



Infor ION Grid Extensions Installation and Administration Guide

Version 11.1.11.1

Published November 20, 2014

Copyright © 2014 Infor. All rights reserved.

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

Publication Information

Release: 11.1.11.1

Publication date: November 20, 2014

Document Number: GRIDEXTIG_11.1.11.1_UWA_02

Version Log

The version log describes the changes between versions of this document.

Part Number	Release Date	Description
GRIDEXTIG-111111	2014-05	New version for Infor ION Grid Extensions 11.1.11.1 Add section about Event Hub Visualization and Recording UI.

Contents

Chapter 1: Installation Overview.....	8
What Are ION Grid Extensions?.....	8
Knowledge Prerequisites.....	9
System Requirements.....	9
 Chapter 2: General Grid Extension Procedures.....	 11
Downloading the ION Grid Extensions.....	11
Uploading the ION Grid Extensions.....	11
Upgrading ION Grid Extensions.....	12
 Chapter 3: Session Provider Grid Extensions.....	 14
Session Provider Requirements and Selection.....	14
Installing and Configuring the LDAP Session Provider Grid Extension.....	17
Installing the DSSO Session Provider.....	22
Installing the Windows Session Provider.....	25
Installing and Configuring the SAML Session Provider.....	26
Configuring Assertion Consumer Services.....	33
Uninstalling a SAML Session Provider.....	35
 Chapter 4: Grid Database Connectivity Grid Extension.....	 36
Installing the Grid Database Connectivity Grid Extension.....	36
Viewing Grid Database Connectivity Application Configuration Information.....	37
Grid Database Connectivity and H2 Databases.....	37

Accessing the H2 Web Console.....	38
Managing Database Drivers for the Grid Database Connectivity Grid Extension.....	39
Creating and Changing H2 and GDBC Application Users.....	41
Changing H2 User and Application User Passwords.....	42
Backing Up an H2 Database.....	43
Restoring an H2 Database from a Backup.....	45
Chapter 5: Event Hub and Event Analytics Grid Extensions.....	47
Installing the Event Hub Grid Extension.....	47
Installing the Event Analytics Grid Extension.....	48
Introduction.....	49
Event Hub Background.....	49
What is Event Hub?.....	49
Highlights of Event Hub.....	50
What Is Event Analytics?.....	51
Overview.....	51
Events.....	51
Publisher.....	52
Subscriber.....	52
Subscription.....	52
Persistence.....	53
Event Hub Schematic Overview.....	53
Event Analytics Technical Overview.....	54
Administration.....	55
Event Hub Grid Application Properties.....	55
Event Analytics Grid Application Properties.....	57

Starting and Stopping the Event Hub.....	57
Starting and Stopping Event Analytics.....	58
Multiple Nodes for Event Hub.....	58
Event Hub and Event Analytics Management Pages.....	59
Event Hub Management Pages.....	59
Event Analytics Management Pages.....	63
Event Analytics Rules.....	69
Facts.....	69
Subscriptions.....	71
Nonserializable.....	72
Utility Methods.....	73
Code Examples.....	73
Demo dml File.....	73
Item Update Counter Rule.....	74
Event Hub Visualization and Recording UI.....	75
Introduction.....	75
Topology Visualization.....	76
Event Recording.....	77
Viewing Recorded Data.....	78
Search Query Syntax.....	79
Event Recorder Node.....	80
Purging.....	80
Appendix A: M3 BE Event Hub Publisher.....	83
<M3 Table>.....	83
<M3 Batch Program>.....	84

<M3 Interactive Program>.....	86
<M3 Interactive Program> "." <Method>.....	87
<M3 Program>.....	88

This chapter contains the following:

- ["What Are ION Grid Extensions?" on page 8](#)
- ["Knowledge Prerequisites" on page 9](#)
- ["System Requirements" on page 9](#)

What Are ION Grid Extensions?

ION Grid Extensions are optional grid applications that provide additional functionality for other grid applications or applications that interact with the grid. The following are currently available. They are all delivered in the Infor ION Grid Extensions uploadable LCM package named `Infor_ION_Grid_Extensions_version.lcm`.

Session Providers

The grid extensions include four session providers, all of which provide authentication services. For a discussion of when to use the different session providers, see ["Session Provider Requirements and Selection"](#) on page 14.

Event Hub and Event Analytics

The Event Hub and Event Analytics grid extensions are applications that work with subscriber/publisher applications. For applications that have been developed to be either a subscriber or publisher for specific events, the Event Hub provides the means to direct the published data or events from the publisher application to the subscriber application. Event Analytics enables you to analyze the events and develop rules that affect the processing of events.

Grid Database Connectivity

The Grid Database Connectivity (GDBC) Grid Extension is a collection of database-related tools geared towards aiding the usage of a database in a grid application. The purposes are:

- Decouple the application from the database driver and configuration.

With GDBC, each grid application has an implicit database that it may choose to use. The GDBC provides an individual database connection string and database drivers for the grid application to use.

- Make a default database readily accessible for quick development startup.

The GDBC uses an H2 database. Because H2 includes a Microsoft SQL Server mode, it is easier to write grid applications that are compatible with both H2 and SQL Server. A developer can then initially develop using H2 and then switch the application to use SQL Server at a customer site.

Knowledge Prerequisites

To install this product, you should have the following knowledge and experience:

- Have experience installing and configuring applications.
- Have operating system administrator experience.

System Requirements

The following software requirements must be met before you install this product.

Component	Supported Version(s)	Notes
Operating System	Windows 2008 R2	The Windows Session Provider, Event Hub, and Event Analytics grid extensions are only supported on Windows platforms.
	Windows 2012	
	Windows 2012 R2	
	AIX 6.1	
	AIX 7.1	
	IBM i 6.1	
	IBM i 7.1	
LifeCycle Manager	10.1.x	

Component	Supported Version(s)	Notes
JVM	Oracle Java 6, update 45+ (32-bit or 64-bit)) Oracle Java 7, update 21+ (32-bit or 64-bit) IBM for i Java 6, PDF group 23+ (32-bit or 64-bit) IBM for i Java 7, PTF group 12+ (32-bit or 64-bit)	Always use the latest release at the time of installation. Maintain the Java version at the latest version with regular upgrades. Make sure that the LCM service is installed with the J9 JVM and not the classic JVM on IBM i. Note: The Event Hub grid extension requires a 64-bit JVM due to a minimum heap requirement of 2GB/2048MB.
ION Grid	11.1.11.0 for all 11.1.11.x grid extensions	
Infor Federation Services	10.3.2+	This is for the SAML Session Provider.

This section contains procedures that apply to the Grid Extensions as a whole.

