webMethods Mediator 10.1 Readme

October 2017

webMethods Mediator will reach its end-of-life in October 2017. In the coming years, implementations need to be migrated to use API Gateway instead. Software AG has invested significantly in ensuring maximum compatibility and making this migration as smooth as possible.

This file contains important information you must read before using webMethods Mediator 10.1. You can find system requirements, user documentation, and installation and upgrade instructions on the Documentation website or the TECHcommunity website. At those locations, you can also find the suite-related security and globalization information.

Included in this file is information about functionality that has been added, removed, deprecated, or changed for this product. Deprecated functionality continues to work and is supported by Software AG, but may be removed in a future release. Software AG recommends against using deprecated functionality in new projects.

1.0 Critical Information **2**

2.0 Known Issues **2**

3.0 Usage Notes **3**

4.0 Fixes Included in Each Release **3**

5.0 Other Resolved Issues **4**

6.0 Documentation Changes **13**

7.0 Terminology Changes **13**

8.0 Added, Removed, Deprecated, or Changed Items **14**

9.0 Added, Removed, Deprecated, or Changed Built-In Services **21**

10.0 Added, Removed, Deprecated, or Changed APIs **21**

11.0 Copyright Information **22**

12.0 Support **22**

1.0 Critical Information

This section lists any critical issues for the current release that were known when this readme was published. For critical information found later, go to the Knowledge Center on the Empower website.

2.0 Known Issues

This section lists any issues for the current release that were known when this readme was published. For known issues found later, go to the Knowledge Center on the Empower website.

- SMGME-6167
  GET to POST transformation does not remove query parameters.
  When an incoming GET request is transformed into a POST request, the query parameters have to be transformed into the body payload. The query parameters must not be added to the POST request.
  There is currently no workaround for this issue.

- SMGME-6672
  Exception occurs while getting an OAuth token after republishing an API from CentraSite.
  When you bulk publish APIs with OAuth clients, all clients are not published to Mediator and get access token fails for missing consumers.
  The workaround for this issue is to publish APIs individually.

- SMGME-6693
  Invoking a SOAP service as REST fails to respond in error scenarios.
  When a REST enabled SOAP service is invoked and failed, the exception in the response payload in case of JSON payload is incorrect. The expected exception is not sent to the client.
  There is currently no workaround for this issue.

3.0 Usage Notes

This section provides any additional information you need to work with the current release of this product.

webMethods Mediator package in Integration Server, cannot co-exist with the WmAPIGateway or WmCloudStreams packages. WmAPIGateway and WmCloudStreams packages must be disabled for Mediator to function properly.

4.0 Fixes Included in Each Release

This section lists the latest fix level that has been included in each release for each product component. A release is listed in this section only if changes occurred in that release. Go to the Knowledge Center on the Empower website for detailed information about fixes.

Release 10.0

- XB_10.0_Fix3

Release 9.12

- XB_9.12_Fix8

Release 9.10

- XB_9.10_Fix9

Release 9.9

- XB_9.9_Fix15

Release 9.8

- XB_9.8_Fix15

Release 9.7

- XB_9.7_Fix17

5.0 Other Resolved Issues

This section lists the issues that were resolved in each release but were not part of the fixes listed in the previous section. A release is listed in this section only if changes occurred in that release.

Release 9.12

- SMGME-5242
  Password type input with auto-complete enabled.
  An attacker with local access could obtain the cleartext password from the browser cache. The password auto-complete must be disabled in sensitive applications.
  This issue is resolved.

Release 9.10

- SMGME-4814
  Unable to retrieve images that are available on the internal server through virtual services.
  When a Custom Content type of type Binary is defined in Mediator for requests from the client and responses from the native service with the above Content type, Mediator modifies the Content type header to application/octet-stream. Due to this, the custom content type defined by the provider is masked.
  This issue is resolved.

- SMGME-4788
  Allow Anonymous Access Action does not work.
  Virtual service configured with policy Allow Anonymous access set to False, should not be available for anonymous users. Irrespective of the policy configuration, anonymous users are allowed to access virtual services.
  This issue is resolved.

- SMGME-4611
  Mediator returns an empty response when Version 1 certificate is used for Signature.
  Mediator sends empty response to client when a request signed with version 1 certificate is passed. Error message, version 3 certificate has to be used for signature, should be sent to client instead of empty response.
  This issue is resolved.

