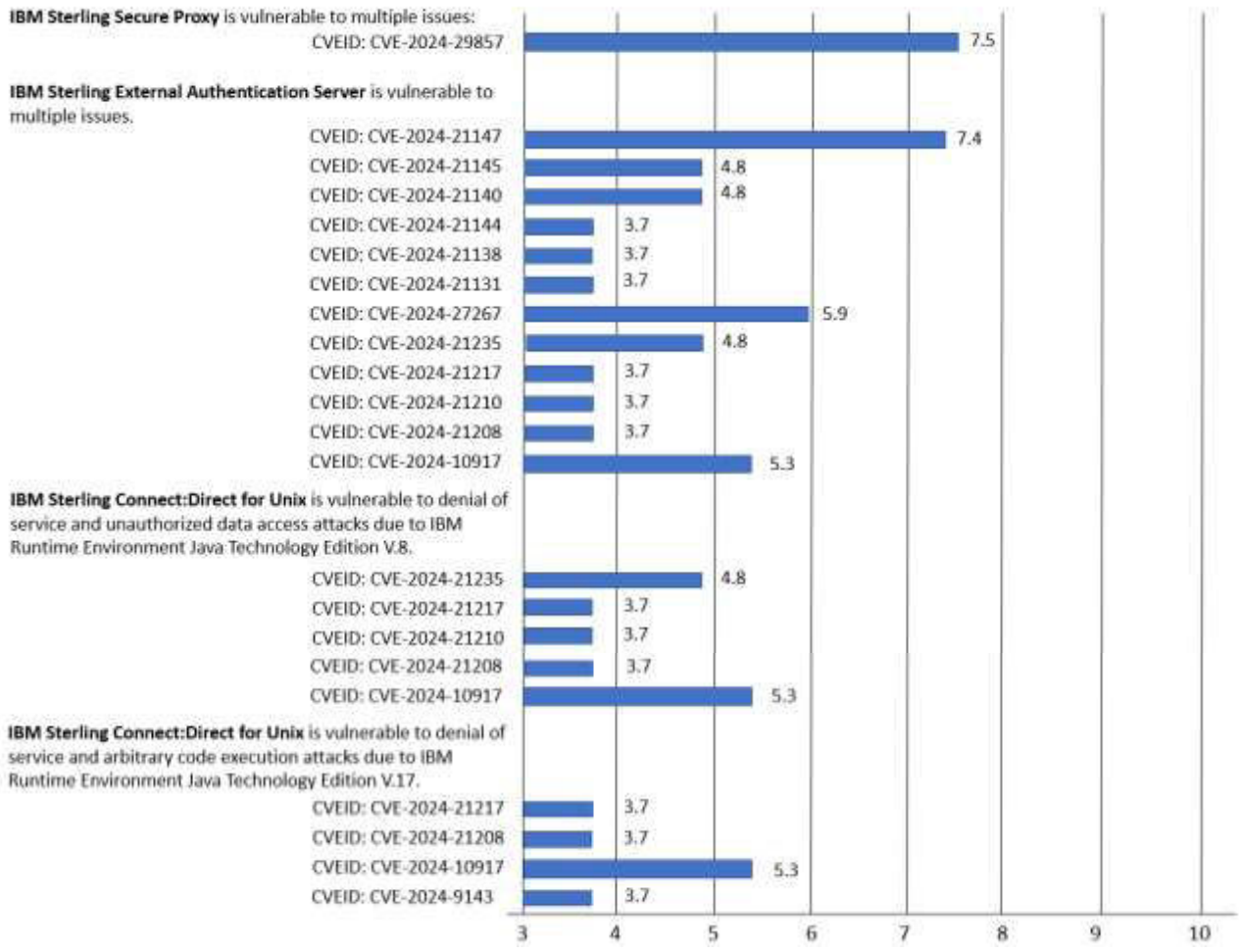
Integration News

T1 2025

In this issue:

IBM Sterling B2B Data Exchange Solutions. SECURITY NEWS:



Other contents:

IBM Sterling Secure Proxy is vulnerable to multiple issues.

Vulnerability Details

CVEID: CVE-2024-29857

DESCRIPTION: The Bouncy Castle Crypto Package For Java is vulnerable to a denial of service, caused by improper input validation. By importing an EC certificate with crafted F2m parameters, a remote attacker could exploit this vulnerability to cause excessive CPU consumption.

