B2B Solutions
Let's build IT together

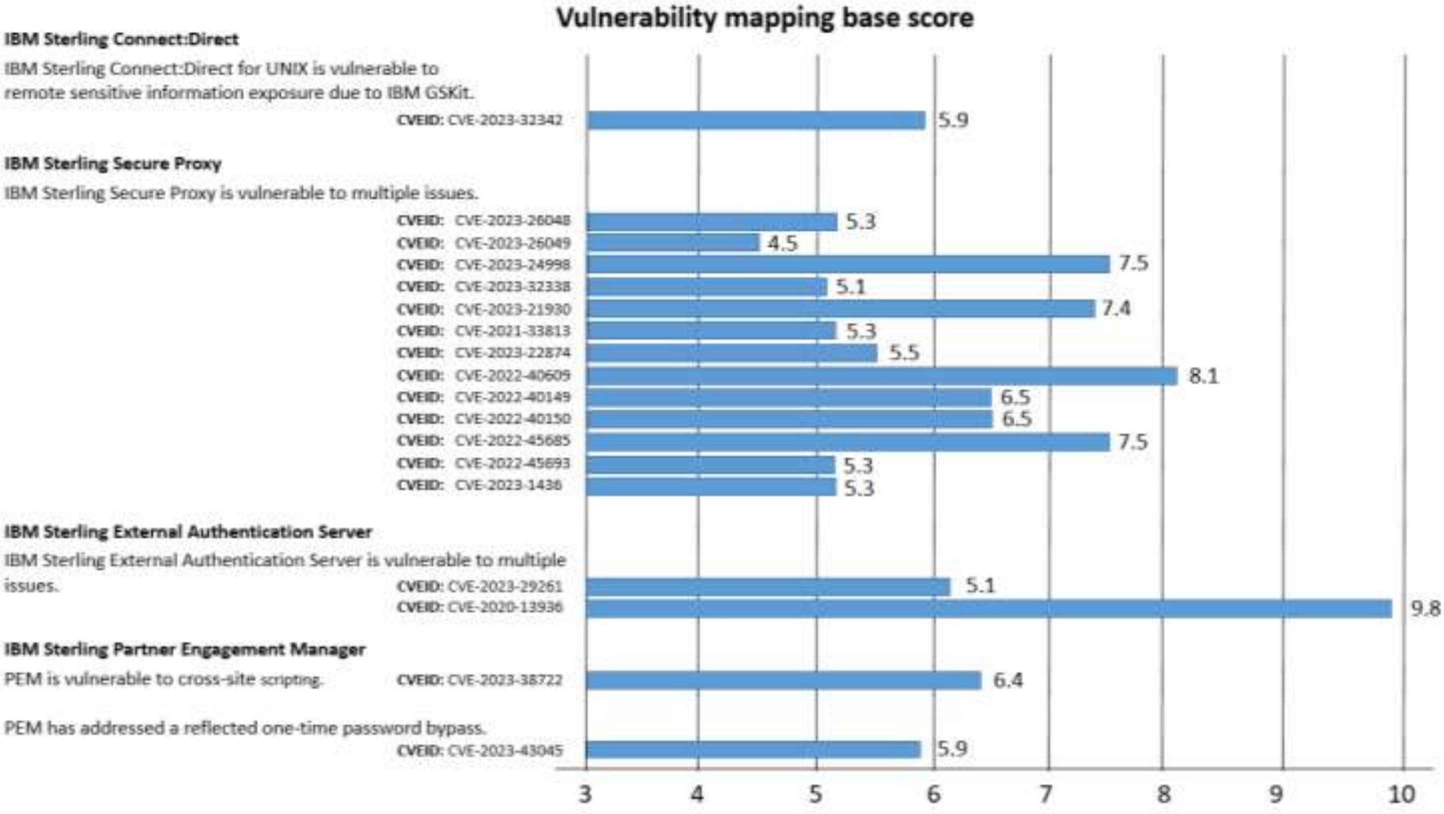
Integration News

T3 2023

In this issue:

IBM Sterling B2B Collaboration Suite: SECURITY NEWS.