- SMGME-4367
  Set Media Type policy action not working for Request after Versioning.
  Set Media Type policy action is enforced on a virtual service request. Once the virtual service is versioned, the policy action enforcement is not done.
  This issue is resolved.

- SMGME-4366
  Unpublish of alias fails when associated to virtual service.

Associate alias to 2 virtual services. Publish and unpublish one of the virtual services. Alias which is published during virtual service publish cannot be unpublished even none of the associated virtual services are in deployed state.
This issue is resolved.

- SMGME-4361
  Mediator returns status code 500 on breaching throttling hard limit.
  On breaching the throttling hard limit, Mediator is expected to send a status code of 503 but instead status code 500 and response code 503 are sent.
  This issue is resolved.

Release 9.9

- SMGME-3157 (PIE-33557)
  Integration Server error occurs when you try to delete an OAuth2 access token if Mediator is in clustered mode.
  When you try to delete an OAuth2 access token of a virtual alias in any one of the Mediator nodes that are in Integration Server cluster mode, you are not allowed to delete the OAuth2 access token. Due to this, an error is logged in the Integration Server log.
  This issue is resolved.

- SMGME-4256
  The "com.ctc.wstx.exc.WstxParsingException: Undeclared namespace prefix "wsse"" exception is displayed in the ESB service. This service is configured to add a SAML Sender Voucher in the outbound call to the native service. The exception occurs after Mediator receives the SAML Assertion from STS.
  A WS security policy is added by the Client to the incoming SOAP request to Mediator virtual service. If this virtual service is also configured with an ESB service to add a SAML Sender Voucher to the Client request, then Mediator 'OnBehalf' of the client requests a Token from the STS that is configured. After receiving the response from STS, the following exception is displayed: "com.ctc.wstx.exc.WstxParsingException: Undeclared namespace prefix "wsse""
  This issue is resolved.

- SMGME-4251
  The following fields in the Edit Security Token Service (STS) Configuration screen in Mediator (Mediator > STS > Add new STS configuration screen) do not accept the "@", "\", "/", "-", and "_" characters on performing a client side validation:
  1) Endpoint field of the Configuration section
  2) Username field of the HTTP Basic Authentication
  3) Username field of the WS-Security Username Token section
  This issue is resolved. The "@", "\", "/", "-", and "_" characters are removed from the validation and are accepted in the fields mentioned above.

- SMGME-4189
  The "Unable to find Bean named:aliasServiceAssociationManager" error is displayed when Mediator package is shutdown.
  The "aliasServiceAssociationManager" bean is shutdown before shutting down the "PGConfiguration" bean. Due to this, the "Unable to find Bean named:aliasServiceAssociationManager" error is displayed when Mediator package is shutdown.
  This issue is resolved.
  The dependency of the "aliasServiceAssociationManager" bean has been added to the "PGConfiguration" bean.

- SMGME-4157
  An error is displayed by Mediator when an invocation with Custom content type having a semicolon (;) occurs.
  Mediator considers the content after a semicolon (;) as a character set or a boundary information and removes them. Due to this, an error is displayed by Mediator when an invocation with Custom content type having a semicolon (;) occurs.
  This issue is resolved.
  Custom content types can have multiple parts separated by ';'.
  Note: This is applicable only for the Custom content types and not the Standard content types.

- SMGME-4068
  "Unable to convert the json to xml" error is displayed by Mediator when a "$" value is available in the json data of the request sent to Mediator.
  This issue is resolved.

- SMGME-4063
  Mediator removes the security header from the SOAP request when sent to a native service. When the security policy is not applied, the endpoint properties are configured with "Remove processed security headers" option, and the mustUnderstand attribute in the SOAP request security headers is set to 1, Mediator removes the security header from the SOAP request sent to a native service.
  This issue is resolved. Mediator does not remove the security header from the SOAP request sent to a native service even when the security policy is not applied, the endpoint properties are configured with "Remove processed security headers" option, and the mustUnderstand attribute in the SOAP request security headers is set to 1.

- SMGME-4053
  When a "GET" request is sent from a Client to Mediator with the accept header value set to */* and when a response is sent to Mediator from native service with no Content-Type Header defined, an error message is sent in the response from Mediator to the Client.
  This issue is resolved. If the Content-Type Header value is missing in the native service response sent to Mediator, Mediator sends the response to the Client with "application/xml" Content-Type which is the default Content-Type for GET method.

- SMGME-4036
  In case of an invalid API Key, The API Key and the Authorization Header values are not removed in a service invocation response message.