CVSS Source: IBM X-Force
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Secure Proxy	6.1.0.0 - 6.1.0.1
IBM Sterling Secure Proxy	6.2.0.0 - 6.2.0.1

Remediation/Fixes

Product	IBM Sterling Secure Proxy	
Affected Version	6.1.0.0 - 6.1.0.1	6.2.0.0 - 6.2.0.1
Fixed-in Version(s)	6.1.0.1 iFix 02	6.2.0.1 iFix 01
Remediation	Fix Central	Fix Central

Workarounds and Mitigations

None.

IBM Sterling External Authentication Server is vulnerable to multiple issues.

Vulnerability Details

CVEID: CVE-2024-21147

DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality, high integrity impacts.

CVSS Source: IBM X-Force
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2024-21145

DESCRIPTION: An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity impacts.

CVSS Source: IBM X-Force
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21140

DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low confidentiality, low integrity impacts.

CVSS Source: IBM X-Force
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21144

DESCRIPTION: An unspecified vulnerability in Java SE related to the Concurrency component could allow a remote attacker to cause low availability impact.

CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21138

DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause a low availability impact.

CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21131

DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low integrity impact.

CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-27267

DESCRIPTION: The Object Request Broker (ORB) in IBM SDK, Java Technology Edition 7.1.0.0 through 8.0.8.26 is vulnerable to remote denial of service, caused by a race condition in the management of ORB listener threads. IBM X-Force ID: 284573.

CVSS Source: IBM X-Force
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2024-21235

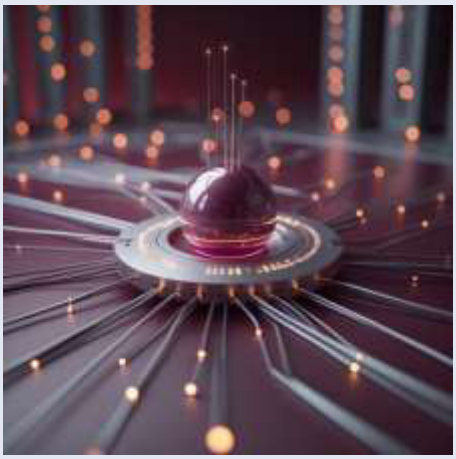
DESCRIPTION: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to accessible data as well as unauthorized read access to a subset of accessible data.

CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21217

DESCRIPTION: Vulnerability in Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)



CVEID: CVE-2024-21210

DESCRIPTION: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data.

CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-21208

DESCRIPTION: Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21208

DESCRIPTION: Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CVSS Source: Oracle
CVSS Base score: 3.7

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-10917
DESCRIPTION: In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.
CVSS Source: NVD
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling External Authentication Server	6.0.0.0 - 6.0.3.1
	6.1.0.0 - 6.1.0.2

Remediation/Fixes

Product	IBM Sterling External Authentication Server	
Affected Version	6.0.0.0 - 6.0.3.1	6.1.0.0 - 6.1.0.2
Fixed-in Version(s)	6.0.3.1 iFix 02	6.1.0.2 iFix 02
Remediation	Fix Central	Fix Central

Workarounds and Mitigations
None.

IBM Sterling Connect:Direct for Unix is vulnerable to denial of service and unauthorized data access attacks due to IBM Runtime Environment Java Technology Edition V.8.

Vulnerability Details

CVEID: CVE-2024-21235
DESCRIPTION: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to accessible data as well as unauthorized read access to a subset of accessible data.
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21217
DESCRIPTION: Vulnerability in Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).
CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21210
DESCRIPTION: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data.
CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-21208
DESCRIPTION: Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in

unauthorized ability to cause a partial denial of service (partial DOS).
CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-10917

DESCRIPTION: In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.
CVSS Source: NVD
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for UNIX	6.1.0.0 - 6.1.0.4.iFix118
	6.2.0.0 - 6.2.0.7.iFix034

Remediation/Fixes

IBM strongly recommends addressing the vulnerability now by upgrading.

Product	IBM Sterling Connect:Direct for Unix	
Version	6.1.0	6.2.0
Remediation	Apply 6.1.0.4.iFix 119, available on Fix Central.	Apply 6.2.0.7.iFix04 4, available on Fix Central.

Workarounds and Mitigations

None.

IBM Sterling Connect:Direct for Unix is vulnerable to denial of service and <attacks due to IBM Runtime Environment Java Technology Edition V.17.