- IBM Sterling Connect:Direct for UNIX is vulnerable to remote sensitive information exposure due to IBM GSKit
- IBM Sterling Secure Proxy is vulnerable to multiple issues
- IBM Sterling External Authentication Server is vulnerable to multiple issues
- IBM Sterling Partner Engagement Manager is vulnerable to cross-site scripting
- IBM Sterling Partner Engagement Manager has addressed a reflected one-time password bypass vulnerability



Other contents:

- IBM Sterling B2B Integrator/Global Mailbox Components Versions
- IBM Sterling B2B Integrator. Error: Java.lang.NoClassDefFoundError: org.apache.bsf.BSFException
- IBM Sterling B2B Integrator. Failure uploading a system certificate using Rest API
- IBM Sterling B2B Integrator. Error sending email to MS Exchange server
- IBM Sterling B2B Integrator. Swiftnet Components in IBM Sterling B2B Integrator
- IBM Sterling B2B Integrator. Cannot open a MXL from a previous version of Sterling Integrator
- IBM Sterling B2B Integrator. Creating a user with less than 5 characters

IBM Sterling Connect:Direct for UNIX is vulnerable to remote sensitive information exposure due to IBM GSKit

IBM GSKit is used by IBM Sterling Connect:Direct for UNIX in product configuration and data transmission. IBM Sterling Connect:Direct for UNIX is impacted by remote sensitive exposure vulnerability in IBM GSKit. IBM Sterling Connect:Direct for UNIX has upgraded IBM GSKit to version 8.0.55.31 to address the issue.

Vulnerability Details

CVEID: CVE-2023-32342

Description: IBM GSKit could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information.

CVSS Base score: 5.9
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for UNIX	6.3.0.0 - 6.3.0.0.iFix003
	6.2.0.0 - 6.2.0.6.iFix018
	6.1.0.0 - 6.1.0.4.iFix085
	6.0.0.0 - 6.0.0.2.iFix150

Remediation/Fixes

Version	Remediation & Fix
6.3.0	Apply 6.3.0.0.iFix011
6.2.0	Apply 6.2.0.6.iFix024
6.1.0	Apply 6.1.0.4.iFix088
6.0.0	Apply 6.0.0.2.iFix152

Workarounds and Mitigations

None.

IBM Sterling Secure Proxy is vulnerable to multiple issues

Multiple vulnerabilities affect IBM Sterling Secure Proxy and are addressed in the latest release and iFix.

Vulnerability Details

CVEID: CVE-2023-26048

Description: Eclipse Jetty is vulnerable to a denial of service, caused by an out of memory flaw in the HttpServletRequest.getParameter() or HttpServletRequest.getParts() function. By sending a specially crafted multipart request, a remote attacker could exploit this vulnerability to cause a denial of service condition.

CVSS Base score: 5.3
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2023-26049

Description: Eclipse Jetty could allow a remote authenticated attacker to obtain sensitive information, caused by a flaw during nonstandard cookie parsing. By sending a specially crafted request to tamper with the cookie parsing mechanism, an attacker could exploit this vulnerability to obtain values from other cookies, and use this information to launch further attacks against the affected system.

CVSS Base score: 4.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N)

CVEID: CVE-2023-24998

Description: Apache Commons FileUpload and Tomcat are vulnerable to a denial of service, caused by not limit the number of request parts to be processed in the file upload function. By sending a specially-crafted request with series of uploads, a remote attacker could exploit this vulnerability to cause a denial of service condition.

CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2023-32338

Description: IBM Sterling Secure Proxy and IBM Sterling External Authentication Server stores user credentials in plain clear text which can be read by a local user with container access.

CVSS Base score: 5.1
CVSS Temporal Score: Click here.
CVSS Vector: CVSS:
(CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2023-21930

Description: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the JSSE component could allow an unauthenticated attacker to cause high confidentiality impact and high integrity impact.

CVSS Base score: 7.4

CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2021-33813

Description: JDOM is vulnerable to a denial of service, caused by an XXE issue in SAXBuilder. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to cause the a denial of service.

CVSS Base score: 5.3
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2023-22874

Description: IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files.

CVSS Base score: 5.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40609

Description: IBM SDK, Java Technology Edition 7.1.5.18 and 8.0.8.0 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization flaw. By sending specially-crafted data, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVSS Base score: 8.1
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2022-40149

Description: jettison-json Jettison is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML or JSON data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40150

Description: jettison-json Jettison is vulnerable to a denial of service, caused by an out of memory flaw. By sending a specially-crafted XML or JSON data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-45685

Description: Jettison is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending an overly long string using JSON data, a remote attacker could exploit this vulnerability to cause a denial of service.

CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-45693

Description: Jettison is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted request using the map parameter, a remote attacker could exploit this vulnerability to cause a denial of service.

CVSS Base score: 5.3
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2023-1436

Description: Jettison is vulnerable to a denial of service, caused by an infinite recursion when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. A remote attacker could exploit this vulnerability to cause a denial of service.

CVSS Base score: 5.3
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Secure Proxy	6.0.3
	6.1.0

Remediation/Fixes

Version	iFix
6.0.3	GA
6.1.0	iFix 08

Workarounds and Mitigations

None.

IBM Sterling External Authentication Server is vulnerable to multiple issues

Multiple vulnerabilities affect IBM Sterling External Authentication

Server and are addressed in the latest iFixes.

Vulnerability Details

CVEID: CVE-2023-29261

Description: IBM Sterling Secure Proxy could allow a local user with specific information about the system to obtain privileged information due to inadequate memory clearing during operations.

CVSS Base score: 5.1
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2020-13936

Description: Apache Velocity could allow a remote attacker to execute arbitrary code on the system, caused by a sandbox bypass flaw. By modifying the Velocity templates, an attacker could exploit this vulnerability to execute arbitrary code with the same privileges as the account running the Servlet container.

CVSS Base score: 9.8
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling External Authentication Server	6.0.3
	6.1.0

Remediation/Fixes

Version	iFix
6.0.3	iFix 08
6.1.0	iFix 04

Workarounds and Mitigations

None.

IBM Sterling Partner Engagement Manager is vulnerable to cross-site scripting

IBM Sterling Partner Engagement Manager has addressed a reflected cross-site scripting vulnerability.

Vulnerability Details

CVEID: CVE-2023-38722

Description: IBM Sterling Partner Engagement Manager is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.

CVSS Base score: 6.4
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Partner Engagement Manager Essentials Edition	6.1.2, 6.2.0, 6.2.2

Remediation/Fixes

Version	Remediation/Fix/ Instructions
6.1.2, 6.2.0, 6.2.2	Download 6.2.2.1.2 and follow installation instructions.

Workarounds and Mitigations

None.

IBM Sterling Partner Engagement Manager is vulnerable to one-time password bypass

IBM Sterling Partner Engagement Manager has addressed a reflected one-time password bypass vulnerability.

Vulnerability Details

CVEID: CVE-2023-43045

Description: IBM Sterling Partner Engagement Manager could allow a remote user to perform unauthorized actions due to improper authentication.

CVSS Base score: 5.9
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Partner Engagement Manager Essentials Edition	6.1.2, 6.2.0, 6.2.2

Remediation/Fixes

Version	Remediation/Fix/ Instructions
6.1.2, 6.2.0, 6.2.2	Download 6.2.2.1.2 and follow installation instructions.

Workarounds and Mitigations

None.

IBM Sterling B2B Integrator/Global Mailbox Components Versions

Abstract

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
6.1.0.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

Troubleshooting
IBM Sterling B2B Integrator
Error: Java.lang.NoClassDefFoundError: org.apache.bsf.BSFException

Problem

Not able to run Script adapter with the latest version of Bsf.jar i.e. **Bsf 3.1 jar**