When a virtual service asset is configured for API key authentication, Mediator does not remove the values for API Key and Authorization Header fields in the service invocation response message before sending to the Client. This occurs only if an invalid API key or an expired API key, is specified for invoking the asset.
This issue is resolved. The API Key and the Authorization Header values are now removed from the service invocation response message if the API key is invalid.

- SMGME-4005
  When migrating from earlier versions of webMethods Mediator, Error Messaging step of a virtual service does not work as expected.
  After migrating webMethods Mediator from previous versions to version 9.7, if the Error Messaging Step of a virtual service contains both the Pre-Processing and Post-Processing steps configured with webMethods IS Service, Mediator returns SOAP request content as EnvelopeString to the IS Service instead of the expected fault response.
  This issue is resolved. In the above scenario, Mediator now returns only the fault response in Post-Processing.

- SMGME-3996
  The data displayed in the MED_EVENT_TXN.log file contains large number of trailing whitespaces.
  When a Log Invocation run-time policy action is used with or without logging the request or response payloads, the data displayed in the MED_EVENT_TXN. log file generated by Mediator 9.7 version contains large number of unwanted trailing whitespaces as compared to the data displayed in the MED_EVENT_TXN.log file generated by Mediator 9.5 version. This is due to the new attribute, native service endpoint URL introduced in Mediator 9.7 version.
  This issue is resolved. The additional whitespaces are now removed from the data displayed in the MED_EVENT_TXN.log file generated by Mediator 9.7 version.

- SMGME-3960
  Mediator does not allow you to change the HTTPS URL of the load balancer after you migrate the Mediator assets from a previous version to 9.7, using the migration tool. After migrating to Mediator 9.7, if you try to modify the port or URL settings in the Mediator Administration page when no HTTPS port is available for selection, the following error is displayed:
  For input string: "".
  The server.log file shows the following entry:
  [MED.0010.0066E] Error while persisting properties to file
  pg-config.prop erties
  This issue is resolved.

- SMGME-3943
  Mediator logs an error in the Integration Server log during server start-up or when the WmMediator package is reloaded, if you have configured SNMP in the Mediator Administration page.
  Mediator logs the following error in the Integration Server server.log file:
  [MED.0205.0010E] No formatter for destination configuration type .There is however no error in Mediator. This stale log entry is misleading and must be removed.

This issue is resolved. Mediator no longer logs this message in the server log.

- SMGME-3919
  Mediator responds with a null pointer exception, if the Accept header of an existing service for which caching is enabled, is changed from application/json or no header to application/xml.
  Mediator should not change the response when retrieving the information from a cache even if the Accept header for the service is changed before the second invocation of the service.
  After the result of the first invocation of a service is stored in the cache, responses to all subsequent invocations should be retrieved from the cache.
  This issue is resolved.

- SMGME-3913
  Mediator logs an error in the Integration Server log when it finds malformed XML in the Runtime Alias doctype.
  The following error is logged in the server.log file in Integration Server when Mediator comes across a malformed XML in the Runtime Alias doctype:
  [ISS.0028.0010E] Unknown service type (null) in mediator
  This error however is not known to cause issues in the Mediator production scenarios.
  This issue is resolved. The malformed XML is now rectified and hence the error is not logged in the server log.

- SMGME-3862
  Issues with respect to pre-processing and post-processing XSLT transformations for SOAP and REST services are resolved.

- SMGME-3848
  In CentraSite and Mediator you can pass on the API key value only using the header, x-CentraSite-APIKey.
  The name of API key header, x-CentraSite-APIKey is not customizable. There should be a way to define the name of the API key header because this header discloses the name of the product used to manage the API.
  This issue is resolved. You can now define the API Key header name in the pg-config.properties file using the pg.apikey.header property. The API key value can be passed using the new header thereafter.
  Note: You must restart Mediator for the updates in the pg-config.properties file to take effect.

- SMGME-3821
  Mediator sends a fault response in XML format even when the Accept header is set to application/json.
  When an error occurs in a virtual REST service with a HTTP GET method, Mediator sends a response in XML when no Content-Type header is specified, although the Accept header is set to application/json.
  This issue is resolved.

- SMGME-3811
  The provider roundtrip time value logged in the CentraSite log differs from the value logged in

other logs. In the events logged in CentraSite, the provider roundtrip time is different from the one logged in the database and from the value in other logging destinations such as audit log, Integration Server Logger, email. The value for the provider roundtrip time must be the same across all logs.
This issue is resolved.

