

webMethods Product Suite 10.11

Release Notes

Software AG's webMethods hybrid integration platform lets you build application integration solutions and integrate cloud-based applications with on-premise systems without coding. This top-rated platform simplifies development with one toolset for both on-premise and cloud integrations and uses a microservices-style architecture to deliver and scale new integrations faster.

The webMethods suite, with integration and API management products, provides a broad collection of capabilities, including application and partner integration, API management, B2B integration, managed file transfer, building micro-services, high-speed messaging, and in-memory caching. With webMethods, you have an extensible, scalable, and reliable backbone running either in the cloud, on-premises, or hybrid scenarios, providing seamless integration for cloud, mobile, APIs, and Internet of Things (IoT).

Release 10.11 of the webMethods product suite provides significant enhancements in every functional area of the suite.

Release Highlights

Integration and B2B

webMethods DataHub is an innovative zero-code solution that can extract data flowing through the Integration Server and make it accessible in near real-time in a data lake. Once the data is offloaded in a data lake of customer's choice, a query engine highly optimized for the data lake usage that has a standard SQL interface can allow BI and AI/ML tools to provide custom dashboards and visual analytics to drive operational analytics and business outcomes.

- Creating a docker image of a Microservices Runtime is now supported without the web services functionality. This is useful for deploying microservices where no SOAP processor is required and results in a 50MB reduction in image size and 2-3 seconds improvement in startup time.
- Richer monitoring with extended metrics from tools (such as Prometheus) allows layered products that run on top of Microservices Runtime to include additional information.
- Importing an Open API 3.0 definition is now supported by Integration Server to generate services that allow a user to call an external API from their services.
- Exposing services for use with clients using the gRPC protocol is now supported. This requires that developers first provide a .proto file from which they can generate the necessary document types and service stubs. Integration Server supports the unary gRPC pattern.
- Adding PKCE to mitigate the Authorization Code Interception Attack. This is optional and can be configured on a server-wide basis via updates to the OAuth settings in the admin console.
- Setting default passwords can now be either set when installing the product or deferred until the first login via the administrative console.
- Integration Server now respects FIPS 140-3 security profile, with the ability to drop TLS 1.1 or lower through the extended setting `watt.net.jsse.server.disabledProtocols`.

- Mapping steps in flow services (within the Service Development perspective in Software AG Designer) can take advantage of our machine learning to intelligently map one structure to another. This requires a network connection to connect to Software AG's Cloud.
- Developers can utilize and take advantage of CloudStreams public APIs to enable the integration of CloudStreams with their own applications in a simple and secure manner.
- Two-way SSL support in OAuth 2.0 to access token generation flows while configuring a new or existing connection.
- Adding, deleting, and viewing certificates and monitoring certificate life cycle for various assets in webMethods Active Transfer UI. Certificates can be automatically migrated from the previous version.
- webMethods ActiveTransfer can now be configured to send emails for scenarios such as post-processing and scheduled actions, new user creation, user password changes, and manual file sharing using web clients.
- Creating Docker images for a Universal Messaging server on Linux operating systems can be done through Software AG Installer.
- Universal Messaging is now backward and forward compatible with the Universal Messaging Java client, JMS, and Resource Adapter.

API Management and Microservices

webMethods Developer Portal features a much simpler and leaner architecture. Developer Portal is a fully API-enabled, headless, and pluggable solution. However, headless does not mean that the Developer Portal is missing the user interface. Though the Developer Portal comes with a fully functional and customizable UI, the API layer offers you the possibility of building a UI of your own. Customers can use the built-in UI if they choose. The Developer Portal 10.11 is functionally equivalent to API Portal 10.7, except for the features to manage apps and download client SDK. Both these features will be implemented in upcoming versions. There is a migration path and a utility to upgrade and migrate API Portal 10.7 instances to Developer Portal 10.11.

- API Gateway now allows registering GraphQL APIs and shows the basic details of the API's query and mutation operations.
- Exposing SOAP APIs as REST APIs allows configuring the JSON response payload based on the native service original XML payload and API schema definitions.
- An enhanced API Gateway UI that provides visual clues to indicate which API endpoints are currently active for an API.
- Additional options for clustering are provided, which simplifies the deployment architecture. API Gateway administrators can now choose between existing Terracotta-based clustering and the new Ignite-based clustering.
- New API tracing mode option for API providers.
- Increased flexibility in API package and plan definitions.
- Enhanced data purging and archiving capabilities allow condition-based purge operations.
- APIs deployed to the Microgateways or APIfied microservices in AppMesh can now be activated in the API Gateway for public access.

webMethods Suite Enhancements

The webMethods Suite includes enhancements that improve functionality across multiple products.