- ["Downloading the ION Grid Extensions" on page 11](#)
- ["Uploading the ION Grid Extensions" on page 11](#)
- ["Upgrading ION Grid Extensions" on page 12](#)

For information on installing and administering specific grid extension types, see the following sections:

- ["Session Provider Grid Extensions" on page 14](#)
- ["Grid Database Connectivity Grid Extension" on page 36](#)
- ["Event Hub and Event Analytics Grid Extensions" on page 47](#)

Downloading the ION Grid Extensions

Download the ION Grid Extensions from the Infor Xtreme download page.

Product name	Contains
ION Grid Extensions	Infor_ION_Grid_Extension_11.1.11.<minorVersionNbrs>.lcm This package includes four session providers as well as the GDBC and Event Hub grid extensions.

Uploading the ION Grid Extensions

Use these procedures to upload the ION Grid Extensions so that they can be installed through LifeCycle Manager.

☐ Upload ION Grid Extensions to LifeCycle Manager

- ___1 Log on to LifeCycle Manager as administrator.
- ___2 Select Admin > Admin View. The Manage Products tab is displayed by default.
- ___3 Click Upload and select the file **Infor_ION_Grid_Extensions_ *version*.lcm** from the place on your client where the downloaded packages are stored.
- ___4 On the Verifying package window, click Yes to accept to register the packages on the LifeCycle Manager Server.
- ___5 When the task is finished, a dialog appears. Click OK.
- ___6 When the dialog appears asking you if you want to update your client, click Yes.
- ___7 When the update is done, a dialog appears informing that the client needs to be restarted. Click OK to restart the client.
- ___8 Log in again.

Upgrading ION Grid Extensions

Use these procedures to upgrade ION Grid Extensions from the 11.1.11.0 ION Grid Extension package to the ones in the ION Grid Extension from the 11.1.11.x package (that is, a newer release than 11.1.11.0). Note that each extension has its own release numbering and this numbering will usually be different between two grid extension packages.

☐ Download ION Grid Extensions for Upgrading

The following components available on the Infor Xtreme download site and will be needed for your installation.

Download page	Product name	Contains
Infor ION Grid Extensions	Infor ION Grid Extensions LCM package	Infor_ION_Grid_Extensions_ <i>version</i>.lcm Infor ION Grid Extensions installation package. Replace <i>version</i> with the actual version of the Infor ION Grid Extensions.

☐ Upload ION Grid Extensions to LifeCycle Manager

- ___1 Log on to LifeCycle Manager as administrator.
- ___2 Select Admin > Admin View. The Manage Products tab is displayed by default.

-
- ___3 Click Upload and select the file **Infor_ION_Grid_Extensions_ version.lcm** from the place on your client where the downloaded packages are stored.
 - ___4 On the Verifying package window, click Yes to accept to register the packages on the LifeCycle Manager Server.
 - ___5 When the task is finished, a dialog appears. Click OK.
 - ___6 When the dialog appears asking you if you want to update your client, click Yes.
 - ___7 When the update is done, a dialog appears informing that the client needs to be restarted. Click OK to restart the client.
 - ___8 Log in again.

☐ **Upgrade an ION Grid Extension**

- ___1 Upgrade the ION Grid to release 11.1.x (that is, a higher release than the current 11.1.11.0 release and the same release as the ION Grid Extensions package you have downloaded). For instructions, see the *Infor ION Grid Installation Guide*.
- ___2 On the Applications tab in the left pane in LifeCycle Manager, locate the release 11.1.11.0 grid extension that you want to upgrade to the one from the 11.1.x package.
- ___3 Right-click on the grid extension, select the name of the grid extension and then select the option to upgrade to a newer version.
- ___4 On the Upgrade Grid extension window, click Next.
- ___5 On the Summary window, click Finish.
- ___6 Repeat these steps for each grid extension.

- ["Session Provider Requirements and Selection" on page 14](#)
- ["Installing and Configuring the LDAP Session Provider Grid Extension" on page 17](#)
- ["Installing the DSSO Session Provider" on page 22](#)
- ["Installing the Windows Session Provider" on page 25](#)
- ["Installing and Configuring the SAML Session Provider" on page 26](#)
- ["Configuring Assertion Consumer Services" on page 33](#)
- ["Uninstalling a SAML Session Provider" on page 35](#)

Session Provider Requirements and Selection

There are four different session providers available as grid extensions for production scenarios. The purpose of each of these session providers is to provide an authentication or validation mechanism for the grid.

Of the four session providers, only the Windows Session Provider is supported for the ION Grid installed through a Java program. For the ION Grid for LifeCycle Manager, all four session providers are supported.

In addition, to determine the most appropriate one to use, consider the following information:

Session Provider Types

Windows Session Provider

This session provider uses the same authentication mechanisms as Windows itself and provides support for NTLM and Kerberos authentication. It must be installed on a Windows 2008 R2 or Windows 2012 server belonging to the Windows domain against which it will authenticate. The Windows Session Provider supports the following authentication methods: basic authentication, NTLM, and Negotiate.

LDAP Session Provider

This session provider supports complex authentication options, including multiple domains, server fail-over options, and authentication against standalone LDAP servers. The LDAP Session Provider can be used for authenticating users to any LDAP server, including Active Directory. The LDAP Session Provider supports basic authentication using the LDAP authentication method Simple Authentication only. This session provider requires configuration for basic setup and to take advantage of its more powerful features.

The LDAP Session Provider should not be configured to directly connect to a Lawson Security LDAP server (such as the Infor Lawson System Foundation LDAP). When authenticating against a Lawson Security system, use the DSSO Session Provider.

DSSO Session Provider

The DSSO Session Provider can authenticate against Lawson Security (in Infor Lawson System Foundation or Infor Java Framework runtime environments) using a DSSO base component. It is also used within Infor Java Framework itself, where the DSSO Session Provider communicates directly with the main Lawson Security installation. This session provider is needed if you are running Infor Smart Office in a grid, and you want to authenticate to your Infor Lawson System Foundation or Infor Java Framework runtime environment. In this scenario, the DSSO Session Provider requires the DSSO base component. For more information, see the *Distributed Single Sign-on for Lawson Smart Office Installation Guide*. The DSSO Session Provider supports basic authentication.

SAML Session Provider

The SAML Session Provider authenticates users using SAML to communicate with AD FS 2.0. User credentials are stored in AD but also synchronized to Infor Federation Services (IFS) for extended attributes (Claims) and also security role assignment (which happens in IFS). The session provider supports the following authentication methods: basic authentication and SAML 2. The SAML Session Provider implements basic authentication using WS-Trust to authenticate users to AD FS 2.0 (for active, non-browser based clients). The SAML 2 authentication method uses WS-Federation (for browser clients that can be automatically redirected).

Requirements and Selection

There are four different deployment scenarios for the session providers:

- **AD FS 2.0 and Infor Federation Services**

In this scenario, the users are authenticated to AD FS 2.0 using the SAML protocol. Infor Federation Services is installed on the AD FS server for the extra attributes it provides and also for automating configurations. This scenario applies when Infor Ming.le™ is used with AD FS 2.0.