Symptom

The symptoms of the issue may be found in the below error generated in the logs:

```
[2023-08-23 11:28:28.092] ERROR 000110060033
WORKFLOW.ACTIVITY_ENGINE.ERR_ActivityEngineHelper_next
ActivityEngineHelper.next caught exception 4253774
java.lang.NoClassDefFoundError: org.apache.bsf.BSFException
at java.lang.Class.forNameImpl(Native Method)
at java.lang.Class.forName(Class.java:339)
at
com.sterlingcommerce.woodstock.workflow.activity.ServiceMetaData.getClassServiceInstance(ServiceMetaData.java:118)
at
com.sterlingcommerce.woodstock.workflow.activity.engine.ActivityEngineHelper.preInvokeService(ActivityEngineHelper.java:1471)
at
com.sterlingcommerce.woodstock.workflow.activity.engine.ActivityEngineHelper.nextMainLogic(ActivityEngineHelper.java:595)
at
com.sterlingcommerce.woodstock.workflow.activity.engine.ActivityEngineHelper.next(ActivityEngineHelper.java:362)
at
com.sterlingcommerce.woodstock.workflow.queue.WorkFlowQueueListener.doWork(WorkFlowQueueListener.java:459)
at
com.sterlingcommerce.woodstock.workflow.queue.WorkFlowQueueListener.run(WorkFlowQueueListener.java:240)
at
com.sterlingcommerce.woodstock.workflow.queue.WorkFlowQueueListener.onMessage(WorkFlowQueueListener.java:197)
at
com.sterlingcommerce.woodstock.workflow.queue.WorkFlowQueueListener.onMessage(WorkFlowQueueListener.java:184)
at
com.sterlingcommerce.woodstock.workflow.queue.wfTransporter.run(wfTransporter.java:447)
at
com.sterlingcommerce.woodstock.workflow.queue.BasicExecutor$Worker.run(BasicExecutor.java:508)
at
java.lang.Thread.run(Thread.java:826)
Caused by:
java.lang.ClassNotFoundException:
org.apache.bsf.BSFException
at java.net.URLClassLoader.findClas
```

```
s(URLClassLoader.java:610)
at
java.lang.ClassLoader.loadClassHelper(ClassLoader.java:948)
at
java.lang.ClassLoader.loadClass(ClassLoader.java:893)
at
com.sterlingcommerce.woodstock.ldr.DynamicClassLoader.loadClass(DynamicClassLoader.java:968)
at
com.sterlingcommerce.woodstock.ldr.DynamicClassLoader.loadClass(DynamicClassLoader.java:955)
... 13 more
```

Cause
The Cause of this error is due to third party jar bsf jars with version **Bsf 3.1 jar** doesn't have **org.apache.bsf.BSFException classs**, which is needed for Sterling B2B Integrator.

This makes Bsf 3.1 jars not compatible with Sterling B2B Integrator.

Environment
Sterling B2B Integrator v6.1.2

Diagnosing The Problem
Upon reviewing the logs for error the error points towards compatibility issue of Bsf 3.1 jars with Sterling B2B Integrator.

```
2023-08-23 11:28:28.092] ERROR
000110060033
WORKFLOW.ACTIVITY_ENGINE.ERR_ActivityEngineHelper_next
ActivityEngineHelper.next caught
exception 4253774
java.lang.NoClassDefFoundError:
org.apache.bsf.BSFException
at
java.lang.Class.forNameImpl(Native Method)
at
java.lang.Class.forName(Class.java:339)
at
com.sterlingcommerce.woodstock.workflow.activity.ServiceMetaData.getClassServiceInstance(ServiceMetaData.java:118).
```

As the class **org.apache.bsf.BSFException** is not present in the latest version of Bsf jar i.e. Bsf 3.1 jars, we come to a conclusion that this version of Bsf.jar is not compatible with Sterling B2B Integrator therefore unable to execute script adapter operations.

Resolving The Problem
The resolution to this issue is by using the compatible version of Bsf jar for configuring and executing Script Adapter Operations i.e. version **2_3 bsf.jar**

IBM Sterling B2B Integrator

- **Component:**
  System Administration->Adapters and Services
- **Software version:**
  All Versions

Troubleshooting
IBM Sterling B2B Integrator Failure uploading a system certificate using Rest API

Problem
Cannot create system certificate using Rest Api when certData contains more than 10.000 characters.

Symptom
The Rest API call to create a system certificate returns the error: "errorCode":400, "errorDescription": "API000467: Length too long for \"certData\"; max length is 10,000 characters."

Resolving The Problem
This is working as designed, system certificates that have more than 10.000 characters when base64 encoded cannot be imported via Rest API.
You will need to use the dashboard UI to import those certificates.

IBM Sterling B2B Integrator

- **Component:**
  Rest Api
- **Software version:**
  All Versions

Troubleshooting
IBM Sterling B2B Integrator Error sending email to MS Exchange server

Problem
Not able to send email from Sterling Integrator to MS Exchange Online using SMTP Send Adapter even though STARTTLS was implemented in the product via the APAR below:

https://www.ibm.com/support/pages/apar/IT43785

Symptom
Error: "com.sun.mail.smtp.SMTPSendFailedException: 530 #5.7.0 Must issue a STARTTLS command first".

Cause
STARTTLS needs to be enable first in Sterling b2B Integrator.