- webMethods 10.11 ships with Azul JDK 11. Software AG delivers the JDK with its products. Software AG products are tested and supported with this shipped version of JDK.
 - Software AG Designer is now feature-compatible with Eclipse 4.19 and Azul JDK11.
 - Software AG Command Central focuses on increasing the server performance when processing many jobs. You can expect significant improvement in the server's responsiveness and better scalability when working with more SPM nodes.
 - The classic web user interface of Software AG Command Central now allows bootstrapping Platform Manager based on the registered bootstrap installers in Software AG Command Central.
 - The enhanced version of the Pre-Upgrade Analyzer now installs as an Integration Server package called WxAnalyzer and includes a simple DSP-based UI.
-

Contents

For more details about the key additions and enhancements for this release, see the product descriptions.

Release Highlights	1
Contents	4
API Engagement Platform.....	6
API Gateway.....	6
CentraSite.....	7
Documentation	8
Software AG Command Central.....	8
Software AG Designer.....	9
Software AG MashZone NextGen.....	9
Software AG Installer	9
Software AG Universal Messaging	10
Upgrade.....	12
webMethods ActiveTransfer Agent	12
webMethods ActiveTransfer Gateway.....	12
webMethods ActiveTransfer Server	12
webMethods AgileApps.....	15
webMethods API Portal.....	16
webMethods ApplinX.....	16
webMethods BPMS (Process Engine, Business Rules, My webMethods Server, Optimize, and Content Adapters)	17
webMethods Broker	18
webMethods CloudStreams	18
webMethods Database Component Configurator	19
webMethods Developer Portal	19
webMethods EntireX	20
webMethods Integration Server	20
webMethods Microgateway.....	23
webMethods Microservices Runtime	23
webMethods OneData.....	24
webMethods Service Development.....	24
webMethods Trading Networks.....	25
webMethods Unit Test Framework	25

For important updates and a list of enhancements and issues that have been addressed since the previous release of each product, see the webMethods product readme files. You can access these documents and all product documentation from the webMethods area on the [Software AG Documentation website](#).

API Engagement Platform

No enhancements in 10.11.

API Gateway

API Management

API Gateway now allows for registering GraphQL APIs. API providers can create GraphQL APIs by providing a GraphQL schema document. In this release, API Gateway shows the basic details of the APIs query and mutation operations.

API Gateway's capability to expose SOAP APIs as REST APIs is enhanced to allow configuring how JSON response payload is constructed based on the native service original XML payload and API schema definitions. API providers now have an option to decide how single entity arrays should be handled, whether the response should include the root element for SOAP operation or should the schema validations be performed.

API Gateway UI is enhanced to provide visual clues to indicate which API endpoints are currently active for an API. Appropriate action will appear if and when API Gateway, Microgateway and/or AppMesh endpoints are active for the API.

Also, API Gateway allows to additionally enable 'public' URLs for 'private' APIs proxied by standalone or sidecar Microgateways as well as AppMesh ones. In such cases, API Gateway manages the public, north-south calls to the private, east-west endpoints.

API providers now have to option to put an API in tracing mode. This mode allows them to see and understand what happened during an API call, including states before and after policy action was executed. API Tracer logs can be exported and shared with others for further analysis and forensics.

API Monetization

API product managers are getting more flexibility when working with their API package and plan definitions. API Gateway now allows for editing them even if they are active and used by subscribers. Both plan and package definitions can be edited. Subscribers will not be impacted unless the edits concern quota or rate limit definitions, or APIs are added or removed.

Plan and package definitions can now include custom data in the 'additional information' section. This could be used to share more information with subscribers or if more information is needed when integrating with external billing solutions.

Additionally, API Gateway can send current subscriber's usage to a custom destination.

Active subscribers can now change their plans or switch to different packages. API Gateway allows API product managers to configure approval workflows for such events.

The public API layer is enhanced to provide an API to create and manage subscriptions.

API Access Control

When API Gateway acts as the authorization server in OAuth 2.0 flow, it can now enforce PKCE (Proof Key for Code Exchange) to secure public clients using authorization code grant.

Architecture and Operations

From this release, API Gateway provides an additional option for clustering, which simplifies the deployment architecture. API Gateway administrators can now choose between existing Terracotta-based clustering and the new Ignite-based clustering. The Ignite-based clustering does not require additional runtime as all the necessary modules are bundled within the API Gateway.

Administrators can now change the default Administrator user's password during the installation and enforce user password change during the first login.

Single sign-on configuration is enhanced and simplified. Now, it guides the administrator through few screens to provide all the necessary information clearly and concisely. Also, this functionality allows user and group attribute mapping between the SSO provider and the API Gateway.

