# Virtual Switch for IVR In-Front T-Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Avaya Communication Manager T-Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

SIP Switch T-Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Stat Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.000.29  01/23/15  General  8.5.000.29  01/23/15  General  8.5.102.20  05/10/16  Hot Fix  8.5.102.20  05/10/16  Hot Fix  8.5.102.20  05/10/16  Hot Fix  8.5.102.25  08/31/16  Hot Fix  8.5.102.25  08/31/16  Hot Fix  8.5.103.21  05/18/16  Hot Fix  8.5.105.10  02/03/17  Hot Fix  8.5.105.10  02/03/17  Hot Fix  8.5.105.10  02/03/17  Hot Fix  8.5.105.10  02/03/17  Hot Fix  8.5.105.10  02/03/17  Hot Fix  8.5.107.16  09/06/17  Hot Fix  8.5.107.16  09/06/17  Hot Fix  8.5.107.16  09/06/17  Hot Fix  8.5.107.16  09/06/17  Hot Fix |  | 8.5.107.20  11/06/17  Hot Fix | 35  35  20  20  20  16  16  13  7  7  7  7  7  3  3  3  3 | 8.5.107.20  11/06/17  Hot Fix | 35  35  20  20  20  16  16  13  7  7  7  7  7  3  3  3  3 |

## **Release 8.5.000.29 (01/23/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.29 | 01/23/15 | General |  | X | X | X | X |

### New Features:

* **In addition to known option [statserver]\check-stuck-calls, two new static integer options may be configured in the [statserver] configuration section:
  check-stuck-calls-duration
  check-stuck-calls-frequency**
* **check-stuck-calls-duration**
* **check-stuck-calls-frequency**
* **Script upgrade\_850\_login\_oracle.sql is now provided with Stat Server to upgrade LOGIN table for Oracle RAC.**
* **In addition to known option [statserver]\check-stuck-calls, two new static integer options may be configured in the [statserver] configuration section:
  check-stuck-calls-duration
  check-stuck-calls-frequency**
* **check-stuck-calls-duration**
* **check-stuck-calls-frequency**
* **Script upgrade\_850\_login\_oracle.sql is now provided with Stat Server to upgrade LOGIN table for Oracle RAC.**

### **Resolved issues:**

## **Release 8.5.000.32 (04/06/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.32 | 04/06/15 | Hot Fix |  | X | X |  | X |

### New Features:

* **Stat Server now supports configurable association between position and extension on the switch level. A new static boolean option can be configured for any switch on the switch Annex in the statserver section:
  position-extension-linked**
* **position-extension-linked**
* **Stat Server now supports configurable association between position and extension on the switch level. A new static boolean option can be configured for any switch on the switch Annex in the statserver section:
  position-extension-linked**
* **position-extension-linked**

### **Resolved issues:**

## **Release 8.5.000.33 (05/04/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.33 | 05/04/15 | Hot Fix |  | X | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.000.34 (05/27/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.34 | 05/27/15 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.000.35 (06/23/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.35 | 06/23/15 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.000.36 (09/11/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.36 | 09/11/15 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.10 (06/15/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.10 | 06/15/15 | General |  | X | X | X | X |

### New Features:

* **Stat Server now reads the configuration in asynchronous mode.**
* **Stat Server now supports the StagingArea statistical object natively. Previously, statistics for the StagingArea were only available through Java extensions.**
* **The following new actions are now supported for the StagingArea statistical object:
  InteractionCreated
  InteractionEntered
  InteractionDistributed
  InteractionCleared
  InteractionDistributedToQueue
  InteractionDeleted**
* **InteractionCreated**
* **InteractionEntered**
* **InteractionDistributed**
* **InteractionCleared**
* **InteractionDistributedToQueue**
* **InteractionDeleted**
* **The static integer option [statserver]\reconnect-timeout now is also regulate the timeout of the reconnection to Configuration Server, in addition to that of T-Server and DB Server.**
* **New standard log message 10067 Application failed to restore session with Configuration Server is introduced. It is logged when Stat Server fails to restore the session with Configuration Server.**
* **The default value of the dynamic BBoolean option [statserver]\show-queued-interactions is changed to false.**
* **Stat Server now reads the configuration in asynchronous mode.**
* **Stat Server now supports the StagingArea statistical object natively. Previously, statistics for the StagingArea were only available through Java extensions.**
* **The following new actions are now supported for the StagingArea statistical object:
  InteractionCreated
  InteractionEntered
  InteractionDistributed
  InteractionCleared
  InteractionDistributedToQueue
  InteractionDeleted**
* **InteractionCreated**
* **InteractionEntered**
* **InteractionDistributed**
* **InteractionCleared**
* **InteractionDistributedToQueue**
* **InteractionDeleted**
* **The static integer option [statserver]\reconnect-timeout now is also regulate the timeout of the reconnection to Configuration Server, in addition to that of T-Server and DB Server.**
* **New standard log message 10067 Application failed to restore session with Configuration Server is introduced. It is logged when Stat Server fails to restore the session with Configuration Server.**
* **The default value of the dynamic BBoolean option [statserver]\show-queued-interactions is changed to false.**

### **Resolved issues:**

## **Release 8.5.101.07 (08/31/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.07 | 08/31/15 | General |  | X | X | X | X |

### New Features:

* **Stat Server supports the following new actions for a regular DN:
  CallObserving...
  CallOutboundOriginated
  CallOutboundReceived**
* **CallObserving...**
* **CallOutboundOriginated**
* **CallOutboundReceived**
* **Stat Server calculates regular statistics on StagingArea for the following new actions:
  InteractionAbandonedDuringOffering
  InteractionAccepted
  InteractionAnswered
  InteractionReleased**
* **InteractionAbandonedDuringOffering**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Absolute paths are now mandatory for the [java-config]/jvm-path option. The JVM will not be initialized if the option is set to a relative path.**
* **Stat Server supports JDK 1.8.**
* **Stat Server includes functionality for the prevention of database update losses due to commit failures or loss of database server connection.
  Two new database-related options may be configured in the [statserver] configuration section:
  db-timeout
  db-txn-max-retries**
* **db-timeout**
* **db-txn-max-retries**
* **Stat Server supports the following new actions for a regular DN:
  CallObserving...
  CallOutboundOriginated
  CallOutboundReceived**
* **CallObserving...**
* **CallOutboundOriginated**
* **CallOutboundReceived**
* **Stat Server calculates regular statistics on StagingArea for the following new actions:
  InteractionAbandonedDuringOffering
  InteractionAccepted
  InteractionAnswered
  InteractionReleased**
* **InteractionAbandonedDuringOffering**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Absolute paths are now mandatory for the [java-config]/jvm-path option. The JVM will not be initialized if the option is set to a relative path.**
* **Stat Server supports JDK 1.8.**
* **Stat Server includes functionality for the prevention of database update losses due to commit failures or loss of database server connection.
  Two new database-related options may be configured in the [statserver] configuration section:
  db-timeout
  db-txn-max-retries**
* **db-timeout**
* **db-txn-max-retries**

### **Resolved issues:**

## **Release 8.5.101.10 (09/24/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.10 | 09/24/15 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.101.13 (10/21/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.13 | 10/21/15 | Hot Fix |  | X | X | X | X |

### New Features:

* **Stat Server improvements in the backup file handling:
  Buffering is turned off.
  Optimizations are introduced to reduce backup file size.
  Additional error-checking is introduced.**
* **Buffering is turned off.**
* **Optimizations are introduced to reduce backup file size.**
* **Additional error-checking is introduced.**
* **Stat Server improvements in the backup file handling:
  Buffering is turned off.
  Optimizations are introduced to reduce backup file size.
  Additional error-checking is introduced.**
* **Buffering is turned off.**
* **Optimizations are introduced to reduce backup file size.**
* **Additional error-checking is introduced.**

### **Resolved issues:**

## **Release 8.5.102.12 (12/10/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.12 | 12/10/15 | General |  | X | X | X | X |

### New Features:

* **Serialization of Statistical Aggregates to/from Backup File.**
* **Enhanced ExpectedWaitTime2 statistic – better precision, no limitation for use with Voice media.**
* **Support for System attributes in filters and formulas.**
* **Support for Tenant as a native statistical object.**
* **Stat Server supports the following new multimedia actions for Tenants:
  InteractionCreated
  InteractionAbandonedDuringOffering (see also known issue)
  InteractionAccepted1
  InteractionDeleted
  InteractionPastAcceptServiceLevel
  InteractionPastCompletionServiceLevel**
* **InteractionCreated**
* **InteractionAbandonedDuringOffering (see also known issue)**
* **InteractionAccepted1**
* **InteractionDeleted**
* **InteractionPastAcceptServiceLevel**
* **InteractionPastCompletionServiceLevel**
* **Stat Server calculates regular statistics on StagingArea for the following new multimedia actions:
  InteractionPastAcceptServiceLevel
  InteractionPastCompletionServiceLevel**
* **InteractionPastAcceptServiceLevel**
* **InteractionPastCompletionServiceLevel**
* **Support for RONA (Revoke On No Answer) on associated Virtual Queues controlled by the multimedia switch.**
* **Two new options may be configured in the [statserver] configuration section:
  backup-file-aggregates-store
  disconnect-from-lca-on-history-log-expired**
* **backup-file-aggregates-store**
* **disconnect-from-lca-on-history-log-expired**
* **New GetList function and IsNull predicate in filters and formulas.**
* **The following scripting enhancements are introduced:
  Added true and false keywords.
  Inline if is now supported: <boolean expression> ? <result1> : <result2>.
  If boolean expression is true then result1 is returned, else result2 is returned.
  DNIS and ThisQueue now can be compared to a variable string expression, in addition to a literal string.
  GetAver, GetSum, GetMin, GetMax, GetNumber, GetString are now applicable not only to UserData but to any key-value list attributes: UserData/Reasons/Extensions/System.**
* **Added true and false keywords.**
* **Inline if is now supported: <boolean expression> ? <result1> : <result2>.
  If boolean expression is true then result1 is returned, else result2 is returned.**
* **DNIS and ThisQueue now can be compared to a variable string expression, in addition to a literal string.**
* **GetAver, GetSum, GetMin, GetMax, GetNumber, GetString are now applicable not only to UserData but to any key-value list attributes: UserData/Reasons/Extensions/System.**
* **Serialization of Statistical Aggregates to/from Backup File.**
* **Enhanced ExpectedWaitTime2 statistic – better precision, no limitation for use with Voice media.**
* **Support for System attributes in filters and formulas.**
* **Support for Tenant as a native statistical object.**
* **Stat Server supports the following new multimedia actions for Tenants:
  InteractionCreated
  InteractionAbandonedDuringOffering (see also known issue)
  InteractionAccepted1
  InteractionDeleted
  InteractionPastAcceptServiceLevel
  InteractionPastCompletionServiceLevel**
* **InteractionCreated**
* **InteractionAbandonedDuringOffering (see also known issue)**
* **InteractionAccepted1**
* **InteractionDeleted**
* **InteractionPastAcceptServiceLevel**
* **InteractionPastCompletionServiceLevel**
* **Stat Server calculates regular statistics on StagingArea for the following new multimedia actions:
  InteractionPastAcceptServiceLevel
  InteractionPastCompletionServiceLevel**
* **InteractionPastAcceptServiceLevel**
* **InteractionPastCompletionServiceLevel**
* **Support for RONA (Revoke On No Answer) on associated Virtual Queues controlled by the multimedia switch.**
* **Two new options may be configured in the [statserver] configuration section:
  backup-file-aggregates-store
  disconnect-from-lca-on-history-log-expired**
* **backup-file-aggregates-store**
* **disconnect-from-lca-on-history-log-expired**
* **New GetList function and IsNull predicate in filters and formulas.**
* **The following scripting enhancements are introduced:
  Added true and false keywords.
  Inline if is now supported: <boolean expression> ? <result1> : <result2>.
  If boolean expression is true then result1 is returned, else result2 is returned.
  DNIS and ThisQueue now can be compared to a variable string expression, in addition to a literal string.
  GetAver, GetSum, GetMin, GetMax, GetNumber, GetString are now applicable not only to UserData but to any key-value list attributes: UserData/Reasons/Extensions/System.**
* **Added true and false keywords.**
* **Inline if is now supported: <boolean expression> ? <result1> : <result2>.
  If boolean expression is true then result1 is returned, else result2 is returned.**
* **DNIS and ThisQueue now can be compared to a variable string expression, in addition to a literal string.**
* **GetAver, GetSum, GetMin, GetMax, GetNumber, GetString are now applicable not only to UserData but to any key-value list attributes: UserData/Reasons/Extensions/System.**

### **Resolved issues:**

## **Release 8.5.102.13 (01/25/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.13 | 01/25/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.15 (02/18/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.15 | 02/18/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.16 (03/14/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.16 | 03/14/16 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.17 (04/07/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.17 | 04/07/16 | Hot Fix |  | X | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.20 (05/10/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.20 | 05/10/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.22 (07/05/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.22 | 07/05/16 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.23 (07/22/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.23 | 07/22/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.24 (08/04/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.24 | 08/04/16 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.25 (08/31/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.25 | 08/31/16 | Hot Fix |  |  | X |  | X |

### New Features:

* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**
* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**
* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**
* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**
* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**
* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**
* **Stat Server now provides the DN name attribute (if applicable) in the LMS message GCTI\_INTERACTION\_MESSAGE\_RECEIVED.**

### **Resolved issues:**

## **Release 8.5.102.27 (06/20/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.27 | 06/20/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.103.17 (04/20/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.17 | 04/20/16 | General |  | X | X | X | X |

### New Features:

* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**
* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**
* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**
* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**
* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**
* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**
* **New GroupBy feature is introduced.**
* **Support of the time zone specification in a growing TimeProfile definition.**
* **Stat Server supports the following new actions for Tenants:**
* **InteractionAccepted**
* **InteractionAnswered**
* **InteractionReleased**
* **Stat Server supports new InteractionWait action on StagingArea.**
* **Stat Server supports new UserEventReceived action for a regular DN and mediation DN.**
* **Stat Server supports the AgentID System attribute on selected actions.**
* **Stat Server supports the GlobalUserData key-value list in filters and formulas.**
* **The following new configuration options are added in the statserver section:
  interaction-wait-on-sa-max-number
  interaction-wait-on-sa-media-list**
* **interaction-wait-on-sa-max-number**
* **interaction-wait-on-sa-media-list**

### **Resolved issues:**

## **Release 8.5.103.21 (05/18/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.21 | 05/18/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.103.24 (08/15/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.24 | 08/15/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.104.22 (10/17/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.22 | 10/17/16 | General |  | X | X | X | X |

### New Features:

* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**
* **Stat Server supports new Routable and NotRoutable actions on an agent or place.**
* **New DistinquishBy feature is introduced.**
* **Stat Server supports new ApplyFilterAtActionEndOnly stat type option.**
* **Stat Server supports new ExternalServiceRequested and ExternalServiceResponded actions for Tenants.**
* **Stat Server supports new ActorType and RequestEnvelope System attributes on selected actions.**
* **Stat Server logs stat type definitions on the Init:6 debug log level.**
* **Stat Server provides the DN name attribute (if applicable) in the GCTI\_INTERACTION\_MESSAGE\_RECEIVED LMS message.**
* **Messages, associated with opening a statistic, are logged at Client:4 instead of Client:5.**
* **The following new configuration options are added in the statserver section:
  consult-acw-mode
  suppress-user-data**
* **consult-acw-mode**
* **suppress-user-data**

### **Resolved issues:**

## **Release 8.5.104.24 (11/08/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.24 | 11/08/16 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.104.25 (11/30/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.25 | 11/30/16 | Hot Fix |  | X | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.105.09 (12/27/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.105.09 | 12/27/16 | General |  | X | X | X | X |

### New Features:

* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**
* **Stat Server can be configured to undertake multiple attempts to register a DN.**
* **Stat Server supports multiple business attribute values in stat types.**
* **Stat Server supports the new InteractionResponded action on a regular DN and on a media channel.**
* **Stat Server reports the progress of building virtual agent groups during the startup in logs, using the new LMS message:
  10069|STANDARD|Building virtual agent groups on tenant '%s', %d percent complete**
* **The following new configuration options are added in the statserver section:
  reg-error-delay
  reg-error-max-count**
* **reg-error-delay**
* **reg-error-max-count**

### **Resolved issues:**

## **Release 8.5.105.10 (02/03/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.105.10 | 02/03/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.106.20 (05/05/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.106.20 | 05/05/17 | General |  | X | X | X | X |

### New Features:

* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**
* **Stat Server supports the statistical category Formula for the Growing time profile.**
* **Stat Server supports the Ever Growing time profile for a limited set of the float-valued categories. See the documentation for more details.**
* **Stat Server supports the new DialRemoteRelease action on Campaign/CallingList statistical objects.**
* **Stat Server supports the enable-thread option, as well as associated throttle-period and throttle-threshold options.**

### **Resolved issues:**

## **Release 8.5.106.21 (08/01/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.106.21 | 08/01/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.107.15 (08/18/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.15 | 08/18/17 | General |  | X | X | X | X |

### New Features:

* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**
* **Stat Server supports Sliding, Selection, and SinceLogin aggregation intervals in the the statistical category Formula.**
* **Stat Server logs operational statistics and current execution context into a special StatFile log file to help with diagnostics and troubleshooting.**
* **Stat Server supports the durable InteractionWait action for Tenants. The action is intended to track an interaction until it is actually handled by an agent.**
* **Stat Server supports the durable DND action on RegDN.**
* **Stat Server supports Red Hat Enterprise Linux 7.**
* **The following new configuration options are added in the [statserver] section:
  interaction-wait-on-tenant-max-number
  interaction-wait-on-tenant-media-list
  stat-file-show-clients-list
  stat-file-show-options
  stat-file-timeout**
* **interaction-wait-on-tenant-max-number**
* **interaction-wait-on-tenant-media-list**
* **stat-file-show-clients-list**
* **stat-file-show-options**
* **stat-file-timeout**

### **Resolved issues:**

## **Release 8.5.107.16 (09/06/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.16 | 09/06/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.107.17 (10/17/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.17 | 10/17/17 | Hot Fix |  |  | X |  | X |

### New Features:

* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**
* **Stat Server now keeps the ports with protocol="http" open when running in the backup mode, regardless of the value of the [statserver]/accept-clients-in-backup-mode option.**

### **Resolved issues:**

## **Release 8.5.107.20 (11/06/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.20 | 11/06/17 | Hot Fix |  | X | X |  | X |

### New Features:

### **Resolved issues:**

Call Concentrator

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Outbound Contact Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Universal Routing Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Configuration Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.100.11  12/22/15  General  8.5.100.11  12/22/15  General  8.5.100.11  12/22/15  General  8.5.100.11  12/22/15  General  8.5.100.11  12/22/15  General  8.5.101.01  01/27/17  General  8.5.101.01  01/27/17  General  8.5.101.01  01/27/17  General |  | 8.5.101.17  11/10/17  General | 19  19  19  19  19  9  9  9 | 8.5.101.17  11/10/17  General | 19  19  19  19  19  9  9  9 |

## **Release 8.5.100.11 (12/22/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.11 | 12/22/15 | General |  | X | X | X | X |

### New Features:

* **Configuration Server port segmentation: You can configure separate ports on Configuration Server and Configuration Server Proxy that are restricted for use only by client User Interface (UI) type applications.**
* **Enhanced security on UNIX:
  Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.
  Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.
  For more information, refer to the Security Pack on UNIX 8.5.x Release Note.**
* **Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.**
* **Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.**
* **Enhanced Logging:To simplify troubleshooting of secure connections, Configuration Server offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **Updated Language Pack support: Refer to Translation Support for details about the updated language packs supported.**
* **In this release, Configuration Server external authentication uses OpenSSL version 1.0.2d for secure connections to LDAP Servers.**
* **Configuration Server port segmentation: You can configure separate ports on Configuration Server and Configuration Server Proxy that are restricted for use only by client User Interface (UI) type applications.**
* **Enhanced security on UNIX:
  Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.
  Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.
  For more information, refer to the Security Pack on UNIX 8.5.x Release Note.**
* **Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.**
* **Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.**
* **Enhanced Logging:To simplify troubleshooting of secure connections, Configuration Server offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **Updated Language Pack support: Refer to Translation Support for details about the updated language packs supported.**
* **In this release, Configuration Server external authentication uses OpenSSL version 1.0.2d for secure connections to LDAP Servers.**
* **Configuration Server port segmentation: You can configure separate ports on Configuration Server and Configuration Server Proxy that are restricted for use only by client User Interface (UI) type applications.**
* **Enhanced security on UNIX:
  Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.
  Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.
  For more information, refer to the Security Pack on UNIX 8.5.x Release Note.**
* **Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.**
* **Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.**
* **Enhanced Logging:To simplify troubleshooting of secure connections, Configuration Server offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **Updated Language Pack support: Refer to Translation Support for details about the updated language packs supported.**
* **In this release, Configuration Server external authentication uses OpenSSL version 1.0.2d for secure connections to LDAP Servers.**
* **Configuration Server port segmentation: You can configure separate ports on Configuration Server and Configuration Server Proxy that are restricted for use only by client User Interface (UI) type applications.**
* **Enhanced security on UNIX:
  Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.
  Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.
  For more information, refer to the Security Pack on UNIX 8.5.x Release Note.**
* **Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.**
* **Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.**
* **Enhanced Logging:To simplify troubleshooting of secure connections, Configuration Server offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **Updated Language Pack support: Refer to Translation Support for details about the updated language packs supported.**
* **In this release, Configuration Server external authentication uses OpenSSL version 1.0.2d for secure connections to LDAP Servers.**
* **Configuration Server port segmentation: You can configure separate ports on Configuration Server and Configuration Server Proxy that are restricted for use only by client User Interface (UI) type applications.**
* **Enhanced security on UNIX:
  Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.
  Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.
  For more information, refer to the Security Pack on UNIX 8.5.x Release Note.**
* **Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite.**
* **Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.**
* **Enhanced Logging:To simplify troubleshooting of secure connections, Configuration Server offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **Updated Language Pack support: Refer to Translation Support for details about the updated language packs supported.**
* **In this release, Configuration Server external authentication uses OpenSSL version 1.0.2d for secure connections to LDAP Servers.**

### **Resolved issues:**

## **Release 8.5.100.14 (04/05/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.14 | 04/05/16 | General |  | X | X | X | X |

### New Features:

* **More secure and efficient agent data retrieval: You can now configure Configuration Server to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. This reduces the volume of object data downloaded by an application when it discovers available objects. Check with Genesys documentation specific to an application to determine if the application supports using the brief API and if the application can benefit from getting a limited list of brief objects. Use the following new option to enable this functionality:
  [security]
  objbrief-api-permission-check
  Default Value: false
  Valid Values: true, false
  Changes Take Effect: Immediately
  When set to true, the results returned by the brief API calls are based on the permissions of the client account that submitted the request.**
* **Implementing Support of Load-Balancing by Configuration Server Proxy: For one of the ways in which this functionality can be implemented, refer to the "Load Balancing Using Clusters" section of the Workspace Desktop Edition Deployment Guide.**
* **Secure connections with Microsoft SQL DBMS: You can now configure secure connections between Microsoft SQL databases and Genesys components running Microsoft SQL database client software.**
* **More secure and efficient agent data retrieval: You can now configure Configuration Server to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. This reduces the volume of object data downloaded by an application when it discovers available objects. Check with Genesys documentation specific to an application to determine if the application supports using the brief API and if the application can benefit from getting a limited list of brief objects. Use the following new option to enable this functionality:
  [security]
  objbrief-api-permission-check
  Default Value: false
  Valid Values: true, false
  Changes Take Effect: Immediately
  When set to true, the results returned by the brief API calls are based on the permissions of the client account that submitted the request.**
* **Implementing Support of Load-Balancing by Configuration Server Proxy: For one of the ways in which this functionality can be implemented, refer to the "Load Balancing Using Clusters" section of the Workspace Desktop Edition Deployment Guide.**
* **Secure connections with Microsoft SQL DBMS: You can now configure secure connections between Microsoft SQL databases and Genesys components running Microsoft SQL database client software.**
* **More secure and efficient agent data retrieval: You can now configure Configuration Server to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. This reduces the volume of object data downloaded by an application when it discovers available objects. Check with Genesys documentation specific to an application to determine if the application supports using the brief API and if the application can benefit from getting a limited list of brief objects. Use the following new option to enable this functionality:
  [security]
  objbrief-api-permission-check
  Default Value: false
  Valid Values: true, false
  Changes Take Effect: Immediately
  When set to true, the results returned by the brief API calls are based on the permissions of the client account that submitted the request.**
* **Implementing Support of Load-Balancing by Configuration Server Proxy: For one of the ways in which this functionality can be implemented, refer to the "Load Balancing Using Clusters" section of the Workspace Desktop Edition Deployment Guide.**
* **Secure connections with Microsoft SQL DBMS: You can now configure secure connections between Microsoft SQL databases and Genesys components running Microsoft SQL database client software.**
* **More secure and efficient agent data retrieval: You can now configure Configuration Server to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. This reduces the volume of object data downloaded by an application when it discovers available objects. Check with Genesys documentation specific to an application to determine if the application supports using the brief API and if the application can benefit from getting a limited list of brief objects. Use the following new option to enable this functionality:
  [security]
  objbrief-api-permission-check
  Default Value: false
  Valid Values: true, false
  Changes Take Effect: Immediately
  When set to true, the results returned by the brief API calls are based on the permissions of the client account that submitted the request.**
* **Implementing Support of Load-Balancing by Configuration Server Proxy: For one of the ways in which this functionality can be implemented, refer to the "Load Balancing Using Clusters" section of the Workspace Desktop Edition Deployment Guide.**
* **Secure connections with Microsoft SQL DBMS: You can now configure secure connections between Microsoft SQL databases and Genesys components running Microsoft SQL database client software.**
* **More secure and efficient agent data retrieval: You can now configure Configuration Server to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. This reduces the volume of object data downloaded by an application when it discovers available objects. Check with Genesys documentation specific to an application to determine if the application supports using the brief API and if the application can benefit from getting a limited list of brief objects. Use the following new option to enable this functionality:
  [security]
  objbrief-api-permission-check
  Default Value: false
  Valid Values: true, false
  Changes Take Effect: Immediately
  When set to true, the results returned by the brief API calls are based on the permissions of the client account that submitted the request.**
* **Implementing Support of Load-Balancing by Configuration Server Proxy: For one of the ways in which this functionality can be implemented, refer to the "Load Balancing Using Clusters" section of the Workspace Desktop Edition Deployment Guide.**
* **Secure connections with Microsoft SQL DBMS: You can now configure secure connections between Microsoft SQL databases and Genesys components running Microsoft SQL database client software.**