- **Active Directory**

In this scenario, Active Directory is used as the user information storage, but AD FS is not used. Users are authenticated directly to the AD.

- **Lawson Security**

In this scenario, Lawson Security is used for user authentication. The session provider used in this scenario will relay the authentication request to the configured Lawson Security System (Infor

Lawson System Foundation or Infor Java Framework runtime environment). Lawson Security may store the user credentials in any LDAP or even Active Directory, but this is irrelevant from the session provider's point of view.

- **Other LDAP**

This scenario is for all other scenarios where users are stored in LDAP. The session provider authenticates the users directly to the LDAP server.

Choosing a Session Provider Based on the Scenario

An **X** in the matrix below means that the session provider supports the given scenario.

Session Provider	AD FS 2.0/IFS	Active Directory	Lawson Security	Other LDAP
Windows		-- X --		
LDAP		-- X --		-- X --
DSSO			-- X --	
SAML	-- X --			

Choosing between the LDAP Session Provider and the Windows Session Provider

If your choice is between the LDAP Session Provider and the Windows Session Provider, consider the following information:

	LDAP Session Provider 1.9	Windows Session Provider 1.9
Platform Requirements	All platforms supported by ION Grid 11.1.11.0 and higher.	Windows 2012 only, where that server is part of the domain that the session provider should authenticate against. Grid 11.1.11.0 in an M3 context.
Fail-over Support	Explicit fail-over support to selected secondary servers.	Implicit fail-over support from the built-in fail-over support in Windows.
Multiple Domain Support	Explicit support for multiple domains or for just standalone LDAP servers.	
Configuration Differences	Requires configuration for basic setup and to take advantage of its more powerful features	No configuration required.

If you meet the requirements for the Windows Session Provider and do not need the explicit fail-over support or multiple domain support, use the Windows Session Provider.

Installing and Configuring the LDAP Session Provider Grid Extension

Use these procedures to install the LDAP session provider for a grid. To determine if this is the appropriate session provider to install, see "[Session Provider Requirements and Selection](#)" on page 14.

☐ **The user login name**

In some LDAP configurations, the user name used for login is not the same as the one that is assigned to the Grid Principal after a successful login. This depends on the overall configuration of the LDAP connections such as the selected user attribute, if any domain information is removed from the user name before login or if any advanced user search filter is used.

Some grid applications depend on being able to retrieve the original user login name from the Grid Principal. Therefore, there is a setting to provide the login name to these applications even if the Grid Principal gets another name. The ability to add the extra data to the Grid Principal was introduced in the LDAP Session Provider 1.9.20 and 1.10.9. You can set the property using the Grid Management UI and during installation. This feature might have a negative effect on performance in systems with many concurrent users. Therefore, do not enable this feature if not necessary.

☐ **Install the LDAP Session Provider Grid Extension**

- ___ **1** In LifeCycle Manager, select Actions > Install Product.
- ___ **2** From the list, select the product **Infor LDAP Session Provider <version>**.
Click Next.
- ___ **3** On the Install window, select the location for the session provider. This is the grid on which the extension will be installed.
Click Next.
- ___ **4** On the LDAP Server Configuration window, enter the host where the grid extension will be installed.
Click Next.
- ___ **5** If you have a configuration where the login name is not the name of the Grid Principal after a successful login, on the Keep additional session data window, select Create Property Principal and add login name. See "[The user login name](#)" on page 17.
- ___ **6** On the Summary window, verify the properties provided.
Click Finish.
- ___ **7** Configure the LDAP Session Provider. See "[Configure the LDAP Session Provider](#)" on page 18.

❑ Configure the LDAP Session Provider

___ **1** In the left pane in LifeCycle Manager, locate the LDAPSessionProvider application within the grid where you installed it.

___ **2** Right-click the LDAPSessionProvider application and select Configure Session Provider.

If this is the first time that you are attempting to configure the session provider, the Server Connection window appears. If you have entered configuration information previously, the LDAP Session Provider Editor page appears in the right pane of LifeCycle Manager. This page has several tabs where you configure different aspects of the session provider.

___ **3** On the Server Connection window or Connection tab, enter the following:

Primary Server	The host name of the primary LDAP server.
Port	The port the LDAP service is listening on. Unless you have a very unique environment, leave it undefined and the correct defaults will be used (389 or 636).
Encryption method	<p>Select "Use StartTLS extension," "Use SSL Encryption (ldaps://)," or "No encryption." The default is "Use StartTLS extension."</p> <p>The "Use StartTLS extension" and "Use SSL Encryption (ldaps://)" methods allow password to be sent securely. Both of these use SSL/TLS protocol to secure the transmission. The main difference is that ldaps:// encrypts the entire conversation while StartTLS only encrypts the transmission of sensitive data (such as the password). This means that StartTLS is much faster and less demanding of resources. For those reasons, it is the default setting for a new connection.</p> <p>The certificates needed for successful communication are saved automatically by the configuration editor.</p> <p>Click Validate to check if the configuration editor can connect to the LDAP server. Depending on the encryption method you selected, you may need to respond to a Certificate Trust dialog box.</p> <p>This dialog box is displayed in different places depending on if you are configuring for StartTLS or LDAPS. When a StartTLS connection is used, the Certificate Trust dialog box is displayed when you click on Validate in the "Connection" window or tab (step 3). When LDAPS is used, the Certificate Trust dialog box is displayed when the Validate button is clicked in the "Authentication & Search Base" window or tab (see step 4). You have to select "Always trust this certificate" in order for the LDAP Session Provider to be able to connect to the LDAP server.</p>
Secondary servers	<p>Optionally, you can add secondary servers for fail-over purposes. For more information, see "Add a secondary server" on page 21.</p>

Click Next on the Server Connection window or click Save on the LDAP Session Provider Editor page.

4 On the Authentication & Search Base window or tab, enter the following:

Username	The user name or DN to bind with. This is the user to connect to the LDAP server with and to search for users being validated. It must be either a fully qualified name in the form " cn=User, ou=Users, dc=corp, dc=example, dc=com ", or in the case of an Active Directory environment, " User@corp.example.com " will also work.
Password	The password to bind with. Click Validate to confirm that the user name and password are correct.
Search base	LDAP location to be added to the connection URL in searches, for example, dc=corp, dc=example, dc=com . You can click Lookup to list all possible bases.

Click Next on the Authentication & Search Base window or click Save on the LDAP Session Provider Editor page.

5 On the User Element Mapping window or tab, configure the user element mapping. There are two different configuration modes available. The Simple Search offers basic configuration that is enough in most cases. With the Advanced Search mode, a complete user search filter can be configured. Most of the configuration elements are common for both configuration modes.