API Gateway capabilities around data purging and archiving are enhanced to allow condition-based purge operations. The API Gateway UX is improved, and UI now shows detailed job status information for purge and archive actions.

Backup and restore actions now allow index selection and configuration of log level and log file location. Now, it is also possible to monitor backup and restore activities in progress.

API Gateway now exposes a public API to manage server ports.

CentraSite

CentraSite Business User Interface Enhancements

CentraSite Business User Interface (BUI) is enhanced with the following functionalities:

- View and export asset types
- Deployment History screen
- User Deactivation screen
- Policy Log screen
- Audit Logs screen
- LCM Purge
- Approval Logs screen
- Taxonomies export screen
- Supporting documents screen

Control UI is removed.

Documentation

Significant changes to product documentation sets or to individual documents are described in the readmes for each product.

Product documentation is public

- The product documentation is publicly available at <https://documentation.softwareag.com>. A login to Empower is no longer required.

Version picker on the documentation website

- On the documentation website at <https://documentation.softwareag.com>, it is now possible to select a specific document version via a pull-down menu. The latest version is always preselected as the default.
- If the documentation is available in languages other than English, it can also be selected directly from that menu.

Software AG Command Central

Java 11 adoption

Command Central now ships with Azul JDK 11.

Use case-based documentation

With 10.11 we introduce new documentation that goes through common use cases instead of hovering over technical details and tasks.

Server performance enhancements

The 10.11 release of Command Central focuses on increasing the server performance when processing many jobs. You can expect significant improvement in the server's responsiveness and better scalability when working with more SPM nodes. To leverage those benefits, you will need to migrate to the 10.11 version of the Command Central server.

Reworked SPM bootstrap in the Command Central classic web user interface

The classic web user interface of Command Central now allows bootstrapping Platform Manager only based on the registered bootstrap installers in Command Central. The option to auto-generate the bootstrap installer is now removed after it was deprecated for several releases.

Custom administrator user passwords

Command Central provides a new ADMINSTRATOR credentials alias for setting custom administrator user passwords when installing version 10.11 of Software AG products, including Command Central and Platform Manager.

Software AG Designer

Designer upgraded to Eclipse 4.19 and Java Azul 11

Designer is now feature-compatible with Eclipse 4.19 and Java 11.0. Java 11 is a major upgrade from Java 8 and removes many deprecated libraries. Check your code for compatibility.

- https://www.eclipse.org/eclipse/development/readme_eclipse_4.19.php
 - <https://www.oracle.com/java/technologies/javase/11all-relnotes.html>
-

Software AG MashZone NextGen

No new features in this release.

Software AG Installer

Enhanced Container Creation Using Command Line Interface

Software AG Installer 10.11 offers a new command line interface that enables you to create container images more easily for these products:

- Microservices Runtime
- Products that run on top of Microservices Runtime
- My webMethods Server
- Universal Messaging

The new command line interface does not require on-premise installations and does not expect any recorded input, only a list of arguments that can trigger image creation.

For more information and examples, see the Software AG Installer 10.11 documentation.

Software AG Universal Messaging

Java 11 adoption

Universal Messaging now ships with Azul JDK 11. Refer to the Java release notes to check for compatibility with any custom Java libraries or code that you have developed.

Changes in Java 11 can be found at <http://openjdk.java.net/projects/jdk/11/>.

Support for creating Docker images for Universal Messaging using Software AG Installer

You can use Software AG Installer to create Docker images for a Universal Messaging server on Linux operating systems. The Installer client creates a Docker image with a Universal Messaging server entry point and support for command-line tools similar to the images provided in the Software AG repository on Docker Hub. For a detailed description of this feature with usage examples, see the documentation about creating Docker images with Software AG Installer on Linux in the Using Software AG Installer guide.

Support for exporting Protobuf definitions from a store

You can export Protobuf definitions from a Universal Messaging store in the following ways:

- Using a new command-line tool named `ExportProtobufDefinitions`.
- Using the Enterprise Manager. A new option, `Export Protobuf Definitions`, has been added to the context menu for a store.

Server support for TLS 1.3

For more information about configuring SSL/TLS in Universal Messaging, see the section “Server SSL Configuration” in the Universal Messaging Concepts guide.

Support for JAAS authentication using HTTP headers

You can configure Universal Messaging to use custom HTTP headers from the client HTTP connection request for JAAS authentication. To enable JAAS authentication using HTTP headers, you configure a new system property, `com.softwareag.um.server.authentication.http.extraHeaders`.

For more information about JAAS authentication with HTTP headers, see the section “Configuring JAAS Authentication with HTTP Headers” in the Universal Messaging Concepts guide.