### **Resolved issues:**

## **Release 8.5.100.15 (04/29/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.15 | 04/29/16 | General |  | X | X | X | X |

### New Features:

* **You can now configure Configuration Server or Configuration Server Proxy to perform case-insensitive searches to identify Person objects authorized by the Kerberos ticket. If more than one user object is identified, those users are not authenticated and an error is generated. This feature uses the new ignore-case-username configuration option, and is especially relevant if you are using Microsoft Windows Active Directory as the Key Distribution Center. This feature and its new option are described in the detail in the Kerberos page of the Framework External Authentication Reference Manual.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **You can now configure Configuration Server or Configuration Server Proxy to perform case-insensitive searches to identify Person objects authorized by the Kerberos ticket. If more than one user object is identified, those users are not authenticated and an error is generated. This feature uses the new ignore-case-username configuration option, and is especially relevant if you are using Microsoft Windows Active Directory as the Key Distribution Center. This feature and its new option are described in the detail in the Kerberos page of the Framework External Authentication Reference Manual.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **You can now configure Configuration Server or Configuration Server Proxy to perform case-insensitive searches to identify Person objects authorized by the Kerberos ticket. If more than one user object is identified, those users are not authenticated and an error is generated. This feature uses the new ignore-case-username configuration option, and is especially relevant if you are using Microsoft Windows Active Directory as the Key Distribution Center. This feature and its new option are described in the detail in the Kerberos page of the Framework External Authentication Reference Manual.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **You can now configure Configuration Server or Configuration Server Proxy to perform case-insensitive searches to identify Person objects authorized by the Kerberos ticket. If more than one user object is identified, those users are not authenticated and an error is generated. This feature uses the new ignore-case-username configuration option, and is especially relevant if you are using Microsoft Windows Active Directory as the Key Distribution Center. This feature and its new option are described in the detail in the Kerberos page of the Framework External Authentication Reference Manual.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **You can now configure Configuration Server or Configuration Server Proxy to perform case-insensitive searches to identify Person objects authorized by the Kerberos ticket. If more than one user object is identified, those users are not authenticated and an error is generated. This feature uses the new ignore-case-username configuration option, and is especially relevant if you are using Microsoft Windows Active Directory as the Key Distribution Center. This feature and its new option are described in the detail in the Kerberos page of the Framework External Authentication Reference Manual.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**

### **Resolved issues:**

## **Release 8.5.100.17 (06/03/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.17 | 06/03/16 | General |  | X | X | X | X |

### New Features:

* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**

### **Resolved issues:**

## **Release 8.5.100.18 (07/08/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.18 | 07/08/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.21 (08/05/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.21 | 08/05/16 | General |  | X | X | X | X |

### New Features:

* **Improved migration of HA Configuration Servers: You can now allow an upgraded version of Configuration Server to run alongside its HA partner that is not upgraded, for a brief period of time. This provides for a more streamlined migration procedure, with less downtime for clients.
  As part of this new functionality, the following new Configuration Server Log Events are used to track the procedure:**
* **21-21270 [+] show details
  Level
  Standard
  Text
  Configuration Server ready to accept client connections.
  Attributes
  None
  Description
  Reports that Configuration Server has completed initialization/switchover and opened its ports for clients. There still might be initialization steps to complete if event 21-21271 is not generated immediately after this message.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21271 [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully operational in primary mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized, and is in fully writable primary master server mode for the Configuration Database.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21272
  [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully synchronized in backup mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized as the backup server of the currently running primary server. You can only switch over this server to primary mode after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21273
  [+] show details
  Level
  Standard
  Text
  Proxy Configuration Server is fully synchronized with master server
  Attributes
  None
  Description
  Reports that Configuration Server in proxy mode is fully operational. If server is in primary mode, it is confirmed with this message. If server is in backup mode, you are free to switch over to primary mode at any time after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25300
  [+] show details
  Level
  Standard
  Text
  Backup Server ignored because server is starting in upgrade mode [1]
  Attributes
  [1]
  Type of upgrade mode. Currently, only one upgrade mode is available: 1 (simple).
  Description
  The master Configuration Server is in upgrade mode, and is starting in backup mode. The backup Configuration Server will switch to primary mode and will be ignored by the primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25301
  [+] show details
  Level
  Standard
  Text
  Configuration Server entered upgrade mode. Backup Server ignored because of incompatible schema [<schema>]
  Attributes
  <schema>
  Configuration Database schema
  Description
  The master Configuration Server has detected an older primary Configuration Server and is initializing as the primary server. The older primary Configuration Server will switch over to backup mode and be ignored by the newer primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25302
  [+] show details
  Level
  Standard
  Text
  Configuration Server ignored switchover request because another upgrade/switchover already in progress
  Attributes
  None
  Description
  Reports Configuration Server ignored a switchover request from Solution Control Server, most likely because Configuration Server is in upgrade mode. During upgrade, Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe this log event reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **Support for IBM DB2 10.5 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for the VMware ESXi 6 virtualization environment. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported virtual machines.**
* **Improved migration of HA Configuration Servers: You can now allow an upgraded version of Configuration Server to run alongside its HA partner that is not upgraded, for a brief period of time. This provides for a more streamlined migration procedure, with less downtime for clients.
  As part of this new functionality, the following new Configuration Server Log Events are used to track the procedure:**
* **21-21270 [+] show details
  Level
  Standard
  Text
  Configuration Server ready to accept client connections.
  Attributes
  None
  Description
  Reports that Configuration Server has completed initialization/switchover and opened its ports for clients. There still might be initialization steps to complete if event 21-21271 is not generated immediately after this message.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21271 [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully operational in primary mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized, and is in fully writable primary master server mode for the Configuration Database.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21272
  [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully synchronized in backup mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized as the backup server of the currently running primary server. You can only switch over this server to primary mode after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21273
  [+] show details
  Level
  Standard
  Text
  Proxy Configuration Server is fully synchronized with master server
  Attributes
  None
  Description
  Reports that Configuration Server in proxy mode is fully operational. If server is in primary mode, it is confirmed with this message. If server is in backup mode, you are free to switch over to primary mode at any time after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25300
  [+] show details
  Level
  Standard
  Text
  Backup Server ignored because server is starting in upgrade mode [1]
  Attributes
  [1]
  Type of upgrade mode. Currently, only one upgrade mode is available: 1 (simple).
  Description
  The master Configuration Server is in upgrade mode, and is starting in backup mode. The backup Configuration Server will switch to primary mode and will be ignored by the primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25301
  [+] show details
  Level
  Standard
  Text
  Configuration Server entered upgrade mode. Backup Server ignored because of incompatible schema [<schema>]
  Attributes
  <schema>
  Configuration Database schema
  Description
  The master Configuration Server has detected an older primary Configuration Server and is initializing as the primary server. The older primary Configuration Server will switch over to backup mode and be ignored by the newer primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25302
  [+] show details
  Level
  Standard
  Text
  Configuration Server ignored switchover request because another upgrade/switchover already in progress
  Attributes
  None
  Description
  Reports Configuration Server ignored a switchover request from Solution Control Server, most likely because Configuration Server is in upgrade mode. During upgrade, Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe this log event reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **Support for IBM DB2 10.5 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for the VMware ESXi 6 virtualization environment. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported virtual machines.**
* **Improved migration of HA Configuration Servers: You can now allow an upgraded version of Configuration Server to run alongside its HA partner that is not upgraded, for a brief period of time. This provides for a more streamlined migration procedure, with less downtime for clients.
  As part of this new functionality, the following new Configuration Server Log Events are used to track the procedure:**
* **21-21270 [+] show details
  Level
  Standard
  Text
  Configuration Server ready to accept client connections.
  Attributes
  None
  Description
  Reports that Configuration Server has completed initialization/switchover and opened its ports for clients. There still might be initialization steps to complete if event 21-21271 is not generated immediately after this message.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21271 [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully operational in primary mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized, and is in fully writable primary master server mode for the Configuration Database.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21272
  [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully synchronized in backup mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized as the backup server of the currently running primary server. You can only switch over this server to primary mode after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21273
  [+] show details
  Level
  Standard
  Text
  Proxy Configuration Server is fully synchronized with master server
  Attributes
  None
  Description
  Reports that Configuration Server in proxy mode is fully operational. If server is in primary mode, it is confirmed with this message. If server is in backup mode, you are free to switch over to primary mode at any time after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25300
  [+] show details
  Level
  Standard
  Text
  Backup Server ignored because server is starting in upgrade mode [1]
  Attributes
  [1]
  Type of upgrade mode. Currently, only one upgrade mode is available: 1 (simple).
  Description
  The master Configuration Server is in upgrade mode, and is starting in backup mode. The backup Configuration Server will switch to primary mode and will be ignored by the primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25301
  [+] show details
  Level
  Standard
  Text
  Configuration Server entered upgrade mode. Backup Server ignored because of incompatible schema [<schema>]
  Attributes
  <schema>
  Configuration Database schema
  Description
  The master Configuration Server has detected an older primary Configuration Server and is initializing as the primary server. The older primary Configuration Server will switch over to backup mode and be ignored by the newer primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25302
  [+] show details
  Level
  Standard
  Text
  Configuration Server ignored switchover request because another upgrade/switchover already in progress
  Attributes
  None
  Description
  Reports Configuration Server ignored a switchover request from Solution Control Server, most likely because Configuration Server is in upgrade mode. During upgrade, Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe this log event reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **Support for IBM DB2 10.5 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for the VMware ESXi 6 virtualization environment. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported virtual machines.**
* **Improved migration of HA Configuration Servers: You can now allow an upgraded version of Configuration Server to run alongside its HA partner that is not upgraded, for a brief period of time. This provides for a more streamlined migration procedure, with less downtime for clients.
  As part of this new functionality, the following new Configuration Server Log Events are used to track the procedure:**
* **21-21270 [+] show details
  Level
  Standard
  Text
  Configuration Server ready to accept client connections.
  Attributes
  None
  Description
  Reports that Configuration Server has completed initialization/switchover and opened its ports for clients. There still might be initialization steps to complete if event 21-21271 is not generated immediately after this message.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21271 [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully operational in primary mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized, and is in fully writable primary master server mode for the Configuration Database.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21272
  [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully synchronized in backup mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized as the backup server of the currently running primary server. You can only switch over this server to primary mode after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21273
  [+] show details
  Level
  Standard
  Text
  Proxy Configuration Server is fully synchronized with master server
  Attributes
  None
  Description
  Reports that Configuration Server in proxy mode is fully operational. If server is in primary mode, it is confirmed with this message. If server is in backup mode, you are free to switch over to primary mode at any time after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25300
  [+] show details
  Level
  Standard
  Text
  Backup Server ignored because server is starting in upgrade mode [1]
  Attributes
  [1]
  Type of upgrade mode. Currently, only one upgrade mode is available: 1 (simple).
  Description
  The master Configuration Server is in upgrade mode, and is starting in backup mode. The backup Configuration Server will switch to primary mode and will be ignored by the primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25301
  [+] show details
  Level
  Standard
  Text
  Configuration Server entered upgrade mode. Backup Server ignored because of incompatible schema [<schema>]
  Attributes
  <schema>
  Configuration Database schema
  Description
  The master Configuration Server has detected an older primary Configuration Server and is initializing as the primary server. The older primary Configuration Server will switch over to backup mode and be ignored by the newer primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25302
  [+] show details
  Level
  Standard
  Text
  Configuration Server ignored switchover request because another upgrade/switchover already in progress
  Attributes
  None
  Description
  Reports Configuration Server ignored a switchover request from Solution Control Server, most likely because Configuration Server is in upgrade mode. During upgrade, Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe this log event reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **Support for IBM DB2 10.5 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for the VMware ESXi 6 virtualization environment. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported virtual machines.**
* **Improved migration of HA Configuration Servers: You can now allow an upgraded version of Configuration Server to run alongside its HA partner that is not upgraded, for a brief period of time. This provides for a more streamlined migration procedure, with less downtime for clients.
  As part of this new functionality, the following new Configuration Server Log Events are used to track the procedure:**
* **21-21270 [+] show details
  Level
  Standard
  Text
  Configuration Server ready to accept client connections.
  Attributes
  None
  Description
  Reports that Configuration Server has completed initialization/switchover and opened its ports for clients. There still might be initialization steps to complete if event 21-21271 is not generated immediately after this message.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21271 [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully operational in primary mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized, and is in fully writable primary master server mode for the Configuration Database.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21272
  [+] show details
  Level
  Standard
  Text
  Master Configuration Server is fully synchronized in backup mode
  Attributes
  None
  Description
  Reports that Configuration Server is fully initialized as the backup server of the currently running primary server. You can only switch over this server to primary mode after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-21273
  [+] show details
  Level
  Standard
  Text
  Proxy Configuration Server is fully synchronized with master server
  Attributes
  None
  Description
  Reports that Configuration Server in proxy mode is fully operational. If server is in primary mode, it is confirmed with this message. If server is in backup mode, you are free to switch over to primary mode at any time after this message is generated.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25300
  [+] show details
  Level
  Standard
  Text
  Backup Server ignored because server is starting in upgrade mode [1]
  Attributes
  [1]
  Type of upgrade mode. Currently, only one upgrade mode is available: 1 (simple).
  Description
  The master Configuration Server is in upgrade mode, and is starting in backup mode. The backup Configuration Server will switch to primary mode and will be ignored by the primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25301
  [+] show details
  Level
  Standard
  Text
  Configuration Server entered upgrade mode. Backup Server ignored because of incompatible schema [<schema>]
  Attributes
  <schema>
  Configuration Database schema
  Description
  The master Configuration Server has detected an older primary Configuration Server and is initializing as the primary server. The older primary Configuration Server will switch over to backup mode and be ignored by the newer primary Configuration Server until the upgrade operation is completed.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **21-25302
  [+] show details
  Level
  Standard
  Text
  Configuration Server ignored switchover request because another upgrade/switchover already in progress
  Attributes
  None
  Description
  Reports Configuration Server ignored a switchover request from Solution Control Server, most likely because Configuration Server is in upgrade mode. During upgrade, Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe this log event reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
  Alarm Advisory
  None
  Action
  Take the appropriate action according to step 7 of Upgrading an HA Pair of Configuration Servers.**
* **Support for IBM DB2 10.5 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for the VMware ESXi 6 virtualization environment. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported virtual machines.**

### **Resolved issues:**

## **Release 8.5.100.22 (09/02/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.22 | 09/02/16 | General |  | X | X | X | X |

### New Features:

* **More secure connections to Centralized Log: Configuration Server can now use Single or Mutual TLS to secure a connection to the Message Server designated for the Centralized Log. Refer to the Secure Network Logging Deployment Procedure for more information and instructions for setting up this connection.**
* **More secure connections to Centralized Log: Configuration Server can now use Single or Mutual TLS to secure a connection to the Message Server designated for the Centralized Log. Refer to the Secure Network Logging Deployment Procedure for more information and instructions for setting up this connection.**
* **More secure connections to Centralized Log: Configuration Server can now use Single or Mutual TLS to secure a connection to the Message Server designated for the Centralized Log. Refer to the Secure Network Logging Deployment Procedure for more information and instructions for setting up this connection.**
* **More secure connections to Centralized Log: Configuration Server can now use Single or Mutual TLS to secure a connection to the Message Server designated for the Centralized Log. Refer to the Secure Network Logging Deployment Procedure for more information and instructions for setting up this connection.**
* **More secure connections to Centralized Log: Configuration Server can now use Single or Mutual TLS to secure a connection to the Message Server designated for the Centralized Log. Refer to the Secure Network Logging Deployment Procedure for more information and instructions for setting up this connection.**

### **Resolved issues:**

## **Release 8.5.100.24 (10/03/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.24 | 10/03/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.25 (11/04/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.25 | 11/04/16 | General |  | X | X | X | X |

### New Features:

* **Monitoring Configuration Performance: New scripts in the Configuration Database Maintenance Scripts IP enable you to trace the configuration areas that consume most of the Configuration Server resources, both overall and for particular types of clients. Use these with the audit trail logs to identify events signalling an increase in the data size object count. For more information about the new scripts, refer to the Release Note for Configuration Database Maintenance Scripts 8.5.100.11.**
* **Monitoring Configuration Performance: New scripts in the Configuration Database Maintenance Scripts IP enable you to trace the configuration areas that consume most of the Configuration Server resources, both overall and for particular types of clients. Use these with the audit trail logs to identify events signalling an increase in the data size object count. For more information about the new scripts, refer to the Release Note for Configuration Database Maintenance Scripts 8.5.100.11.**
* **Monitoring Configuration Performance: New scripts in the Configuration Database Maintenance Scripts IP enable you to trace the configuration areas that consume most of the Configuration Server resources, both overall and for particular types of clients. Use these with the audit trail logs to identify events signalling an increase in the data size object count. For more information about the new scripts, refer to the Release Note for Configuration Database Maintenance Scripts 8.5.100.11.**
* **Monitoring Configuration Performance: New scripts in the Configuration Database Maintenance Scripts IP enable you to trace the configuration areas that consume most of the Configuration Server resources, both overall and for particular types of clients. Use these with the audit trail logs to identify events signalling an increase in the data size object count. For more information about the new scripts, refer to the Release Note for Configuration Database Maintenance Scripts 8.5.100.11.**
* **Monitoring Configuration Performance: New scripts in the Configuration Database Maintenance Scripts IP enable you to trace the configuration areas that consume most of the Configuration Server resources, both overall and for particular types of clients. Use these with the audit trail logs to identify events signalling an increase in the data size object count. For more information about the new scripts, refer to the Release Note for Configuration Database Maintenance Scripts 8.5.100.11.**

### **Resolved issues:**

## **Release 8.5.101.00 (12/16/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.00 | 12/16/16 | General |  | X | X | X | X |

### New Features:

* **Configuration Server no longer requires License Resource Manager (LRM) 8.5 to be present in the environment at any time.**
* **Configuration Server can now use Windows Authentication to access an MS SQL Configuration Database.**
* **Starting in this release, Configuration Server external authentication uses OpenSSL version 1.0.2j for secure connections to LDAP Servers.**
* **Configuration Server no longer requires License Resource Manager (LRM) 8.5 to be present in the environment at any time.**
* **Configuration Server can now use Windows Authentication to access an MS SQL Configuration Database.**
* **Starting in this release, Configuration Server external authentication uses OpenSSL version 1.0.2j for secure connections to LDAP Servers.**
* **Configuration Server no longer requires License Resource Manager (LRM) 8.5 to be present in the environment at any time.**
* **Configuration Server can now use Windows Authentication to access an MS SQL Configuration Database.**
* **Starting in this release, Configuration Server external authentication uses OpenSSL version 1.0.2j for secure connections to LDAP Servers.**
* **Configuration Server no longer requires License Resource Manager (LRM) 8.5 to be present in the environment at any time.**
* **Configuration Server can now use Windows Authentication to access an MS SQL Configuration Database.**
* **Starting in this release, Configuration Server external authentication uses OpenSSL version 1.0.2j for secure connections to LDAP Servers.**
* **Configuration Server no longer requires License Resource Manager (LRM) 8.5 to be present in the environment at any time.**
* **Configuration Server can now use Windows Authentication to access an MS SQL Configuration Database.**
* **Starting in this release, Configuration Server external authentication uses OpenSSL version 1.0.2j for secure connections to LDAP Servers.**

### **Resolved issues:**

## **Release 8.5.101.01 (01/27/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.01 | 01/27/17 | General |  | X | X | X | X |

### New Features:

* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**
* **Configuration Database Monitoring Scripts can now be run from the command line.**
* **HA Configuration Servers can now be migrated from 8.1.3 to 8.5.101 without loss of backup functionality, if they are using the same 8.1.1 Configuration Database.**

### **Resolved issues:**

## **Release 8.5.101.04 (03/03/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.04 | 03/03/17 | General |  | X | X | X | X |

### New Features:

* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Configuration Server or Configuration Server Proxy from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before the log configuration can be loaded from the main Configuration Database.**
* **Increased Kerberos token size: For external authentication, the maximum accepted Kerberos token size has been increased from 12 KB to 64 KB.**

### **Resolved issues:**

## **Release 8.5.101.05 (04/07/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.05 | 04/07/17 | General |  | X | X | X | X |

### New Features:

* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Configuration Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**

### **Resolved issues:**

## **Release 8.5.101.07 (05/05/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.07 | 05/05/17 | General |  | X | X | X | X |

### New Features:

* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**
* **Keep-Alive mechanism for LDAP external authentication: You can increase the robustness of the external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). For more information about this new functionality, refer to "Network Connectivity Options for LDAP" in the Framework External Authentication Options Reference Manual.**

### **Resolved issues:**

## **Release 8.5.101.08 (06/05/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.08 | 06/05/17 | General |  | X | X | X | X |

### New Features:

* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**
* **Configuration Server Proxy management port support: You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. If the port not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option. To specify this port, use the following new configuration option in the [csproxy] section of the Configuration Server Proxy Application object.
  management-port
  Default Value: No default value
  Valid Values: Any valid TCP/IP port
  Changes Take Effect: After restart
  Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server Proxy. If not specified, management agents cannot monitor and control the operation of Configuration Server Proxy. You cannot set this option to the value specified for the port option.
  The default management ports specified by the management-port options in Configuration Server and Configuration Server Proxy Application objects open just after the components are initialized and just before the following log messages are generated:
  21-22171 Master Configuration Server is fully operational in primary mode
  21-22172 Master Configuration Server is fully synchronized in backup mode
  21-22173 Proxy Configuration Server is fully synchronized with master server**
* **21-22171 Master Configuration Server is fully operational in primary mode**
* **21-22172 Master Configuration Server is fully synchronized in backup mode**
* **21-22173 Proxy Configuration Server is fully synchronized with master server**
* **Enhanced interoperability between Configuration Server Proxy 8.5 and Configuration Server 8.1.3 during migration: Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. The proxy server can add, update, and modify the data as required.**

### **Resolved issues:**

## **Release 8.5.101.10 (07/07/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.10 | 07/07/17 | General |  | X | X | X | X |

### New Features:

* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**
* **Improved Connections Between Configuration Servers: You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. If the timeout expires, all pending connection requests are cancelled, enabling the connection to be made. Without the timeout, the connecting client might eventually stop trying to reconnect, and then stop responding completely because of network issues. This timeout applies to the following connections:
  Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server
  Backup master Configuration Server connecting as a client to primary master Configuration Server
  Backup Configuration Server Proxy connecting as a client to primary Configuration Server ProxyTo set the timeout, use the new command-line parameter -cfglib-conn-async-tmout (default 20 seconds). For the backup master Configuration Server, you can use this command-line parameter or you can set the new option cfglib-conn-async-tmout (default 20 seconds) in the configuration file instead. The value of this option overrides that set by the command-line parameter. For more information, refer to the Framework Deployment Guide for the new command-line parameter, or to the
  Framework Configuration Options Reference Manual for the new option.**
* **Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server**
* **Backup master Configuration Server connecting as a client to primary master Configuration Server**
* **Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy**
* **Support for deployment of Genesys Applications in single sign-on environments: Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. Refer to application-specific documentation to determine if the application supports this, and if so, to confirm deployment requirements.**

### **Resolved issues:**

## **Release 8.5.101.11 (08/22/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.11 | 08/22/17 | General |  | X | X | X | X |