Resolving The Problem
You need to add the following line to the customer_overrides.properties and restart the system so that STARTTLS is enabled for the SMTP Send Adapter:

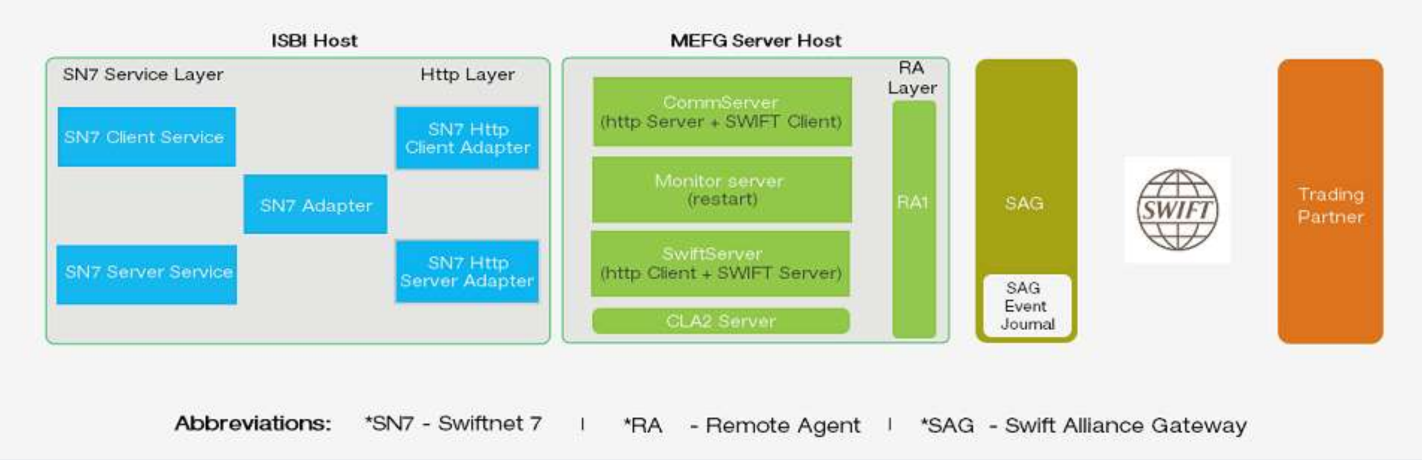
```
b2bMailsvs.enableStartTlsCommandForSMTP=true
```

IBM Sterling B2B Integrator

- **Component:**
  Protocol->SMTP
- **Software version:**
  6.1.2

Swiftnet Components in IBM Sterling B2B Integrator

This article describes the several components implemented in ISBI during a Swiftnet transfer. The diagram below shows the different components:



Swiftnet7 Services in ISBI

Swiftnet7 Adapter is an adapter in ISBI that is configured to communicate to the Swift Network through the MEFG Server. It requires the following information for its configuration:

- Http port
- MEFG SWIFTNet port, address & location
- CLA2 port
- Authentication & SSL information
- SWIFTNet Remote Agent location
- Queue & Channel information

Swiftnet7 Client Service prepares the request and sends it to the MEFG server using Http client.

Swiftnet7 Server Service handles SWIFT messages from the MEFG client application.

Swiftnet7 Http Client & Server Adapter are special instances of the standard Http severices in ISBI. They are used by the Swiftnet7 services for implementing http calls between ISBI and MEFG.

MEFG & RA:

CLA2 Server: The Swiftnet7 Adapter uses the CLA2 server to start and stop the MEFG components like MEFGCommServer, MEFGSwiftServer & MEFGMonitor Server. There are three unique scripts under MEFG/bin directory that CLA2 adapter uses to start these components.

MEFG Comm Server: is a combination of Http server and Swiftnet client implementation. The MEFG Comm Server takes the SOAP call and creates a SwCall for RA.

MEFG Monitor Server: This component is responsible for the auto recovery functionality of the MEFG server and the re-connects to the primary SAG. Every 30 second after the last action it checks the MEFG processes. If necessary, it stops the existing MEFG processes and start the restart script so that the system tries to start the MEFG process with connection to the primary SAG again. If the primary SAG is not avialble it will start the components with the secondary SAG.