Support for authentication when clients do not provide a password

You can use JAAS authentication with HTTP headers to authenticate clients that did not provide a password. To enable authentication without a password, you configure a new system property, `com.softwareag.um.server.authentication.simpleAuthenticationEnabled`.

For more information about authenticating clients that did not provide a password, see the section “Enabling Authentication Without a Password” in the Universal Messaging Concepts guide.

Support for client SSL certificates in PKCS12 format

Bi-directional client compatibility

Universal Messaging is backwards and forwards compatible with the Universal Messaging Java client, JMS, and Resource Adapter. In addition to clients connecting to the same or higher-release servers, Universal Messaging enables Java client's version 10.7 and higher to connect to lower-release servers. The feature was introduced in Universal Messaging 10.7.

For more information about the functionality and compatible client and server versions, see the section "Bi-directional Client and Server Compatibility" in the Universal Messaging Concepts guide.

New release identifiers

You can use the following objects and APIs on the Java client, which were added in version 10.7, to identify the release version of the components that are in use in your landscape:

- `com.pcbssys.nirvana.client.ReleaseDetails` - object that provides release and URL details.
- `com.pcbssys.nirvana.client.ReleasIdentifier` - object that provides a list of release identifiers.
- `com.pcbssys.nirvana.client.nSession` APIs:
 - `getClientReleasIdentifier()` - returns the current client release.
 - `getServerReleasIdentifier()` - returns the current server release or, in case of a horizontal scalability (HS) connection, the release versions of the HS servers.
 - `getConnectionProtocol()` - returns the negotiated release between the server and client components.

For more details, see the Universal Messaging Java Client API documentation.

Horizontal scalability (HS) behaves consistently in mixed environments

Now that Universal Messaging is backwards and forwards compatible with Java clients, for consistency in a mixed server environment, you must restrict the HS URL of your application to use the lowest server release version available in the HS landscape. For the purpose, you can use a new parameter, `hsReleaseVersion`, as part of the HS URL. This functionality has been delivered with Universal Messaging 10.7 Fix 1.

For more information about the functionality and about configuring the `hsReleaseVersion` parameter, see the section "Horizontal Scalability Behavior in a Mixed Landscape" in the Universal Messaging Concepts guide.

A new command-line tool, `ServerReleaseVersion`, that generates HS URLs containing the `hsReleaseVersion` parameter

You can use the `ServerReleaseVersion` tool to obtain the release versions for a list of Universal Messaging servers or for servers that are part of a Horizontal Scalability (HS) URL. For HS servers, the tool generates an HS URL that contains the `hsReleaseVersion` parameter.

For more information about using the tool, see the section "The `ServerReleaseVersion` Tool" in the Universal Messaging Administration Guide.

Support for NHP, NHPS interfaces with AMQP, MQTT protocols

Universal Messaging can use the NHP and NHPS interfaces to communicate with MQTT and AMQP protocol clients. This makes configuring Universal Messaging easier because the NHP and NHPS interfaces can support all protocols of the server on a single interface.

Upgrade

Enhanced Pre-Upgrade Analyzer

- The latest version of the Pre-Upgrade Analyzer now installs as an Integration Server package called WxAnalyzer and includes a simple DSP-based UI.

It continues to produce these reports from previous releases:

- Custom Services Using Deprecated, Removed, or Changed Built-in Services
 - Custom Services Using Built-in Debug Services
 - Custom Packages Using Non-Existent Services or Documents
 - Custom Assets Not Being Used in Integrations
- In the 10.11 release, it uses Integration Server built-in services to produce these new reports:
 - Custom Adapter Assets for All Installed Adapters
 - Custom Adapter Assets for <adapter name>
 - Custom Assets that Depend on <package name>
 - The Pre-Upgrade Analyzer is available on Software AG TechCommunity.
-

webMethods ActiveTransfer Agent

No new features in this release.

webMethods ActiveTransfer Gateway

No new features in this release.

webMethods ActiveTransfer Server

Deprecation warning

ActiveTransfer Server version 10.11 is the final version that will support the ActiveTransfer User Interface in My webMethods. Subsequent releases of ActiveTransfer Server will only support the ActiveTransfer User Interface through the dedicated ActiveTransfer Server User Interface.

New Features

Certificate Management

ActiveTransfer UI supports adding, deleting, and viewing certificates. You can also monitor the certificate life cycle for various assets. Certificates can be automatically migrated from the previous version.

Email Configuration

ActiveTransfer can be configured to send emails for the following scenarios:

- Post-processing and scheduled actions
- New user creation
- User password changes
- Manual file sharing using web clients

Single Sign-On (SSO)

ActiveTransfer now supports logging in with Single Sign-On (SSO).

Added Services

- `wm.mft.admin:updateAssetsWithCertAlias`

This new service will migrate the certificates to Certificate Management without user inputs.

