. Each time a service is resubmitted, the Integration Server assigns that service a new context ID.
Server ID	DNS name and port number of the Integration Server on which the service runs.
Timestamp	Date and time on which the activity indicated by the **Status** (for example, **Failed**) is logged.
Error messages	Most recent error message associated with the service.

Viewing Advanced Service Details

You can view the advanced details of services. The advanced details provide information about service statuses at a given time, activity messages, resubmissions, custom logged fields, and service errors.

To view the advanced service details on the Service detail page, click **Show advanced service details.**

The History panel shows the status of a service at a given date and time.

If a service logs user-defined messages by calling the pub.prt.log:logActivityMessages service, the Activity messages panel shows the date and time a message was logged, the type of the message (that is error, warning, or message), and the brief and long version of the text of the message.

After a service is resubmitted, the Control actions panel shows information about the resubmission. The panel shows the date and time the service was resubmitted, the action taken, the name of the user who resubmitted the service, and the Integration Server on which the service was resubmitted.

If a service logs run-time values for custom fields, the Logged fields panel shows the date and time the custom field was logged, the input or output parameter of the service for which run-time values were logged, and the name and value of the custom logged field.

If errors occur while a service is running, the Service errors panel shows the date and time each error was logged and a description of the error.

Resubmitting Services

You can resubmit a root-level service when the audit logging is configured to log the input pipeline for the service in the audit log. The service can have any status. For details about configuring audit logging, see *webMethods Service Development Help*.

To resubmit a service, an Integration Server remote server alias is required and the default Integration Server alias must exist and be unaltered. The default alias is used to resubmit a service when the original node on which the service was submitted is down.

When you resubmit a service, service monitoring changes the status of the service to **Resubmitted**. Service monitoring then starts a new instance of the service and sets its status to **Started**. Service monitoring uses the context ID of the original service as the parent context ID of the new instance of the service. All data about the resubmission is logged for the new instance of the service.

Resubmitting Services without Editing the Pipelines

You can resubmit a service without editing its pipeline.

To resubmit one or several services without editing their pipelines

1. In the search results on the Services page, select the services you want to resubmit.
2. Click **Resubmit**.

Resubmitting Services After Editing the Service Pipelines

You can edit a service pipeline and then resubmit the service.

To edit a service pipeline and resubmit the service

1. In the search results on the Services page, find the service to resubmit.
2. Click the service name.
3. On the Service detail page, click the **Service actions** icon.

4. Click **Edit pipeline**.
5. Update the pipeline data.
6. Click **Resubmit**.

Editing a Service Pipeline

You can edit a service pipeline and resubmit the service at a future time.

To edit a pipeline without resubmitting it

1. On the Service detail page, click the **Service actions** icon.
2. Click **Edit pipeline**.
3. Edit the pipeline data.
4. Click **Save**.

   The changes to the service pipeline data are saved only in the temporary memory. This means that if you stay on the Service detail page, you will be able to resubmit the service with the edited pipeline data. If you leave the Service detail page, the changes to the service pipeline data will be lost.

Saving a Service Pipeline to a File

You can save a service pipeline to a file and use it for troubleshooting.

To save a service pipeline to a file

1. On the Service detail page, click the **Service actions** icon.
2. Click **Save pipeline to file**.

   The service pipeline is saved to an XML file with the same name as the service.

7 Document Monitoring

Filtering Documents by Name

You can search for a specific document by full name or part of the name.

You can filter documents by Document name using the Basic or Advanced filters. In the Advanced filter, you can combine Document name with other search criteria to narrow down your search results.

Note:
Whether a search is case-sensitive or case-insensitive depends on the way the underlying database (for example, Oracle, DB2, or SQL Server) handles the queries that Monitor issues to obtain data.

To find documents by name

1. On the Documents page, click **Basic** or **Advanced**.
2. In the **Name** field, type a part of the name or the full name of the document that you want to find. For example:
   - The full document name as it exists on the webMethods Broker (deprecated) (such as `wm::is::OrderProcess::Implementation::CanonicalOrder`).
   - The full document name as it exists on the Integration Server (such as `OrderProcess.Implementation:CanonicalOrder`).
   - A partial document name (such as `OrderProcess`) to select all documents that contain the specified string.

   Note:
   If a document was routed through Universal Messaging, search for the fully qualified name of the publishable document type as it exists on Integration Server. You cannot search for the Universal Messaging channel name associated with a publishable document type.
3. Click **Apply**.

   The documents on the page are filtered based on the search criteria. For more information about the details that you can view on the Documents page, see "Viewing Document Details" on page 33.

   Tip:
   Each search filter that you apply is saved and used in subsequent searches until you delete its label. You can clear all saved filters by clicking **Clear all**.