Vulnerability Details

CVEID: CVE-2024-21217

DESCRIPTION: Vulnerability in Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).
CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21208

DESCRIPTION: Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).
CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-10917

DESCRIPTION: In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.
CVSS Source: NVD
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-9143

DESCRIPTION: OpenSSL could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds memory read or write flaw due to the use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code or cause the application to crash.
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for Unix	6.1.0.4.iFix103 - 6.1.0.4.iFix120
	6.3.0.3 - 6.3.0.4.iFix003
	6.4.0.0 - 6.4.0.1.iFix004

Remediation/Fixes

Product	Version	Remediation / Fix / Instructions
IBM Sterling Connect:Direct for Unix	6.1.0	Apply 6.1.0.4.iFix121, available on Fix Central.
	6.3.0	Apply 6.3.0.4.iFix004, available on Fix Central.
	6.4.0	Apply 6.4.0.1.iFix005, available on Fix Central.

Workarounds and Mitigations

None.

Discontinuance of support: IBM Sterling Connect:Direct 6.2.x

(Revised on 5 March 2025)

The effective end of support is extended from 30 September 2025 to 31 December 2025. This announcement is revised to reflect this date change. For details, see AD25-0862.

Discontinuance of select versions

Effective on the dates shown, IBM will discontinue support of select versions of the following programs as licensed under the applicable IBM agreement.

Program name and identifier	IBM Sterling Connect:Direct (5725-C99)
Version	6.2.x
Effective date	6.1.0.2 iFix 02
Supported versions	6.3.x, 6.4.x
Product lifecycle page	5725-C99

Downloadable or recorded media will remain available to clients of record until the discontinuance of support date or, where applicable, for the duration of their support extension terms.

Technical support

Technical support continues to be available based on the announced lifecycle policy, as detailed on the IBM Support Product lifecycle page, until end of support date. Extended support, offered after 31 December 2025, is limited to usage and known defect support only.

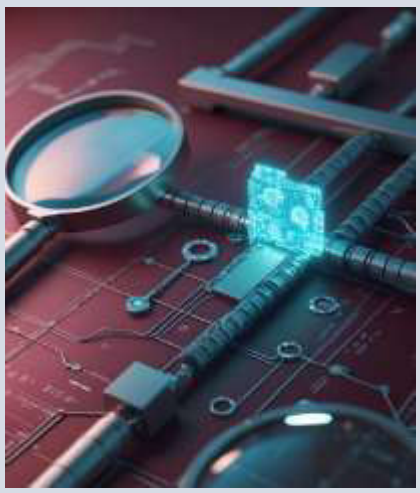
IBM Support offerings can provide additional services and help extend the life of your software investment. For additional information, see the IBM Extended Support web page.

Troubleshooting

Sterling Map with replaceAll user exit gives a java.lang.NoSuchMethod exception

Problem

When running a map that has a user exit rule with a replaceAll function, the translator issues this error message:
java.lang.NoSuchMethodException: java.lang.NoSuchMethodException: java.lang.String.<init>(null)



Cause

The data that was used for the replaceALL function was empty.

```
26  E2EDKT2001                  0100000000294711225000025000001803
```

The characters after the 1803 above refer to the element TDLINE in the map, which is this case is empty
The translator report shows that in Block 26, which is the example data line above, so we know this is the data used which caused the error:

Section: INPUT Severity: ERROR
SyntaxSpecific: false Syntax: -1 Code: 170 Extended Rule Error
Info:
10002: Block Count
26

Diagnosing The Problem

If you search for the error message, this is what was returned:
The error message *java.lang.NoSuchMethodException*: *java.lang.String.<init>(null)* indicates that you're trying to create a String object using a constructor that takes a null argument, but such a constructor doesn't exist.
Here's why this might be happening and how to fix it:

Common Causes:

- Passing *null* to a String constructor: You might be explicitly passing *null* as an argument to a *String* constructor.
- Indirect *null* argument: A variable you're using to create the String might be *null.*

How to Fix:

- Check for *null*:
- Before creating the String object, check if the variable you're using is *null*.
- Handle *null* values:
- If the variable is *null*, you can either:
  - **Use a default value:** Assign a default value (e.g., an empty string) if the variable is *null.*
  - **Throw an exception:** If the variable should never be *null*, throw an exception to handle the error condition.