- `wm.mft.admin:updateCertFromDBToFile`

This new service will move old certificates from File to database during the migration to File-based certificates.

- `wm.mft.admin:updateFileBasedCertToDB`

This new service will move File-based certificates to the database without user inputs.

- `wm.mft.assets.certificate:add`

Use this service to add a new certificate. The following user inputs are supported in this service:

- `mftCertificate/certificateId` – Automatically generates the certificate ID.
- `mftCertificate/certificateAlias` – The name given to the certificate as a string datatype.
- `mftCertificate/description` – The description given to the certificate as a string datatype.
- `mftCertificate/location` – Select the location from the dropdown for the Database/File.
- `mftCertificate/path` – The path of the certificate used as a string datatype.
- `mftCertificate/type` – The type of certificate selected in the dropdown.
- `mftCertificate/keyPassword` - The password given for the certificate key.

- mftCertificate/keyStorePassword – The password given for the certificate keystore.
- wm.mft.assets.certificate:delete

The following user inputs are supported in this service:

- certificateId – You must provide the certificate ID as a string datatype to delete the certificate.
- wm.mft.assets.certificate:list

The following user inputs are supported in this service:

Choose the certificate from the dropdown.

- wm.mft.assets.certificate:update

Use this service to update the existing certificates. The following user inputs are supported in this service:

- mftCertificate/certificateId – Automatically generates the certificate ID.
- mftCertificate/certificateAlias - The name given to the certificate as a string datatype.
- mftCertificate/description - The description given to the certificate as a string datatype.
- mftCertificate/location - Select the location from the dropdown for the Database/File.
- mftCertificate/path - The path of the certificate used as a string datatype.
- mftCertificate/type - The type of certificate selected in the dropdown.
- mftCertificate/keyPassword - The password given for the certificate key.
- mftCertificate/keyStorePassword - The password given for the certificate keystore.
- wm.mft.assets.certificate:usages

This new service displays the certificates used. The following inputs are supported:

- certificateId – You must provide the certificate ID as a string datatype to view the certificate usage.
- wm.mft.assets.certificate:view

This new service is used to view the certificates. The following inputs are supported:

- certificateId – You must provide the certificate ID as a string datatype to view the certificate usage.
- certificateAlias – You must provide the certificate alias as a string datatype to view the certificate

Changed Services

- wm.mft.assets.rec.event.action.properties:EncryptFile

The following parameter is added to this service:

- publicPGPCertificateId: String datatype, requires certificateid as input.
- wm.mft.assets.rec.event.action.properties:DecryptFile

The following parameter is added to this service:

- publicPGPCertificateId: String datatype, requires certificateid as input.
- wm.mft.assets.rec.port:FTPDetails

The following parameters are added to this service:

- ftpsDetails/keystoreCertificateId: String datatype, requires certificateid as input.
- httpsDetails/truststoreCertificateId: String datatype, requires certificateid as input.
- wm.mft.assets.rec.port:HTTPDetails

The following parameters are added to this service:

- httpsDetails/keystoreCertificateId: String datatype, requires certificateid as input.
- httpsDetails/truststoreCertificateId: String datatype, requires certificateid as input.
- wm.mft.assets.rec.vfs:VfsDetails

The following parameters are added to this service:

- Encryption/PublicPGPCertificateId: String datatype, requires certificateid as input.
- Encryption/PrivatePGPCertificateId: String datatype, requires certificateid as input
- wm.mft.assets.rec.user:UserDetails

The following parameters are added to this service:

- fileBasedEncryptionDecryption/privatePGPKeyCertificateId: String datatype, requires certificateid as input.
- fileBasedEncryptionDecryption/publicPGPKeyCertificateId: String datatype, requires certificateid as input.

webMethods AgileApps

AgileApps User Directory sync with ActiveDirectory through SSO

User details like firstname, lastname, email address, and team information from any ActiveDirectory can now be synced with User Management in AgileApps.

Header sorting for subforms and related information section

AgileApps new runtime user interface now supports dynamic sorting in the Related information section and subforms. This functionality provides you with a means of header based sorting on table column headers.

Pagination for new Runtime User Interface

AgileApps new runtime user interface now allows page size control and the ability to go to a specific page in a table.

Case Analytics

AgileApps new runtime user interface now supports Case Analytics dashboard for the servicedesk application.

Support for Secure LDAP

In light of the enhanced security awareness globally, AgileApps now supports Secure LDAP.

Application-wise support for export by Translation WorkBench

AgileApps Translation WorkBench (TWB) now supports export of application labels by application, instead of exporting all applications by default.