Filtering Documents by Type

In the Documents doughnut chart you can view the total number of documents, and the total number of documents by type. Each type is represented by a color as described in the chart legend.

When you click on a colored slice of the doughnut chart, the documents are filtered by the type represented by the color. For example, clicking the red slice of the chart lists all Failed documents.

You can filter documents by **Type** using the **Basic** or **Advanced** filters. In the Advanced filter, you can combine Type with other search criteria to narrow down your search results.

To find documents by type

1. On the Documents page, click **Basic** or **Advanced**.

2. In the **Type** list, select the check-boxes of the types that you are interested in.

If you select...	The search results return...
Broker	Documents logged by webMethods Broker.
In doubt	Documents that are associated with the client IDs for the triggers that processed the documents originally.
Retries exceeded	Documents that have exceeded the number of retries during delivery or publication.
Failed	Documents that are not delivered, published, or retrieved successfully.

3. Click **Apply**.

   The documents on the page are filtered based on the search criteria. For more information about the document details that you can view on the Document page, see "Viewing Document Details" on page 33.

   Tip:
   Each search filter that you apply is saved and used in subsequent searches until you delete its label. You can clear all saved filters by clicking **Clear all**.

Filtering Documents Using Advanced Search Criteria

You use an advanced search criteria, in combination with other criteria or on their own.

Note:
Whether the search is case-sensitive or case-insensitive depends on how the underlying database (for example, Oracle, DB2, or SQL Server) handles the queries that Monitor issues to obtain data.

To find documents using the advanced search

1. On the Documents page, click **Advanced**.

2. In the Search Area, specify search criteria in the fields. To combine several search criteria from the list, click **+**. For example, to search by **Name** and **Document ID**, click **+** to add a search field with Document ID.

   For more information about the search fields, see "Viewing Document Details" on page 33.

3. If you want to narrow down the results based on the document type, use the **Type** list.

4. In the **Search condition** switch, select **AND** to find documents that match all search criteria. Select **OR** to find documents that match any search criteria.

   Note:
   The **OR** condition also applies to the pre-selected monitoring time period.

5. Click **Apply**.

   The documents on the page are filtered based on the search criteria. For more information about the details that you can view on the Documents page, see "Viewing Document Details" on page 33.

   Note:
   Each search filter that you apply is saved and used in subsequent searches until you delete its label. You can clear all saved filters by clicking **Clear all**.

Changing the Document Monitoring Time Period

You can change the time range for which service monitoring lists documents on the Documents page. The default time range is 1 hour. You can select one of the pre-defined time periods in the time-range picker. You can also specify a custom time period, which starts/ends at a specific time and date.

In the History bar chart you can monitor the number of documents by status and time.

- If the time period that you want to select corresponds to one of the predefined values, click the value in the time-range picker.
- If you want to select a custom time period, follow the steps below.

  1. Click **Custom**.
  2. Select start date and time.
  3. Select end date and time.
  4. Click **Apply**.

  The documents on the Documents page are filtered based on the selected time period. For more information about the documents details that you can view on the Documents page, see "Viewing Document Details" on page 33.

  Tip:

The time period that you select is saved and used in subsequent searches until you change it.

Viewing Document Details

Use the details about the documents listed in the search results on the Documents page to track what is the current status of the documents and when the documents were last updated. You can view the following details about the documents:

Column	Description
Last updated	Date and time on which the activity indicated by the **Status** (for example, **Resubmitted**) is logged.
Name	Fully qualified or partial name of the document (such as `wm::is::OrderProcess::Implementation::CanonicalOrder` or `OrderProcess`).
Document ID	Full or partial ID of the document. webMethods Broker (deprecated) generates the ID when it publishes the document.
Client ID	Full or partial client ID associated with the document. Use partial client ID to search for documents associated with multiple clients. The value you specify for **Client ID** depends on the types of documents you are searching for (see the **Type** field). ■ The format for webMethods Broker (deprecated) IDs is *Broker@host:port* (for example, `CustOps@qatest07:6849`, or partial ID `CustOps`. ■ The format for IDs of webMethods Broker (deprecated) clients is *clientprefix_folder1.folder2.foldern_trigger* (for example, `smitha_documenthistory.history.triggers_MsgHistoryWithNoResServiceTrigger`, or partial ID `smitha`). **Note:** A webMethods messaging trigger that subscribes to document types routed through webMethods Broker (deprecated) has a corresponding client on the webMethods Broker (deprecated). ■ An In doubt document received from Universal Messaging does not have a client ID. In the search results, Service Monitoring displays “NA” for the client ID.
Type	Type of the document (Broker, In doubt, Retries exceeded, or Failed). For a short description of each type, see “Filtering Documents by Type” on page 30.

Viewing Details about a Document

You can view the details of each document in the search results.