Resolving The Problem

As stated in the Diagnose section, we will have to check before creating the String object that the variable we're using is *null.*
We will then need to change the extended rule as follows,

```
object ob;

If exist(#TDLINE) then
 Begin
  ob= new("java.lang.String",#TDLINE);
  #TDLINE = ob.replaceALL("[^^A-Za-z0-9\\s]" , " ");
 End
```

This link shows more about using the replaceALL function, [replacing-characters-string-value-replaceall-javalangstring-user-exit]

Troubleshooting
ITX launcher stops processing Kafka messages if a message is invalid

Problem
The IBM Sterling Transformation Extender (ITX) Launcher stops processing Kafka messages if a message is invalid and does not then process any new messages.

Symptom
The ITX Launcher stops processing Kafka messages if a message is invalid and does not then process any new messages.

Cause
Using the ITX Kafka adapter and processing an invalid Kafka message but not using either -ETP or -ERRORTOPIC.

Environment
Using the ITX Launcher with the ITX Kafka adapter as a Launcher source event to process messages on a Kafka topic.

Diagnosing The Problem
The ITX Launcher stops processing a Kafka message while consuming an invalid Kafka message and no further messages are processed.

Resolving The Problem
Use either the -ETP or -ERRORTOPIC parameter with the ITX Kafka adapter to specify an error topic on Kafka so that after encountering an error the listener resumes processing new events.

How to update Apache Tomcat version used by Design Server or standalone REST API on Windows

Steps
The ITX Design Server installation uses the same Apache Tomcat installation as the ITX standalone REST API but different scripts are used.

The Design Server scripts are located in ***<itx_install_dir>\DesignServer*** direc tory and should be used if using the Design Server.

The REST API scripts are located in the ***<itx_install_dir>\restapi\tomcat*** d irectory and should used only if using the REST API without the Design Server.

The Design Server and REST API are included as part of the ITX Runtime and Monitoring installation. The Design Server may be optionally selected during the installation. A separate Mongodb database is required for the Design Server installation.

How to obtain the new version of the Apache Tomcat software:
Download the new Apache Tomcat version from https://archive.apache.org/dist/tomcat/ server. Change to the tomcat version tomcat-x directory (such as tomcat-9 for ITX 11.0.0 and older or tomcat-10 for ITX 11.0.1) then change to the new version directory (such as v9.0.z for ITX 11.0.0 and older or v10.1.z for ITX 11.0.1) then change to the bin directory.

Example for version *9.0.100: https://archive.apache.org/dist/tomcat/tomcat-9/v9.0.100/bin/ . For Windows, download: apache-tomcat-x.y.z-windows-x64.zip file where x.y is the major version, z is the release and z is the revision within the major version. Example for version 9.0.100: apache-tomcat-9.0.100-windows-x86.zip*

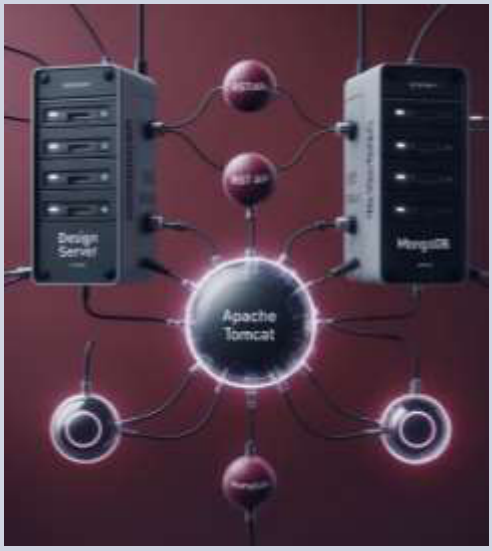
The following steps may be used to update the Apache Tomcat version used by the ITX Design Server on Windows.

*Open a Windows Command Prompt (cmd.exe command line prompt) with **Elevated / Administrator** permission (Run as Administrator).*

1. *Open a Windows Command Prompt (cmd.exe command line prompt) with **Elevated / Administrator** permission (Run as Administrator).*
2. *Change to the **<itx_install_dir>\DesignServer** directory.*
3. *Stop Design Server Windows services by running the **<itx_install_dir>\DesignServer\stop.bat** command.*
4. *Uninstall* Design Server *by running the **<itx_install_dir>\restapi\DesignSever\clean.bat*** command.