Additional language support

AgileApps now supports 35 additional languages only for the new runtime user interface, which can be acquired by the customer by paying a small license fee for the required language. The additional languages now include Arabic and Hebrew as well, and the RTL orientation for these languages is also on the way.

webMethods API Portal

There is no 10.11 version of the API Portal. In 10.11, the product is released as Developer Portal.

webMethods ApplinX

REST API Enhancement

You can now generate a page in Angular, and also execute a procedure (stateless or stateful) using the ApplinX REST APIs.

Security Enhancement

Improvements to the existing hotfix script mean you can now update or replace a JAR file, making it easier to address security vulnerabilities.

Japanese Composition Mode

Japanese composition mode is now supported.

webMethods BPMS (Process Engine, Business Rules, My webMethods Server, Optimize, and Content Adapters)

All BPMS components now support Java 11 at runtime.

All BPMS components now support supplying a new password for their default administrator users during installation.

Docker support

BPM and Integration Server assets can be deployed to a Docker image/container.

- Process Engine can enable for execution assets that you deploy to an image/container using the docker copy command.

Business Rules Enhancements

- A low-code graphical function editor is now available in the Business Rules user interface in My webMethods.
- Rules Engine now supports MySQL 8.x.

Optimize Enhancements

- Optimize for Process now supports MySQL 8.x.

My webMethods Server now supports the RelayState parameter for SP Initiated Single Sign-on (SSO)

- Optimize for Process now supports MySQL 8.x.

Creating My webMethods Server container images with Software AG Installer

- Optimize for Process now supports MySQL 8.x

Improved startup time for My webMethods Server containers

- My webMethods Server containers are now optimized to initialize about 20% faster.
 - My webMethods Server containers are now optimized to start up (after successful initialization) about 50% faster.
-

webMethods Broker

Java 11 adoption

webMethods Broker now ships with Azul JDK 11. Refer to the Java Release Notes to check for compatibility with any custom Java libraries or code that you have developed.

The changes in Java 11 can be found at <http://openjdk.java.net/projects/jdk/11/>.

webMethods CloudStreams

CloudStreams public APIs

Developers can utilize and take advantage of CloudStreams public APIs to enable integration of CloudStreams with their own applications, in a simple and secure manner.

Connection status for CloudStreams connectors

Introduction of a new connection runtime status: `suspended`. This status indicates a connection that is either waiting to be initialized, or not having a valid token due to a failure in the most recent refresh cycle. This status is displayed in the status column of the Connections List page.

Update connectors using an updated OpenAPI/Swagger definition

You can now update a connector which was created using an OpenAPI/Swagger specification by providing an updated OpenAPI/Swagger specification file.

Two-way SSL support in OAuth 2.0 access token generation flows

In the generate access token flows while configuring a new or existing connection, you can now choose SSL connector to support two-way SSL where required.

Lazy asset loading

When restarting the Integration Server or while reloading a custom package containing a CloudStreams connection, you can defer the initialization of the connection assets till first usage rather than on restart/reload.

Configure circular redirection of a connection

You can now control (and disable) circular redirection of a connection.

webMethods Database Component Configurator

No user-facing changes in this release.

webMethods Developer Portal

webMethods Developer Portal is the next-generation version of Software AG's current API Portal.

The new Developer Portal features a much simpler and leaner architecture. Developer Portal is a fully API-enabled, headless, and pluggable solution. However, headless doesn't mean that the Developer Portal is missing the user interface. Though the Developer Portal comes with a fully functional and customizable UI, the API layer offers you the possibility of building a UI of your own. Customers are also welcome to use the built-in UI if they choose.

The Developer Portal 10.11 is functionally equivalent to API Portal 10.7, except for the following:

- Managing Apps
- Downloading client SDK

Both these features will be implemented in upcoming versions.

Other advantages that Developer Portal offers over API Portal are:

- Simplified and lean architecture that is easier to run and requires fewer resources.
- Fully API-enabled; that is, APIs to accomplish all tasks (including Sign-in).
- Headless, pluggable, and extensible nature. Thanks to the fact that there's an API for everything, customers will be able to use the Developer Portal without the UI we ship (and build their own) or build additional UI for a different type of asset (For example, events or workflows).
- Simpler and richer UI customization capabilities.
- Event-enabled nature of the product; events generated for each action can be notified to external endpoints.

There is a migration path and a utility to upgrade and migrate API Portal 10.7 instances to Developer Portal 10.11. Two types of assets that cannot be migrated are:

- Collaboration data (For example, discussion forum data)
- User interface customization. UI customization will have to be re-done manually in the new Developer Portal.

The Developer Portal is compatible with all the products that API Portal works with, for example, API Gateway, CentraSite, and Designer.