### New Features:

* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**

### **Resolved issues:**

## **Release 8.5.101.13 (09/26/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.13 | 09/26/17 | General |  | X | X | X | X |

### New Features:

* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**

### **Resolved issues:**

## **Release 8.5.101.17 (11/10/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.17 | 11/10/17 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

IVR Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Message Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.100.02  04/10/15  General  8.5.100.04  12/22/15  General  8.5.100.04  12/22/15  General  8.5.100.04  12/22/15  General |  | 8.5.100.14  08/22/17  General | 10  8  8  8 | 8.5.100.14  08/22/17  General | 10  8  8  8 |

## **Release 8.5.100.02 (04/10/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.02 | 04/10/15 | General |  | X | X | X | X |

### New Features:

* **Secure connections to Oracle databases: You can now configure secure connections between Message Server and Oracle databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Default threading mode is single-threaded: Genesys recommends that you do not change the threading mode for the current version of Message Server. Refer to the Network Connectivity section of the Framework Deployment Guide for more information.**

### **Resolved issues:**

## **Release 8.5.100.03 (10/09/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.03 | 10/09/15 | General |  | X | X | X | X |

### New Features:

* **Instructions for upgrading Message Server to release 8.5 and later have been completely rewritten in a more concise and clearer manner. Refer to the Framework Migration Guide.**

### **Resolved issues:**

## **Release 8.5.100.04 (12/22/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.04 | 12/22/15 | General |  | X | X | X | X |

### New Features:

* **To simplify troubleshooting of secure connections, Message Server now offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **To simplify troubleshooting of secure connections, Message Server now offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **To simplify troubleshooting of secure connections, Message Server now offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**
* **To simplify troubleshooting of secure connections, Message Server now offers additional logging of the secure connection establishment phase when used with Security Pack 8.5.100.06 or newer.**

### **Resolved issues:**

## **Release 8.5.100.08 (04/29/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.08 | 04/29/16 | General |  | X | X | X | X |

### New Features:

* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**
* **Support for MS SQL Server 2014 database. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported databases.**

### **Resolved issues:**

## **Release 8.5.100.09 (06/03/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.09 | 06/03/16 | General |  | X | X | X | X |

### New Features:

* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**

### **Resolved issues:**

## **Release 8.5.100.10 (07/08/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.10 | 07/08/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.11 (11/04/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.11 | 11/04/16 | General |  | X | X | X | X |

### New Features:

* **New and modified scripts for initializing Log Database: A new Message Server script, drop\_tables\_<DBMS>.sql drops existing tables and procedures. The existing Log Database initialization scripts, init\_<DBMS>.sql and init\_multilang\_<DBMS>.sql, no longer drop existing tables and procedures. Run drop\_tables\_<DBMS>.sql before running the initialization scripts if you have to re-initialize an existing Log Database.**
* **New and modified scripts for initializing Log Database: A new Message Server script, drop\_tables\_<DBMS>.sql drops existing tables and procedures. The existing Log Database initialization scripts, init\_<DBMS>.sql and init\_multilang\_<DBMS>.sql, no longer drop existing tables and procedures. Run drop\_tables\_<DBMS>.sql before running the initialization scripts if you have to re-initialize an existing Log Database.**
* **New and modified scripts for initializing Log Database: A new Message Server script, drop\_tables\_<DBMS>.sql drops existing tables and procedures. The existing Log Database initialization scripts, init\_<DBMS>.sql and init\_multilang\_<DBMS>.sql, no longer drop existing tables and procedures. Run drop\_tables\_<DBMS>.sql before running the initialization scripts if you have to re-initialize an existing Log Database.**
* **New and modified scripts for initializing Log Database: A new Message Server script, drop\_tables\_<DBMS>.sql drops existing tables and procedures. The existing Log Database initialization scripts, init\_<DBMS>.sql and init\_multilang\_<DBMS>.sql, no longer drop existing tables and procedures. Run drop\_tables\_<DBMS>.sql before running the initialization scripts if you have to re-initialize an existing Log Database.**

### **Resolved issues:**

## **Release 8.5.100.12 (01/27/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.12 | 01/27/17 | General |  | X | X | X | X |

### New Features:

* **Message Server can now use Windows Authentication to access an MS SQL Log Database. To implement this, refer to step 3 of
  Deploying Message Server.**
* **Message Server can now use Windows Authentication to access an MS SQL Log Database. To implement this, refer to step 3 of
  Deploying Message Server.**
* **Message Server can now use Windows Authentication to access an MS SQL Log Database. To implement this, refer to step 3 of
  Deploying Message Server.**
* **Message Server can now use Windows Authentication to access an MS SQL Log Database. To implement this, refer to step 3 of
  Deploying Message Server.**

### **Resolved issues:**

## **Release 8.5.100.13 (04/07/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.13 | 04/07/17 | General |  | X | X | X | X |

### New Features:

* **Bootstrap logging: You can now specify an initial logging configuration when starting Message Server from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before Message Server loads its log configuration from the Configuration Database.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Message Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Message Server from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before Message Server loads its log configuration from the Configuration Database.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Message Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Message Server from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before Message Server loads its log configuration from the Configuration Database.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Message Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Message Server from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before Message Server loads its log configuration from the Configuration Database.**
* **Secure Connections to PostgreSQL Databases: You can now configure secure connections between Message Server and PostgreSQL databases. Refer to the Environment Settings section of the Framework Database Connectivity Reference Guide.**

### **Resolved issues:**

## **Release 8.5.100.14 (08/22/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.14 | 08/22/17 | General |  | X | X | X | X |

### New Features:

* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **As of 9/26/17, Message Server supports the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **As of 9/26/17, Message Server supports the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **As of 9/26/17, Message Server supports the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **As of 9/26/17, Message Server supports the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**

### **Resolved issues:**

Solution Control Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.100.20  11/04/16  General  8.5.100.20  11/04/16  General |  | 8.5.100.25  08/22/17  General | 5  5 | 8.5.100.25  08/22/17  General | 5  5 |

## **Release 8.5.100.20 (11/04/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.20 | 11/04/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.21 (12/16/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.21 | 12/16/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.22 (04/07/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.22 | 04/07/17 | General |  | X | X | X | X |

### New Features:

* **Bootstrap logging: You can now specify an initial logging configuration when starting Solution Control Server from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before Solution Control Server loads its log configuration from the Configuration Database. An example of how this new feature can be used is described in the Resolved Issue below.**
* **Bootstrap logging: You can now specify an initial logging configuration when starting Solution Control Server from the command line. This provides logs to assist you in troubleshooting startup and connectivity issues that occur before Solution Control Server loads its log configuration from the Configuration Database. An example of how this new feature can be used is described in the Resolved Issue below.**

### **Resolved issues:**

## **Release 8.5.100.24 (05/05/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.24 | 05/05/17 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.25 (08/22/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.25 | 08/22/17 | General |  | X | X | X | X |

### New Features:

* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **As of 9/26/17, Solution Control Server supports the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**
* **Support for the Windows 2016 64-bit operating system. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **As of 9/26/17, Solution Control Server supports the Microsoft Hyper-V Server 2016 virtualization platform. Refer to the Supported Operating Environment: Display by Product, Operating System, and Other page for more detailed information and a list of all supported virtualization platforms.**

### **Resolved issues:**

SNMP Master Agent

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.100.07  10/09/15  General  8.5.100.07  10/09/15  General |  | 8.5.100.08  10/04/17  Hot Fix | 2  2 | 8.5.100.08  10/04/17  Hot Fix | 2  2 |

## **Release 8.5.100.07 (10/09/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.07 | 10/09/15 | General |  | X | X | X | X |

### New Features:

* **Instructions for upgrading SNMP Master Agent to release 8.5 and later have been completely rewritten in a more concise and clear manner. Refer to the Framework Migration Guide.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system was added on June 3, 2016. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**
* **Instructions for upgrading SNMP Master Agent to release 8.5 and later have been completely rewritten in a more concise and clear manner. Refer to the Framework Migration Guide.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system was added on June 3, 2016. See the Supported Operating Environment: Framework page for more detailed information and a list of all supported operating systems.**

### **Resolved issues:**

## **Release 8.5.100.08 (10/04/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.08 | 10/04/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

DB Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Chat Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.1.000.26  04/17/15  General  8.5.108.03  05/03/17  General  8.5.108.03  05/03/17  General  8.5.109.06  06/26/17  General  8.5.109.06  06/26/17  General |  | 8.5.201.07  09/08/17  Hot Fix | 14  4  4  3  3 | 8.5.201.07  09/08/17  Hot Fix | 14  4  4  3  3 |

## **Release 8.5.000.30 (04/17/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.30 | 04/17/15 | General |  | X | X | X | X |

### New Features:

* **The default values of the following options have changed:
  In the [log] section: verbose
  In the [log-filter-data] section: MessageText
  In the [settings] section: flex-disconnect-timeout, max-waiting-requests, message-log-print-size, stop-abandoned-interaction, user-register-timeout.**
* **In the [log] section: verbose**
* **In the [log-filter-data] section: MessageText**
* **In the [settings] section: flex-disconnect-timeout, max-waiting-requests, message-log-print-size, stop-abandoned-interaction, user-register-timeout.**
* **You can enhance performance by limiting the maximum number of chat sessions that each Chat Server can accept and/or restore.**
* **You can enable and configure masking of sensitive data (such as credit card numbers, Social Security numbers, and other patterns) in logs and transcripts.**
* **Support for UTF-8.**
* **Support for the following operating systems. See the Supported Operating Environment: eServices page for more detailed information and a list of all supported operating systems.
  Windows Server 2012
  Red Hat Enterprise Linux 6**
* **Windows Server 2012**
* **Red Hat Enterprise Linux 6**

### **Resolved issues:**

## **Release 8.5.101.07 (07/31/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.07 | 07/31/15 | General |  | X | X | X | X |

### New Features:

* **In High Availability mode, Chat Server now restores interrupted sessions only if it is properly configured for High Availability. In particular, setting session-restoration-mode to simple (which enables Chat Server's session restoration functionality) has no effect unless transcript-auto-save is enabled (has a valid positive value).**
* **The option attach-session-statistics is added. If this option is set to all or fired, Chat Server generates statistics about the chat transcript and attaches them to the interaction's user data at the end of the chat session.**

### **Resolved issues:**

## **Release 8.5.102.08 (10/09/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.08 | 10/09/15 | General |  | X | X | X | X |

### New Features:

* **It is possible to establish inactivity control monitoring, which automatically closes inactive chat sessions.**
* **Chat Server can replace all digits in typing preview content, if desired for purposes of masking sensitive information.**
* **Chat Server can output KPI counters to logs, monitoring the health of the chat deployment.**
* **Log messages are improved, making tracing of activity more efficient.**
* **Support for the following operating systems.See the Supported Operating Environment: eServices page for more detailed information and a list of all supported operating systems.
  Windows Server 2012 Hyper-V
  Red Hat Enterprise Linux 7**
* **Windows Server 2012 Hyper-V**
* **Red Hat Enterprise Linux 7**

### **Resolved issues:**

## **Release 8.5.103.22 (01/06/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.22 | 01/06/16 | General |  | X | X | X | X |

### New Features:

* **In Chat Server the personally identifiable information (PII) configuration can now be read from UCS, where it must be specified by the Privacy Manager (GAX plugin). This expands the currently available ability of the Chat Server configuration to mask sensitive data. See the Chat Server Administration Guide for more information. Note: UCS 8.5.200.08 or later is required.**
* **Chat Server now publishes Key Performance Indicator (KPI) counters about the server performance through the HTTP API interface. See the Chat Server Administration Guide for more information.**
* **Chat Server now prints application configurations in the header of log files to assist with troubleshooting.**

### **Resolved issues:**

## **Release 8.5.104.07 (03/28/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.07 | 03/28/16 | General |  | X | X | X | X |

### New Features:

* **To provide better scalability, high availability, and reduce the UCS load, Chat Server now supports optional storage of intermediate transcripts in Cassandra. Please see Deploying Chat Server with Cassandra for more information.**

### **Resolved issues:**

## **Release 8.5.104.08 (04/06/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.08 | 04/06/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.104.10 (04/22/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.10 | 04/22/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.105.05 (07/29/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.105.05 | 07/29/16 | General |  | X | X | X | X |

### New Features:

* **Documentation regarding data retention (TTL) and sample initialization scripts for automating cleanup procedures in case of failure.**
* **Ability for agent to alter participant nicknames while a chat session is in progress.**
* **Improvement to Chat Server load control management (configuration option limit-for-reply-delay). This improvement is essential for deployments running several Chat Server instances.**
* **New key-value pairs attached at the end of a session describing the reason that the session ended:
  csg\_SessionEndedBy indicates the type of user that initiated the end of the session: CLIENT (i.e. end customer), AGENT, SUPERVISOR, SYSTEM.
  csg\_SessionEndedReason describes how the session was closed: DISCONNECT, QUIT (participant logged out), FORCE (participant requested that the session be closed), INACTIVE, DB\_ERROR**
* **csg\_SessionEndedBy indicates the type of user that initiated the end of the session: CLIENT (i.e. end customer), AGENT, SUPERVISOR, SYSTEM.**
* **csg\_SessionEndedReason describes how the session was closed: DISCONNECT, QUIT (participant logged out), FORCE (participant requested that the session be closed), INACTIVE, DB\_ERROR**
* **Support of read receipt notifications. Notification can be used by widgets and desktops to display read receipts to agents and customers.\***
* **Ability to send notifications to participants when an agent or supervisor joins a chat session for coaching or silent monitoring, based on configuration. The notification message can then be used by Chat Widget or Desktop to notify the respective attendees.\***

### **Resolved issues:**

## **Release 8.5.106.10 (11/14/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.106.10 | 11/14/16 | General |  | X | X | X | X |

### New Features:

* **Inactivity control configurations can be set differently for each chat session, either manually by a request from the agent desktop (currently supported only for custom desktops) or triggered by the workflow.**
* **A new configuration option, unmask-live-dialog (section [transcript-cleanup]), makes it possible to suppress sensitive data masking (when enabled) in an ongoing chat session only for the customer and the active/serving agent, keeping it masked for other participants and in the contact history transcript.**
* **Chat Server provides control and notification API for GMS and Workspace (supported by Desktop Edition only, not supported by Web Edition) for bidirectional file transfer between a customer and an agent. See File Transfer for more information.**
* **New health metrics about Cassandra operation were added.**
* **eServices Administrator's Guide (Chat Server Administration) was rearranged and extended with several useful topics.**

### **Resolved issues:**

## **Release 8.5.107.11 (03/24/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.11 | 03/24/17 | General |  | X | X | X | X |

### New Features:

* **Chat Server now supports case-insensitive file extensions (see the option upload-file-types).**
* **A language code can be assigned for every chat session. This language code is used to display inactivity control messages according to the language configuration in Configuration Server.**
* **The end session and transcript statistic are always attached to an interaction in Interaction Server. Previously, depending on the value of the stop-abandoned-interaction option, the end session and transcript statistic were not always attached.**
* **Two new configuration options, message-alert2 and timeout-alert2, allow you to specify an additional intermediate timer for inactivity monitoring control. See documentation for more details.**
* **A new configuration option, security-token-size, allows you to increase the security token length in a chat protocol.**
* **New documentation topics:**
* **How to send messages from routing workflow/strategies in different languages.**
* **How Chat Server reports end session reason codes and transcript statistics.**

### **Resolved issues:**

## **Release 8.5.108.03 (05/03/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.108.03 | 05/03/17 | General |  | X | X | X | X |

### New Features:

* **Chat Server now supports push notifications about session activity via flex protocol, which is required by GMS for CometD support.**
* **Chat Server now provides the ability to send a direct message in a chat conference and/or coaching mode. For example, in a conference with 3 agents, an agent can send a direct message to another agent, and this message will not be visible to the third agent.**
* **Chat Server now supports push notifications about session activity via flex protocol, which is required by GMS for CometD support.**
* **Chat Server now provides the ability to send a direct message in a chat conference and/or coaching mode. For example, in a conference with 3 agents, an agent can send a direct message to another agent, and this message will not be visible to the third agent.**
* **Chat Server now supports push notifications about session activity via flex protocol, which is required by GMS for CometD support.**
* **Chat Server now provides the ability to send a direct message in a chat conference and/or coaching mode. For example, in a conference with 3 agents, an agent can send a direct message to another agent, and this message will not be visible to the third agent.**

### **Resolved issues:**

## **Release 8.5.109.06 (06/26/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.109.06 | 06/26/17 | General |  | X | X | X | X |

### New Features:

* **GMS CometD support improvements.**
* **Agent and supervisor participants can now be marked as automated chat bot participants, which implies a special handling during session closure and for reporting purposes.**
* **Chat Server can now associate an optional session password (a crypto-random security token) with the chat session ID. This feature prevents join attempts from unintended participants.**
* **If any PII rule is executed for a chat message, Chat Server now attaches information about what was changed/modified or detected in the message.**
* **GMS CometD support improvements.**
* **Agent and supervisor participants can now be marked as automated chat bot participants, which implies a special handling during session closure and for reporting purposes.**
* **Chat Server can now associate an optional session password (a crypto-random security token) with the chat session ID. This feature prevents join attempts from unintended participants.**
* **If any PII rule is executed for a chat message, Chat Server now attaches information about what was changed/modified or detected in the message.**
* **GMS CometD support improvements.**
* **Agent and supervisor participants can now be marked as automated chat bot participants, which implies a special handling during session closure and for reporting purposes.**
* **Chat Server can now associate an optional session password (a crypto-random security token) with the chat session ID. This feature prevents join attempts from unintended participants.**
* **If any PII rule is executed for a chat message, Chat Server now attaches information about what was changed/modified or detected in the message.**
* **GMS CometD support improvements.**
* **Agent and supervisor participants can now be marked as automated chat bot participants, which implies a special handling during session closure and for reporting purposes.**
* **Chat Server can now associate an optional session password (a crypto-random security token) with the chat session ID. This feature prevents join attempts from unintended participants.**
* **If any PII rule is executed for a chat message, Chat Server now attaches information about what was changed/modified or detected in the message.**
* **GMS CometD support improvements.**
* **Agent and supervisor participants can now be marked as automated chat bot participants, which implies a special handling during session closure and for reporting purposes.**
* **Chat Server can now associate an optional session password (a crypto-random security token) with the chat session ID. This feature prevents join attempts from unintended participants.**
* **If any PII rule is executed for a chat message, Chat Server now attaches information about what was changed/modified or detected in the message.**

### **Resolved issues:**

## **Release 8.5.201.05 (08/23/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.201.05 | 08/23/17 | General |  |  | X |  | X |

### New Features:

* **Redesigned Chat Server IP to align with new Genesys branding.**
* **Chat Server now accepts event attributes in nested lists in ESP requests from a workflow.**
* **A new configuration option, allow-duplicated-kvp, allows you to prohibit duplicated key-value pairs in userdata and event attributes in chat protocol requests.**
* **Chat Server now attaches an additional set of chat session characteristics at the end of each chat session. For more information on these chat session characteristics, refer to the Chat Server Reporting Data section in the Administrator's Guide.**
* **Chat Server now allows you to retain the latest version of the intermediate transcript in the Cassandra Database when Cassandra is used for High Availability mode.**
* **Improved support for GMS CometD, including combined flex join and subscription, repeating reply as push-notification, and return transcript in system notice reply.**
* **Redesigned Chat Server IP to align with new Genesys branding.**
* **Chat Server now accepts event attributes in nested lists in ESP requests from a workflow.**
* **A new configuration option, allow-duplicated-kvp, allows you to prohibit duplicated key-value pairs in userdata and event attributes in chat protocol requests.**
* **Chat Server now attaches an additional set of chat session characteristics at the end of each chat session. For more information on these chat session characteristics, refer to the Chat Server Reporting Data section in the Administrator's Guide.**
* **Chat Server now allows you to retain the latest version of the intermediate transcript in the Cassandra Database when Cassandra is used for High Availability mode.**
* **Improved support for GMS CometD, including combined flex join and subscription, repeating reply as push-notification, and return transcript in system notice reply.**
* **Redesigned Chat Server IP to align with new Genesys branding.**
* **Chat Server now accepts event attributes in nested lists in ESP requests from a workflow.**
* **A new configuration option, allow-duplicated-kvp, allows you to prohibit duplicated key-value pairs in userdata and event attributes in chat protocol requests.**
* **Chat Server now attaches an additional set of chat session characteristics at the end of each chat session. For more information on these chat session characteristics, refer to the Chat Server Reporting Data section in the Administrator's Guide.**
* **Chat Server now allows you to retain the latest version of the intermediate transcript in the Cassandra Database when Cassandra is used for High Availability mode.**
* **Improved support for GMS CometD, including combined flex join and subscription, repeating reply as push-notification, and return transcript in system notice reply.**
* **Redesigned Chat Server IP to align with new Genesys branding.**
* **Chat Server now accepts event attributes in nested lists in ESP requests from a workflow.**
* **A new configuration option, allow-duplicated-kvp, allows you to prohibit duplicated key-value pairs in userdata and event attributes in chat protocol requests.**
* **Chat Server now attaches an additional set of chat session characteristics at the end of each chat session. For more information on these chat session characteristics, refer to the Chat Server Reporting Data section in the Administrator's Guide.**
* **Chat Server now allows you to retain the latest version of the intermediate transcript in the Cassandra Database when Cassandra is used for High Availability mode.**
* **Improved support for GMS CometD, including combined flex join and subscription, repeating reply as push-notification, and return transcript in system notice reply.**
* **Redesigned Chat Server IP to align with new Genesys branding.**
* **Chat Server now accepts event attributes in nested lists in ESP requests from a workflow.**
* **A new configuration option, allow-duplicated-kvp, allows you to prohibit duplicated key-value pairs in userdata and event attributes in chat protocol requests.**
* **Chat Server now attaches an additional set of chat session characteristics at the end of each chat session. For more information on these chat session characteristics, refer to the Chat Server Reporting Data section in the Administrator's Guide.**
* **Chat Server now allows you to retain the latest version of the intermediate transcript in the Cassandra Database when Cassandra is used for High Availability mode.**
* **Improved support for GMS CometD, including combined flex join and subscription, repeating reply as push-notification, and return transcript in system notice reply.**

### **Resolved issues:**

## **Release 8.5.201.07 (09/08/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.201.07 | 09/08/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

Universal Contact Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.1.1  08/21/14  General  8.1.1  08/21/14  General  8.5.0  08/21/14  General  8.5.0  08/21/14  General  8.5.100.04  01/20/15  General  8.5.100.04  01/20/15  General  8.5.100.04  01/20/15  General  8.5.200.17  12/07/16  General  8.5.200.17  12/07/16  General |  | 8.5.300.05  10/16/17  General | 11  11  11  11  9  9  9  3  3 | 8.5.300.05  10/16/17  General | 11  11  11  11  9  9  9  3  3 |

## **Release 8.5.000.12 (08/21/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.12 | 08/21/14 | General |  | X | X | X | X |