- SMGME-3800
  Mediator Services page shows an incorrect link to the service WSDL if you configure a HTTPS port as the primary port in the Integration Server Administration page.
  This issue is resolved.

Release 9.7

- SMGME-3146
  The HTTP headers in a Mediator requests are case sensitive.
  RFC2616 protocol requires that all HTTP header fields should not be case sensitive. The HTTP headers in a Mediator request are case sensitive and should be changed as per the RFC2616 protocol.
  This issue is resolved.

Release 9.6

- SMGME-2099
  Deploying a virtual service with an invalid password for a valid user can also result in failures of valid service invocations.
  This issue occurs with virtual services whose Routing Protocol step use either HTTP Basic authentication or NTLM authentication and with the "Use credentials from incoming request" option selected. If such a virtual service is deployed to Mediator with an invalid password for a valid user, the password gets updated in the passman. As a result, valid service invocations will fail as well. Note that in Mediator, the password for the user to authenticate to back-end services is shared through the passman infrastructure.
  This issue is resolved.

- SMGME-2017
  Mediator mistakenly closes the connection with a WCF client after a long pause.
  When a WCF client makes a request after a long pause to access a virtual service which is configured to run in NTLM Transparent mode, Mediator closes the connection which is supposed to be kept alive.
  This issue is resolved.

- SMGME-2181
  Mediator does not properly handle requests with the Accept header set to multiple Content-Types.
  When handling requests with an Accept header set to multiple Content-Types (for example, Accept:application/soap+xml, multipart/related, text/html,image/gif, image/jpeg, *; q=.2, */*; q=.2), Mediator encounters issues while parsing native service responses.
  This issue is resolved.

- SMGME-2277
  EnvelopeString is not passed when watt.server.SOAP.MTOMStreaming is set to true.
  When virtual services invoke IS services, EnvelopeString is not passed if the IS property watt.server.SOAP.MTOMStreaming.enable property is set to true. This occurs for both MTOM and non-MTOM requests.
  With this fix applied, when watt.server.SOAP.MTOMStreaming.enable is set to true, EnvelopeString will be passed for non-MTOM requests.
  Limitation: EnvelopeString will not be sent to IS services if a request uses the "MTOM" SOAP Optimization Method and if the Integration Server property watt.server.SOAP.MTOMStreaming.enable is set to true.

- SMGME-2449
  For a virtual REST service request with multi-root node JSON content, Mediator incorrectly logs the requests and responses.
  This issue occurred when both of the following conditions were met:
  a) The "Log Invocation" run-time action is configured to log both requests and responses.
  b) A virtual REST service request contains multi-root node JSON content such as this:

  ```
  {
    {  node1  }
    {  node2  }
  }
  ```

  Then Mediator incorrectly logs only the first node:

  ```
  {
    { node1 }
  }
  ```

  This issue is resolved. Mediator now logs all nodes of the JSON content.

- SMGME-2364
  Mediator changes the Content-Type of REST service responses to application/octet-stream in case of an error or fault.
  When an error or fault occurs for a REST service invocation, Mediator always changes the Content-Type of responses sent by the native service to application/octet-stream.
  With this fix applied, Mediator retains the Content-Type of the responses sent by the native service.

- SMGME-2206
  Mediator's NTLM authentication support in "Transparent" mode is not stable.
  Mediator's NTLM authentication support in "Transparent" mode is not stable when tried with clients that use a connection pool.
  This issue is resolved. Users who have clients that use connection pools are advised to instead configure Mediator's NTLM "Transparent" mode so that it enables Kerberos authentication. To do this, set the property watt.pg.disableNtlmAuthHandler to true. Thus, if you select "NTLM" authentication in "Transparent" mode, Mediator will perform the Kerberos Windows authentication (and not NTLM Windows authentication).

- SMGME-2317
  Performance metrics are sometimes not communicated properly between Mediator and CentraSite due to a "connection closed" exception.
  Performance metrics are published from Mediator to CentraSite using UDDI. A UDDI authToken is required to save the performance metrics. If CentraSite is restarted, or if CentraSite and Mediator are disconnected, this authToken expires. Refetching this authToken throws a "connection closed" exception in CentraSite.