10.7 is the last version of the API Portal. Starting 10.11, we will be developing the new Developer Portal. No further updates will be made to API Portal; and it will be maintained and supported according to the Software AG standard maintenance policy.

webMethods EntireX

Security Enhancements

- **Default Password Handling**
For greater security, default password handling has been enhanced for Software AG products that are installed with the SAG Installer. On the Administrator Password panel, enter a default product administrator password for the products you are installing, and choose whether to require the password to be changed on first product login.
- **PassTicket Support**
PassTickets are now supported for connections to CICS ECI and IMS Connect with the EntireX Adapter and the respective RPC servers.
- **Encrypted Password for ETBINFO and ETBCMD**
Security for command-line utilities ETBINFO and ETBCMD under UNIX and Windows has been enhanced. Instead of specifying a cleartext password when you call a secure broker, you can now encrypt a password and store this in a file.
- **Encrypted Password for EntireX Monitoring Scripts**
Password encryption is also available for EntireX monitoring scripts

Command Central Enhancements

- **Administrating EntireX Mainframe Broker Monitoring**
You can now administer EntireX Mainframe Broker Monitoring in Command Central. You can enable and disable the monitoring of the real mainframe broker (z/OS and BS2000) from within Command Central running under UNIX or Windows. This feature is particularly useful for major configuration changes in the mainframe environment, for example changing the user password.
- **User Transaction ID field for CICS Socket Listener**
User Transaction ID has been added as an additional field for CICS Socket Listener.
- **Location of EntireX Broker Trace File**
You can now change the directory of the EntireX Broker trace file.

webMethods Integration Server

Java 11 adoption

Integration Server now ships with Azul JDK 11. Refer to the Java release notes to check for compatibility with any custom java libraries or code that you have developed.

Changes in Java 11 can be found at <http://openjdk.java.net/projects/jdk/11/>.

Admin console now defaults to new version

In the 10.7 release, a new admin console was introduced alongside the existing Integration Server Administrator and could be accessed by either clicking on the "Try" button or explicitly by

adding “/WmAdmin” to the end of the URL path. As of 10.11 accessing the server with an empty URL path (e.g., https://server:port/) will show the new console by default.

Open API 3.0 Consumer support

The 10.7 release introduced Open API 3.0 providers. In this release you can now import an Open API 3.0 definition to generate services, allowing you to call an external API from your services.

gRPC provider support

Developers can now expose services for use with clients using the gRPC protocol. This requires that developers first provide a .proto file from which they can generate the necessary document types and service stubs. Integration Server supports the unary gRPC pattern.

Quiesce mode enhanced for improved “warm standby”

Quiesce mode introduces new options to allow the administrator to disable all auditing and system tasks that may write to a shared database. This ensures that the server can be up and running without activity, until required.

JWT support enhancements

New services in WmPublic package to allow developers to create JWT tokens, verify them and extract claims from existing tokens.

- pub.jwt:generateSignedJWT
- pub.jwt:verifyJWT
- pub.jwt:extractClaimsFromJWT

New encrypt/decrypt services

New services in WmPublic package to allow developers to easily encrypt/decrypt text as well as sign/verify arbitrary text, using the PGP library.

- pub.security:sign
- pub.security:encrypt
- pub.security:signAndEncrypt
- pub.security:decrypt
- pub.security:decryptAndVerify
- pub.security:verify

PKCE support added for OAuth 2.0

PKCE was added to mitigate the Authorization Code Interception Attack. This is optional and can be configured on a server-wide basis, via updates to the OAuth settings in the admin console.

LDAP updated to support 3.0

Native LDAP support in Integration Server has been upgraded to support version 3.0.

FIPS 140-3 adoption

Integration Server now respects FIPS 140-3 security profile, with the ability to drop TLS 1.1 or lower through the extended setting `watt.net.jsse.server.disabledProtocols`.

Default passwords forced update

Default passwords can now be either set when installing the product or deferred until first login via the administrative console.

Improved HTTP logging

Administrators can activate a log file to trace http requests/responses via the extended setting `watt.server.httplog`. The http log format can be the standardized Common Log Format or Combined Log Format or can be the legacy format.

Administrative API Patch Behavior improvements

The Admin API now supports the `application/merge-patch+json` media type for PATCH operations.

Path-based routing support in administration console

Path-based routing from products such as NGINX and Kubernetes ingresses can now be mapped to the new administration console at `/WmAdmin`.

Deprecated WmMobileSupport package

This package has now been marked as deprecated and will be removed at some time in future.

Metering improvements

Metered customers will now be informed of connectivity issues directly from the admin console either via an alert or banner.

Event lifecycle logging

Detailed event life cycle logging for Universal Messaging events can now be configured from the administration console in the logging section, without requiring the server to be restarted.