### New Features:

* **UCS now uses the NOLOCK select hint to improve performance when connected to a MSSQL database. (ESR-8149)**
* **UCS now allows HTML content in field codes while rendering a Standard Response. To enable this feature, start UCS with the -Dsrl-field-code-allow-html=true option. When enabled, agent's signatures that contain carriage returns will no longer be automatically replaced by
  HTML tag. (ESR-8045)**
* **UCS initialization scripts are now provided in two separate files:
  ucs\_drop\_<db>.sql—drop all tables
  ucs\_<db>.sql—create all tables (ESR-7958)**
* **ucs\_drop\_<db>.sql—drop all tables**
* **ucs\_<db>.sql—create all tables (ESR-7958)**
* **When creating, updating or deleting a Context Service profile, the core attributes are now automatically updated in the UCS Full Text Search index. This, for example, allows updating profiles with the Context Services API, and searching corresponding contacts using the Interaction Workspace quick search function. Previously, a complete index rebuild was necessary for such contact/profiles to be searchable in Full Text Search. Note that these updates are automatically applied every two minutes. (ESR-7913)**
* **UCS now uses the index update recovery functionality. If full text search index files are unavailable or UCS is stopped while index updates are still to be processed, those updates will be resumed as soon as files are available or UCS is restarted. (ESR-7782)**
* **UCS can now manage Full Text Search files locally on Primary and Backup applications. Index files no longer need to be shared on the network when the Primary and Backup are not on the same host. For more information, see Collocated and Distributed Deployment section of eService Administrator's Guide. (ESR-7256)**
* **The UCS queue is now long enough to handle a burst of ESP requests and respond to all of them. (ESR-7744)**
* **UCS now reports the INITIALIZING status instead of the START\_TRANSITION status to Solution Control Server (SCS) when starting. Previously, when the START\_TRANSITION status was reported, Solution Control Interface would allow sending a switchover request while the server was initializing, and could prevent UCS from starting successfully. (ESR-7740)**
* **UCS no longer silently discards requests when receiving bursts of more than 300 requests per second under a high load. Requests are now displayed in logs as soon as they are received instead of being buffered (ESR-7711)**
* **This release supports MS SQL Server 2012. (ESR-7682)**
* **This release supports Oracle 12c. (ESR-7680)**
* **This release supports Oracle 12g RAC. (ESR-7679)**
* **This release supports Windows 2012 Server. (ESR-7673)**
* **This release supports Windows Server 2012 64-bit native. (ESR-7672)**
* **UCS now uses the NOLOCK select hint to improve performance when connected to a MSSQL database. (ESR-8149)**
* **UCS now allows HTML content in field codes while rendering a Standard Response. To enable this feature, start UCS with the -Dsrl-field-code-allow-html=true option. When enabled, agent's signatures that contain carriage returns will no longer be automatically replaced by
  HTML tag. (ESR-8045)**
* **UCS initialization scripts are now provided in two separate files:
  ucs\_drop\_<db>.sql—drop all tables
  ucs\_<db>.sql—create all tables (ESR-7958)**
* **ucs\_drop\_<db>.sql—drop all tables**
* **ucs\_<db>.sql—create all tables (ESR-7958)**
* **When creating, updating or deleting a Context Service profile, the core attributes are now automatically updated in the UCS Full Text Search index. This, for example, allows updating profiles with the Context Services API, and searching corresponding contacts using the Interaction Workspace quick search function. Previously, a complete index rebuild was necessary for such contact/profiles to be searchable in Full Text Search. Note that these updates are automatically applied every two minutes. (ESR-7913)**
* **UCS now uses the index update recovery functionality. If full text search index files are unavailable or UCS is stopped while index updates are still to be processed, those updates will be resumed as soon as files are available or UCS is restarted. (ESR-7782)**
* **UCS can now manage Full Text Search files locally on Primary and Backup applications. Index files no longer need to be shared on the network when the Primary and Backup are not on the same host. For more information, see Collocated and Distributed Deployment section of eService Administrator's Guide. (ESR-7256)**
* **The UCS queue is now long enough to handle a burst of ESP requests and respond to all of them. (ESR-7744)**
* **UCS now reports the INITIALIZING status instead of the START\_TRANSITION status to Solution Control Server (SCS) when starting. Previously, when the START\_TRANSITION status was reported, Solution Control Interface would allow sending a switchover request while the server was initializing, and could prevent UCS from starting successfully. (ESR-7740)**
* **UCS no longer silently discards requests when receiving bursts of more than 300 requests per second under a high load. Requests are now displayed in logs as soon as they are received instead of being buffered (ESR-7711)**
* **This release supports MS SQL Server 2012. (ESR-7682)**
* **This release supports Oracle 12c. (ESR-7680)**
* **This release supports Oracle 12g RAC. (ESR-7679)**
* **This release supports Windows 2012 Server. (ESR-7673)**
* **This release supports Windows Server 2012 64-bit native. (ESR-7672)**
* **UCS now uses the NOLOCK select hint to improve performance when connected to a MSSQL database. (ESR-8149)**
* **UCS now allows HTML content in field codes while rendering a Standard Response. To enable this feature, start UCS with the -Dsrl-field-code-allow-html=true option. When enabled, agent's signatures that contain carriage returns will no longer be automatically replaced by
  HTML tag. (ESR-8045)**
* **UCS initialization scripts are now provided in two separate files:
  ucs\_drop\_<db>.sql—drop all tables
  ucs\_<db>.sql—create all tables (ESR-7958)**
* **ucs\_drop\_<db>.sql—drop all tables**
* **ucs\_<db>.sql—create all tables (ESR-7958)**
* **When creating, updating or deleting a Context Service profile, the core attributes are now automatically updated in the UCS Full Text Search index. This, for example, allows updating profiles with the Context Services API, and searching corresponding contacts using the Interaction Workspace quick search function. Previously, a complete index rebuild was necessary for such contact/profiles to be searchable in Full Text Search. Note that these updates are automatically applied every two minutes. (ESR-7913)**
* **UCS now uses the index update recovery functionality. If full text search index files are unavailable or UCS is stopped while index updates are still to be processed, those updates will be resumed as soon as files are available or UCS is restarted. (ESR-7782)**
* **UCS can now manage Full Text Search files locally on Primary and Backup applications. Index files no longer need to be shared on the network when the Primary and Backup are not on the same host. For more information, see Collocated and Distributed Deployment section of eService Administrator's Guide. (ESR-7256)**
* **The UCS queue is now long enough to handle a burst of ESP requests and respond to all of them. (ESR-7744)**
* **UCS now reports the INITIALIZING status instead of the START\_TRANSITION status to Solution Control Server (SCS) when starting. Previously, when the START\_TRANSITION status was reported, Solution Control Interface would allow sending a switchover request while the server was initializing, and could prevent UCS from starting successfully. (ESR-7740)**
* **UCS no longer silently discards requests when receiving bursts of more than 300 requests per second under a high load. Requests are now displayed in logs as soon as they are received instead of being buffered (ESR-7711)**
* **This release supports MS SQL Server 2012. (ESR-7682)**
* **This release supports Oracle 12c. (ESR-7680)**
* **This release supports Oracle 12g RAC. (ESR-7679)**
* **This release supports Windows 2012 Server. (ESR-7673)**
* **This release supports Windows Server 2012 64-bit native. (ESR-7672)**
* **UCS now uses the NOLOCK select hint to improve performance when connected to a MSSQL database. (ESR-8149)**
* **UCS now allows HTML content in field codes while rendering a Standard Response. To enable this feature, start UCS with the -Dsrl-field-code-allow-html=true option. When enabled, agent's signatures that contain carriage returns will no longer be automatically replaced by
  HTML tag. (ESR-8045)**
* **UCS initialization scripts are now provided in two separate files:
  ucs\_drop\_<db>.sql—drop all tables
  ucs\_<db>.sql—create all tables (ESR-7958)**
* **ucs\_drop\_<db>.sql—drop all tables**
* **ucs\_<db>.sql—create all tables (ESR-7958)**
* **When creating, updating or deleting a Context Service profile, the core attributes are now automatically updated in the UCS Full Text Search index. This, for example, allows updating profiles with the Context Services API, and searching corresponding contacts using the Interaction Workspace quick search function. Previously, a complete index rebuild was necessary for such contact/profiles to be searchable in Full Text Search. Note that these updates are automatically applied every two minutes. (ESR-7913)**
* **UCS now uses the index update recovery functionality. If full text search index files are unavailable or UCS is stopped while index updates are still to be processed, those updates will be resumed as soon as files are available or UCS is restarted. (ESR-7782)**
* **UCS can now manage Full Text Search files locally on Primary and Backup applications. Index files no longer need to be shared on the network when the Primary and Backup are not on the same host. For more information, see Collocated and Distributed Deployment section of eService Administrator's Guide. (ESR-7256)**
* **The UCS queue is now long enough to handle a burst of ESP requests and respond to all of them. (ESR-7744)**
* **UCS now reports the INITIALIZING status instead of the START\_TRANSITION status to Solution Control Server (SCS) when starting. Previously, when the START\_TRANSITION status was reported, Solution Control Interface would allow sending a switchover request while the server was initializing, and could prevent UCS from starting successfully. (ESR-7740)**
* **UCS no longer silently discards requests when receiving bursts of more than 300 requests per second under a high load. Requests are now displayed in logs as soon as they are received instead of being buffered (ESR-7711)**
* **This release supports MS SQL Server 2012. (ESR-7682)**
* **This release supports Oracle 12c. (ESR-7680)**
* **This release supports Oracle 12g RAC. (ESR-7679)**
* **This release supports Windows 2012 Server. (ESR-7673)**
* **This release supports Windows Server 2012 64-bit native. (ESR-7672)**

### **Resolved issues:**

## **Release 8.5.000.14 (04/10/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.14 | 04/10/15 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.04 (01/20/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.04 | 01/20/15 | General |  | X | X | X | X |

### New Features:

* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**
* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**
* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**
* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**
* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**
* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**
* **Oracle Driver is updated to version 11.2.0.4.0.**
* **PostgreSQL 9.3 is supported with the following limitations:
  No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.
  High availability and load balancing are not supported.**
* **No clustering: Although PostgreSQL supports clustering and replication streams, this release of UCS does not support those features.**
* **High availability and load balancing are not supported.**
* **When connected to an Oracle database, UCS now sets oracle.net.CONNECT\_TIMEOUT to 3000 (nine seconds). Previously, the database might accept the connection but never respond, in which case UCS's database connections remained stuck.**
* **When the max-connections option has a value of 0 (zero), the number of connections that Universal Contact Server can open simultaneously to this database is internally set to the default value of 40. Previously, UCS interpreted a value of 0 as meaning no connections and did not start.**
* **When connected to an Oracle database, UCS now sets oracle.jdbc.ReadTimeout to 5 minutes, so that a timeout occurs if no network packet is received within that period. Previously, network packets might be lost, which caused UCS's database connections to be permanently stuck. Note that in normal situations the DAP timeout is still taken into account.**

### **Resolved issues:**

## **Release 8.5.100.06 (04/10/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.06 | 04/10/15 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.07 (09/03/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.07 | 09/03/15 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.10 (10/23/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.10 | 10/23/15 | Hot Fix |  | X | X | X | X |

### New Features:

* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**
* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**
* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**
* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**
* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**
* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**
* **Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.**
* **UCS now provides three log messages to monitor its performance:**

### **Resolved issues:**

## **Release 8.5.200.08 (11/18/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.08 | 11/18/15 | General |  | X | X | X | X |

### New Features:

* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**
* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**
* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**
* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**
* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**
* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**
* **The default memory setting for JVM was increased to 2 GB, in order to avoid the system running out of memory or freezing while loading.**
* **The option time-format with the default value ISO8601 has been added to the [log] section. This sets the format of timestamps in log messages; the default was previously HH:MM:SS.sss.**
* **Masking of sensitive data is now enabled by default in the UCS template. You can modify this behavior using the default-filter-type option in the [log-filter] section.**

### **Resolved issues:**

## **Release 8.5.200.09 (03/30/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.09 | 03/30/16 | General |  | X | X | X | X |

### New Features:

* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**
* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**
* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**
* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**
* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**
* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**
* **UCS no longer generates a LogPrintStream err:Argument 'key' cannot be null or empty exception in console output for RMI connection logs.**
* **Interactions are correctly threaded when you engage a non-voice media from the Desktop.**

### **Resolved issues:**

## **Release 8.5.200.17 (12/07/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.17 | 12/07/16 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.200.19 (04/10/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.19 | 04/10/17 | Hot Fix |  | X | X | X | X |

### New Features:

* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**
* **The GetScreeningRules method now returns all screening rules, even if there are more than 2000. Previously, only the first 2000 were returned.**
* **UCS now uses the custom field code default value in scenarios where OMFieldCodes.RenderFieldCodes has no value with which to substitute a custom field code (for example: CompanyName). Previously in such a scenario, UCS would produce the following error: <$Error: No value provided or unknown identifier (CompanyName)$>.**

### **Resolved issues:**

## **Release 8.5.300.05 (10/16/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.300.05 | 10/16/17 | General |  | X | X | X | X |

### New Features:

* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**
* **UCS supports the new Genesys brand in this release.**
* **Support for the following Supported Operating Environment scenarios:**
* **Discontinued support for the following Supported Operating Environment scenarios:**

### **Resolved issues:**

E-mail Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.103.18  03/10/17  General  8.5.103.18  03/10/17  General  8.5.103.18  03/10/17  General |  | 8.5.104.17  11/09/17  Hot Fix | 8  8  8 | 8.5.104.17  11/09/17  Hot Fix | 8  8  8 |

## **Release 8.5.103.18 (03/10/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.18 | 03/10/17 | General |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.103.19 (03/23/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.19 | 03/23/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.103.20 (05/08/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.20 | 05/08/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.103.21 (05/25/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.21 | 05/25/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.103.22 (09/27/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.22 | 09/27/17 | Hot Fix |  | X | X | X | X |

### New Features:

* **This release improves logging to show when a POP client is picked up and scheduled.**
* **This release improves logging to show when a POP client is picked up and scheduled.**
* **This release improves logging to show when a POP client is picked up and scheduled.**

### **Resolved issues:**

## **Release 8.5.104.13 (07/26/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.13 | 07/26/17 | General |  | X | X | X | X |

### New Features:

* **The JavaMail used in this release is upgraded to version 1.5.6 (javax.mail.jar). As a result, the format used for email addresses now strictly follows
  RFC 3696 Section 3.**
* **E-mail Server Java now supports TLS 1.2.**
* **The JavaMail used in this release is upgraded to version 1.5.6 (javax.mail.jar). As a result, the format used for email addresses now strictly follows
  RFC 3696 Section 3.**
* **E-mail Server Java now supports TLS 1.2.**
* **The JavaMail used in this release is upgraded to version 1.5.6 (javax.mail.jar). As a result, the format used for email addresses now strictly follows
  RFC 3696 Section 3.**
* **E-mail Server Java now supports TLS 1.2.**

### **Resolved issues:**

## **Release 8.5.104.14 (10/12/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.14 | 10/12/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.104.17 (11/09/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.17 | 11/09/17 | Hot Fix |  | X | X | X | X |

### New Features:

* **E-mail Server now uses JavaMail 1.6.0 (javax.mail.jar). This version includes support for internationalized email addresses (RFC 6530/RFC 6531/RFC 6532). (ESR-13578)**
* **E-mail Server now uses JavaMail 1.6.0 (javax.mail.jar). This version includes support for internationalized email addresses (RFC 6530/RFC 6531/RFC 6532). (ESR-13578)**
* **E-mail Server now uses JavaMail 1.6.0 (javax.mail.jar). This version includes support for internationalized email addresses (RFC 6530/RFC 6531/RFC 6532). (ESR-13578)**

### **Resolved issues:**

Web API Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.1.2  09/30/14  General  8.1.200.03  09/30/14  General  8.1.200.03  09/30/14  General  8.1.200.05  09/30/14  General |  | 8.5.000.20  10/19/15  Hot Fix | 8  8  8  8 | 8.5.000.20  10/19/15  Hot Fix | 8  8  8  8 |

## **Release 8.5.000.09 (09/30/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.09 | 09/30/14 | General |  |  | X | X | X |

### New Features:

* **Includes the new Web Server API for RESTful chat interactions**
* **Exposes the ability to submit e-mail interactions from web forms**
* **Includes support for the following Host Operating System Support:
  Windows Server 2012 - 64 bit
  IBM AIX 7.1 - 64 bit
  Solaris 10 - 64 bit
  Red Hat Enterprise Linux 6 - 64 bit
  New Windows Server 2012 - Hyper-V**
* **Windows Server 2012 - 64 bit**
* **IBM AIX 7.1 - 64 bit**
* **Solaris 10 - 64 bit**
* **Red Hat Enterprise Linux 6 - 64 bit**
* **New Windows Server 2012 - Hyper-V**
* **The Chat Widget includes support for the following web browsers:
  Google Chrome
  Mozilla Firefox
  Microsoft Internet Explorer 10, 11
  Apple Safari 7**
* **Google Chrome**
* **Mozilla Firefox**
* **Microsoft Internet Explorer 10, 11**
* **Apple Safari 7**
* **Includes the new Web Server API for RESTful chat interactions**
* **Exposes the ability to submit e-mail interactions from web forms**
* **Includes support for the following Host Operating System Support:
  Windows Server 2012 - 64 bit
  IBM AIX 7.1 - 64 bit
  Solaris 10 - 64 bit
  Red Hat Enterprise Linux 6 - 64 bit
  New Windows Server 2012 - Hyper-V**
* **Windows Server 2012 - 64 bit**
* **IBM AIX 7.1 - 64 bit**
* **Solaris 10 - 64 bit**
* **Red Hat Enterprise Linux 6 - 64 bit**
* **New Windows Server 2012 - Hyper-V**
* **The Chat Widget includes support for the following web browsers:
  Google Chrome
  Mozilla Firefox
  Microsoft Internet Explorer 10, 11
  Apple Safari 7**
* **Google Chrome**
* **Mozilla Firefox**
* **Microsoft Internet Explorer 10, 11**
* **Apple Safari 7**
* **Includes the new Web Server API for RESTful chat interactions**
* **Exposes the ability to submit e-mail interactions from web forms**
* **Includes support for the following Host Operating System Support:
  Windows Server 2012 - 64 bit
  IBM AIX 7.1 - 64 bit
  Solaris 10 - 64 bit
  Red Hat Enterprise Linux 6 - 64 bit
  New Windows Server 2012 - Hyper-V**
* **Windows Server 2012 - 64 bit**
* **IBM AIX 7.1 - 64 bit**
* **Solaris 10 - 64 bit**
* **Red Hat Enterprise Linux 6 - 64 bit**
* **New Windows Server 2012 - Hyper-V**
* **The Chat Widget includes support for the following web browsers:
  Google Chrome
  Mozilla Firefox
  Microsoft Internet Explorer 10, 11
  Apple Safari 7**
* **Google Chrome**
* **Mozilla Firefox**
* **Microsoft Internet Explorer 10, 11**
* **Apple Safari 7**
* **Includes the new Web Server API for RESTful chat interactions**
* **Exposes the ability to submit e-mail interactions from web forms**
* **Includes support for the following Host Operating System Support:
  Windows Server 2012 - 64 bit
  IBM AIX 7.1 - 64 bit
  Solaris 10 - 64 bit
  Red Hat Enterprise Linux 6 - 64 bit
  New Windows Server 2012 - Hyper-V**
* **Windows Server 2012 - 64 bit**
* **IBM AIX 7.1 - 64 bit**
* **Solaris 10 - 64 bit**
* **Red Hat Enterprise Linux 6 - 64 bit**
* **New Windows Server 2012 - Hyper-V**
* **The Chat Widget includes support for the following web browsers:
  Google Chrome
  Mozilla Firefox
  Microsoft Internet Explorer 10, 11
  Apple Safari 7**
* **Google Chrome**
* **Mozilla Firefox**
* **Microsoft Internet Explorer 10, 11**
* **Apple Safari 7**

### **Resolved issues:**

## **Release 8.5.000.11 (11/24/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.11 | 11/24/14 | General |  |  | X | X | X |

### New Features:

* **Performance enhancements obtained through the use of information caching.**
* **Added a data.zip archive for use with Microsoft Windows servers.**
* **Performance enhancements obtained through the use of information caching.**
* **Added a data.zip archive for use with Microsoft Windows servers.**
* **Performance enhancements obtained through the use of information caching.**
* **Added a data.zip archive for use with Microsoft Windows servers.**
* **Performance enhancements obtained through the use of information caching.**
* **Added a data.zip archive for use with Microsoft Windows servers.**

### **Resolved issues:**

## **Release 8.5.000.13 (02/10/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.13 | 02/10/15 | General |  |  | X | X | X |

### New Features:

* **The status codes in the HTTP response are now represented as follows:
  statusCode 0 - represents a successful communication with Chat Server.
  statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.
  statusCode 2 - represent a non-recoverable error.**
* **statusCode 0 - represents a successful communication with Chat Server.**
* **statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.**
* **statusCode 2 - represent a non-recoverable error.**
* **WebAPI now allows the endpoint definition to submit Chat interactions.**
* **Web API Server now provides aggregate operation statistics across all Chat Servers.**
* **The status codes in the HTTP response are now represented as follows:
  statusCode 0 - represents a successful communication with Chat Server.
  statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.
  statusCode 2 - represent a non-recoverable error.**
* **statusCode 0 - represents a successful communication with Chat Server.**
* **statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.**
* **statusCode 2 - represent a non-recoverable error.**
* **WebAPI now allows the endpoint definition to submit Chat interactions.**
* **Web API Server now provides aggregate operation statistics across all Chat Servers.**
* **The status codes in the HTTP response are now represented as follows:
  statusCode 0 - represents a successful communication with Chat Server.
  statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.
  statusCode 2 - represent a non-recoverable error.**
* **statusCode 0 - represents a successful communication with Chat Server.**
* **statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.**
* **statusCode 2 - represent a non-recoverable error.**
* **WebAPI now allows the endpoint definition to submit Chat interactions.**
* **Web API Server now provides aggregate operation statistics across all Chat Servers.**
* **The status codes in the HTTP response are now represented as follows:
  statusCode 0 - represents a successful communication with Chat Server.
  statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.
  statusCode 2 - represent a non-recoverable error.**
* **statusCode 0 - represents a successful communication with Chat Server.**
* **statusCode 1 - represents a connection error with Chat Server, or if Chat Server gives an error response that corresponds to a recoverable error.**
* **statusCode 2 - represent a non-recoverable error.**
* **WebAPI now allows the endpoint definition to submit Chat interactions.**
* **Web API Server now provides aggregate operation statistics across all Chat Servers.**

### **Resolved issues:**

## **Release 8.5.000.16 (03/27/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.16 | 03/27/15 | Hot Fix |  |  | X | X | X |

### New Features:

* **Web API Server Chat Service now includes status codes in the HTTP response. Here is a list of the codes and their meanings:
  statusCode 0—The attempted communication with Chat Server was successful.
  statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.
  statusCode 2—There was a non-recoverable error.**
* **statusCode 0—The attempted communication with Chat Server was successful.**
* **statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.**
* **statusCode 2—There was a non-recoverable error.**
* **The Web API now allows endpoints other than the default endpoint to submit Chat interactions. This means that your applications can now choose which queue to use for chat applications, based on the needs of your business logic.**
* **The Send Email request now allows you to add attached data.**
* **Web API Server Chat Service now includes status codes in the HTTP response. Here is a list of the codes and their meanings:
  statusCode 0—The attempted communication with Chat Server was successful.
  statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.
  statusCode 2—There was a non-recoverable error.**
* **statusCode 0—The attempted communication with Chat Server was successful.**
* **statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.**
* **statusCode 2—There was a non-recoverable error.**
* **The Web API now allows endpoints other than the default endpoint to submit Chat interactions. This means that your applications can now choose which queue to use for chat applications, based on the needs of your business logic.**
* **The Send Email request now allows you to add attached data.**
* **Web API Server Chat Service now includes status codes in the HTTP response. Here is a list of the codes and their meanings:
  statusCode 0—The attempted communication with Chat Server was successful.
  statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.
  statusCode 2—There was a non-recoverable error.**
* **statusCode 0—The attempted communication with Chat Server was successful.**
* **statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.**
* **statusCode 2—There was a non-recoverable error.**
* **The Web API now allows endpoints other than the default endpoint to submit Chat interactions. This means that your applications can now choose which queue to use for chat applications, based on the needs of your business logic.**
* **The Send Email request now allows you to add attached data.**
* **Web API Server Chat Service now includes status codes in the HTTP response. Here is a list of the codes and their meanings:
  statusCode 0—The attempted communication with Chat Server was successful.
  statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.
  statusCode 2—There was a non-recoverable error.**
* **statusCode 0—The attempted communication with Chat Server was successful.**
* **statusCode 1—If Chat Server sends an error response that corresponds to a recoverable error, then there was a recoverable error. Otherwise, there was a connection error with Chat Server.**
* **statusCode 2—There was a non-recoverable error.**
* **The Web API now allows endpoints other than the default endpoint to submit Chat interactions. This means that your applications can now choose which queue to use for chat applications, based on the needs of your business logic.**
* **The Send Email request now allows you to add attached data.**

### **Resolved issues:**

## **Release 8.5.000.17 (04/17/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.17 | 04/17/15 | Hot Fix |  |  | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.000.18 (08/21/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.18 | 08/21/15 | Hot Fix |  |  | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.000.19 (09/04/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.19 | 09/04/15 | Hot Fix |  |  | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.000.20 (10/19/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.20 | 10/19/15 | Hot Fix |  |  | X | X | X |

### New Features:

* **The Send Email API now allows you to specify a specific endpoint when you submit an interaction, as long as you are using Genesys E-mail Server version 8.5.101.06 and higher.**
* **The Send Email API now allows you to specify a specific endpoint when you submit an interaction, as long as you are using Genesys E-mail Server version 8.5.101.06 and higher.**
* **The Send Email API now allows you to specify a specific endpoint when you submit an interaction, as long as you are using Genesys E-mail Server version 8.5.101.06 and higher.**
* **The Send Email API now allows you to specify a specific endpoint when you submit an interaction, as long as you are using Genesys E-mail Server version 8.5.101.06 and higher.**

### **Resolved issues:**

Classification Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.200.05  03/10/17  General  8.5.200.05  03/10/17  General |  | 8.5.300.03  09/27/17  General | 2  2 | 8.5.300.03  09/27/17  General | 2  2 |

## **Release 8.5.200.05 (03/10/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.05 | 03/10/17 | General |  | X | X | X | X |