Enter the following:

Base Locations	Base locations in the LDAP where the users are found, relative to the search base (for example, "ou=Users"). Multiple base locations can be added, if you have users located in more than one part of the LDAP tree. Click on Add on the right and browse to the preferred part of the LDAP tree. Select a Base DN location from the list and click on Remove to delete the Base DN location from the list.
User Scope	Select Sub-tree or leave the check box clear. If Sub-tree is selected, the search is from the Base DN and down, rather than just in the base locations. In most cases, Sub-tree should be selected. The User Scope setting is identical for all configured base locations.
User ID Attribute	LDAP attribute containing user id. Default value: cn . The default is used if no value is entered. The User ID Attribute setting is identical for all configured base locations.
Simple Search	For the simple search, only the object class the users belong to needs to be configured.
Object Class	LDAP class for user objects. Default value: user . The default is used if no value is entered. The Object Class setting is identical for all configured base locations.

Advanced Search	With an advanced search, the complete user search filter can be supplied. When switching from simple to advanced, a proposed example filter is provided based on the values in Object Class and the User ID Attribute.
Filter	<p>A user search filter can be entered in the enabled text field when Advanced Search is selected. If a filter is entered, the Object Class property is not used any longer and that field is disabled. Enter %USER% in the filter where substitution should take place for the name of the user who is logging in or for the user name being searched for. A typical filter can look like this:</p> <pre>(& (objectClass=user) (sAMAccountName=%USER%))</pre> <p>The Filter setting is identical for all configured base locations.</p>
Strip domain	If this option is selected, the provided domain information in the user names will be removed before the login is made. Do not select this option in configurations where the domain information must be kept for login.

Click Validate to confirm that a search can return a list of users. The validation will test each of the provided base locations provided above. If no base location is provided, the relative search base is used for validation. The validation will show an example result for each base location

Click Next on the User Element Mapping window or click Save on the LDAP Session Provider Editor page.

6 On the Group Element Mapping window or tab, enter the following:

Base Locations	<p>Base location in the LDAP where the groups are found, relative to the search base ("ou=Groups"). For performance reasons, it is best to specify the most specific Base DN possible. This is because the search must search and map all groups under the Base DN in order to find the groups a user is a member of. Note that the LDAP session provider can only find groups that users are direct members of. You therefore cannot use groups within groups.</p> <p>You can add multiple different Base DNs if you have groups located in more than one part of the LDAP tree. Click on Add on the right and browse to the preferred part of the LDAP tree. Select a Base DN from the list and click on Remove to delete the Base DN from the list.</p>
Object Class	LDAP class for group objects. Default value: group . The default is used if no value is entered. The Object Class setting is identical for all configured base locations.
Group Member Attribute	LDAP attribute containing group id. Default value: member . The default is used if no value is entered. The Group Member Attribute setting is identical for all configured base locations.

Group Scope	Select subtree or leave the check box clear. The default is to leave the check box clear. If subtree is selected, the search is from the Base DN and down, rather than just in the Base DN. In most cases, subtree should be selected. The Group Scope setting is identical for all configured base locations.
--------------------	---

Click Validate to confirm that a search can return groups. The validation will test each of the provided group mapping base locations provided above. If no base location is provided, the relative search base is used for validation. The validation will show the result for each base location.

Click Finish on the Group Element Mapping window and then click Save on the LDAP Session Provider Editor page.

- ___7 After you have configured the LDAP session provider, you can set up role mapping for securing users.

☐ Add a secondary server

You can add secondary LDAP servers to your configuration for fail-over purposes. The implementation checks each call to the LDAP server (that fails) and looks for some specific exceptions/errors. When one of the known errors is seen, it is interpreted as a failed server and the session provider switches to the next server in the list. The switch is done in a round-robin fashion, and the state is not saved between restarts of the session provider. Therefore, you must make sure to keep the primary server first in the list.

Note that if a fail-over occurs during an attempted logon, that logon will fail. The new server will be used by the next logon attempt. When a switch happens, an INFO message similar to the following is logged in the SessionProvider log:

```
2013-03-04 08:12:38,525 INFO SessionProvider SessionProvider: Switching server from
sestw426.corpnet.infor.com to ldapemea.corpnet.infor.com
```

The configured servers, as well as the currently active server, can be seen by selecting the session provider in the LifeCycle Manager, and selecting Manage Application. If fail-over is configured, a list of the servers is shown, with an asterisk ("*") next to the currently active server

- ___1 Locate the LDAPSessionProvider application for the grid in the left pane in LifeCycle Manager.
- ___2 Right-click the LDAPSessionProvider application and select Configure Session Provider.
- ___3 On the Connection tab, click the Add... button by the Secondary server list field.
- ___4 Enter the address to the secondary server you want to add and click OK. After you click OK, a check is made to see if it is possible to connect to the server.
- ___5 Click Add... again if you want to add more secondary servers.
- ___6 When you are finished adding secondary servers, click Save.
- ___7 Switch to the Authentication & Search Base tab and click Validate. This will validate that the username and password are valid on all servers. You might also get additional certificate dialogs if you use any of the SSL-based encryption methods.

❑ Add additional domains

If you have users in multiple domains, you can add those domains to the configuration. The session provider will look for users in all domains simultaneously. Should a username exist in more than one domain, the logon will fail. The reason for this is that the session provider cannot know if the two users are identical, or if they should be treated differently.

- ___1 Locate the LDAPSessionProvider application for the grid in the left pane in LifeCycle Manager.
- ___2 Right-click the LDAPSessionProvider application and select Configure Session Provider.
- ___3 Click the Add Domain button in the upper right corner.
- ___4 When you are presented with the Server connection window, enter values just as if you were configuring the session provider, except with values appropriate for the new domain. For information on the session provider configuration fields, see "[Configure the LDAP Session Provider](#)" on page 18.

Installing the DSSO Session Provider

Use this procedure to install the DSSO session provider. To determine if this is the appropriate session provider to install, see "[Session Provider Requirements and Selection](#)" on page 14.

Important: For Lawson Security servers using Kerberos authentication, you must use the DSSO Session Provider 1.3. For installation instructions, see "[Install the DSSO Session Provider 1.3 in a grid](#)" on page 25.

For all other scenarios, use the DSSO Session Provider 2.0.

The installation for the DSSO Session Provider 2.0 is divided into three phases or tasks. The first phase and the last phase are performed using the DSSO Session Provider LifeCycle Manager plugin. The second phase is performed using one of the LifeCycle Manager plugins that can install a DSSO instance (minimum versions: DSSO 9.0.2.3.14 and DSP 10.0.1).

- ___1 "[Install a new grid router for the DSSO Session Provider 2.0](#)" on page 23
- ___2 "[Install DSSO using either the DSSO or the DSP LifeCycle Manager package](#)" on page 23
- ___3 "[Install the DSSO Session Provider 2.0 in a grid](#)" on page 24

Before you start Before you can install the DSSO Session Provider 2.0, you must have an installation package for DSSO uploaded on the LifeCycle Manager server.