5. *Copy the downloaded Apache Tomcat 9.0.xx zip file to <install_dir>\restapi\tomcat directory. Example: apache-tomcat-9.0.100-windows-x86.zip*
6. *Create a backup copy of the **"<itx_install_dir>\restapi\tomcat\dtxtomcat.ini"** file then edit the file to update the TomcatVersion property value to specify the new version of Apache Tomcat. Example: **"TomcatVersion=9.0.100"***
7. *Install Design Server by running the **<itx_install_dir>\DesignServer\install.bat** command.*
8. *Display the Apache Tomcat version by running the **<itx_install_dir>\restapi\tomcat\dtxtomcatservice.bat ping** command.*
9. *Login and test the Design Server to verify the server is operational.*

The following steps may be used to update the Apache Tomcat version used by standalone REST API on Windows.



1. *Open a Windows Command Prompt (cmd.exe command line prompt) with **Elevated / Administrator** permission (Run as Administrator).*
2. *Change to the **<itx_install_dir>\restapi\restapi** directory.*
3. *Stop the restapi service ITX REST API Runtime Server by running the **<itx_install_dir>\restapi\tomcat\dtxtomcatservice.bat stop** command if using the Apache Tomcat Windows service (or by running the **<itx_install_dir>\restapi\tomcat\dtxtomcat.bat stop** command if using the Apache Tomcat as a non-service).*
4. *Uninstall the* current Apache Tomcat install *by running the inside the **<itx_install_dir>\restapi\tomcat\dtxtomcatservice.bat uninstall** command if using the Apache Tomcat Windows service (or by running the **<itx_install_dir>\restapi\tomcat\dtxtomcat.bat uninstall** command if using the Apache Tomcat as a non-service).*
5. *Copy the downloaded Apache Tomcat 9.0.xx zip file to <install_dir>\restapi\tomcat directory. Example:apache-tomcat-9.0.100-windows-x86.zip*
6. *The previous apache-tomcat zip file may be backed up and / or removed.*
7. *Create a backup copy of the **"<itx_install_dir>\restapi\tomcat\dtxtomcat.ini"** file then edit the file to update the TomcatVersion property value to specify the new version of Apache Tomcat. Example: **"TomcatVersion=9.0.100"***
8. *Run the command **<itx_install_dir>\restapi\tomcat\dtxtomcatservice.bat install** if using the Apache Tomcat Windows service (or by running the **<itx_install_dir>\restapi\tomcat\dtxtomcat.bat install** command if using the Apache Tomcat as a non-service).*
9. *Display the Apache Tomcat version by running the **<itx_install_dir>\restapi\tomcat\dtxtomcatservice.bat ping** command if using the Apache Tomcat Windows service (or by running the **<itx_install_dir>\restapi\tomcat\dtxtomcat.bat ping** command if using the Apache Tomcat as a non-service).*
10. *Test the ITX REST API to verify the server is operational.*

B2B Integrator/Global Mailbox Components Versions

Refer to the below table to determine which version of Apache Cassandra, Apache ZooKeeper, Reaper for Apache Cassandra, or WebSphere Application Server Liberty comes with your IBM Sterling B2B Integrator/Global Mailbox fix pack.

Content

IBM Sterling B2Bi/GM Fix Pack Version	Apache Cassandra Version	Apache ZooKeeper Version	Reaper for Apache Cassandra Version	WebSphere Application Server Liberty Version
6.0.3.x				
6.0.3.3	3.11.0	3.5.5	1.1.0	20.0.0.9
6.0.3.4	3.11.0	3.5.5	1.1.0	20.0.0.12
6.0.3.5	3.11.0	3.5.5	1.1.0	21.0.0.6
6.0.3.6	3.11.0	3.5.5	1.1.0	21.0.0.6
6.0.3.7	3.11.0	3.5.5	1.1.0	22.0.0.5
6.0.3.8	3.11.0	3.5.5	1.1.0	22.0.0.13
6.0.3.9	3.11.0	3.5.5	1.1.0	23.0.0.9
6.1.0.x				
6.1.0.0	3.11.6	3.5.5	1.1.0	20.0.0.5
6.1.0.1	3.11.6	3.5.5	1.1.0	20.0.0.12
6.1.0.2	3.11.6	3.5.5	1.1.0	20.0.0.12
6.1.0.3	3.11.6	3.5.5	1.1.0	20.0.0.12
6.1.0.4	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.4_1	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.4_2	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.5	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.5_2	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.6	3.11.6	3.5.5	1.1.0	22.0.0.5
6.1.0.7	3.11.6	3.5.5	1.1.0	22.0.0.13
6.1.1.x				
6.1.1.0	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.0_1	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.1	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.2	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.3	3.11.10	3.6.3	2.3.1	22.0.0.10
6.1.1.4	3.11.10	3.6.3	2.3.1	23.0.0.3
6.1.2.x				
6.1.2.0	3.11.10	3.6.2	2.3.1	21.0.0.3
6.1.2.1	4.0.6	3.8.0	3.2.0	22.0.0.10
6.1.2.2	4.0.7	3.8.0	3.2.1	22.0.0.13
6.1.2.3	4.0.10	3.8.1	3.3.1	23.0.0.4