### New Features:

* **Classification Server now uses all models specified in the Analyze request, regardless of whether the models are set to Active or Not Active.**
* **The parameter TestingMode has been added to the ClassifyScreenUniversal method of the Analyze service. If this parameter has the value all, disabled screening rules are treated as enabled for this ESP request, allowing Classification Server to test all Screening Rules specified in the Analyze request, regardless of whether the rules are enabled or disabled.**
* **Classification Server no longer creates special "CEngine" log files. That information is now included in the regular logs.**
* **The setup procedure for the Windows platform now allows you to specify the location of application startup log files.**
* **Classification Server now uses all models specified in the Analyze request, regardless of whether the models are set to Active or Not Active.**
* **The parameter TestingMode has been added to the ClassifyScreenUniversal method of the Analyze service. If this parameter has the value all, disabled screening rules are treated as enabled for this ESP request, allowing Classification Server to test all Screening Rules specified in the Analyze request, regardless of whether the rules are enabled or disabled.**
* **Classification Server no longer creates special "CEngine" log files. That information is now included in the regular logs.**
* **The setup procedure for the Windows platform now allows you to specify the location of application startup log files.**

### **Resolved issues:**

## **Release 8.5.300.03 (09/27/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.300.03 | 09/27/17 | General |  |  | X |  | X |

### New Features:

* **Support for the following operating systems. See the Supported Operating Environment: eServices page for more detailed information and a list of all supported operating systems.
  Red Hat Enterprise Linux 7.
  Oracle Linux 7 coupled with Unbreakable Enterprise Kernel Release 4.**
* **Red Hat Enterprise Linux 7.**
* **Oracle Linux 7 coupled with Unbreakable Enterprise Kernel Release 4.**
* **Classification Server can now classify chat transcripts after the interaction has concluded.**
* **Genesys Content Analyzer adds support for the following languages:
  Bulgarian
  Czech
  Danish
  Dutch (Netherlands)
  Finnish
  Greek
  Korean
  Norwegian
  Polish
  Romanian
  Slovakian
  Swedish
  Turkish**
* **Bulgarian**
* **Czech**
* **Danish**
* **Dutch (Netherlands)**
* **Finnish**
* **Greek**
* **Korean**
* **Norwegian**
* **Polish**
* **Romanian**
* **Slovakian**
* **Swedish**
* **Turkish**
* **Support for the following operating systems. See the Supported Operating Environment: eServices page for more detailed information and a list of all supported operating systems.
  Red Hat Enterprise Linux 7.
  Oracle Linux 7 coupled with Unbreakable Enterprise Kernel Release 4.**
* **Red Hat Enterprise Linux 7.**
* **Oracle Linux 7 coupled with Unbreakable Enterprise Kernel Release 4.**
* **Classification Server can now classify chat transcripts after the interaction has concluded.**
* **Genesys Content Analyzer adds support for the following languages:
  Bulgarian
  Czech
  Danish
  Dutch (Netherlands)
  Finnish
  Greek
  Korean
  Norwegian
  Polish
  Romanian
  Slovakian
  Swedish
  Turkish**
* **Bulgarian**
* **Czech**
* **Danish**
* **Dutch (Netherlands)**
* **Finnish**
* **Greek**
* **Korean**
* **Norwegian**
* **Polish**
* **Romanian**
* **Slovakian**
* **Swedish**
* **Turkish**

### **Resolved issues:**

Interaction Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.1.4  08/21/14  General  8.5.1  11/26/14  General  8.5.100.03  11/26/14  General  8.5.100.03  11/26/14  General  8.5.100.03  11/26/14  General  8.5.105.04  10/09/15  General  8.5.105.04  10/09/15  General  8.5.107.14  09/02/16  Hot Fix  8.5.107.14  09/02/16  Hot Fix  8.5.107.14  09/02/16  Hot Fix  8.5.108.05  11/10/16  General  8.5.108.05  11/10/16  General  8.5.109.11  09/08/17  General  8.5.109.11  09/08/17  General |  | 8.5.110.10  09/08/17  General | 19  17  17  17  17  12  12  6  6  6  5  5  1  1 | 8.5.110.10  09/08/17  General | 19  17  17  17  17  12  12  6  6  6  5  5  1  1 |

## **Release 8.5.000.10 (08/21/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.10 | 08/21/14 | General |  | X | X | X | X |

### New Features:

* **Interaction Server can now cancel conferences and transfers. When it does this, it also sends EventRevoked to the invited party. (ESR-7741)**
* **The single Interaction Server in a multi-tenant environment now distributes events only to reporting clients that belong to the same tenant. (ESR-7704)**
* **This release supports MS SQL Server 2012. (ESR-7682)**
* **This release supports Oracle 12c. (ESR-7680)**
* **This release supports Windows Server 2012 Hyper-V. (ESR-7673)**
* **This release supports Windows Server 2012 64-bit native. (ESR-7672)**

### **Resolved issues:**

## **Release 8.5.000.11 (02/20/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.000.11 | 02/20/15 | Hot Fix |  | X | X | X | X |

### New Features:

* **This version updates the assigned\_to field of the interactions table after the interaction is accepted as a result of transfer or conference.**

### **Resolved issues:**

## **Release 8.5.100.18 (11/26/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.18 | 11/26/14 | General |  | X | X | X | X |

### New Features:

* **Support for MS SQL Server 2012 Cluster**
* **Support for Oracle 12g RAC**
* **Support for Windows Server 2012 Hyper-V**
* **Support for functionality that enables new features and enhancements of
  Orchestration Server (ORS).**
* **Support for UTF-8 on Windows as well as on other platforms. On Windows, this support requires Interaction Server to connect to its database using ODBC (not DB Server).**
* **The way that Interaction Server communicates with its database has been modified to optimize performance (limited to Windows and Linux only with IBM DB2, MSSQL and Oracle). The following new options were added:
  In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pauseIn the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pauseAlso in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.
  Corrections and ModificationsThis release also includes the following corrections or modifications:
  Interaction Server now provides standard-level messaging to indicate that all Capture Points are working as expected. (ESR-6010)
  Interaction Server now sends the correct EventTakenFromQueue message to Interaction Concentrator (ICON). (ESR-8534)
  Interaction Server now delays checking out licenses if there are errors encountered after checking out any non-feature license. (ESR-8234)
  If DB Server disconnects just when a database transaction is about to start, this particular interaction continues to be available for further requests. (ESR-8185)
  Now Interaction Server supports a mechanism for removing attached data keys, based on the response from ESP servers.
  (ESR-8070)
  This release corrects the limitation with the use of the Web Service Capture Point on Linux hosts that occurred when the number of open client connections to Interaction Server came close to or exceeded 1024. Previously, the Web Service Capture Point stopped working in such cases. (ESR-8382)**
* **In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pause**
* **In the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pause**
* **Also in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.**
* **Support for MS SQL Server 2012 Cluster**
* **Support for Oracle 12g RAC**
* **Support for Windows Server 2012 Hyper-V**
* **Support for functionality that enables new features and enhancements of
  Orchestration Server (ORS).**
* **Support for UTF-8 on Windows as well as on other platforms. On Windows, this support requires Interaction Server to connect to its database using ODBC (not DB Server).**
* **The way that Interaction Server communicates with its database has been modified to optimize performance (limited to Windows and Linux only with IBM DB2, MSSQL and Oracle). The following new options were added:
  In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pauseIn the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pauseAlso in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.
  Corrections and ModificationsThis release also includes the following corrections or modifications:
  Interaction Server now provides standard-level messaging to indicate that all Capture Points are working as expected. (ESR-6010)
  Interaction Server now sends the correct EventTakenFromQueue message to Interaction Concentrator (ICON). (ESR-8534)
  Interaction Server now delays checking out licenses if there are errors encountered after checking out any non-feature license. (ESR-8234)
  If DB Server disconnects just when a database transaction is about to start, this particular interaction continues to be available for further requests. (ESR-8185)
  Now Interaction Server supports a mechanism for removing attached data keys, based on the response from ESP servers.
  (ESR-8070)
  This release corrects the limitation with the use of the Web Service Capture Point on Linux hosts that occurred when the number of open client connections to Interaction Server came close to or exceeded 1024. Previously, the Web Service Capture Point stopped working in such cases. (ESR-8382)**
* **In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pause**
* **In the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pause**
* **Also in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.**
* **Support for MS SQL Server 2012 Cluster**
* **Support for Oracle 12g RAC**
* **Support for Windows Server 2012 Hyper-V**
* **Support for functionality that enables new features and enhancements of
  Orchestration Server (ORS).**
* **Support for UTF-8 on Windows as well as on other platforms. On Windows, this support requires Interaction Server to connect to its database using ODBC (not DB Server).**
* **The way that Interaction Server communicates with its database has been modified to optimize performance (limited to Windows and Linux only with IBM DB2, MSSQL and Oracle). The following new options were added:
  In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pauseIn the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pauseAlso in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.
  Corrections and ModificationsThis release also includes the following corrections or modifications:
  Interaction Server now provides standard-level messaging to indicate that all Capture Points are working as expected. (ESR-6010)
  Interaction Server now sends the correct EventTakenFromQueue message to Interaction Concentrator (ICON). (ESR-8534)
  Interaction Server now delays checking out licenses if there are errors encountered after checking out any non-feature license. (ESR-8234)
  If DB Server disconnects just when a database transaction is about to start, this particular interaction continues to be available for further requests. (ESR-8185)
  Now Interaction Server supports a mechanism for removing attached data keys, based on the response from ESP servers.
  (ESR-8070)
  This release corrects the limitation with the use of the Web Service Capture Point on Linux hosts that occurred when the number of open client connections to Interaction Server came close to or exceeded 1024. Previously, the Web Service Capture Point stopped working in such cases. (ESR-8382)**
* **In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pause**
* **In the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pause**
* **Also in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.**
* **Support for MS SQL Server 2012 Cluster**
* **Support for Oracle 12g RAC**
* **Support for Windows Server 2012 Hyper-V**
* **Support for functionality that enables new features and enhancements of
  Orchestration Server (ORS).**
* **Support for UTF-8 on Windows as well as on other platforms. On Windows, this support requires Interaction Server to connect to its database using ODBC (not DB Server).**
* **The way that Interaction Server communicates with its database has been modified to optimize performance (limited to Windows and Linux only with IBM DB2, MSSQL and Oracle). The following new options were added:
  In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pauseIn the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pauseAlso in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.
  Corrections and ModificationsThis release also includes the following corrections or modifications:
  Interaction Server now provides standard-level messaging to indicate that all Capture Points are working as expected. (ESR-6010)
  Interaction Server now sends the correct EventTakenFromQueue message to Interaction Concentrator (ICON). (ESR-8534)
  Interaction Server now delays checking out licenses if there are errors encountered after checking out any non-feature license. (ESR-8234)
  If DB Server disconnects just when a database transaction is about to start, this particular interaction continues to be available for further requests. (ESR-8185)
  Now Interaction Server supports a mechanism for removing attached data keys, based on the response from ESP servers.
  (ESR-8070)
  This release corrects the limitation with the use of the Web Service Capture Point on Linux hosts that occurred when the number of open client connections to Interaction Server came close to or exceeded 1024. Previously, the Web Service Capture Point stopped working in such cases. (ESR-8382)**
* **In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pause**
* **In the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pause**
* **Also in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.**
* **Support for MS SQL Server 2012 Cluster**
* **Support for Oracle 12g RAC**
* **Support for Windows Server 2012 Hyper-V**
* **Support for functionality that enables new features and enhancements of
  Orchestration Server (ORS).**
* **Support for UTF-8 on Windows as well as on other platforms. On Windows, this support requires Interaction Server to connect to its database using ODBC (not DB Server).**
* **The way that Interaction Server communicates with its database has been modified to optimize performance (limited to Windows and Linux only with IBM DB2, MSSQL and Oracle). The following new options were added:
  In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pauseIn the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pauseAlso in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.
  Corrections and ModificationsThis release also includes the following corrections or modifications:
  Interaction Server now provides standard-level messaging to indicate that all Capture Points are working as expected. (ESR-6010)
  Interaction Server now sends the correct EventTakenFromQueue message to Interaction Concentrator (ICON). (ESR-8534)
  Interaction Server now delays checking out licenses if there are errors encountered after checking out any non-feature license. (ESR-8234)
  If DB Server disconnects just when a database transaction is about to start, this particular interaction continues to be available for further requests. (ESR-8185)
  Now Interaction Server supports a mechanism for removing attached data keys, based on the response from ESP servers.
  (ESR-8070)
  This release corrects the limitation with the use of the Web Service Capture Point on Linux hosts that occurred when the number of open client connections to Interaction Server came close to or exceeded 1024. Previously, the Web Service Capture Point stopped working in such cases. (ESR-8382)**
* **In the [settings] section of the Interaction Server DAP:
  blob-chunk-size
  connection-string
  connections
  dbprotocol
  odbc-string
  queue-size
  reconnection-pause**
* **In the [logger-settings] section of the Event Logger DAP:
  connection-string
  odbc-string
  reconnection-pause**
* **Also in the [logger-settings] section of the Event Logger DAP, the delivery-protocol option adds the valid value odbc.**

### **Resolved issues:**

## **Release 8.5.100.20 (12/24/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.20 | 12/24/14 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.102.02 (03/03/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.102.02 | 03/03/15 | General |  | X | X | X | X |

### New Features:

* **This release provides additional KPI counters for monitoring the number of requests of different types received from clients.**
* **This release provides additional KPI counters for monitoring the number of error responses sent to clients, including ESP (External Service Protocol) errors.**
* **This release provides a means for Interaction Server clients to request agent state from the server--for example, in order to synchronize the agent state across multiple connections. This is done by means of the new RequestAgentState and its response, EventAgentState, both of which are documented in the Platform SDK API Reference.**
* **This release includes the following new configuration options:**
* **With this release it is possible to set a limit on the number of records returned in response to RequestGetWorkbinContent. The limit may be set within the request attribute, and as an option in the configuration object of Workbin type. If both are present, the value from the request is applied. As part of this feature, the following option is added to the Workbin section of the workbin script object:**
* **With this release it is possible to set attributes in RequestGetWorkbinContent that specify a filtering condition and the order in which records are returned in response to the request.**
* **Support of PostgreSQL database on Windows and Linux via an ODBC connection was added in this release. This requires using version 9.03.0400 of the client driver. Note: The use of PostgreSQL database via Genesys DB Server is not currently possible.**
* **This release enables the following options from the log library:
  enable-thread
  throttle-period
  throttle-threshold**
* **enable-thread**
* **throttle-period**
* **throttle-threshold**
* **This release provides additional KPI counters for monitoring the number of requests of different types received from clients.**
* **This release provides additional KPI counters for monitoring the number of error responses sent to clients, including ESP (External Service Protocol) errors.**
* **This release provides a means for Interaction Server clients to request agent state from the server--for example, in order to synchronize the agent state across multiple connections. This is done by means of the new RequestAgentState and its response, EventAgentState, both of which are documented in the Platform SDK API Reference.**
* **This release includes the following new configuration options:**
* **With this release it is possible to set a limit on the number of records returned in response to RequestGetWorkbinContent. The limit may be set within the request attribute, and as an option in the configuration object of Workbin type. If both are present, the value from the request is applied. As part of this feature, the following option is added to the Workbin section of the workbin script object:**
* **With this release it is possible to set attributes in RequestGetWorkbinContent that specify a filtering condition and the order in which records are returned in response to the request.**
* **Support of PostgreSQL database on Windows and Linux via an ODBC connection was added in this release. This requires using version 9.03.0400 of the client driver. Note: The use of PostgreSQL database via Genesys DB Server is not currently possible.**
* **This release enables the following options from the log library:
  enable-thread
  throttle-period
  throttle-threshold**
* **enable-thread**
* **throttle-period**
* **throttle-threshold**
* **This release provides additional KPI counters for monitoring the number of requests of different types received from clients.**
* **This release provides additional KPI counters for monitoring the number of error responses sent to clients, including ESP (External Service Protocol) errors.**
* **This release provides a means for Interaction Server clients to request agent state from the server--for example, in order to synchronize the agent state across multiple connections. This is done by means of the new RequestAgentState and its response, EventAgentState, both of which are documented in the Platform SDK API Reference.**
* **This release includes the following new configuration options:**
* **With this release it is possible to set a limit on the number of records returned in response to RequestGetWorkbinContent. The limit may be set within the request attribute, and as an option in the configuration object of Workbin type. If both are present, the value from the request is applied. As part of this feature, the following option is added to the Workbin section of the workbin script object:**
* **With this release it is possible to set attributes in RequestGetWorkbinContent that specify a filtering condition and the order in which records are returned in response to the request.**
* **Support of PostgreSQL database on Windows and Linux via an ODBC connection was added in this release. This requires using version 9.03.0400 of the client driver. Note: The use of PostgreSQL database via Genesys DB Server is not currently possible.**
* **This release enables the following options from the log library:
  enable-thread
  throttle-period
  throttle-threshold**
* **enable-thread**
* **throttle-period**
* **throttle-threshold**
* **This release provides additional KPI counters for monitoring the number of requests of different types received from clients.**
* **This release provides additional KPI counters for monitoring the number of error responses sent to clients, including ESP (External Service Protocol) errors.**
* **This release provides a means for Interaction Server clients to request agent state from the server--for example, in order to synchronize the agent state across multiple connections. This is done by means of the new RequestAgentState and its response, EventAgentState, both of which are documented in the Platform SDK API Reference.**
* **This release includes the following new configuration options:**
* **With this release it is possible to set a limit on the number of records returned in response to RequestGetWorkbinContent. The limit may be set within the request attribute, and as an option in the configuration object of Workbin type. If both are present, the value from the request is applied. As part of this feature, the following option is added to the Workbin section of the workbin script object:**
* **With this release it is possible to set attributes in RequestGetWorkbinContent that specify a filtering condition and the order in which records are returned in response to the request.**
* **Support of PostgreSQL database on Windows and Linux via an ODBC connection was added in this release. This requires using version 9.03.0400 of the client driver. Note: The use of PostgreSQL database via Genesys DB Server is not currently possible.**
* **This release enables the following options from the log library:
  enable-thread
  throttle-period
  throttle-threshold**
* **enable-thread**
* **throttle-period**
* **throttle-threshold**
* **This release provides additional KPI counters for monitoring the number of requests of different types received from clients.**
* **This release provides additional KPI counters for monitoring the number of error responses sent to clients, including ESP (External Service Protocol) errors.**
* **This release provides a means for Interaction Server clients to request agent state from the server--for example, in order to synchronize the agent state across multiple connections. This is done by means of the new RequestAgentState and its response, EventAgentState, both of which are documented in the Platform SDK API Reference.**
* **This release includes the following new configuration options:**
* **With this release it is possible to set a limit on the number of records returned in response to RequestGetWorkbinContent. The limit may be set within the request attribute, and as an option in the configuration object of Workbin type. If both are present, the value from the request is applied. As part of this feature, the following option is added to the Workbin section of the workbin script object:**
* **With this release it is possible to set attributes in RequestGetWorkbinContent that specify a filtering condition and the order in which records are returned in response to the request.**
* **Support of PostgreSQL database on Windows and Linux via an ODBC connection was added in this release. This requires using version 9.03.0400 of the client driver. Note: The use of PostgreSQL database via Genesys DB Server is not currently possible.**
* **This release enables the following options from the log library:
  enable-thread
  throttle-period
  throttle-threshold**
* **enable-thread**
* **throttle-period**
* **throttle-threshold**

### **Resolved issues:**

## **Release 8.5.103.05 (05/15/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.103.05 | 05/15/15 | General |  | X | X | X | X |

### New Features:

* **Starting with this release, the InteractionId property may include ASCII characters "hyphen-minus" (decimal code 45) and "underscore" (decimal code 95). Previously, only letters [A-Za-z] and numbers [0-9] were allowed in InteractionId.**
* **This release implements a new option have-segmentation-indexes that controls how segmentation SELECTs are generated. If this option is set to 'true', Interaction Server generates SELECT statements relating to segmentation with the assumption that there are appropriate covering indexes that account for specific segmentation fields, view condition, and view order. This option must be set to 'false' unless appropriate tests are done to show that indexes are appropriately used by the database to execute the segmentation SELECTs efficiently. When set to 'false' (the default), the SELECT statements are generated without using a UNION clause. If changed, the option takes effect after server restart.**
* **An agent can get statistics about all of their workbins or about group workbins, using the new RequestAgentWorkbinStats. The specification of the request is as follows:**
* **Proxy clients can now subscribe to workbin change notifications. To do this, the proxy must specify the following new attribute in RequestWorkbinNotification and RequestCancelWorkbinNotification:
  Attribute name: attr\_tenant\_id (12)
  Type: Integer
  Description: Tenant identifier (DBID) of the agent.**
* **Attribute name: attr\_tenant\_id (12)**
* **Type: Integer**
* **Description: Tenant identifier (DBID) of the agent.**
* **Starting with this release, the InteractionId property may include ASCII characters "hyphen-minus" (decimal code 45) and "underscore" (decimal code 95). Previously, only letters [A-Za-z] and numbers [0-9] were allowed in InteractionId.**
* **This release implements a new option have-segmentation-indexes that controls how segmentation SELECTs are generated. If this option is set to 'true', Interaction Server generates SELECT statements relating to segmentation with the assumption that there are appropriate covering indexes that account for specific segmentation fields, view condition, and view order. This option must be set to 'false' unless appropriate tests are done to show that indexes are appropriately used by the database to execute the segmentation SELECTs efficiently. When set to 'false' (the default), the SELECT statements are generated without using a UNION clause. If changed, the option takes effect after server restart.**
* **An agent can get statistics about all of their workbins or about group workbins, using the new RequestAgentWorkbinStats. The specification of the request is as follows:**
* **Proxy clients can now subscribe to workbin change notifications. To do this, the proxy must specify the following new attribute in RequestWorkbinNotification and RequestCancelWorkbinNotification:
  Attribute name: attr\_tenant\_id (12)
  Type: Integer
  Description: Tenant identifier (DBID) of the agent.**
* **Attribute name: attr\_tenant\_id (12)**
* **Type: Integer**
* **Description: Tenant identifier (DBID) of the agent.**
* **Starting with this release, the InteractionId property may include ASCII characters "hyphen-minus" (decimal code 45) and "underscore" (decimal code 95). Previously, only letters [A-Za-z] and numbers [0-9] were allowed in InteractionId.**
* **This release implements a new option have-segmentation-indexes that controls how segmentation SELECTs are generated. If this option is set to 'true', Interaction Server generates SELECT statements relating to segmentation with the assumption that there are appropriate covering indexes that account for specific segmentation fields, view condition, and view order. This option must be set to 'false' unless appropriate tests are done to show that indexes are appropriately used by the database to execute the segmentation SELECTs efficiently. When set to 'false' (the default), the SELECT statements are generated without using a UNION clause. If changed, the option takes effect after server restart.**
* **An agent can get statistics about all of their workbins or about group workbins, using the new RequestAgentWorkbinStats. The specification of the request is as follows:**
* **Proxy clients can now subscribe to workbin change notifications. To do this, the proxy must specify the following new attribute in RequestWorkbinNotification and RequestCancelWorkbinNotification:
  Attribute name: attr\_tenant\_id (12)
  Type: Integer
  Description: Tenant identifier (DBID) of the agent.**
* **Attribute name: attr\_tenant\_id (12)**
* **Type: Integer**
* **Description: Tenant identifier (DBID) of the agent.**
* **Starting with this release, the InteractionId property may include ASCII characters "hyphen-minus" (decimal code 45) and "underscore" (decimal code 95). Previously, only letters [A-Za-z] and numbers [0-9] were allowed in InteractionId.**
* **This release implements a new option have-segmentation-indexes that controls how segmentation SELECTs are generated. If this option is set to 'true', Interaction Server generates SELECT statements relating to segmentation with the assumption that there are appropriate covering indexes that account for specific segmentation fields, view condition, and view order. This option must be set to 'false' unless appropriate tests are done to show that indexes are appropriately used by the database to execute the segmentation SELECTs efficiently. When set to 'false' (the default), the SELECT statements are generated without using a UNION clause. If changed, the option takes effect after server restart.**
* **An agent can get statistics about all of their workbins or about group workbins, using the new RequestAgentWorkbinStats. The specification of the request is as follows:**
* **Proxy clients can now subscribe to workbin change notifications. To do this, the proxy must specify the following new attribute in RequestWorkbinNotification and RequestCancelWorkbinNotification:
  Attribute name: attr\_tenant\_id (12)
  Type: Integer
  Description: Tenant identifier (DBID) of the agent.**
* **Attribute name: attr\_tenant\_id (12)**
* **Type: Integer**
* **Description: Tenant identifier (DBID) of the agent.**
* **Starting with this release, the InteractionId property may include ASCII characters "hyphen-minus" (decimal code 45) and "underscore" (decimal code 95). Previously, only letters [A-Za-z] and numbers [0-9] were allowed in InteractionId.**
* **This release implements a new option have-segmentation-indexes that controls how segmentation SELECTs are generated. If this option is set to 'true', Interaction Server generates SELECT statements relating to segmentation with the assumption that there are appropriate covering indexes that account for specific segmentation fields, view condition, and view order. This option must be set to 'false' unless appropriate tests are done to show that indexes are appropriately used by the database to execute the segmentation SELECTs efficiently. When set to 'false' (the default), the SELECT statements are generated without using a UNION clause. If changed, the option takes effect after server restart.**
* **An agent can get statistics about all of their workbins or about group workbins, using the new RequestAgentWorkbinStats. The specification of the request is as follows:**
* **Proxy clients can now subscribe to workbin change notifications. To do this, the proxy must specify the following new attribute in RequestWorkbinNotification and RequestCancelWorkbinNotification:
  Attribute name: attr\_tenant\_id (12)
  Type: Integer
  Description: Tenant identifier (DBID) of the agent.**
* **Attribute name: attr\_tenant\_id (12)**
* **Type: Integer**
* **Description: Tenant identifier (DBID) of the agent.**