The DSSO Session Provider 2.x is not backwards compatible and an upgrade is not possible from previous versions. If DSSO Session Provider 1.x is already installed, this installation must be removed prior to the new installation as well as the DSSO instance for that session provider.

Note: When you install the DSSO Session Provider 2.0, you must install the grid router, the DSSO instance, and the DSSO Session Provider on the same grid host.

❑ Install a new grid router for the DSSO Session Provider 2.0

- ___1 In LifeCycle Manager, select Actions > Install Product.
- ___2 From the list, select the **DSSO Session Provider** version product with the description "Create a new Grid Router adapted for DSSO use."
- ___3 Select the host to install the router on and click Next.
- ___4 Provide the external FQDN and the ports for the router.

Both the Lawson Security Server and the clients must be able to resolve and reach the provided FQDN.

Write down the provided FQDN and ports since they must be provided when you install DSSO. For more information, see "[Install DSSO using either the DSSO or the DSP LifeCycle Manager package](#)" on page 23.

Click Next.
- ___5 On the Summary window, click Finish.

❑ Install DSSO using either the DSSO or the DSP LifeCycle Manager package

- ___1 If you are installing DSSO using the DSP LifeCycle Manager package, follow the instructions in the *Distributable Security Package Installation Guide*. Review the section for Infor Smart Office or ION Enterprise Search.
 - ___a In the installation step "DSSO Instance," the provided instance name will be the name of the DSSO Service you will provide when completing the third task for installing the DSSO Session Provider. See "[Install the DSSO Session Provider 2.0 in a grid](#)" on page 24.
 - ___b In the installation step "Web Application Server," select the application server type of "Manual deployment but create service." For the FQDN, enter the external FQDN of the DSSO router you provided in the first task of installing the DSSO Session Provider. For the HTTP/HTTPS ports, use the ports defined in the first task of installing the DSSO Session Provider. See "[Install a new grid router for the DSSO Session Provider 2.0](#)" on page 23.
 - ___c When the DSSO installation is finished, create new identities for the users that should have access to the newly created service. These identities must be on the newly created service. In addition, these users must have identities on the primary domain service (usually SSOP) as those identities are used for authentication for the DSSO Session Provider.
- ___2 If you are installing DSSO using the DSSO LifeCycle Manager package, follow the instructions in the *Distributed Single Sign-on for Lawson Smart Office Installation Guide* (available on the download page at Technology > Enterprise Search > Shared Security Platform All supported platforms) or the *Lawson Enterprise Search for LifeCycle Manager Installation Guide* (available in the Lawson Enterprise Search infocenter or the download page at Technology > Enterprise

Search > Lawson Enterprise Search VMware ESX). Review the section for Lawson Smart Office or Lawson Enterprise Search.

- ___ **a** In the installation step "Create DSSO Service," the provided Unique Service name will be the name of the DSSO Service you will provide when completing the third task for installing the DSSO Session Provider. See "[Install the DSSO Session Provider 2.0 in a grid](#)" on page 24. Select the check box for "Create DSSO Service instance" and select "Create new service" in the "Installation type" drop-down box.
- ___ **b** In the installation step "Web Application Server," select the application server type of "No App server or manual configuration." For the "Web frontend server FQDN," enter the external FQDN of the DSSO Router provided in the first task of installing the DSSO Session Provider. For the HTTP/HTTPS ports, use the ports defined in the first task of installing the DSSO Session Provider. See "[Install a new grid router for the DSSO Session Provider 2.0](#)" on page 23.
- ___ **c** When the DSSO installation is finished, create new identities for the users that should have access to the newly created service. These identities must be on the newly created service. In addition, these users must have identities on the primary domain service (usually SSOP) as those identities are used for authentication for the DSSO Session Provider.

☐ **Install the DSSO Session Provider 2.0 in a grid**

- ___ **1** In LifeCycle Manager, select Actions > Install Product.
- ___ **2** From the list, select the **Infor DSSO Session Provider <version>** product with the description "Deploy the DSSO Session Provider."
- ___ **3** On the Install window, select the location for the DSSO Session Provider. This is the grid on which the DSSO Session Provider will be installed.
Click Next.
- ___ **4** On the DSSO Base installation window, select the DSSO base installation created in the "Install DSSO" task and click Next.
- ___ **5** On the Lawson Environment window, consider the following fields and click Next when you are done:

Connected to Environment	This read-only field displays the name of the Lawson Environment based on the DSSO base installation value you entered earlier.
Authentication service name	Enter the name of the authentication service as defined in the "Install DSSO" task. That is, if you are installing DSSO using the DSP LifeCycle Manager package, this is the name of the DSSO Service you provided in the "DSSO Instance" step. If you are installing DSSO using the DSSO LifeCycle Manager package, this is the name of the DSSO Service you provided in the "Create DSSO Service" step.
- ___ **6** On the Grid properties window, select which router to use. This should be the DSSO router created in the "Install a new Grid router for the DSSO Session Provider."

- ___7 On the Summary window, click Finish.
- ___8 After you have installed the DSSO session provider, you can set up role mapping for securing users.

❑ Install the DSSO Session Provider 1.3 in a grid

Before you start Before you can install the DSSO Session Provider 1.3, you must have already installed the DSSO base components. For more information, see the *Distributed Single Sign-on for Lawson Smart Office Installation Guide*.

The minimum grid version for using the DSSO Session Provider 1.3 is 10.1.9.0.

- ___1 In LifeCycle Manager, select Actions > Install Product.
- ___2 From the list, select the product **DSSOSessionProvider_version** product.
- ___3 On the Install window, select the location for the DSSO Session Provider. This is the grid on which the DSSO Session Provider will be installed.
Click Next.
- ___4 On the DSSO Base installation window, select the DSSO base installation and click Next.
- ___5 On the Lawson Environment window, consider the following fields and click Next when you are done:

Connected to Environment	This read-only field displays the name of the Lawson Environment based on the DSSO base installation value you entered earlier.
Authentication service name	Enter the name of the authentication service. (The default value is the primary service for the Lawson Environment). You can check the name of the primary service by accessing the following URL: <code>http://servername:port/ssconfig/SSOCfgInfoServlet</code> .

- ___6 On the Grid properties window, enter a name for the DSSO Session Provider installation and select the JDK version (either 32-bit or 64-bit).
- ___7 On the Summary window, click Finish.
- ___8 After you have installed the DSSO Session Provider, you can set up role mapping for securing users.

Installing the Windows Session Provider

Use this procedure to install the Windows Session Provider grid extension. You can install this session provider only in Lawson Grid 10.1.9.0 or higher or Infor ION Grid 11.1.10.0 or higher on a Windows server with a Windows domain.