The diagnostic data utility can now include custom log file

Layered products, such as ActiveTransfer, can now have their log files included in the zip file generated by the diagnostic utility (`wm.server.admin:getDiagnosticData`). This must be set up by the layered product.

New Administrative APIs

Integration Server 10.11 includes the following new Administrator APIs to allow remote management of your server:

- SAML

- Outbound Passwords
 - ACLs
 - FTP/FTPS ports
 - URL aliases
 - Threat protection/Enterprise Gateway Rules
 - OAuth global settings, tokens, clients, scopes, and external servers
-

webMethods Microgateway

Microgateway and AppMesh

APIs deployed to the Microgateways or APIfied microservices in AppMesh can now be activated in the API Gateway for public access.

- Users can assign an API Gateway endpoint to the APIs deployed to the Microgateways or the APIfied AppMesh microservices.
 - The APIs page in API Gateway indicates which endpoints of the APIs are active:
 - APIs deployed to the API Gateway
 - APIs deployed to the Microgateways
 - APIfied Microservices
 - A combination of those
 - The API details page in the API Gateway lists the active endpoint URLs.
-

webMethods Microservices Runtime

Optional Web Services Stack

You can create a Docker image of a Microservices Runtime without the web services functionality. This is useful for deploying microservices where no SOAP processor is required as it results in 50MB reduction in image size and 2-3 seconds improvement in startup time.

Optional gRPC Stack

You can install Microservices Runtime without gRPC, which is useful for deploying microservices where no gRPC services are required.

K8s secrets can be used via environment variables

Passwords can now be externalized to your cloud vault via environment variables, e.g.,
`truststore.DEFAULT_IS_TRUSTSTORE.ksPassword=$secret{securepwd}`.

Health metrics improved for Prometheus

Extended metrics to allow richer monitoring from tools such as Prometheus and allow layered products that run on top of Microservices Runtime to include additional information.

webMethods OneData

Enhancements In Manage Data and Workflow Module

- Capability to navigate through a large number of records in the foreign key reference popup screens in Manage Data module.
- Capability to control the visibility of columns in the Update Bulk screen in Manage Data module.
- Capability to differentiate between the pending approvals in the workflow module appearing in the inbox of the approver for the first time from the pending approvals appearing after the rejection from the next level.

Enhancements In Data Quality Module

The Locate library is upgraded to the latest version, thereby providing improved address cleansing capabilities resulting in better matching results in the Data Quality module.

webMethods Service Development

Designer upgraded to Eclipse 4.19 & Java Azul 11

Designer is now feature-compatible with Eclipse 4.19 and Java 11.0. Java 11 is a major upgrade from Java 8 and removes many deprecated libraries. Check your code for compatibility.

- https://www.eclipse.org/eclipse/development/readme_eclipse_4.19.php
- <https://www.oracle.com/java/technologies/javase/11all-relnotes.html>

Smart Mapping Introduced in Designer

Map steps in flow services can now take advantage of our machine learning to intelligently map one structure to another. Requires a network connection to connect to Software AG's cloud.

Open API 3.0 Consumer Creation

Developers can now import an Open API 3.x definition to create the necessary document types and services to invoke the API without coding.

gRPC Providers

Developers can now take advantage of Integration Server's new gRPC stack easily; by importing a gRPC .proto file to generate the necessary document types and service stubs, to accept inbound gRPC requests from clients over HTTP/2.

Support for BigDecimal/BigInteger

Introduced support for using BigDecimal and BigInteger Java types in document types and flow services.

UDDI Support removed

CentraSite has dropped UDDI v2/v3 support. Hence, UDDI is now removed from Designer Service Development.

Default password handling

The Software AG Installer now allows the user to change the Integration Server Administrator's password during installation or at first login. Hence, Designer does not set the default password in the default server definition and does not connect automatically to Integration Server. Now, you must set the password in the server definition and connect manually.

webMethods Trading Networks

Test partner connections

You can test connections for a trading partner to ensure it is working.

MySQL 8.0 Community Edition support

You can configure MySQL Community Edition 8.0 with Trading Networks Server 10.11.

webMethods Unit Test Framework

Unit Test Framework supports Eclipse 4.19 & Java Azul 11

Unit Test Framework is now feature-compatible with Eclipse 4.19 and Java 11.0. Java 11 is a major upgrade from Java 8 and removes many deprecated libraries. Check your code for compatibility.

- https://www.eclipse.org/eclipse/development/readme_eclipse_4.19.php
- <https://www.oracle.com/java/technologies/javase/11all-relnotes.html>

Copyright © 2021 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to “License Texts, Copyright Notices and Disclaimers of Third Party Products”. For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under “License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products”. These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

WEBM-RN-1011-20211015