### **Resolved issues:**

## **Release 8.5.104.05 (08/04/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.104.05 | 08/04/15 | General |  | X | X | X | X |

### New Features:

* **This version supports dates up to the year 2999 on Windows platforms or up to the year 9999 on other platforms. Previously the dates were limited to year 2037. Among the drawbacks of that limit was that it prevented scheduling interaction processing far into the future.**
* **This version supports dates up to the year 2999 on Windows platforms or up to the year 9999 on other platforms. Previously the dates were limited to year 2037. Among the drawbacks of that limit was that it prevented scheduling interaction processing far into the future.**
* **This version supports dates up to the year 2999 on Windows platforms or up to the year 9999 on other platforms. Previously the dates were limited to year 2037. Among the drawbacks of that limit was that it prevented scheduling interaction processing far into the future.**
* **This version supports dates up to the year 2999 on Windows platforms or up to the year 9999 on other platforms. Previously the dates were limited to year 2037. Among the drawbacks of that limit was that it prevented scheduling interaction processing far into the future.**
* **This version supports dates up to the year 2999 on Windows platforms or up to the year 9999 on other platforms. Previously the dates were limited to year 2037. Among the drawbacks of that limit was that it prevented scheduling interaction processing far into the future.**

### **Resolved issues:**

## **Release 8.5.105.04 (10/09/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.105.04 | 10/09/15 | General |  | X | X | X | X |

### New Features:

* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**
* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**
* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**
* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**
* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**
* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**
* **Now EventPartyRemoved, EventPlacedInQueue, and EventPlacedInWorkbin contain timestamps that show when the interaction was previously placed in a queue (specified in attr\_old\_queue). This feature enables Genesys real-time reporting (Stat Server) to provide additional metrics related to time in queue.**
* **This release corrects an issue with strict checking of the Interaction Server database tables in ODBC mode. Now Interaction Server does not check fields for the NOT NULL constraint, allowing for more flexible structure and making ODBC mode consistent with DB Server mode. Specifically, the strict check caused issues with the "external\_id" field, which by design may be either nullable or not nullable, allowing external interaction IDs to be either unique or non-unique.**

### **Resolved issues:**

## **Release 8.5.106.04 (02/05/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.106.04 | 02/05/16 | General |  | X | X | X | X |

### New Features:

* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**
* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**
* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**
* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**
* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**
* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**
* **PartyTenantId, PartyType, PartyStrategyId, PartyRouterId, PartyPlaceId, and PartyAgentId are available for Database Capture Point queries.**
* **Third-party Groovy libraries are upgraded to the most recent available version. The -Djava.class.path configuration option in the [jvm-options] section needs to be updated with the new jar file name.**
* **The media-types configuration option is added. This option requires Interaction Server Proxy version 8.5.106.14 (a Restricted release) or later.**

### **Resolved issues:**

## **Release 8.5.106.05 (02/09/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.106.05 | 02/09/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.107.06 (05/20/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.06 | 05/20/16 | General |  | X | X | X | X |

### New Features:

* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**
* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**
* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**
* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**
* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**
* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**
* **Interaction Server prints out the current license usage upon any attempt to log an agent in or out, including any automatic logouts due to timeouts, license cut or client/proxy disconnect.**
* **The option log-custom-message-content, added to the log-control section, allows you to enable or disable (the default) printing of the binary content of EventCustom in the Interaction Server log.**
* **This release introduces agent auto-logout, which allows logging out agents due to inactivity. The new option login-session-timeout in the settings section specifies the inactivity timeout in minutes. If an agent application does not send any request to Interaction Server for the duration specified by the option, Interaction Server logs out and disconnects that agent.**
* **The option reset-states-on-shutdown, added to the settings section, controls the behavior of Interaction Server when it is shut down normally. Previously, as part of shutting down when working with DB Server, Interaction Server finished all database updates and reset all interaction states to queued. Now, if this option is set to false, the Server does not update interaction states, so the agents have a chance to use the session restoration feature after reconnecting to a backup server. Note that when working with ODBC, the option has no effect and interaction states are not reset on shutdown.**
* **Interaction Server supports Red Hat Enterprise Linux (RHEL) 7 64-bit native.**

### **Resolved issues:**

## **Release 8.5.107.08 (06/03/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.08 | 06/03/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.107.11 (06/09/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.11 | 06/09/16 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.107.22 (09/02/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.107.22 | 09/02/16 | Hot Fix |  | X | X | X | X |

### New Features:

* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**
* **This release introduces the option max-database-request-queue-size in the [settings] section. It sets the maximum size for the database request queue. Any client request that generates a database request will be rejected if the current queue size reaches the specified maximum. The default value is 10,000 and the valid value is any integer in the range 5,000–200,000. Changes take effect immediately.**
* **There are two new KPI counters: current\_request\_queue\_size and current\_request\_queue\_wait. Like all other counters, these are accessible in ping messages, the health monitor, or datastream reporting. This feature relates to the resolved issue described below.**
* **A new configuration option in the [health-service] section controls whether and how often the current counters are written to the log file: log-output-timeout specifies the time, in seconds, between these log messages. The default value is 0 seconds (no logging), and the valid value is an integer in the range 1–600 (10 minutes). Changes take effect immediately. This feature also relates to the resolved issue described below.**

### **Resolved issues:**

## **Release 8.5.108.05 (11/10/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.108.05 | 11/10/16 | General |  | X | X | X | X |

### New Features:

* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**
* **This release includes the most recent available version of third-party Groovy libraries. Be sure that you update the -Djava.class.path configuration option in the [jvm-options] section with the new .jar file name.**
* **MS SQL Server 2014 and MS SQL Server 2014 Cluster are supported.**
* **Java version 1.8 update 101 is supported.**

### **Resolved issues:**

## **Release 8.5.108.06 (01/24/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.108.06 | 01/24/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.109.01 (05/01/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.109.01 | 05/01/17 | General |  | X | X | X | X |

### New Features:

* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**
* **This release supports Universal Contact Server v9.0 in N+1 mode.**
* **In this release, besides resetting the agent login session timeout when it receives requests that relate to interactions or agent states, Interaction Server also resets the timeout when it receives RequestGetWorkbinContent, RequestFindInteractions, or RequestTakeSnapshot from a client.
  Also, the valid range for the option login-session-timeout has been extended to include 0; a value of 0 disables the agent login session timeout.**
* **This release is accompanied by the new component Cluster Manager Plug-in for GAX, a user interface that you can use to configure Interaction Server and Interaction Server Proxy clusters.**

### **Resolved issues:**

## **Release 8.5.109.03 (06/02/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.109.03 | 06/02/17 | Hot Fix |  | X | X | X | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.110.10 (09/08/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.110.10 | 09/08/17 | General |  | X | X | X | X |

### New Features:

* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**
* **Interaction Server now supports TLS 1.2.**
* **Interaction Server can now generate a new reporting event, EventAbandoned, if a customer abandons an interaction (the attribute IsOnline changes value from 1 to 0) before an agent was assigned to it. You can use this event to track abandoned interactions, which are then calculated by reporting clients such as Stat Server. The Genesys Chat solution supports this feature out-of-the-box.**
* **Interaction Server no longer supports the T-Server application type. Customers must now use the Interaction Server application type. Additionally, the installation procedure no longer offers to install Interaction Server using the T-Server application type.**
* **This release adjusts the default values of the following options in section [log-control]:
  max-protocol-message-size=16384
  max-protocol-attribute-size=256**
* **max-protocol-message-size=16384**
* **max-protocol-attribute-size=256**
* **You can now use the Groovy Event Logger to process reporting events using custom Groovy scripts.**
* **This release adds the configuration option max-userdata-size to the section [settings]. Use this option to specify the maximum user data size, in kilobytes, that can be stored for any specific interaction. The value 0 disables the check.**
* **This release adds the configuration options trace-segmented-views and max-segments-traced-number in the section [log-control]. Use these options to control log messages regarding the segmentation process.**

### **Resolved issues:**

Media Control Platform

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.1.410.21  12/20/13  General  8.1.410.36  12/20/13  General  8.5.0  12/20/13  General  8.5.050.37  03/10/14  Hot Fix  8.5.050.37  03/10/14  Hot Fix  8.5.050.40  05/23/14  Hot Fix  8.5.050.40  05/23/14  Hot Fix  8.5.050.40  05/23/14  Hot Fix  8.5.050.40  05/23/14  Hot Fix |  | 8.5.181.78  09/15/17  General | 32  32  32  30  30  28  28  28  28 | 8.5.181.78  09/15/17  General | 32  32  32  30  30  28  28  28  28 |

## **Release 8.5.041.14 (12/20/13)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.041.14 | 12/20/13 | General |  |  | X |  | X |

### New Features:

* **Additional features in support of the Genesys Interaction Recording (GIR) Solution:
  Call Recording Encryption Support.
  Stereo MP3 encoding for call recording.
  Submission to S3 storage and webDAV support.
  Interactions with GIR.**
* **Call Recording Encryption Support.**
* **Stereo MP3 encoding for call recording.**
* **Submission to S3 storage and webDAV support.**
* **Interactions with GIR.**
* **Additional features in support of the Genesys Interaction Recording (GIR) Solution:
  Call Recording Encryption Support.
  Stereo MP3 encoding for call recording.
  Submission to S3 storage and webDAV support.
  Interactions with GIR.**
* **Call Recording Encryption Support.**
* **Stereo MP3 encoding for call recording.**
* **Submission to S3 storage and webDAV support.**
* **Interactions with GIR.**
* **Additional features in support of the Genesys Interaction Recording (GIR) Solution:
  Call Recording Encryption Support.
  Stereo MP3 encoding for call recording.
  Submission to S3 storage and webDAV support.
  Interactions with GIR.**
* **Call Recording Encryption Support.**
* **Stereo MP3 encoding for call recording.**
* **Submission to S3 storage and webDAV support.**
* **Interactions with GIR.**

### **Resolved issues:**

## **Release 8.5.050.13 (12/20/13)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.13 | 12/20/13 | Hot Fix |  |  | X |  | X |

### New Features:

* **A new configuration parameter specifies the mode (HTTP or HTTPS)
  to be used for uploading recording files to Amazon s3 during MSML call recording.
  section: msml
  parameter: record.amazonpostmode
  Valid values: http (default) or https
  Takes effect: immediately / session
  Use this parameter to specify the mode (HTTP or HTTPS) used to upload recording
  files to Amazon s3 during MSML call recording.
  Set to http to enable that mode.
  Set to https to enable that mode.
  (GVP-20990)**
* **Set to http to enable that mode.**
* **Set to https to enable that mode.**
* **A new configuration parameter specifies the To Header mode (location
  of the Request URI parameters) for Third Party Call Recording:
  section: vrmrecorder
  parameter: toheadermode
  Valid values: legacy, uriparams, toparams,
  bothtoanduriparams
  Takes effect: immediately / session
  Use this parameter to specify the To Header mode (location of the Request
  URI parameters) for Third Party Call Recording.
  Set to legacy to specify that the MCP will copy the Request
  URI of the INVITE request into the To Header (this is identical to pre-GVP
  8.5.0 behavior).
  Set to uriparams to specify that the Request
  URI parameters will be included in the Request URI part of the To Header.
  Set to toparams (default) to specify that
  the Request URI parameters will be included in the To params
  of the To Header.
  Set to bothtoanduriparams to specify that the Request
  URI parameters will be included in both the Request URI part
  of the To Header and the To params of the To Header.
  (GVP-20875)**
* **Set to legacy to specify that the MCP will copy the Request
  URI of the INVITE request into the To Header (this is identical to pre-GVP
  8.5.0 behavior).**
* **Set to uriparams to specify that the Request
  URI parameters will be included in the Request URI part of the To Header.**
* **Set to toparams (default) to specify that
  the Request URI parameters will be included in the To params
  of the To Header.**
* **Set to bothtoanduriparams to specify that the Request
  URI parameters will be included in both the Request URI part
  of the To Header and the To params of the To Header.**
* **A new configuration parameter specifies the mode (HTTP or HTTPS)
  to be used for uploading recording files to Amazon s3 during MSML call recording.
  section: msml
  parameter: record.amazonpostmode
  Valid values: http (default) or https
  Takes effect: immediately / session
  Use this parameter to specify the mode (HTTP or HTTPS) used to upload recording
  files to Amazon s3 during MSML call recording.
  Set to http to enable that mode.
  Set to https to enable that mode.
  (GVP-20990)**
* **Set to http to enable that mode.**
* **Set to https to enable that mode.**
* **A new configuration parameter specifies the To Header mode (location
  of the Request URI parameters) for Third Party Call Recording:
  section: vrmrecorder
  parameter: toheadermode
  Valid values: legacy, uriparams, toparams,
  bothtoanduriparams
  Takes effect: immediately / session
  Use this parameter to specify the To Header mode (location of the Request
  URI parameters) for Third Party Call Recording.
  Set to legacy to specify that the MCP will copy the Request
  URI of the INVITE request into the To Header (this is identical to pre-GVP
  8.5.0 behavior).
  Set to uriparams to specify that the Request
  URI parameters will be included in the Request URI part of the To Header.
  Set to toparams (default) to specify that
  the Request URI parameters will be included in the To params
  of the To Header.
  Set to bothtoanduriparams to specify that the Request
  URI parameters will be included in both the Request URI part
  of the To Header and the To params of the To Header.
  (GVP-20875)**
* **Set to legacy to specify that the MCP will copy the Request
  URI of the INVITE request into the To Header (this is identical to pre-GVP
  8.5.0 behavior).**
* **Set to uriparams to specify that the Request
  URI parameters will be included in the Request URI part of the To Header.**
* **Set to toparams (default) to specify that
  the Request URI parameters will be included in the To params
  of the To Header.**
* **Set to bothtoanduriparams to specify that the Request
  URI parameters will be included in both the Request URI part
  of the To Header and the To params of the To Header.**
* **A new configuration parameter specifies the mode (HTTP or HTTPS)
  to be used for uploading recording files to Amazon s3 during MSML call recording.
  section: msml
  parameter: record.amazonpostmode
  Valid values: http (default) or https
  Takes effect: immediately / session
  Use this parameter to specify the mode (HTTP or HTTPS) used to upload recording
  files to Amazon s3 during MSML call recording.
  Set to http to enable that mode.
  Set to https to enable that mode.
  (GVP-20990)**
* **Set to http to enable that mode.**
* **Set to https to enable that mode.**
* **A new configuration parameter specifies the To Header mode (location
  of the Request URI parameters) for Third Party Call Recording:
  section: vrmrecorder
  parameter: toheadermode
  Valid values: legacy, uriparams, toparams,
  bothtoanduriparams
  Takes effect: immediately / session
  Use this parameter to specify the To Header mode (location of the Request
  URI parameters) for Third Party Call Recording.
  Set to legacy to specify that the MCP will copy the Request
  URI of the INVITE request into the To Header (this is identical to pre-GVP
  8.5.0 behavior).
  Set to uriparams to specify that the Request
  URI parameters will be included in the Request URI part of the To Header.
  Set to toparams (default) to specify that
  the Request URI parameters will be included in the To params
  of the To Header.
  Set to bothtoanduriparams to specify that the Request
  URI parameters will be included in both the Request URI part
  of the To Header and the To params of the To Header.
  (GVP-20875)**
* **Set to legacy to specify that the MCP will copy the Request
  URI of the INVITE request into the To Header (this is identical to pre-GVP
  8.5.0 behavior).**
* **Set to uriparams to specify that the Request
  URI parameters will be included in the Request URI part of the To Header.**
* **Set to toparams (default) to specify that
  the Request URI parameters will be included in the To params
  of the To Header.**
* **Set to bothtoanduriparams to specify that the Request
  URI parameters will be included in both the Request URI part
  of the To Header and the To params of the To Header.**

### **Resolved issues:**

## **Release 8.5.050.37 (03/10/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.37 | 03/10/14 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.38 (03/24/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.38 | 03/24/14 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.40 (05/23/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.40 | 05/23/14 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.41 (05/27/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.41 | 05/27/15 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.100.58 (12/19/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.100.58 | 12/19/14 | General |  |  | X |  | X |

### New Features:

* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**

### **Resolved issues:**

## **Release 8.5.101.41 (07/15/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.41 | 07/15/14 | General |  |  | X |  | X |

### New Features:

* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**
* **Support for Nuance Vocalizer 6.0.2 and Nuance Speech Server 6.2.5**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Third Party Recording with MCP and the Resource Manager**
* **Configuration Options Changed**

### **Resolved issues:**

## **Release 8.5.101.52 (08/20/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.52 | 08/20/14 | General |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.110.33 (09/19/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.110.33 | 09/19/14 | General |  |  | X |  | X |

### New Features:

* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**
* **Added support for Windows 2012 64-bit.**

### **Resolved issues:**

## **Release 8.5.120.66 (12/18/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.120.66 | 12/18/14 | General |  |  | X |  | X |

### New Features:

* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**
* **This release adds support for MP3 encoding at 16kbps (default) and 24kbps, via the existing session configurable configuration parameter [mpc]mp3.bitrate.**

### **Resolved issues:**

## **Release 8.5.120.68 (02/03/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.120.68 | 02/03/15 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.130.82 (04/17/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.82 | 04/17/15 | General |  |  | X |  | X |

### New Features:

* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**
* **The following parameters now have a maximum limit to their values of 2,147,483,647:
  [vxmli] cache.document.max\_count
  [vxmli] cache.document.max\_size
  [vxmli] cache.document.max\_entry\_size**
* **[vxmli] cache.document.max\_count**
* **[vxmli] cache.document.max\_size**
* **[vxmli] cache.document.max\_entry\_size**
* **The Media Server function Call Progress Detection (CPD) now performs voice print analysis and beep analysis to identify the specific preconnect carrier messages that occur in different countries.
  Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.
  Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.
  Some new VoicePrint Configuration Options support this functionality.**
* **Media Server's configurable database of preconnect tones is initiated during installation and loaded when Media Server starts. You can update the database with different carrier messages at any time, without stopping Media Control Platform. Refer to the page Setting Up Voiceprint Carrier Message Detection for more details on how to setup and use the voiceprints.**
* **Other features include the ability to leave postconnection messages such as voicemail.
  You can read about additional CPD functionality in "Appendix C: Tuning Call Progress Detection" of the
  GVP 8.5 User's Guide.**
* **Some new VoicePrint Configuration Options support this functionality.**
* **Media Control Platform now plays a dynamic prompt correctly. Previously, MCP incorrectly encoded the symbols < and > in SSML tags before queuing a dynamic prompt to TTS Servers.**

### **Resolved issues:**

## **Release 8.5.130.91 (05/21/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.91 | 05/21/15 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.130.93 (06/10/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.93 | 06/10/15 | Hot Fix |  |  | X |  |  |

### New Features:

* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**
* **The new configuration parameter [fm]revalidatestaleresponse changes the rules for handling a stale response: you can specify to revalidate only a stale response, or to revalidate any response that contains a “must-revalidate” directive.
  Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.
  Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.
  Your new setting takes effect following a start or a restart.
  (GVP-22409)**
* **Set revalidatestaleresponse to 0 (for false) to specify revalidation of all responses having the “must-revalidate” directive.**
* **Set revalidatestaleresponse to 1 (for true, the default) to specify that only stale responses are revalidated.**
* **DTMF clamping (also known as masking) guards a customer's sensitive credit card information from an agent's ears and from call recording. An MSML conference request enables clamping. To filter DTMFs from the recording, set the new option callrecording.dtmfhandling to no-digits.
  [msml]callrecording.dtmfhandling has three settings:
  no-digits: Mask all DTMF digits.
  as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.
  all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.presilencepackets to define the length of time that silence occurs before a clamped DTMF. This is important when a DTMF tone appears before the DTMF RFC2833 event, which might happen when the SIP gateway converts DTMF tones to DTMF RFC2833 events. Beware: setting a big number will cause more audio delays in a conference.
  [msml]clampdtmf.presilencepackets has a default setting of zero (0), and must be an integer from 0-50. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
   
  Use the new option clampdtmf.postsilencepackets to define the length of time that silence occurs after a clamped DTMF. This is important when a DTMF tone appears after the DTMF RFC2833 event.
  [msml]clampdtmf.postsilencepackets has a default setting of zero (0), and must be an integer from 0 or greater. This number specifies how many audio packets are replaced with silence after a clamped DTMF. 1 packet usually = 20ms, but that varies with traffic and other factors.
  Your new setting is effective immediately.
  (GVP-22370)**
* **no-digits: Mask all DTMF digits.**
* **as-is: Record everything from the RTP stream as-is. Inband DTMFs are recorded, but not RFC2833 digits.**
* **all-digits: Record all DTMF digits, including inband; generate audio for RFC2833 digits.**

### **Resolved issues:**

## **Release 8.5.141.00 (08/28/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.141.00 | 08/28/15 | General |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.141.08 (11/24/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.141.08 | 11/24/15 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.150.63 (12/15/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.150.63 | 12/15/15 | General |  |  | X |  | X |

### New Features:

* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**
* **The Sip.Body value in the [vxmli] session\_vars configuration option enables access to the body of SIP INVITE messages. Now VXML application developers can take advantage of the additional information available in the body of an INVITE message, to better customize their applications.
  To enable, add this line to your [vxmli] session\_vars default configuration and restart MCP:
  session.connection.protocol.sip.body | Sip.Body |0
  Note: Requires SIP Server v8.1.102.00.**
* **Use the configuration parameter [callmgr] enable\_sip\_response\_in\_transfer\_metric to configure Media Control Platform to append the SIP response code (when it is available) to transfer\_result metrics. This improves standard/interaction logging and simplifies analysis of the SIP response code in case of a failure.
  enable\_sip\_response\_in\_transfer\_metric
  Application: Media Control Platform
  Section: callmgr
  Valid Values: true (enabled) , false (disabled and the default value)
  Takes Effect: Immediately
  Specifies whether or not the SIP response code is appended in the transfer\_result metrics. If the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.
  Metrics Examples of Valid Value Usage
  False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho
  True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>
  True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **False (disabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho**
* **True (enabled):
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho|sip<span style="color:red"> [401]</span>**
* **True (enabled), but the SIP response code is not available:
  transfer\_result sip:Restricted@10.5.135.13|1111|N/A|REFER|noautho<span style="color:red"> |sip[N/A]</span>**
* **TCP Timer Setup
  You can configure the wait time to keep a needed resource available, when waiting to establish a TCP or TLS connection.
  transport.setuptimer.tcp
  Application: MCP
  Section: SIP
  Takes effect: At start/restart
  Valid values: Integers 1,000-32,000 (milliseconds)
  Default: 3,0000 (3 seconds)**

### **Resolved issues:**

## **Release 8.5.150.81 (01/21/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.150.81 | 01/21/16 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.150.84 (02/15/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.150.84 | 02/15/16 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.150.90 (03/24/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.150.90 | 03/24/16 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.150.91 (04/28/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.150.91 | 04/28/16 | Hot Fix |  |  |  |  | X |

### New Features:

* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**

### **Resolved issues:**

## **Release 8.5.161.34 (06/16/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.161.34 | 06/16/16 | General |  |  | X |  | X |

### New Features:

* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**
* **GIR call recording can now continue even if the public key recording certificate has expired. This feature is enabled by default, and configured by this option:**
* **Now you can use the option curlredirect to control how HTTP redirects are handled, so that HTTP redirection can function properly.**
* **Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Genesys Media Server now supports Apple's HTTP Live streaming (draft-pantos-http-live-streaming-16) subset of features. Media Server can now play media and master playlists of the type On-Demand, Event and Live.**

### **Resolved issues:**

## **Release 8.5.161.49 (07/13/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.161.49 | 07/13/16 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.170.71 (09/27/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.170.71 | 09/27/16 | General |  |  | X |  | X |

### New Features:

* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**
* **Media Control Platform supports TCP keep-alive functionality. Manage Keep Alive functionality with these configuration options, all in the Media Control Platform application:**
* **To support IVR Recording , Media Control Platform honors these recording Request URI parameters when executing VoiceXML applications: start, stop, pause, and resume. Previously for recording IVR, MCP supported only the start and stop parameters.**
* **Media Control Platform supports pass-through when caller and agent are using the same codecs and GIR recording is enabled. This parameter, new in release 8.5.170.71, configures pass-through:**

### **Resolved issues:**

## **Release 8.5.170.86 (11/28/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.170.86 | 11/28/16 | Hot Fix |  |  | X |  |  |