To determine if this is the appropriate session provider to install, see "[Session Provider Requirements and Selection](#)" on page 14.

❑ Install the Windows session provider in a grid

- ___ **1** In LifeCycle Manager, select Actions > Install Product.
- ___ **2** From the list, select the product **Infor Windows Session Provider version**.
Click Next.
- ___ **3** On the Install window, select the location for the Windows Session Provider. This is the grid on which the Windows Session Provider will be installed.
Click Next.
- ___ **4** On the Summary window, click Finish.
- ___ **5** After you have installed the Windows session provider, you can set up role mapping for securing users.

Installing and Configuring the SAML Session Provider

Use this procedure to install the SAML Session Provider grid extension. The SAML Session Provider should only be deployed on a single host and started in a single node.

Before you start If you want to use the SAML Session Provider, your system must meet the following requirements:

- The browser used must support Integrated Windows Authentication (IWA).
- AD FS 2.0 is used as the Identity Provider (IdP).
- Infor Federation Services (minimum version 10.3.2+) is installed on the AD FS server.
- You have a domain account that is an IFSApplicationAdmin and AttributeServiceCaller in the IFS application. Preferably this account should not expire since the SAML SP will use that account configuration for role lookup in IFS during logins.
- In AD FS the Endpoint "/adfs/services/trust/13/usernamemixed" for WS-Trust 1.3 is both Enabled and Proxy Enabled.
- You have added security roles in IFS (Manage > Master Data, double-click on Security Role) to the grid roles (grid-admin, grid-poweruser, grid-user, grid-runas) and the SAML SP test role (TestRole).

Note: Due to third-party requirements, the SAML Session Provider only supports Java 1.6.x. After installing the SAML Session Provider, ensure that the Java version for the SAML Session Provider is Java 1.6.x. Otherwise, update the Java Executable grid property for the SAML Session Provider binding. Restart the node after updating the Java version. For more information, see the *Infor ION Grid Administration Guide*.

❑ Install the SAML Session Provider in a grid using LifeCycle Manager

- ___1 In LifeCycle Manager, select Actions > Install Product.
- ___2 From the list, select the product **Infor SAML Session Provider <version>**.
Click Next.
- ___3 On the Host selection window, select the grid host you want to deploy the SAML Session Provider to, and click Next.
- ___4 If a SAML router already exists, you will be asked if you want to reuse that router. If no SAML router exists, on the Router properties window, define the properties for the router to be used by the session provider and click Next:

External address	The external address for the router.
IP Address	The external IP address of the router.
Http port	The HTTP port for the router. The installation provides the next highest available ports as a suggestion for this field and the next field.
Https port	The HTTPS port for the router.

- ___5 On the Session Provider Properties window, define the following and click Next:

Service Provider Entity ID	Provide a service provider entity ID. The recommended format is the fully qualified domain name concatenated with the HTTPS port, for example, acme.corp.com_61008 . This ID will be configured in the IdP (and IFS if used).
IdP FQDN	The fully qualified domain name of the AD FS.
IdP http port	The HTTP port of the AD FS endpoint.
IdP https port	The SSL port of the AD FS endpoint.
Metadata URI	Provide the URI to the federation metadata. The default AD FS 2.0 value is "/FederationMetadata/2007-06/FederationMetadata.xml" . If AD FS is used as the IdP, the URI can be found by looking in the "AD FS 2.0 Management." Open the Service folder and look in the Endpoints folder. Check the Metadata point of the screen and the "Metadata" type.

After you click Next, the installer will get the SSL certificates from the AD FS server and you will have to confirm them before continuing. The installer will retrieve the AD FS metadata and parse it for suggested values for a later installation step.

- ___6 On the IFS Properties window, define the following and click Next:

Use IFS	Select this check box if it is not already selected.
----------------	--

IFS base URL	Provide the base URL for IFS. The suggested URL should be correct for a standard installed IFS server. If you change this value, do not include more of the URL than the virtual directory of IFS. The default value is <code>http://IFSserver:port/IFSServices</code> . Do not provide an HTTPS URL if that is not a defined endpoint in the IFS ConfigurationService WSDL.
---------------------	--

Username	Provide the name for a domain user that belongs to the IFSApplicationAdmin and AttributeServiceCaller roles in IFS so that a new application can be created in IFS. The username MUST be in the domain\uid format.
-----------------	--

Password	Provide the password for the domain user from the previous field. After you click Next, the EntityID defined previously is validated against IFS and if the EntityID already exists as an application in AD FS, you will have to confirm that you want to overwrite the existing application in IFS.
-----------------	---

___7 Review the fields on the SAML Properties window and click Next. These properties are used by the SAML session provider when talking to the IdP and also define the endpoints the SAML Session Provider will provide for logging in and logging out. The suggested values are based on the AD FS metadata provided in previous steps. Do not change them if you are not sure of what you are doing.

___8 Review the values on the Summary window and click Finish to start the installation.

☐ Install the SAML Session Provider in a grid manually

To install the SAML Session Provider manually, you must set up a properties file containing the deployment profile configuration data. This procedure also requires Grid version 10.1.10.0+ to enable the passing of the properties file containing the configuration data to the deployment profile.

There are 18 possible properties to configure for the manual SAML Session Provider deployment. Only eight of those are required. The other 10 will get their default value if omitted in the properties file.

Property	Required?	Description
routerFqdn	Yes	SAML-enabled grid router external FQDN.
routerIP	Yes	IP address for external access to the SAML router.
idpFqdn	No	IFS/ADFS server FQDN.
useIFS	No	Dictates if IFS setup should be performed or not. If set to false , all IFS/ADFS configuration has to be done manually. Default is true .

Property	Required?	Description
IFSUser	Yes, if useIFS is true or if useIFS is not defined	Username for an IFS Administrator. This user must be member of the IFSApplicationAdmin and the AttributeServiceCaller Security Roles in IFS.
IFSPass	Yes, if useIFS is true or if useIFS is not defined	The password for the IFSUser.
routerHttpPort	Yes	HTTP port to the SAML router.
routerHttpsPort	Yes	SSL port to the SAML router.
idpHttp	No	HTTP port to ADFS/IFS. Default is 80 . IFS installation guide recommends changing the port.
idpHttps	No	SSL port to ADFS/IFS. Default is 443 . IFS installation guide recommends changing the port.
idpUri	No	The URI to the Federation metadata xml file of ADFS. The value can be found in the AD FS 2.0 management tool under Service > Endpoints. At the bottom are the Metadata links. Default is /FederationMetadata/2007-06/FederationMetadata.xml .
idpMultiTenant	No	A boolean property to indicate if the session provider should operate in multi-tenant mode. Default is false .
ifsCfgsvcUrl	No	The virtual directory of the IFS web application on the idpFqdn. Default is IFSServices .
SignAssertions	No	Requests the IdP to sign assertions. Default is true .
identityClaimName	No	Provides which claim in an assertion to be used to decide the identity. Default is http://schemas.infor.com/claims/Identity .
assertionTimeout	No	Provides the timeout in seconds for an assertion. Default is 300 .
nameidFormat	No	Provides the NameIDFormat used for WS-Federation. Default is urn:oasis:names:tc:SAML:2.0:nameid-format:transient .
IFSAppType	No	Decides which IFS application type to create. If IFS version 10.3+ is used, then use GRID . For earlier versions, use SAMLP . Default is GRID .