This issue is resolved. If the authToken expires or if a disconnect occurs, Mediator will fetch the authToken again and publish the Performance metrics in CentraSite. In CentraSite, this issue was fixed by properly handling the closed connection so that refetching the authToken will not cause a "connection closed" exception.

- SMGME-2558
  Audit records containing Mediator transaction events are lost.
  When an exception occurs during audit logging, the audit records should be written to the failed audit log. However, Mediator does not write to the failed audit log in this scenario, thus resulting in the loss of audit records.
  This issue is resolved.

- SMGME-2181
  Mediator does not properly handle request with an Accept header set to multiple Content-Types.
  When handling requests with an Accept header set to multiple Content-Types (for example, Accept: application/soap+xml, multipart/related, text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2), Mediator encounters issues while parsing native service responses.
  This issue is resolved.

- SMGME-2553
  For a virtual REST service request with JSON content, Mediator improperly sends a null value of a parameter as a "null" string to the native service.
  If a virtual REST service request contains JSON content with a null value as follows:

```
{
  "_id": "2e572eb7aa7358324cfa0b96bb001a7c",
  "_rev": "1-d13e06d7d560a7395dc240c90858da30",
  "Data": {
     "name": "JoeSmith",
     "age": null
  }
}
```

  Then Mediator considers the null value as a String and, while sending it to native service, it converts null to "null", which is not acceptable.
  This issue is resolved.

Release 9.5

- SMGME-1936
  The WSDL for a virtual service deployed to Mediator contains the virtual service name twice in the <soap:address location>. This issue occurs when both HTTP and HTTPS are selected in the service's Entry Protocol Step. (When only HTTP or only HTTPS is selected, the value for <soap:address location> is generated correctly).
  This issue is resolved so that Mediator's <soap:address location> is unique from CentraSite's. With this fix, if a WSDL has a multiple-port endpoint (e.g., both HTTP and HTTPS), Mediator will

generate the WSDL so that the <soap:address location> will update the endpoint with the port name, and the WSDL that appears in CentraSite will not contain the port name.

- SMGME-2086
  Web service with "WS-Security" header and "Content-Based" routing returns a SOAP fault. If a SOAP request contains a "WS-Security" header, Mediator passes it to the native service. When you have configured a virtual service for "Content-based" or "Context-based" routing, Mediator passes the "WS-Security" header in the SOAP request to the native service.
  This issue is resolved. However, Software AG recommends that you redeploy the virtual services that are configured for "Content-based" routing or "Context-based" routing.

- SMGME-1935 (Fix 14)
  Mediator keeps all virtual service application references, even when the application is removed from the virtual service and is redeployed. When changing the consumer application definitions for a deployed virtual service, Mediator retains the old application definitions and uses them for run-time governance.
  This issue is resolved.

- SMGME-1821 (Fix 14)
  Mediator Administration page is not accepting the URL without a port. When setting the HTTP Load Balancer URL, the port is mandatory. Some users would like that the default, standard port (80) not to be present there. With this fix, the user can configure a load balancer URL without specifying a port.

- SMGME-1681 (Fix 13)
  Protocol violation exception reported by WCF client when running Mediator in transparent mode. Please see the related issue SMGME-1679. Please note that this issue is fixed only in the Windows environment.
  This issue is resolved.

- SMGME-1679 (Fix 13)
  Mediator does not support Kerberos when a virtual service is configured to use NTLM in Transparent mode. A virtual service does not support a Kerberos handshake when it is configured for NTLM authentication scheme in transparent mode. Mediator now supports Kerberos in Transparent mode.

6.0 Documentation Changes

This section describes significant changes to the documentation, such as the addition, relocation, or removal of product guides, online help, chapters, or other major content. A release is listed in this section only if changes occurred in that release.

7.0 Terminology Changes

A release is listed in this section only if changes occurred in that release.

8.0 Added, Removed, Deprecated, or Changed Items

This section lists functionality, controls, portlets, properties, or other items that have been added, removed, deprecated, or changed. A release is listed in this section only if changes occurred in that release.