### New Features:

* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Media Control Platform now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**

### **Resolved issues:**

## **Release 8.5.176.05 (01/30/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.176.05 | 01/30/17 | General |  |  | X |  | X |

### New Features:

* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**
* **Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.**
* **MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **You can now mask a customer’s sensitive information in MCP log files with asterisks (\*) by using a new configuration option mask\_sensitive\_data in the [log] section. Masking sensitive data using this new option applies only when the MCP logging level is set to trace, debug, or all. This masking capability is not available for the standard or interaction levels of MCP logging, use the gvp:private option in such cases.**
* **MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.**

### **Resolved issues:**

## **Release 8.5.176.13 (02/17/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.176.13 | 02/17/17 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.176.16 (04/24/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.176.16 | 04/24/17 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.178.78 (05/24/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.178.78 | 05/24/17 | General |  |  | X |  | X |

### New Features:

* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**
* **Media Control Platform (MCP) now supports two new security parameters specific to Nuance Server (version 10.2 and above). The supported parameters are swirec.secure\_context and swirec.mute\_wcr. According to Nuance's requirement, MCP sends the swirec.secure\_context parameter in the RECOGNIZE and DEFINE-GRAMMAR requests; and swirec.mute\_wcr in the RECOGNIZE request only.**
* **The description for the codec option in the [mpc] section within the MCP XML file now provides additional information about the order of codecs that MCP offers.**
* **The description for the record.appenduniqueid option in the [MSML] section within the MCP XML file now includes additional information about the exact MSML Dialog Based recording.**

### **Resolved issues:**

## **Release 8.5.178.94 (06/05/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.178.94 | 06/05/17 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.181.78 (09/15/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.181.78 | 09/15/17 | General |  |  | X |  | X |

### New Features:

* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**
* **Media Control Platform (MCP) no longer sends the swirec.secure\_context or swirec.mute\_wcr property to the ASR server through MRCPv1. Nuance Recognizer does not support these parameters with MRCPv1.**
* **A new MCP configuration option cpa.no\_ring\_result specifies the call progress analysis (CPA) result if no ringback is detected before the postconnect event arrives. The default option value is none (0), that is, postconnect CPA proceeds normally after the postconnect event arrives. Other valid values are busy (2), human (15), machine (16), fax (17), and no\_media (18). If this option value is set to any one of these values, the specified CPA result is returned immediately after the postconnect event arrives, and no further CPA occurs.**
* **MCP now supports MRCP 201 response. Previously, MCP was sending an error response for 201 responses.**
* **MCP now supports a new codec library for MP3 encoding/decoding. Using this codec library resolves the issue where MCP unexpectedly terminates in specific environments while performing MP3 recording using the earlier MP3 encoding library. As this issue occurs only in specific environments, Genesys recommends continuing with the existing default configuration if no issues are observed while performing MP3 recording. The legacy codec continues to be available and is set as the default option.**
* **MCP now supports configuring the TCP\_NODELAY option for LibCurl. Enabling enabletcpnodelay (default) causes small segments of data to be sent without delay (disabling the Nagle algorithm).**

### **Resolved issues:**

Resource Manager

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.1.502.76  12/20/13  General  8.1.502.76  12/20/13  General  8.5.050.34  03/05/14  Hot Fix  8.5.050.36  05/05/14  Hot Fix  8.5.130.58  03/23/15  General  8.5.130.58  03/23/15  General  8.5.130.58  03/23/15  General |  | 8.5.181.66  10/06/17  Hot Fix | 29  29  27  26  19  19  19 | 8.5.181.66  10/06/17  Hot Fix | 29  29  27  26  19  19  19 |

## **Release 8.5.001.89 (12/20/13)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.001.89 | 12/20/13 | General |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.27 (01/20/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.27 | 01/20/14 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.34 (03/05/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.34 | 03/05/14 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.36 (05/05/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.36 | 05/05/14 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.050.37 (07/25/14)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.050.37 | 07/25/14 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.101.21 (07/15/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.101.21 | 07/15/14 | General |  |  | X |  | X |

### New Features:

* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Configuration Options Changed**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Configuration Options Changed**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Configuration Options Changed**
* **Route Unavailable Wakeup**
* **Reliable Connection Retry**
* **Configuration Options Changed**

### **Resolved issues:**

## **Release 8.5.110.26 (09/19/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.110.26 | 09/19/14 | General |  |  | X |  | X |

### New Features:

* **Resource Manager now retries sending inter-node messages that receive the 10035 socket error (WSAEWOULDBLOCK) while being sent.**
* **Added support for Windows 2012 64-bit, in Active-Active High Availability configurations.**
* **Resource Manager now retries sending inter-node messages that receive the 10035 socket error (WSAEWOULDBLOCK) while being sent.**
* **Added support for Windows 2012 64-bit, in Active-Active High Availability configurations.**
* **Resource Manager now retries sending inter-node messages that receive the 10035 socket error (WSAEWOULDBLOCK) while being sent.**
* **Added support for Windows 2012 64-bit, in Active-Active High Availability configurations.**
* **Resource Manager now retries sending inter-node messages that receive the 10035 socket error (WSAEWOULDBLOCK) while being sent.**
* **Added support for Windows 2012 64-bit, in Active-Active High Availability configurations.**

### **Resolved issues:**

## **Release 8.5.110.50 (09/26/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.110.50 | 09/26/14 | General |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.120.62 (12/18/14)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.120.62 | 12/18/14 | General |  |  | X |  | X |

### New Features:

* **Resource Manager supports Windows 2012 64-bit, in Active-Standby High Availability configurations.**
* **Resource Manager supports Windows 2012 64-bit, in Active-Standby High Availability configurations.**
* **Resource Manager supports Windows 2012 64-bit, in Active-Standby High Availability configurations.**
* **Resource Manager supports Windows 2012 64-bit, in Active-Standby High Availability configurations.**

### **Resolved issues:**

## **Release 8.5.120.67 (02/11/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.120.67 | 02/11/15 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.130.58 (03/23/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.58 | 03/23/15 | General |  |  | X |  | X |

### New Features:

* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**
* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**
* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**
* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**
* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**
* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**
* **Resource Manager can now be configured to reject a call request if the geo-location of the targeted Logical Resource Group (LRG) does not match with geo-location attribute of the call request. This extends to all calls, a behavior that previously applied only to recording solution calls. Read about this behavior and the option that controls it, reject-on-geo-location-nomatch (new in release 8.5.1), in Locating Resources Using Geo-Location.**
* **A new option for the Resource Manager application enables releasing the connection when the ActiveMQ Producer sends a method that is blocked due to network disconnect or congestion issues.
  Section: ems
  Option: rc.amq\_connection\_send\_timeout
  Valid Values: Any integer greater than or equal to 45.
  Default Value: 60.
  Takes effect: After start/restart.
  When this option is set to true, Resource manager waits for the time specifies in AMQ Thread Connection Send Timeout and then releases the connection.**

### **Resolved issues:**

## **Release 8.5.130.73 (05/22/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.73 | 05/22/15 | General |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.130.74 (06/01/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.74 | 06/01/15 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.130.75 (07/01/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.130.75 | 07/01/15 | Hot Fix |  |  | X |  |  |

### New Features:

* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**
* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**
* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**
* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**
* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**
* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**
* **Set to true to disable Resource Manager's use of the gvp.rm.resource-req option for VXML fallback after a CTIC 404 error.**
* **Set to false, to enable Resource Manager's use of gvp.rm.resource-req.**

### **Resolved issues:**

## **Release 8.5.141.18 (08/28/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.141.18 | 08/28/15 | General |  |  | X |  | X |

### New Features:

* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**
* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**
* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**
* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**
* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**
* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**
* **You can now direct Resource Manager to not reapply RURI capability when falling back to VXML after CTIC returns a 404 error. Previously, reapplying RURI capability caused the fallback to fail.
  Use a new configuration option in the Gateway LRG section in order to achieve this functionality:
  remove-ruri-capability-on-fallback
  Section: Gateway Resource group section
  Valid Values: true or false (default)
  Set to true to disable Resource Manager's use of the gvp.rm.resource-req option's capability during VXML fallback after a CTIC 404 error.
  Set to false, to enable Resource Manager's use of the gvp.rm.resource-req.
  Note: This option is NOT available during configuration of a Gateway Resource Group via Genesys Administrator. Specify this parameter manually in the Gateway Logical Resource Group (GW LRG) section, using the format remove-ruri-capability-on-fallback = true (or = false).**
* **Resource Manager now supports dynamic updating of a child tenant name change.**

### **Resolved issues:**

## **Release 8.5.141.27 (11/17/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.141.27 | 11/17/15 | Hot Fix |  |  | X |  |  |

### New Features:

* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**
* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**
* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**
* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**
* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**
* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**
* **The TCP setup timer is now configurable.
  Use sip.transport.setuptimer.tcp parameter in the proxy, monitor, subscription, and registrar sections to configure the timer.
  Default value : 30000 ms
  Min Value: 1000 ms
  Max value: 32000 ms**

### **Resolved issues:**

## **Release 8.5.141.29 (12/18/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.141.29 | 12/18/15 | Hot Fix |  |  | X |  |  |

### New Features:

* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  cti-unavailable-respcode
  Valid Values: not specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes effect: after restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.
  When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action - answer/reject/script
  Valid Values: reject (default), answer, script;service-type;URL
  Takes effect: after restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When set to not specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action .**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any any error from CTIC.**
* **When set to not specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;service-type;URL to specify that RM redirects the call to the service service-type and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**

### **Resolved issues:**

## **Release 8.5.141.30 (01/13/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.141.30 | 01/13/16 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.150.94 (02/05/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.150.94 | 02/05/16 | General |  |  | X |  | X |

### New Features:

* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**
* **Resource Manager (RM) has three new options in the CTI Connector (CTIC) Logical Resource Group (LRG) for handling CTIC failover.
  Important: These options are not available during configuration of a CTIC Resource Group via Genesys Administrator. You must specify them manually in the CTIC LRG.
  fail-over-cti-handling
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  This option specifies RM behavior when all attempts to use CTIC fail. For example: all CTICs are down, or port capacity of the CTIC LRG is exceeded, or all CTICs in the LRG were tried but failed.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).
  cti-unavailable-respcode
  Valid Values: No value specified (default), none, SIP response codes for which next CTI resource should not be retried.
  Takes Effect: After restart
  Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.
  When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.
  When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.
  Note: cti-unavailable-respcode overrides the server parameter rm.cti-unavailable-respcode.
  cti-unavailable-action
  Valid Values: reject (default), answer, script;<service-type>;<URL>
  Takes Effect: After restart
  Specifies the behavior expected when the SIP response code received from CTIC matches a response code that is configured in rm.cti-unavailable-respcode.
  Set to reject to reject the call.
  Set to answer to answer the call.
  Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).
  When no value is specified, RM uses the server-level parameter rm.cti-unavailable-action.
  Note: This option overrides rm.cti-unavailable-action.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailable-action).**
* **Specifies a list of response codes to be intercepted and given special treatment. Separate each code in the list with a semicolon (;).
  If CTIC returns a response code matching a code provided in the list, RM does not retry any other CTIC; instead RM takes action based on the group-level option cti-unavailable-action, or based on the server-level option rm.cti-unavailable-action.**
* **When set to empty or none, RM retries the next CTIC available in the CTI LRG in response to any error from CTIC.**
* **When no value is specified, RM checks the server-level parameter rm.cti-unavailable-respcode and takes the action specified there.**
* **Set to reject to reject the call.**
* **Set to answer to answer the call.**
* **Set to script;<service-type>;<URL> to specify that RM redirects the call to the service <service-type> and informs that service to run the page at the URL (same behavior as rm.cti-unavailble-action).**
* **The TCP setup timer is now configurable.**

### **Resolved issues:**

## **Release 8.5.160.74 (06/16/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.160.74 | 06/16/16 | General |  |  | X |  | X |

### New Features:

* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**
* **Support for the Red Hat Enterprise Linux (RHEL) 7 operating system. See the Supported Operating Environment: Genesys Voice Platform page for more detailed information and a list of all supported operating systems.**

### **Resolved issues:**

## **Release 8.5.170.64 (09/27/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.170.64 | 09/27/16 | General |  |  | X |  | X |

### New Features:

* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**
* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**
* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**
* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**
* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**
* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**
* **With this release, Resource Manager enables VXML IVR Recording, in a way similar to MSML GIR recording. Use the configuration option gvp.policy.voicexml-recording-allowed to configure VXML IVR Recording. When set to true (the default), this option instructs Resource Manager to:**
* **Resource Manager supports the service-type record in an IVR Profile. RM locates and selects the appropriate record IVR profile.**
* **Resource Manager supports geo-location based selection of the record IVR profile, configured by the gvp.general.geo-location option in the IVR profile.**

### **Resolved issues:**

## **Release 8.5.170.77 (12/20/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.170.77 | 12/20/16 | Hot Fix |  |  | X |  |  |

### New Features:

* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**

### **Resolved issues:**

## **Release 8.5.175.95 (01/30/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.175.95 | 01/30/17 | General |  |  | X |  | X |

### New Features:

* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**
* **Resource Manager (RM) now uses OpenSSL libraries version 1.0.2j. RM supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3, and SSLv23.**
* **RM now checks the write permission of the directory in which the SQLite DB file will be created and does not start if the DB file fails to open.**
* **You can now override the policy setting for IVR recording by enabling a new configuration option voicexml-recording-allowed in the [rm] section of the Resource Manager application.**

### **Resolved issues:**

## **Release 8.5.176.04 (03/03/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.176.04 | 03/03/17 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.178.66 (05/15/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.178.66 | 05/15/17 | General |  |  | X |  | X |

### New Features:

* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) additionally records notice level logs for enhanced debugging, when the logging level is set to trace. The additional notice level records logged for a call are:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**

### **Resolved issues:**

## **Release 8.5.178.79 (06/09/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.178.79 | 06/09/17 | General |  |  | X |  | X |

### New Features:

* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**
* **Resource Manager (RM) logging has been enhanced to enable better debugging, when the logging level is set to trace. The additional log details for a call now include:**
* **RM no longer accepts calls when the weight parameter of a site is set to zero in the corresponding gvp.site folder.**
* **You can now use the new configuration option optionsofflineresp to configure SIP OPTIONS response codes that RM checks while marking a resource offline.**

### **Resolved issues:**

## **Release 8.5.178.80 (06/30/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.178.80 | 06/30/17 | Hot Fix |  |  | X |  |  |

### New Features:

### **Resolved issues:**

## **Release 8.5.181.61 (09/15/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.181.61 | 09/15/17 | General |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.181.66 (10/06/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.181.66 | 10/06/17 | Hot Fix |  |  |  |  | X |

### New Features:

### **Resolved issues:**

Orchestration Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Business Rules Execution Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Business Rules Application Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
|  |  |  |  |  |  |

Genesys Administrator Extension

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current deployed  version** | **Last Care recommendation** | **Latest version, same code stream** | **Version "delta", deployed  latest, same code stream** | **Latest version, all code streams** | **Version "delta", deployed  latest, all code streams** |
| 8.5.2  02/10/15  General  8.5.2  02/10/15  General |  | http://  undefined  undefined | 24  24 | http://  undefined  undefined | 24  24 |

## **Release 8.5.200.12 (02/10/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.12 | 02/10/15 | General |  |  | X |  | X |

### New Features:

* **Bulk import and export of agents—You can now provision new and existing agents in bulk by preparing a CSV (comma-separated values) file outside of GAX, and then importing it into GAX. You can also export data for selected (or all) agents from GAX into a CSV file, modify it as required, and import back into GAX. GAX can also generate template CSV files, which you can save and use to prepare import CSV files.**
* **Bulk import and export of agents—You can now provision new and existing agents in bulk by preparing a CSV (comma-separated values) file outside of GAX, and then importing it into GAX. You can also export data for selected (or all) agents from GAX into a CSV file, modify it as required, and import back into GAX. GAX can also generate template CSV files, which you can save and use to prepare import CSV files.**

### **Resolved issues:**

## **Release 8.5.200.13 (02/26/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.13 | 02/26/15 | Hot Fix |  |  | X |  | X |

### New Features:

* **New Privileges for Bulk Operations: The new group of role privileges, User Bulk Operations, contains the following role privileges, which can be used to control who can perform bulk import and export using .csv files:
  CREATE\_USER\_BULK\_OPS—Allows a user to access the History window; to start, resume, or stop operations in the History window; and to import a .csv file.
  ADMINISTER\_USER\_BULK\_OPS—Allows a user to access the History window; and to delete operations in the History window.
  EXPORT\_SPREADSHEET\_USER\_BULK\_OPS—Allows a user to create a .csv template.**
* **CREATE\_USER\_BULK\_OPS—Allows a user to access the History window; to start, resume, or stop operations in the History window; and to import a .csv file.**
* **ADMINISTER\_USER\_BULK\_OPS—Allows a user to access the History window; and to delete operations in the History window.**
* **EXPORT\_SPREADSHEET\_USER\_BULK\_OPS—Allows a user to create a .csv template.**
* **New Privileges for Bulk Operations: The new group of role privileges, User Bulk Operations, contains the following role privileges, which can be used to control who can perform bulk import and export using .csv files:
  CREATE\_USER\_BULK\_OPS—Allows a user to access the History window; to start, resume, or stop operations in the History window; and to import a .csv file.
  ADMINISTER\_USER\_BULK\_OPS—Allows a user to access the History window; and to delete operations in the History window.
  EXPORT\_SPREADSHEET\_USER\_BULK\_OPS—Allows a user to create a .csv template.**
* **CREATE\_USER\_BULK\_OPS—Allows a user to access the History window; to start, resume, or stop operations in the History window; and to import a .csv file.**
* **ADMINISTER\_USER\_BULK\_OPS—Allows a user to access the History window; and to delete operations in the History window.**
* **EXPORT\_SPREADSHEET\_USER\_BULK\_OPS—Allows a user to create a .csv template.**

### **Resolved issues:**

## **Release 8.5.200.18 (04/06/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.200.18 | 04/06/15 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.210.10 (05/08/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.210.10 | 05/08/15 | General |  |  | X |  | X |

### New Features:

* **Bulk assignment of Skills to multiple Agents—You can now assign Skills and associated ratings to multiple Agents with one click. You can also create and assign a new Skill within a single view.**
* **Preferred hosts for Solution Deployment—You can now specify a list of preferred hosts (called whitelisted hosts) to and from which Installation Packages are sent and retrieved.**
* **Support for new version of PostgreSQL Database Management System—GAX now supports PostgreSQL version 9.3.**
* **Instructions for installing ARM Runtime Server on Windows—Instructions are now available for setting up the Audio Resource Management Runtime Server on Windows.**
* **Language Packs—This release of Genesys Administrator Extension supports the following Language Packs. Consult the Language Pack release notes for information on changes to the Language Pack that may affect the functionality of Genesys Administrator Extension.
  Chinese (Simplified) 8.5.210.10
  Czech 8.5.210.10
  French (France) 8.5.210.10
  French (Canada) 8.5.210.10
  German 8.5.210.10
  Italian 8.5.210.10
  Japanese 8.5.210.10
  Korean 8.5.210.10
  Polish 8.5.210.10
  Portuguese (Brazilian) 8.5.210.10
  Russian 8.5.210.10
  Spanish (Latin American) 8.5.210.10
  Turkish 8.5.210.10**
* **Chinese (Simplified) 8.5.210.10**
* **Czech 8.5.210.10**
* **French (France) 8.5.210.10**
* **French (Canada) 8.5.210.10**
* **German 8.5.210.10**
* **Italian 8.5.210.10**
* **Japanese 8.5.210.10**
* **Korean 8.5.210.10**
* **Polish 8.5.210.10**
* **Portuguese (Brazilian) 8.5.210.10**
* **Russian 8.5.210.10**
* **Spanish (Latin American) 8.5.210.10**
* **Turkish 8.5.210.10**
* **Bulk assignment of Skills to multiple Agents—You can now assign Skills and associated ratings to multiple Agents with one click. You can also create and assign a new Skill within a single view.**
* **Preferred hosts for Solution Deployment—You can now specify a list of preferred hosts (called whitelisted hosts) to and from which Installation Packages are sent and retrieved.**
* **Support for new version of PostgreSQL Database Management System—GAX now supports PostgreSQL version 9.3.**
* **Instructions for installing ARM Runtime Server on Windows—Instructions are now available for setting up the Audio Resource Management Runtime Server on Windows.**
* **Language Packs—This release of Genesys Administrator Extension supports the following Language Packs. Consult the Language Pack release notes for information on changes to the Language Pack that may affect the functionality of Genesys Administrator Extension.
  Chinese (Simplified) 8.5.210.10
  Czech 8.5.210.10
  French (France) 8.5.210.10
  French (Canada) 8.5.210.10
  German 8.5.210.10
  Italian 8.5.210.10
  Japanese 8.5.210.10
  Korean 8.5.210.10
  Polish 8.5.210.10
  Portuguese (Brazilian) 8.5.210.10
  Russian 8.5.210.10
  Spanish (Latin American) 8.5.210.10
  Turkish 8.5.210.10**
* **Chinese (Simplified) 8.5.210.10**
* **Czech 8.5.210.10**
* **French (France) 8.5.210.10**
* **French (Canada) 8.5.210.10**
* **German 8.5.210.10**
* **Italian 8.5.210.10**
* **Japanese 8.5.210.10**
* **Korean 8.5.210.10**
* **Polish 8.5.210.10**
* **Portuguese (Brazilian) 8.5.210.10**
* **Russian 8.5.210.10**
* **Spanish (Latin American) 8.5.210.10**
* **Turkish 8.5.210.10**

### **Resolved issues:**

## **Release 8.5.210.12 (07/09/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.210.12 | 07/09/15 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.210.13 (09/11/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.210.13 | 09/11/15 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.210.14 (10/20/15)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.210.14 | 10/20/15 | Hot Fix |  |  | X |  | X |

### New Features:

* **GAX now supports PSDK 851.3.4.**
* **GAX now supports PSDK 851.3.4.**

### **Resolved issues:**

## **Release 8.5.220.20 (11/20/15)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.20 | 11/20/15 | General |  |  | X |  | X |

### New Features:

* **Enhanced secure connections for Solution Deployment: You can now configure Mutual TLS on connections between Genesys Deployment Agent and the Genesys Administrator Extension server.**
* **Centralized Log: You can now view the Centralized Log in GAX. Besides viewing the log records, you can sort them and use filters to find specific logs.**
* **Increased number of available Audio Resource IDs: In a single-tenant configuration, the number of available Audio Resource IDs is increased from 1000 to 9000, with the range increasing from 9000–9999 to 1000–9999.**
* **Support for Apache Tomcat 7 web server: See Supported Operating Environment: Genesys Administrator Extension for more detailed information and a list of all prerequisites.**
* **Support for the following web browsers:
  Apple Safari 7
  Apple Safari 8
  See Supported Operating Environment: Genesys Administrator Extension for more detailed information and a list of all supported browsers.**
* **Apple Safari 7**
* **Apple Safari 8**
* **Enhanced secure connections for Solution Deployment: You can now configure Mutual TLS on connections between Genesys Deployment Agent and the Genesys Administrator Extension server.**
* **Centralized Log: You can now view the Centralized Log in GAX. Besides viewing the log records, you can sort them and use filters to find specific logs.**
* **Increased number of available Audio Resource IDs: In a single-tenant configuration, the number of available Audio Resource IDs is increased from 1000 to 9000, with the range increasing from 9000–9999 to 1000–9999.**
* **Support for Apache Tomcat 7 web server: See Supported Operating Environment: Genesys Administrator Extension for more detailed information and a list of all prerequisites.**
* **Support for the following web browsers:
  Apple Safari 7
  Apple Safari 8
  See Supported Operating Environment: Genesys Administrator Extension for more detailed information and a list of all supported browsers.**
* **Apple Safari 7**
* **Apple Safari 8**

### **Resolved issues:**

## **Release 8.5.220.22 (03/23/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.22 | 03/23/16 | Hot Fix |  |  | X |  | X |

### New Features:

* **GAX now properly displays the Audio Resource ID in the title bar of the Details view of the corresponding Audio Resource. Previously, the Audio Resource ID was not displayed anywhere in the Details view.**
* **GAX now allows the user to set a different day, month, and/or year when cloning a Statistical Day object. Previously, the original day, month and year was used in the cloned object.**
* **GAX now properly displays the Audio Resource ID in the title bar of the Details view of the corresponding Audio Resource. Previously, the Audio Resource ID was not displayed anywhere in the Details view.**
* **GAX now allows the user to set a different day, month, and/or year when cloning a Statistical Day object. Previously, the original day, month and year was used in the cloned object.**

### **Resolved issues:**

## **Release 8.5.220.24 (04/07/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.24 | 04/07/16 | Hot Fix |  |  | X |  | X |

### New Features:

* **GAX now supports gzip compression for static files. This can significantly decrease the time it takes to load data.**
* **GAX now supports gzip compression for static files. This can significantly decrease the time it takes to load data.**