- ___1 Access the Configuration Manager for the grid and log on as a grid-admin.
- ___2 Click Routers.
- ___3 If there already is a SAML router, note the external FQDN, HTTP and HTTPS ports, and external IP address, and put these into the configuration data file. Ensure that the SAML router supports the saml2 authentication method for both HTTP and HTTPS. Also remember the host it is running on for the configuration in step 4b below.
- ___4 If there is no SAML router, add one:

___a Click Add Router.

___b Enter the following on the Router window:

Name	Enter SAML Router .
Host	Select the host where the router should run.
External Address	Provide the external FQDN for the host. This FQDN must be resolvable and reachable from both the IFS server and the connecting clients.
HTTP	On the Port tab, select an HTTP port. It is recommended to use the next port in line after the other router. On the WWW Authentications Methods tab, select saml2 .
HTTPS	Select an HTTPS port. Recommended is to use the next port in line after the HTTP port. On the WWW Authentications Methods tab, select saml2 .

- ___5 Click Add.
- ___6 Enter the router properties into the configuration data file.
- ___7 Prepare the rest of the configuration data in the file to be used during deployment. See "Deployment profile configuration data" on page 25 for information about the properties.
- ___8 Navigate back to the Configuration Manager home page.
- ___9 Click Applications.
- ___10 Click Install New Application.
- ___11 On the Select Application tab, if the SAMLSessionProvider is not available in the list, click Upload. Browse to the gar file and click Upload.
- ___12 When the SAMLSessionProvider is available on the Select Application tab, select it and click Next.
- ___13 On the Install Options tab, ensure that the name is SAMLSessionProvider and that the selected deployment profile is StandaloneDeploymentProfile. Browse for the configuration data file and select which host to deploy it to. The selected host must be the same as the SAML router is running on. Click Finish.
- ___14 After the deployment is done, the SAML Session Provider will start and be in status "Starting" for up to 2 minutes. The reason for this is that the actual IFS configuration takes place the

first time the SAML Session Provider is started and not during the deployment. When the IFS setup is finished, the SAML Session Provider should be put into status "OK". If there was no other session provider previously installed and activated, the SAML Session Provider is now the active session provider.

☐ **Configure Infor Federation Services for the SAML Session Provider**

- ___1 Log in to the IFS/AD FS server and log on to the "Infor Federation Services" application as an IFSApplicationAdmin
- ___2 Select Configure > Applications and select the newly created application (at the bottom of the list).
- ___3 Link security roles (grid-admin, grid-poweruser, grid-user, grid-runas, TestRole, and any other required roles) to the new application and save.
- ___4 For testing, add the grid-admin security role to the active account.

☐ **Add Assertion Consumer Service endpoint to AD FS**

- ___1 Find the federation metadata URL for the SAML Session Provider:
 - ___a From the Grid Management Pages, open the management pages of the SAMLSessionProvider application.
 - ___b Select Metadata.
 - ___c Copy the federation metadata URL displayed on the page for use in step 6.
- ___2 Log on to the IFS/AD FS server, and start "AD FS 2.0 Management."
- ___3 Expand "Trust Relationships" in the left side menu and select "Relying Party Trusts."
- ___4 Select the application that corresponds to your SAML Session Provider installation.
- ___5 Right-click and select Properties.
- ___6 On the Monitoring tab, enter the federation metadata URL for your SAML Session Provider (see step 1c for the value).
- ___7 Click Test URL to make sure that the address is reachable and trusted by AD FS. If you get an error message, see the Microsoft Windows Server documentation on troubleshooting trust management problems with AD FS 2.0.
- ___8 When you get a message saying that the URL was validated successfully, click OK and then OK again.
- ___9 Select again the application that corresponds to your SAML Session Provider installation.
- ___10 Right-click and select "Update from Federation Metadata."
- ___11 On the Endpoints tab, verify the SAML Assertion Consumer Endpoints, and then select Update.

❑ Test the SAML Session Provider installation

- ___1 In LifeCycle Manager, right-click on the Grid and select General tasks > URL > Java web start.
- ___2 After the Grid Management tool is started, ensure that the SAML router and the SAML Session Provider are started.
- ___3 Click on [login] in the bottom left corner. Provide the credentials used for IFS admin (which was given the grid-admin role).
- ___4 When the login succeeds, the "<not logged in>" is changed to the user name of the logged in user. Hover the cursor over the user name to see the provided roles. Ensure that the grid-admin role is assigned to the user.
- ___5 Configure the test servlet. See "[Configure the test servlet](#)" on page 32.

❑ Configure the test servlet

For test purposes, the saml-session-provider-gar contains a web servlet, `com.infor.gridextension.sessionprovider.webapp.HelloServlet`. When the IdP has been configured, this servlet can be set up to test the communication between the grid and the IdP. Setting this up also helps with understanding how roles should be configured in IFS and the grid.

- ___1 If you want, you can try to access the test servlet at this point to see what happens when a role hasn't been configured. The servlet should be available at `https://[SAML router IP address]:[SAML router https port]/test/hello`. The expected behavior is to get an error message saying that you don't have the required role for this application.
- ___2 After trying this, you will have a grid session set for your user. In order to make further tests after setting the roles, remove this session. Click Advanced on the Grid Management start page, then Sessions, and then remove the desired session. On this page, you can also see which roles have been mapped for your user.
- ___3 Create and map roles for the test.

The test servlet has been set up for role-based access control in its web.xml file. If you examine the web.xml file, you will see that only users with the role `TestRole` are allowed to perform a GET operation on the servlet. To give a user the `TestRole` role, you must create that role in IFS and then map the role in the grid.

 - ___a Make sure that you have configured IFS and AD FS to emit Security Roles as claims.
 - ___b Create a role called `TestRole` in IFS, according to "[Add security roles in IFS](#)" on page 33. Make sure to give the role to your test user.
 - ___c The role must be explicitly mapped in the grid. On the Grid Management start page, click Applications, then Configuration for the SAML Session Provider, and then Edit Role Mappings.

You will see the TestRole in the list of available roles. This is the role name that is referenced in the web.xml file.

Then click Edit... in the Included Members column of the TestRole, and click Add.... In the Global box, add TestRole as a custom role name. This is the role name that arrives in the claim from IFS. Remember to save your changes.