Release 9.12

Added Item	Description
Mediator support for Outbound SAML Authentication	Mediator supports Outbound SAML authentication through a new policy action SAML Authentication, available in the Outbound Authentication section of CentraSite. Mediator can act as a client using policy configuration for Outbound SAML authentication. Mediator can also act as delegation for the incoming SAML credentials.
Mediator support for Kerberos over Transport	Mediator supports Kerberos Authentication over Transport for both Inbound and Outbound. Kerberos support over transport will enable REST services also to be secured with Kerberos. REST services can be implemented with Inbound, Outbound, or delegation scenarios of Kerberos.
Axis free mediation support	Mediation of REST services is with or without the Axis framework. This is controlled by a CentraSite configuration parameter. Once this parameter is set to not use Axis for REST services, all newly deployed services do not use it. Existing services continue using Axis until and unless it's manually changed by unpublishing and republishing the service.
HTTP Verbs Support	Mediator supports HTTP PATCH verb for REST services when performing Axis free mediation.

Release 9.10

Added Item	Description
Mediator support for Kerberos Outbound Authentication	Mediator supports Kerberos outbound via Outbound Authentication policy action. Three scenarios can be achieved via this policy: • Use Existing Credentials - Client Credentials should be passed by client and Service Principal is configured in policy. On Successful invocation of inbound policies, Mediator routes the request with Kerberos configuration as part of message level settings. • Custom Credentials - Client Credentials and Service Principal are configured in policy. On Successful invocation of inbound policies, Mediator routes the request with Kerberos configuration as part of message level settings. • Secure Alias - Define Secure Alias of Kerberos type with Client Credentials and Service Principal. Configure alias in Kerberos outbound policy. On Successful invocation of inbound policies, Mediator routes the request with Kerberos configuration as part of message level settings.
Mediator support for Dynamic Routing	Mediator provides a configurable HTTP Header parameter and a new routing action "dynamic routing" to enable dynamic routing. The purpose of the explicit "dynamic routing" action is to allow a user specifically enable dynamic routing for a given service. The client will populate the HTTP header parameter value with the URL where the request is expected to be routed by Mediator. Mediator introduces a new predefined context variable ROUTING_ENDPOINT. Users can dynamically set the context variable in IS or Java based Request Processing Steps based on their own criteria and custom logic.

Added Item	Description
Mediator support for Elastic Search as Events and Metrics destination	Mediator needs to be able to send Metrics and Events to elastic search so that the standalone usage of elastic search or kibana is possible.
Mediator support for API Portal as Events and Metrics destination	Mediator needs to be able to send Metrics and Events to API Portal so that API Portal users can use Dashboards to visualize runtime data.
Mediator SAML Audience element validation	Mediator supports Audience element validation via policy action validate SAML Audience URIs. This action can be configured for the validation to be done as Exact Match or Allow Sublevels. Mediator validates the Audience URI in the conditions section of the SAML assertion against policy configuration.
OData Support	In addition to REST and SOAP services, Mediator also supports Open Data Protocol (OData) services. The mediation capabilities applicable to native OData services correspond to ones applicable to REST services. The support covers OData version 2 and version 4 and is only available after applying the XB_9.10_Fix1.

Release 9.9

Changed Item	Description
Custom API key header	The name of API key header, x-CentraSite-APIKey was not customizable. Custom API Key header name can be configured as property pg.apikey.header in Mediator pg-config.properties. The same can be done via CentraSite command set APIKey header name.

Changed Item	Description
Virtual Service naming restrictions	Virtual service names were nc name validated in the UI during virtual service creation. This is now changed to validate during deployment and if the virtual service name contains any non-conformant character, upon

	deploying the virtual service to any gateway, the non-conformant characters are replaced with the underscore character (_).

Release 9.8

Added Item	Description
The results of service invocations can be cached in Mediator.	Mediator supports caching of the results of native service invocations for incoming requests based on the caching criteria that you specify. The caching criteria can be based on one of following: • HTTP Header • Path • XPath Expression You can use this option to store and retrieve results for services which do not require state values and live data. Caching the service results helps in reducing the overall response time and bridges any temporary network failures when Mediator invokes a native service.
Mediator supports REST to SOAP conversion of a REST request to invoke a SOAP service.	Mediator clients can now invoke SOAP APIs using a REST request as well as a SOAP request. This functionality enables you to expose the existing SOAP based services as REST services to the new API scenarios. You no longer have to write new REST services for this purpose. Restful invocation of SOAP APIs is enabled by default in CentraSite using the Enable REST Support policy action. You can disable the support by deleting the Enable REST Support policy action for the service. If the REST support is enabled, Mediator converts SOAP services to REST services during runtime invocation of the services.