To view the details of a document

1. In the search results on the Documents page, find the document that you want to view.
2. Click the document name.

   On the Document Detail page you can view the following details about the document:

Field	Description
Status	Current status of the document (**Broker**, **In doubt**, **Retries exceeded**, or **Failed**).
Last updated	Date and time on which the activity indicated by the **Status** (for example, **Resubmitted**) is logged.
Document name	Name of the document.
Document ID	Full or partial ID of the document.
Client ID	Full or partial client ID associated with the document.
Enqueued	Whether a Broker document is in a client or forwarding queue.
Timestamp	Date and time on which the activity indicated by the **Status** (for example, **Resubmitted**) is logged.

Resubmitting Documents

When you resubmit a document, Integration Server logs a new instance of the document and all data about the resubmission is logged for the new instance.

Resubmitting Documents

To resubmit one or several documents without editing:

1. In the search results on the Documents page, select the documents you want to resubmit.
2. Click **Resubmit**.

   Service Monitoring resubmits each type of document as follows in the table below:

Document Type	Service Monitoring
webMethods Broker (deprecated)	Publishes the document to the webMethods Broker (deprecated) to which the Integration Serverwith Service Monitoring is connected.
In doubt	Delivers the document to the triggers that originally processed the document.
Failed	■ **Failed during delivery**: Delivers the document to the original destination webMethods Broker (deprecated) client. ■ **Failed during publication**: Publishes the document to the webMethods Broker (deprecated) to which the Integration Serverwith Service Monitoring is connected. ■ **Failed during retrieval**: Delivers the document to the triggers for which Integration Server originally tried to retrieve the document.
Retries exceeded	■ **Exceeded during delivery**: Delivers the document to the original destination webMethods Broker (deprecated) client. ■ **Exceeded during publication**: Publishes the document to the webMethods Broker (deprecated) to which the Integration Serverwith Service Monitoring is connected.

Editing and Resubmitting Documents

You can edit a document and resubmit it.

To edit and resubmit a document

1. In the search results on the Documents page, find the document which you want to edit and resubmit.
2. Click the document name.
3. On the Document detail page, click the **Document actions** icon.
4. Click **Edit document**.
5. Update the fields on the Edit document page.
6. Click **Resubmit**.

8 Data Management

About Data Management

You can remove audit data from the IS Core Audit Log database component to keep the logging at peak performance. You can view the archive data and choose whether to remove it by archiving or deleting it.

The following table describes the archive and delete operations.

Operation	Description
Archive	Moves audit data from the IS Core Audit Log database component to the Archive database component.
Delete	Permanently deletes audit data from the IS Core Audit Log database component without storing it to any other location.

Note:
Before archiving or deleting data, you must create an Archive database component. For more information, see *Installing Software AG Products*.

After you archive audit data, you can no longer view it in Service Monitoring but you can still query the archive database using SQL.

Viewing Archived Data Details

On the Data management page, you can view a summary of the current contents of the IS Core Audit Log database, and details about archive operations that were performed in the past.

You can determine if it is safe to archive or delete audit data by checking the Archive summary table, which displays a summary of the data that is currently available in the IS Core Audit Log database. You can use this information to determine the amount of data in the audit log tables, and decide how long to retain data. If you have a high count of table rows, kept over a long period of time, and you try to delete it at once, you might run into issues. To avoid these issues, always choose the largest retention period possible for the archive run.

The following table describes the fields of the Archive summary table.

Column Name	Description
Component	Component type (service, document, or server data).
Table name	Name of the database table that holds the data.
Count rows	Number of rows in the table.
Earliest	Date and time of the earliest record in the table.
Latest	Date and time of the latest record in the table.

In the Archive history table, you can view a record of the past archive operations.

Note:
The Archive history table does not display information about the delete operations that were completed in the past.

The following table describes the fields of the Archive history table.

Column Name	Description
Operation	Type of event that occurred.
Procedure name	Name of the stored procedure that was invoked by the archive process.
Status	Code that shows whether the archive operation was a service archive or a document archive, as follows: ■ 0 - document archive ■ 1 - service archive
Event text	Message that the database returns after the stored procedure completes.
Insert date/time	Date and time when the data was inserted into the Archive database component.
Update date/time	Date and time when the data was updated in the Archive database component.
Log ID	Unique counter for each record in the operation_log table in the Archive database component.

Archiving Data

On the Data management page, you can archive obsolete audit data for a specified Retention time period. You must carefully choose the Retention time period, as archiving too much data at once might have negative effects on the database, such as an increased time of the archive operation, locking issues, a large increase of the database size, an increase of the transaction log, and an increase of the temp table size. To avoid these negative effects, for each archive operation, choose the largest retention period possible.