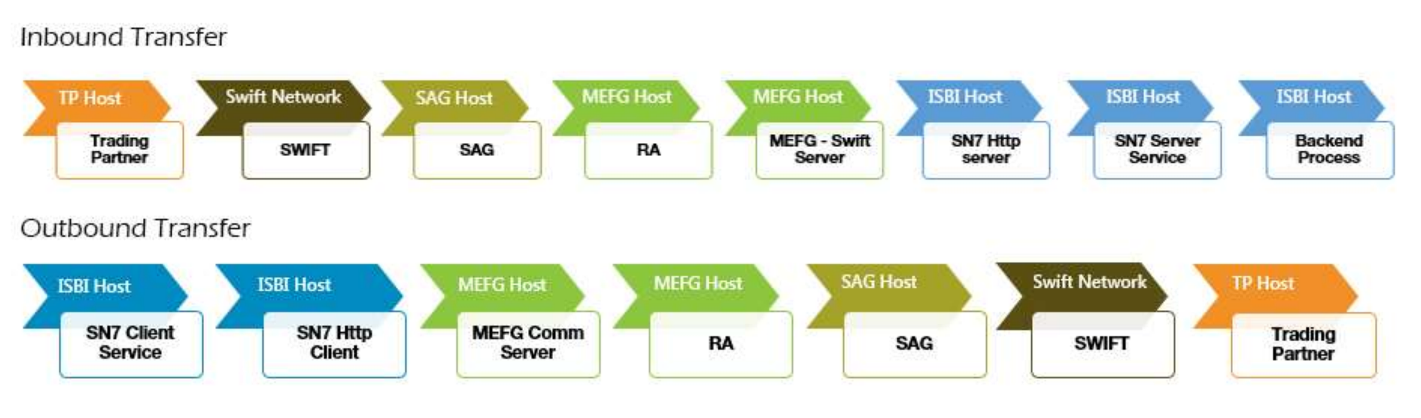
MEFG Swift Server: is a combination of Http Client and Swift Server implementation. The MEFG Swift Server takes SwCallback and create SOAP call for ISBI.

Swiftnet Remote API (RA): is a software distributed by swift, that connects the MEFG server and Swift Alliance Gateway (SAG). The RA needs to be installed on the same machine as the MEFG server.

Swift Alliance Gateway (SAG)

SAG is a interface product to connect with Swift network. This contains information of the partners and the Swift message / SNL (Swiftnet Net Link) transfers.

Below is a pictorial representation of the different SWIFT transfers using ISBI:



Troubleshooting

IBM Sterling B2B Integrator. Cannot open a MXL from a previous version of ISBI

Problem

When attempting to open a map with an MXL extension, a pop up is encountered with the following text in a pop up window:

'188608' violates maxInclusive constraint of '32767'. The element '{http://www.stercomm.com/Si/Map}ConditionalFieldID with value '188608' failed to parse.

Cause

The issue is the number assigned to the ConditionalFieldID is over the format length of 32767.

Resolving The Problem

In a text editor, open the *.MXL file and look for the following tree:

<ImplicitRuleDef>
<UseConstant>
<ConstantID>8</ConstantID>
<ConditionalFieldID>188608</ConditionalFieldID>
</UseConstant>
</ImplicitRuleDef>

Change the value to any number under 32767. For example: **<ConditionalFieldID>32700</ConditionalFieldID>**.

All the elements that are over that number need changed. But you should also keep in mind they should be unique.

Do not change the value to -1 though. This will also correct the issue and allow the map to be opened, but the fields in question will lose the standard rule "Use Constant".

IBM Sterling B2B Integrator

- **Component:** Translation->Map Editor
- **Software version:** All versions

Troubleshooting

IBM Sterling B2B Integrator. Creating a user with less than 5 characters

Problem

IBM Sterling B2B Integrator (SBI) allows user account creation atleast if it contains five characters. However, Are there any options to create a user with less than five characters?

Resolving The Problem

1) Stop SBI
2) Traverse to <SI_INSTALL_DIR>/properties folder and locate customer_overrides.properties file.
3) If customer_overrides.properties file does not exists then create one.
4) Add the below property into customer_overrides.properties file. ui.userIdMinLength=4 (Ex: to create a user id with 4 characters)
5) Start SBI

IBM Sterling B2B Integrator

- **Software version:** 5.2.6
- **Operating system(s):** Linux, Windows

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.

info@b2b.solutions