IBM Sterling B2Bi/GM Fix Pack Version	Apache Cassandra Version	Apache ZooKeeper Version	Reaper for Apache Cassandra Version	WebSphere Application Server Liberty Version
6.1.2.5	4.0.10	3.9.1	3.3.1	23.0.0.11
6.1.2.6	4.0.13	3.9.1	3.6.0	24.0.0.9
6.2.0.x				
6.2.0.0	4.0.10	3.8.1	3.3.1	23.0.0.4
6.2.0.1	4.0.10	3.9.1	3.3.1	23.0.0.12
6.2.0.2	4.0.10	3.9.1	3.3.1	23.0.0.4
6.2.0.3	4.0.13	3.9.1	3.6.0	24.0.0.7
6.2.0.4	4.0.13	3.9.3	3.7.0	24.0.0.11

IBM Sterling B2B Integrator. Upgrade Compatibility

Modified date: 07 March 2025

This document describes upgrade scenarios and supported upgrade paths for IBM Sterling B2B Integrator.

Content

Always check upgrade compatibility before planning an upgrade.
To upgrade the IBM Sterling B2B Integrator environment to a higher version, choose a version compatible with the existing version.
In general, you must upgrade to a version that is released after the existing version.
For example:

- Upgrade from v5.2.6.3_6 (release date July-2018) to v6.0.0.0 (release date August-2018) – Compatible
- Upgrade from v5.2.6.3_9 (release date February 2019) to v6.0.0.0 (release date August-2018) – Not compatible

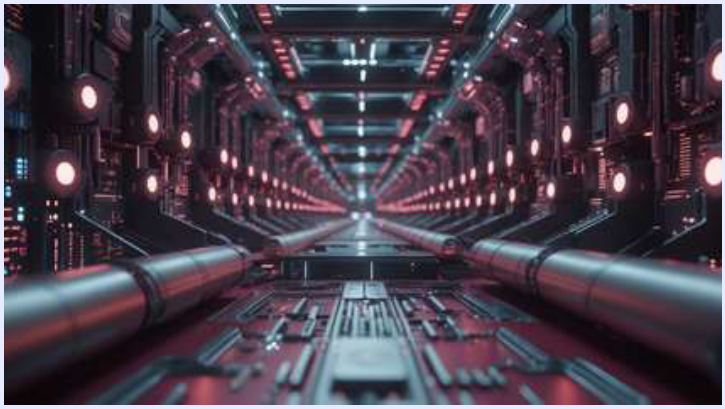
Note: The release date of each version is available in the Release Timeline illustration. For details on release policy, refer to Release strategy for IBM Sterling B2B Integrator and IBM Sterling File Gateway v6.0.x, v6.1.x, and v6.2.x onwards.

Refer to Sterling B2B Integrator System Requirements for detailed information on JDK versions in IBM B2B Integrator releases.

Previous Releases:

If you are on any of the following versions, you can upgrade to any of the latest versions as illustrated in the Upgrade Matrix below.

- 5.2.5_19 or earlier versions
- 5.2.6.0 all versions
- 5.2.6.1_9 or earlier versions
- 5.2.6.2_5 or earlier versions
- 5.2.6.3_12 or earlier versions



Upgrade Paths

The chart below lists the compatible upgrade paths for IBM B2B Integrator releases.

Supported	**Y**	Indicates the upgrade is compatible.
Intermediate	**I**	Indicates an in-between upgrade and needs to upgrade further. When you upgrade to the latest Fix Pack release of a particular version, first upgrade to the Base release of that version. This is the Intermediate state. You must later upgrade to the Fix Pack release. **Note**:Do not use the system if the Base release on a higher version is older than the current release. The system remains in a transient state until you upgrade to the latest Fix Pack release. For example: If you want to upgrade to v6.0.0.1 from v5.2.6.3_9, first upgrade to v6.0.0.0 and later upgrade to v6.0.0.1. You must not use the instance at v6.0.0.0.
Not supported	**X**	Indicates the upgrade is not compatible.