### **Resolved issues:**

## **Release 8.5.220.25 (05/31/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.25 | 05/31/16 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.220.28 (07/05/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.28 | 07/05/16 | Hot Fix |  |  | X |  | X |

### New Features:

* **This release reduces the potential vulnerability to a Reflected File Download (RFD) attack.**
* **This release reduces the potential vulnerability to a Reflected File Download (RFD) attack.**

### **Resolved issues:**

## **Release 8.5.220.34 (08/31/16)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.34 | 08/31/16 | Hot Fix |  |  | X |  | X |

### New Features:

* **More efficient assignment of Agent Logins: When assigning an Agent Login to an Agent using Configuration Manager or Agent Management, GAX now displays a list of only unassigned Agent Logins for assignment.**
* **Increased granularity for scheduling Operational Parameters: In the Operational Parameters Management module of GAX, the granularity of scheduling Operation Parameters can be set to 5 minutes, and the default value has been reduced to 15 minutes from 30. This option is set in User Preferences.**
* **DB Server switchover enabled: GAX now enables you to switch over DB Server from backup to primary mode when required.**
* **Enhanced interface: The GAX interface has been enhanced as follows:
  When exporting agents, the default Action is now UPDATE, instead of ADD. This is designed to prevent errors arising from multiple (and accidental) ADDs.
  The list of Agents now includes an Employee ID column, making it easier to view Employee IDs without viewing the agent details.**
* **When exporting agents, the default Action is now UPDATE, instead of ADD. This is designed to prevent errors arising from multiple (and accidental) ADDs.**
* **The list of Agents now includes an Employee ID column, making it easier to view Employee IDs without viewing the agent details.**
* **More efficient assignment of Agent Logins: When assigning an Agent Login to an Agent using Configuration Manager or Agent Management, GAX now displays a list of only unassigned Agent Logins for assignment.**
* **Increased granularity for scheduling Operational Parameters: In the Operational Parameters Management module of GAX, the granularity of scheduling Operation Parameters can be set to 5 minutes, and the default value has been reduced to 15 minutes from 30. This option is set in User Preferences.**
* **DB Server switchover enabled: GAX now enables you to switch over DB Server from backup to primary mode when required.**
* **Enhanced interface: The GAX interface has been enhanced as follows:
  When exporting agents, the default Action is now UPDATE, instead of ADD. This is designed to prevent errors arising from multiple (and accidental) ADDs.
  The list of Agents now includes an Employee ID column, making it easier to view Employee IDs without viewing the agent details.**
* **When exporting agents, the default Action is now UPDATE, instead of ADD. This is designed to prevent errors arising from multiple (and accidental) ADDs.**
* **The list of Agents now includes an Employee ID column, making it easier to view Employee IDs without viewing the agent details.**

### **Resolved issues:**

## **Release 8.5.220.45 (08/04/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.45 | 08/04/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.220.47 (10/27/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.220.47 | 10/27/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.230.03 (10/31/16)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.230.03 | 10/31/16 | General |  |  | X |  | X |

### New Features:

* **Improved access control for operational Parameter Groups: Parameter Group Templates can now be deployed to Folders of type Transaction within the Tenant. The resulting Parameter Group has the same access permissions as the Folder.**
* **Enhanced interface: The GAX interface has been enhanced as follows:
  The Agents View now displays the total number of agents associated with the Tenant and available for display, the number of agents (if any) selected by a filter applied to that list, and the number of agents (if any) selected for editing.
  After editing an agent or an Audio Resource, GAX now retains the sort order and filter results of the list from which the object was selected for editing. The modified record is displayed in its proper place in the sorted list, so no scrolling is needed to view it.**
* **The Agents View now displays the total number of agents associated with the Tenant and available for display, the number of agents (if any) selected by a filter applied to that list, and the number of agents (if any) selected for editing.**
* **After editing an agent or an Audio Resource, GAX now retains the sort order and filter results of the list from which the object was selected for editing. The modified record is displayed in its proper place in the sorted list, so no scrolling is needed to view it.**
* **Language Packs—Two additional languages are supported beginning with this release of Genesys Administrator Extension:
  Arabic (Saudi Arabia)
  Chinese (Traditional)**
* **Arabic (Saudi Arabia)**
* **Chinese (Traditional)**
* **Improved access control for operational Parameter Groups: Parameter Group Templates can now be deployed to Folders of type Transaction within the Tenant. The resulting Parameter Group has the same access permissions as the Folder.**
* **Enhanced interface: The GAX interface has been enhanced as follows:
  The Agents View now displays the total number of agents associated with the Tenant and available for display, the number of agents (if any) selected by a filter applied to that list, and the number of agents (if any) selected for editing.
  After editing an agent or an Audio Resource, GAX now retains the sort order and filter results of the list from which the object was selected for editing. The modified record is displayed in its proper place in the sorted list, so no scrolling is needed to view it.**
* **The Agents View now displays the total number of agents associated with the Tenant and available for display, the number of agents (if any) selected by a filter applied to that list, and the number of agents (if any) selected for editing.**
* **After editing an agent or an Audio Resource, GAX now retains the sort order and filter results of the list from which the object was selected for editing. The modified record is displayed in its proper place in the sorted list, so no scrolling is needed to view it.**
* **Language Packs—Two additional languages are supported beginning with this release of Genesys Administrator Extension:
  Arabic (Saudi Arabia)
  Chinese (Traditional)**
* **Arabic (Saudi Arabia)**
* **Chinese (Traditional)**

### **Resolved issues:**

## **Release 8.5.240.19 (03/03/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.240.19 | 03/03/17 | General |  |  | X |  | X |

### New Features:

* **Bulk provisioning of configuration objects—You can now provision new and existing objects in bulk by preparing a CSV (comma-separated values) file outside of GAX, and then importing it into GAX. You can also export data for selected (or all) objects of those types from GAX into a CSV file, modify it as required, and import it back into GAX. GAX can also generate template CSV files, which you can save and use to prepare import CSV files. This feature applies to the following object types:
  DN and DN Groups
  Places and Place Groups
  Persons (Users)
  Agent Groups**
* **DN and DN Groups**
* **Places and Place Groups**
* **Persons (Users)**
* **Agent Groups**
* **Bulk provisioning of configuration options—You can now provision new and existing configuration options for a given object by preparing a CSV (comma-separated values) or CFG (configuration) file outside of GAX, and then importing it into GAX. You can also export configuration options for an object from GAX into a CSV or CFG file, modify it as required, and import it back into GAX. GAX can also generate template CSV files, which you can save and use to prepare import CSV files.**
* **Enhanced change confirmation dialogs—Before completing configuration changes, especially those involving deletion of data or objects, the user must explicitly acknowledge the impact of the changes before submitting the changes.**
* **Enhanced interface and improved usability: The GAX interface has been enhanced as follows:
  The Applications tab in System Dashboard now includes a column that shows the folder path for each Application, starting with the Tenant name, making it easier to find specific Applications.
  Tables of configuration options now include two more columns, one showing the name including the section, and the other showing the section name only. The sections can still be collapsed, as before.
  On configuration screens, the text of the Delete button now reads Delete <object type>, to prevent the unintentional deletion of the whole object when the intent was to delete only a property.
  The object list views in Configuration Manager now display the total number of objects in the Folder, the number selected by a filter (if any) applied to that list, and the number of agents selected (if any).
  When cloning an object, specific properties can be configured to not be copied to the new object.
  Personalities are now displayed in order of their names. Specific columns can also be configured to be shown/hidden in the view. In addition, the number of personalities available to Audio Resource IDs in single-tenant configurations is increased from 100 to 1000, with the range changing from 0-99 to 0-999. Use this option with extreme caution.
  Applications and Solutions can now be started and stopped directly from the Application object list and Solution object list views, respectively, in Configuration Manager.
  The GAX Capacity Wizard now accepts a value of 0 (zero) as maximum capacity, thereby disabling routing to a particular media.
  Statistical Day objects can now be adjusted to account for the extra day in a leap year.**
* **The Applications tab in System Dashboard now includes a column that shows the folder path for each Application, starting with the Tenant name, making it easier to find specific Applications.**
* **Tables of configuration options now include two more columns, one showing the name including the section, and the other showing the section name only. The sections can still be collapsed, as before.**
* **On configuration screens, the text of the Delete button now reads Delete <object type>, to prevent the unintentional deletion of the whole object when the intent was to delete only a property.**
* **The object list views in Configuration Manager now display the total number of objects in the Folder, the number selected by a filter (if any) applied to that list, and the number of agents selected (if any).**
* **When cloning an object, specific properties can be configured to not be copied to the new object.**
* **Personalities are now displayed in order of their names. Specific columns can also be configured to be shown/hidden in the view. In addition, the number of personalities available to Audio Resource IDs in single-tenant configurations is increased from 100 to 1000, with the range changing from 0-99 to 0-999. Use this option with extreme caution.**
* **Applications and Solutions can now be started and stopped directly from the Application object list and Solution object list views, respectively, in Configuration Manager.**
* **The GAX Capacity Wizard now accepts a value of 0 (zero) as maximum capacity, thereby disabling routing to a particular media.**
* **Statistical Day objects can now be adjusted to account for the extra day in a leap year.**
* **Support for the following Databases and Browsers:
  MS SQL Server 2014 DBMS
  Microsoft Edge browser
  See the Supported Operating Environment: Genesys Administrator page for more detailed information and a list of all supported databases.**
* **MS SQL Server 2014 DBMS**
* **Microsoft Edge browser**
* **Bulk provisioning of configuration objects—You can now provision new and existing objects in bulk by preparing a CSV (comma-separated values) file outside of GAX, and then importing it into GAX. You can also export data for selected (or all) objects of those types from GAX into a CSV file, modify it as required, and import it back into GAX. GAX can also generate template CSV files, which you can save and use to prepare import CSV files. This feature applies to the following object types:
  DN and DN Groups
  Places and Place Groups
  Persons (Users)
  Agent Groups**
* **DN and DN Groups**
* **Places and Place Groups**
* **Persons (Users)**
* **Agent Groups**
* **Bulk provisioning of configuration options—You can now provision new and existing configuration options for a given object by preparing a CSV (comma-separated values) or CFG (configuration) file outside of GAX, and then importing it into GAX. You can also export configuration options for an object from GAX into a CSV or CFG file, modify it as required, and import it back into GAX. GAX can also generate template CSV files, which you can save and use to prepare import CSV files.**
* **Enhanced change confirmation dialogs—Before completing configuration changes, especially those involving deletion of data or objects, the user must explicitly acknowledge the impact of the changes before submitting the changes.**
* **Enhanced interface and improved usability: The GAX interface has been enhanced as follows:
  The Applications tab in System Dashboard now includes a column that shows the folder path for each Application, starting with the Tenant name, making it easier to find specific Applications.
  Tables of configuration options now include two more columns, one showing the name including the section, and the other showing the section name only. The sections can still be collapsed, as before.
  On configuration screens, the text of the Delete button now reads Delete <object type>, to prevent the unintentional deletion of the whole object when the intent was to delete only a property.
  The object list views in Configuration Manager now display the total number of objects in the Folder, the number selected by a filter (if any) applied to that list, and the number of agents selected (if any).
  When cloning an object, specific properties can be configured to not be copied to the new object.
  Personalities are now displayed in order of their names. Specific columns can also be configured to be shown/hidden in the view. In addition, the number of personalities available to Audio Resource IDs in single-tenant configurations is increased from 100 to 1000, with the range changing from 0-99 to 0-999. Use this option with extreme caution.
  Applications and Solutions can now be started and stopped directly from the Application object list and Solution object list views, respectively, in Configuration Manager.
  The GAX Capacity Wizard now accepts a value of 0 (zero) as maximum capacity, thereby disabling routing to a particular media.
  Statistical Day objects can now be adjusted to account for the extra day in a leap year.**
* **The Applications tab in System Dashboard now includes a column that shows the folder path for each Application, starting with the Tenant name, making it easier to find specific Applications.**
* **Tables of configuration options now include two more columns, one showing the name including the section, and the other showing the section name only. The sections can still be collapsed, as before.**
* **On configuration screens, the text of the Delete button now reads Delete <object type>, to prevent the unintentional deletion of the whole object when the intent was to delete only a property.**
* **The object list views in Configuration Manager now display the total number of objects in the Folder, the number selected by a filter (if any) applied to that list, and the number of agents selected (if any).**
* **When cloning an object, specific properties can be configured to not be copied to the new object.**
* **Personalities are now displayed in order of their names. Specific columns can also be configured to be shown/hidden in the view. In addition, the number of personalities available to Audio Resource IDs in single-tenant configurations is increased from 100 to 1000, with the range changing from 0-99 to 0-999. Use this option with extreme caution.**
* **Applications and Solutions can now be started and stopped directly from the Application object list and Solution object list views, respectively, in Configuration Manager.**
* **The GAX Capacity Wizard now accepts a value of 0 (zero) as maximum capacity, thereby disabling routing to a particular media.**
* **Statistical Day objects can now be adjusted to account for the extra day in a leap year.**
* **Support for the following Databases and Browsers:
  MS SQL Server 2014 DBMS
  Microsoft Edge browser
  See the Supported Operating Environment: Genesys Administrator page for more detailed information and a list of all supported databases.**
* **MS SQL Server 2014 DBMS**
* **Microsoft Edge browser**

### **Resolved issues:**

## **Release 8.5.240.23 (06/02/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.240.23 | 06/02/17 | Hot Fix |  |  | X |  | X |

### New Features:

* **Improved sorting of Audio Resources, Parameters, Group Templates, and Parameters Groups: You can now sort lists of Audio Resources, Parameters, Group Templates, and Parameters Groups by Name and Type. You can also toggle the sort order between ascending and descending by clicking the Toggle icon in the column header. By default, the lists are sorted in ascending order by Name. (GAX-9394)**
* **Improved sorting of Audio Resources, Parameters, Group Templates, and Parameters Groups: You can now sort lists of Audio Resources, Parameters, Group Templates, and Parameters Groups by Name and Type. You can also toggle the sort order between ascending and descending by clicking the Toggle icon in the column header. By default, the lists are sorted in ascending order by Name. (GAX-9394)**

### **Resolved issues:**

## **Release 8.5.250.15 (07/27/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.250.15 | 07/27/17 | General |  |  | X |  | X |

### New Features:

* **GAX Configuration Manager improvements:
  GAX can be put into Read Only or Emergency Mode to prevent any changes to the Configuration Database by anyone except a member of the Super Administrators Group. (GAX-9235)
  You can now perform Global Searches for configuration objects in Configuration Manager based on type, name, tenant, and state. (GAX-9286)
  You can now modify and edit options of multiple configuration objects simultaneously. (GAX-8855)
  You can now bulk provision Agent Logins for agents. (GAX-9246)
  Bulk Change Set (BCS) functionality is now hidden by default and not recommended for use. BCS will not be enhanced in the future and will be deprecated over time. Users are encouraged to use the Bulk Provisioning functions from the Configuration Manager menu instead. However, BCS capability can still be enabled using the option enable\_bulk\_change\_sets if required. (GAX-8846)**
* **GAX can be put into Read Only or Emergency Mode to prevent any changes to the Configuration Database by anyone except a member of the Super Administrators Group. (GAX-9235)**
* **You can now perform Global Searches for configuration objects in Configuration Manager based on type, name, tenant, and state. (GAX-9286)**
* **You can now modify and edit options of multiple configuration objects simultaneously. (GAX-8855)**
* **You can now bulk provision Agent Logins for agents. (GAX-9246)**
* **Bulk Change Set (BCS) functionality is now hidden by default and not recommended for use. BCS will not be enhanced in the future and will be deprecated over time. Users are encouraged to use the Bulk Provisioning functions from the Configuration Manager menu instead. However, BCS capability can still be enabled using the option enable\_bulk\_change\_sets if required. (GAX-8846)**
* **Audio Resource Management Auditing: You can now determine who added, modified, or removed Audio Resources and Personalities, and who reprocessed, downloaded, or deleted Audio Resources by viewing Audit logs in Centralized Logs. (GAX-9287)**
* **Security enhancements:
  GAX now supports the cipher suites used by Jetty, which must be configured based on your security requirements. (GAX-9361)
  You can configure GAX to use token-based authentication on user connections with Configuration Server. This enables GAX users to be authenticated externally using SAML with the customer’s IDP without the need for Configuration Server to go through LDAP connections. (GAX-8851)**
* **GAX now supports the cipher suites used by Jetty, which must be configured based on your security requirements. (GAX-9361)**
* **You can configure GAX to use token-based authentication on user connections with Configuration Server. This enables GAX users to be authenticated externally using SAML with the customer’s IDP without the need for Configuration Server to go through LDAP connections. (GAX-8851)**
* **Enhanced database connections:
  GAX now uses Microsoft JDBC Driver for MS SQL Server connections. (GAX-9360)
  You can now use a customized JDBC URL when configuring a Database Access Point (DAP) for the GAX Database instead of using a connection based on the DAP object itself. (GAX-9388)**
* **GAX now uses Microsoft JDBC Driver for MS SQL Server connections. (GAX-9360)**
* **You can now use a customized JDBC URL when configuring a Database Access Point (DAP) for the GAX Database instead of using a connection based on the DAP object itself. (GAX-9388)**
* **GAX Configuration Manager improvements:
  GAX can be put into Read Only or Emergency Mode to prevent any changes to the Configuration Database by anyone except a member of the Super Administrators Group. (GAX-9235)
  You can now perform Global Searches for configuration objects in Configuration Manager based on type, name, tenant, and state. (GAX-9286)
  You can now modify and edit options of multiple configuration objects simultaneously. (GAX-8855)
  You can now bulk provision Agent Logins for agents. (GAX-9246)
  Bulk Change Set (BCS) functionality is now hidden by default and not recommended for use. BCS will not be enhanced in the future and will be deprecated over time. Users are encouraged to use the Bulk Provisioning functions from the Configuration Manager menu instead. However, BCS capability can still be enabled using the option enable\_bulk\_change\_sets if required. (GAX-8846)**
* **GAX can be put into Read Only or Emergency Mode to prevent any changes to the Configuration Database by anyone except a member of the Super Administrators Group. (GAX-9235)**
* **You can now perform Global Searches for configuration objects in Configuration Manager based on type, name, tenant, and state. (GAX-9286)**
* **You can now modify and edit options of multiple configuration objects simultaneously. (GAX-8855)**
* **You can now bulk provision Agent Logins for agents. (GAX-9246)**
* **Bulk Change Set (BCS) functionality is now hidden by default and not recommended for use. BCS will not be enhanced in the future and will be deprecated over time. Users are encouraged to use the Bulk Provisioning functions from the Configuration Manager menu instead. However, BCS capability can still be enabled using the option enable\_bulk\_change\_sets if required. (GAX-8846)**
* **Audio Resource Management Auditing: You can now determine who added, modified, or removed Audio Resources and Personalities, and who reprocessed, downloaded, or deleted Audio Resources by viewing Audit logs in Centralized Logs. (GAX-9287)**
* **Security enhancements:
  GAX now supports the cipher suites used by Jetty, which must be configured based on your security requirements. (GAX-9361)
  You can configure GAX to use token-based authentication on user connections with Configuration Server. This enables GAX users to be authenticated externally using SAML with the customer’s IDP without the need for Configuration Server to go through LDAP connections. (GAX-8851)**
* **GAX now supports the cipher suites used by Jetty, which must be configured based on your security requirements. (GAX-9361)**
* **You can configure GAX to use token-based authentication on user connections with Configuration Server. This enables GAX users to be authenticated externally using SAML with the customer’s IDP without the need for Configuration Server to go through LDAP connections. (GAX-8851)**
* **Enhanced database connections:
  GAX now uses Microsoft JDBC Driver for MS SQL Server connections. (GAX-9360)
  You can now use a customized JDBC URL when configuring a Database Access Point (DAP) for the GAX Database instead of using a connection based on the DAP object itself. (GAX-9388)**
* **GAX now uses Microsoft JDBC Driver for MS SQL Server connections. (GAX-9360)**
* **You can now use a customized JDBC URL when configuring a Database Access Point (DAP) for the GAX Database instead of using a connection based on the DAP object itself. (GAX-9388)**

### **Resolved issues:**

## **Release 8.5.250.17 (08/04/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.250.17 | 08/04/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.250.18 (08/31/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.250.18 | 08/31/17 | Hot Fix |  |  | X |  | X |

### New Features:

* **This release of Genesys Administrator Extension supports the following Language Pack:
  French (Canada) 8.5.250.18**
* **French (Canada) 8.5.250.18**
* **This release of Genesys Administrator Extension supports the following Language Pack:
  French (Canada) 8.5.250.18**
* **French (Canada) 8.5.250.18**

### **Resolved issues:**

## **Release 8.5.250.19 (10/20/17)-Hot Fix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.250.19 | 10/20/17 | Hot Fix |  |  | X |  | X |

### New Features:

### **Resolved issues:**

## **Release 8.5.260.11 (12/07/17)-General**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| 8.5.260.11 | 12/07/17 | General |  |  | X |  | X |

### New Features:

* **You can now import an application metadata XML file into an existing or a new Application Template for Application objects. For more information, see the Importing Application Metadata section in the Application Templates page. (GAX-9234)**
* **GAX now supports SIP Business Continuity Switch Synchronization Wizard. For more information, see the Disaster Recovery tab in the Switches page. (GAX-8826)**
* **The following Apache Common Libraries are updated:
  commons-fileupload 1.3.3
  commons-io 2.5
  commons-lang3-3.6
  httpclient-4.5.3
  commons-beanutils 1.9.3
  commons-codec 1.10
  commons-io 2.5
  commons-pool2 2.4.2(GAX-9376)**
* **commons-fileupload 1.3.3**
* **commons-io 2.5**
* **commons-lang3-3.6**
* **httpclient-4.5.3**
* **commons-beanutils 1.9.3**
* **commons-codec 1.10**
* **commons-io 2.5**
* **commons-pool2 2.4.2**
* **Support for Tomcat 8. (GAX-9464)**
* **Support for MS SQL Server 2016 and MS SQL Server 2016 Cluster (AlwaysOn). See the Supported Operating Environment: Genesys Administrator page for more detailed information and a list of all supported operating systems. (GAX-9435)**
* **Support for JDK 1.6 is withdrawn starting from release 8.5.260.11 and JDK 1.7 is mandatory to install GAX 8.5.260.11. However, JDK 1.6 is still supported for releases prior to GAX 8.5.260.11 (GAX-9529)**
* **Now GAX can read the custom SSL key configurations from the gax.properties file. (GAX-9538)**
* **You can now configure Content Security Policy (CSP) headers for GAX in the gax.properties file. (GAX-9451)**
* **GAX now supports HTTP Strict Transport Security and you can enable it by configuring enable\_hsts=true in the gax.properties file. (GAX-9450)**
* **Personality and Audio Resource-related information is now written to GAX logs. (GAX-9424)**
* **You can now import an application metadata XML file into an existing or a new Application Template for Application objects. For more information, see the Importing Application Metadata section in the Application Templates page. (GAX-9234)**
* **GAX now supports SIP Business Continuity Switch Synchronization Wizard. For more information, see the Disaster Recovery tab in the Switches page. (GAX-8826)**
* **The following Apache Common Libraries are updated:
  commons-fileupload 1.3.3
  commons-io 2.5
  commons-lang3-3.6
  httpclient-4.5.3
  commons-beanutils 1.9.3
  commons-codec 1.10
  commons-io 2.5
  commons-pool2 2.4.2(GAX-9376)**
* **commons-fileupload 1.3.3**
* **commons-io 2.5**
* **commons-lang3-3.6**
* **httpclient-4.5.3**
* **commons-beanutils 1.9.3**
* **commons-codec 1.10**
* **commons-io 2.5**
* **commons-pool2 2.4.2**
* **Support for Tomcat 8. (GAX-9464)**
* **Support for MS SQL Server 2016 and MS SQL Server 2016 Cluster (AlwaysOn). See the Supported Operating Environment: Genesys Administrator page for more detailed information and a list of all supported operating systems. (GAX-9435)**
* **Support for JDK 1.6 is withdrawn starting from release 8.5.260.11 and JDK 1.7 is mandatory to install GAX 8.5.260.11. However, JDK 1.6 is still supported for releases prior to GAX 8.5.260.11 (GAX-9529)**
* **Now GAX can read the custom SSL key configurations from the gax.properties file. (GAX-9538)**
* **You can now configure Content Security Policy (CSP) headers for GAX in the gax.properties file. (GAX-9451)**
* **GAX now supports HTTP Strict Transport Security and you can enable it by configuring enable\_hsts=true in the gax.properties file. (GAX-9450)**
* **Personality and Audio Resource-related information is now written to GAX logs. (GAX-9424)**

### **Resolved issues:**

## **Release http:// (undefined)-undefined**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Release | Date | Release type | Restricted | Aix | Linux | Solaris | Windows |
| http:// | undefined | undefined |  |  |  |  |  |

### New Features:

### **Resolved issues:**