Service Monitoring can archive user-defined messages for a service only if customized logging is set up for the service. If service logging is globally enabled in Integration Server, but customized logging is not set up for the service in Designer, then Service Monitoring cannot archive user-defined messages written by the service.

To archive audit data

1. In the **Retention time period** area of the screen, specify how long you want to keep the data in the IS Core Audit Log tables. Service Monitoring archives data that is older than the retention period you specify.

The following table describes the data retention options.

Option	Description
Number of days to retain (including today)	Number of days for which you want Service Monitoring to keep archive data. For example, if you specify 15, Service Monitoring will archive data that is 16 days old or older.
Retention period start date (including today)	Date of the oldest data to keep. Click the calendar icon and select the date and time. For example, if you specify 6/3/2020 0:00:00, Service Monitoring will keep data from 6/3/2020 until the current date, and will archive data logged before 6/3/2020.

Note:
Service Monitoring archives services based on their end timestamp, and documents and server data based on the timestamp.

2. Select **Data types** to archive.

   a. Select the check boxes corresponding to the types of data to archive.

      The following table describes the types of data.

Select	To archive
Services	Service log entries, input pipelines, error data, user-defined messages, and service control data (resubmit actions).
Documents	Logged documents for all webMethods Broker (deprecated) clients and document control data (resubmit actions). If selected, Service Monitoring archives all logged documents.
Server data	Integration Server session and guaranteed delivery log entries, and error log entries that are not associated with logged processes, services, or documents (for example, errors that occur during startup or during the run of unlogged services, activations, and documents). If selected, Service Monitoring archives all server data.

   b. If you want to archive services, select which status to archive.

      The following table lists the status options.

Option	Archives or deletes
Completed	Audit data for services with status Completed.
Completed-Failed	Data for services with status Completed, Failed, Failed (Escalated), and Resubmitted.

3. In the **Archiving batch size** field, indicate the number of primary items and accompanying items to archive at a time.

   For example, to archive 100 services, activity logs, and errors at a time, choose a number that takes the size of each record and other performance factors into consideration. If the record size is large, consider reducing the batch size; if the record size is small, increasing the batch size might increase the archiving speed.

4. Click **Archive and delete**.

Deleting Data

On the Data management page, you can permanently delete obsolete audit data for a specified Retention time period. You must carefully choose the Retention time period, as deleting too much data at once might have negative effects on the database, such as an increased time of the archive operation, locking issues, a large increase of the database size, an increase of the transaction log, and an increase of the temp table size. To avoid these negative effects, for each delete operation, choose the largest retention period possible.

Service Monitoring can archive user-defined messages for a service only if customized logging is set up for the service. If service logging is globally enabled in Integration Server, but customized logging is not set up for the service in Designer, then Service Monitoring cannot delete user-defined messages written by the service.

To delete audit date

1. In the **Retention time period** area of the screen, specify how long you want to keep the data in the IS Core Audit Log tables. Service Monitoring deletes data that is older than the retention period you specify.

   The following table describes the data retention options.

Option	Description
Number of days to retain (ending with today)	Number of days for which you want Service Monitoring to keep archive data. For example, if you specify 15, Service Monitoring will delete data that is 16 days old or older.

Option	Description
Retention period start date	Date of the oldest data to keep. Click the calendar icon and select the date and time.
(ending with today)	For example, if you specify 6/3/2020 0:00:00, Service Monitoring will keep data from 6/3/2020 until the current date, and will delete data logged before 6/3/2020.

Note:
Service Monitoring deletes services based on their end timestamp, and documents and server data based on the timestamp.

2. Select **Data types** to delete.

   a. Select the check boxes corresponding to the types of data to delete.

      The following table describes the types of data.

Select	To archive
Services	Service log entries, input pipelines, error data, user-defined messages, and service control data (resubmit actions).
Documents	Logged documents for all webMethods Broker (deprecated) clients and document control data (resubmit actions). If selected, Service Monitoring deletes all logged documents.
Server data	Integration Server session and guaranteed delivery log entries, and error log entries that are not associated with logged processes, services, or documents (for example, errors that occur during startup or during the run of unlogged services, activations, and documents). If selected, Service Monitoring deletes all server data.

   b. If you want to delete services, select which status to delete.

      The following table lists the status options.

Option	Archives or deletes
Completed	Audit data for services with status Completed.
Completed-Failed	Data for services with status Completed, Failed, Failed (Escalated), and Resubmitted.

3. In the **Archiving batch size** field, indicate the number of primary items and accompanying items to delete at a time.

For example, to delete 100 services, activity logs, and errors at a time, choose a number that takes the size of each record and other performance factors into consideration. If the record size is large, consider reducing the batch size; if the record size is small, increasing the batch size might increase the speed of the deletion.

4. Click **Delete only**.