Compatible Versions

Upgrade To →

Upgrade From ↓

IBM B2B Integrator Releases	5.2.6.3_16	5.2.6.4	5.2.6.4_4	5.2.6.5	5.2.6.5_4	6.0.0.0	6.0.0.8	6.0.1.0	6.0.1.2	6.0.2.0	6.0.2.3	6.0.3.0	6.0.3.9	6.1.0.0	6.1.0.8	6.1.1.0	6.1.1.4	6.1.2	6.1.2.7	6.2	6.2.0.4
5.2.5_20	Y	I	Y	Y	Y	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.1_10	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.2_6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.3_14	Y	I	Y	I	Y	I	Y	X	X	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.3_15	Y	X	X	I	Y	I	Y	X	X	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.3_16	NA	X	X	I	Y	I	Y	X	X	X	X	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.4	X	NA	Y	Y	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.4_2	X	X	Y	Y	Y	I	Y	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.4_3	X	X	Y	I	Y	I	Y	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.4_4	X	X	NA	I	Y	I	Y	X	X	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.5	X	X	X	NA	Y	I	Y	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.5_2	X	X	X	X	Y	I	Y	X	X	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
5.2.6.5_3	X	X	X	X	Y	I	Y	X	X	I	Y	I	Y	X	Y	Y	Y	Y	Y	Y	Y
5.2.6.5_4	X	X	X	X	NA	I	Y	X	X	X	X	I	Y	X	Y	Y	Y	Y	Y	Y	Y
6.0.0.0	X	X	X	X	X	NA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.0.6	X	X	X	X	X	X	Y	X	X	X	X	I	Y	X	Y	Y	Y	Y	Y	Y	Y
6.0.0.7	X	X	X	X	X	X	Y	X	X	X	X	I	Y	X	Y	Y	Y	Y	Y	Y	Y
6.0.0.8	X	X	X	X	X	X	NA	X	X	X	X	I	Y	X	Y	I	Y	Y	Y	Y	Y
6.0.1.0	X	X	X	X	X	X	X	NA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.1.2	X	X	X	X	X	X	X	X	NA	I	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.2.0	X	X	X	X	X	X	X	X	X	NA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.2.1	X	X	X	X	X	X	X	X	X	X	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.2.2	X	X	X	X	X	X	X	X	X	X	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.2.3	X	X	X	X	X	X	X	X	X	X	NA	I	Y	X	Y	Y	Y	Y	Y	Y	Y
6.0.3.0	X	X	X	X	X	X	X	X	X	X	X	NA	Y	Y	Y	Y	Y	Y	Y	Y	Y
6.0.3.7	X	X	X	X	X	X	X	X	X	X	X	I	Y	X	Y	I	Y	I	Y	Y	Y
6.0.3.8	X	X	X	X	X	X	X	X	X	X	X	X	Y	X	Y	I	Y	I	Y	Y	Y
6.0.3.9	X	X	X	X	X	X	X	X	X	X	X	X	NA	X	Y	I	Y	I	Y	Y	Y
6.1.0.0	X	X	X	X	X	X	X	X	X	X	X	X	X	NA	Y	Y	Y	Y	Y	Y	Y
6.1.0.6	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	I	Y	I	Y	Y	Y
6.1.0.7	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	I	Y	I	Y	Y	Y
6.1.0.8	X	X	X	X	X	X	X	X	X	X	X	X	X	X	NA	X	X	I	Y	I	Y
6.1.1.0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	NA	Y	Y	Y	Y	Y
6.1.1.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	I	Y	Y	Y
6.1.1.3	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	I	Y	Y	Y
6.1.1.4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	NA	I	Y	Y	Y
6.1.2.0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	NA	Y	Y	Y
6.1.2.3	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	Y	Y
6.1.2.5	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	I	Y
6.1.2.6	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y	I	Y
6.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	NA	Y
6.2.0.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y
6.2.0.3	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Y
6.2.0.4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	NA

Communication

If you need more information about any of the contents of our newsletter, please do not hesitate to contact us. We will be happy to answer your questions