Added Item	Description
Mediator Logging enhancements	New Mediator components added in the Integration Server Logging page. These logging facilities are listed under Mediator in the Server Logger Configuration list and cover among other things monitoring and event logging, service deployment, CentraSite communication, Mediator policies and runtime, alerts, cache management. You can set the log level for each of these facilities. Mediator Listener is the component added newly to enable logging of incoming messages before Mediator processes a request. Incoming Messages is another component added newly to enable logging of incoming messages after Mediator receives a request. For additional details, see *webMethods Integration Server Administrator's Guide*.
Cross-platform NTLM Support	Added NTLM Authentication support for virtual services in UNIX platforms like Linux. A virtual service deployed on Mediator running on a Linux system can be enabled with NTLM authentication.
Set default message type for REST request and response messages	A default message type can be defined for Request and Response messages. This message type is used if no Content-Type is set by the client. Mediator will use the Content-Type set in the Set Media Type policy action configured for the request and response steps in CentraSite if the client sends a request without the Content-Type and Accept headers.

Added Item	Description
pg.rampartdeploymenthandler.responseTimeToLive property	Added to allow Mediator to set the Time to Live (TTL) value of a SOAP response sent to client. The TTL value set using this property can be used to include timestamp along with the assertions: WS-Security username token, X509 certificate token, Encryption, or Signature. A timestamp assertion is used to indicate the expiry of a message initiated by Mediator. The response message becomes invalid if the timestamp has expired. To change the default TTL value (300 seconds), include this property in the pg-config.properties file at Integration Server_directory \instances\instance_name \packages\ WmMediator\config\resources\ as follows: pg.rampartdeploymenthandler.responseTimeToLive = 120 Reload the WmMediator package in Integration Server. In the example above, the TTL value is set to 2 minutes (120 seconds). This value applies to all virtual services deployed to Mediator.

Changed Item	Description
Dependency on Win32 package is removed	When NTLM authentication was supported only on the Windows platform, it was necessary to enable the Win32 package. Starting with this version, the dependency on the Win32 package is removed and it is no longer necessary for NTLM authentication.

Release 9.7

Added Item	Description
Multiple resources can be defined for virtual REST APIs.	The enhanced REST framework in CentraSite allows you to explicitly define multiple resources for a RESTful API. You can use the resource path tokenizer to handle the multiple resources at run-time. The tokenizer for substituting a resource path is automatically appended to the API's endpoint (base URL) by a path variable `${sys:resource_path}`. If you have defined multiple resources for an API, Mediator replaces the resource path tokenizer at run-time with the appropriate resource path that is defined for the particular resource call. If you have defined an XSLT transformation or webMethods Integration Server services in the request or response processing step of a REST service, then you need to append the resource name to the method name in order to refer to that resource. For example, if you have defined a resource "phones" for the GET method, you will refer to the resource using GET_phones.

Release 9.6

Added Item	Description
The watt.pg.disableNtlmAuthHandler property.	Added to support Kerberos Transparent mode support (see "Kerberos Transparent mode support" below).

Changed Item	Description
Kerberos Transparent mode support.	In the Routing Protocols processing step of a virtual service, if you select the HTTP Authentication mode “NTLM” in “Transparent” mode, Mediator performs the Kerberos Windows authentication (and not NTLM Windows authentication) if the property watt.pg.disableNtlmAuthHandler is set to true. If the property is set to false (the default), Mediator performs the NTLM Windows authentication.

9.0 Added, Removed, Deprecated, or Changed Built-In Services

A release is listed in this section only if changes occurred in that release.

Release 9.10

Added Service	Description
pub.mediator.security.utils:getSamlClaims	A Java service which reads incoming SAML attributes and return them as Claims class instance. Service constructs a ClaimsIdentity class which has methods to be used to get list of claims given claim type and it also has methods to get Actor.

10.0 Added, Removed, Deprecated, or Changed APIs

A release is listed in this section only if changes occurred in that release.

Release 9.10

Added API	Description
com.softwareag.pg.security.saml.Claim	This class file can be used to read incoming SAML attributes and return them as Claims class instance.
com.softwareag.pg.security.saml.ClaimsIdentity	This class can be used to construct a ClaimsIdentity class which has methods to be used to get list of claims given claim type and it also has methods to get Actor.

11.0 Copyright Information

12.0 Support

Visit the Empower website to learn about support policies and critical alerts, read technical articles and papers, download products and fixes, submit feature/enhancement requests, and more.

Visit the TECHcommunity website to access additional articles, demos, and tutorials, technical information, samples, useful resources, online discussion forums, and more.

SMG-RM-101-20171017