- ___d Access the test servlet as described in the first step. The expected behavior is to get the message "Test successful."

Note: The roles in IFS and the grid could very well have different names, but this is not a problem as long as they are mapped correctly in the grid.

☐ Add security roles in IFS

- ___1 Start the Infor Federation Services application and log on with a user that is an IFSApplicationAdmin.
- ___2 Select Manage > Master Data.
- ___3 Double-Click on Security Role.
- ___4 Click on the New button and add the name of the Security Role (called Node name in the UI) and a description.
- ___5 You may assign users now to the new role by clicking the Add User button.
- ___6 Click Save when finished.
- ___7 Select Configure > Applications in the menu.
- ___8 Select the application that should be emitting this role
- ___9 Select all roles that the application should emit and click Save.
- ___10 To add additional users to the role after it is created, either:
 - Enter the Manage > Master Data and add users to a role.
 - Enter the Manage > Users, select a user, and add the role to that user.

The roles should not be emitted as Claims in the SAML Assertion token.

Configuring Assertion Consumer Services

In order to authenticate a given user, the SAML Session Provider sends an authentication request to the identity provider (AD FS 2.0). The response (assertion) is returned to one of a set of pre-configured assertion consumer service locations. These are endpoints where the SAML Session Provider receives and handles assertions from AD FS.

When a web application in the grid requires a session, this session is set as a cookie on the HTTP response. It is important that the assertion from AD FS is sent to the same host address as the one used in the original request from the client. Otherwise, the session will be set on the wrong context, and the client will not be able to access the desired resources. Both the SAML Session Provider and AD FS 2.0 must be configured to use the correct assertion consumer services.

If you access secured web applications in the grid via a proxy, you must add assertion consumer services representing the proxy host.

Initial Configuration

By default, the LifeCycle Manager installer will set up two assertion consumer service endpoints in the configuration: one for the FQDN, and one for the IP number of the SAML router. Unfortunately, only one of these can be automatically set up in AD FS. The installation must therefore be completed with a manual step, as described in the installation procedure for the SAML Session Provider. See "[Installing and Configuring the SAML Session Provider](#)" on page 26.

Updating Assertion Consumer Services

This section describes how to add more assertion consumer services to the configuration of the SAML Session Provider and AD FS 2.0. This is needed if you access secured web applications running in the grid via a host and port other than those already specified as assertion consumer service endpoints, for example, via a router different from the SAML router, or if you have a proxy in front of the grid.

Before you start This procedure assumes that the initial configuration of assertion consumer service endpoints has already been performed.

☐ To update assertion consumer services

___1 Add an assertion consumer service endpoint to the SAML Session Provider:

- ___a From the Grid Management Pages, open the Management Pages of the SAMLSessionProvider application.
- ___b Select Assertion Consumer Services.
- ___c Type the desired host address and port, and then select Generate ACS URL.
- ___d Click on the disk button to save your changes.

___2 Add the assertion consumer service endpoint to AD FS 2.0:

- ___a Log on to the IFS/AD FS server, and start "AD FS 2.0 Management."
- ___b Expand Trust Relationships in the left side menu and select Relying Party Trusts.
- ___c Select the application that corresponds to your SAML Session Provider installation. Right-click and select "Update from Federation Metadata."

- ___d On the Endpoints tab, verify the SAML Assertion Consumer Endpoints, and then select Update.

Uninstalling a SAML Session Provider

To uninstall a SAML Session Provider, see the general instructions for uninstalling applications in the *Infor ION Grid Administration Guide for LifeCycle Manager 10*. In addition, note the following:

- When you uninstall a SAML Session Provider, the SAML router created during installation does not get uninstalled. It can be re-used for a new installation, or removed manually.
- The IFS/AD FS configuration does not get automatically removed. The application in IFS and Relying Party Trust in AD FS should be manually removed.
- Similar to the case of uninstalling a SAML Session Provider, if the installation of a SAML Session Provider fails, the IFS and AD FS configuration may need to be manually removed.

- "Installing the Grid Database Connectivity Grid Extension" on page 36
- "Viewing Grid Database Connectivity Application Configuration Information" on page 37
- "Grid Database Connectivity and H2 Databases" on page 37
- "Accessing the H2 Web Console" on page 38
- "Managing Database Drivers for the Grid Database Connectivity Grid Extension" on page 39
- "Creating and Changing H2 and GDBC Application Users" on page 41
- "Changing H2 User and Application User Passwords" on page 42
- "Backing Up an H2 Database" on page 43
- "Restoring an H2 Database from a Backup" on page 45

Installing the Grid Database Connectivity Grid Extension

Use this procedure to install the Grid Database Connectivity grid extension in a grid.

☐ Install Grid Database Connectivity Grid Extension

___1 In LifeCycle Manager, select Actions > Install Product.

___2 From the list, select the product **GDBC** <version>.

Click Next.

___3 On the Install window, select the location for the Grid Database Connectivity:

Name Select the grid on which the grid extension should be installed.

Click Next.

___4 On the Install Grid Database Connectivity window, enter values for the following:

Host The host for the grid extension.

H2 port The port for the H2 database used by GDBC.

Click Next.

- ___5 On the Summary window, verify the properties provided.

Click Finish.

Viewing Grid Database Connectivity Application Configuration Information

Use this procedure to view information on the applications using GDBC to make a database connection. The information available includes:

- Application - name of the application using the driver
- Driver - GDBC driver in use for that connection
- Driver Class - class file used to implement the JDBC connection
- User - database connection user name
- URL - database connection URL
- Version - database version
- H2 Web Console - direct link to the web console for embedded H2 database connections only

☐ View GDBC application configuration information

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___2 In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___3 On the Grid DB Broker page, click View application configuration.

Grid Database Connectivity and H2 Databases

The Grid Database Connectivity grid extension includes an H2 database. Some applications may be delivered using an embedded H2 database through GDBC. The application's installation guide will indicate if this is the case.

The default location for the H2 database files on a grid installed through LifeCycle Manager is:

X:\LifeCycle\hostname\grid\gridname\applications\GDBC_application_name\h2db

The default user that is created is **sa** with a password of **null**.

The H2 database files take the following format:

File	Description
<database_name>.h2	the physical database file
<database_name>.lock	H2 lock management file for the database
<database_name>.lobs	folder containing the large objects (BLOB/CLOB) for the database – deprecated in newer versions of H2 where the objects are now stored in the main DB so this folder and its contents may not exist

A full reference guide for H2 DB is available at: <http://www.h2database.com/h2.pdf>.

For procedures to managing the H2 database, see

- ["Managing Database Drivers for the Grid Database Connectivity Grid Extension"](#) on page 39
- ["Creating and Changing H2 and GDBC Application Users"](#) on page 41
- ["Backing Up an H2 Database"](#) on page 43
- ["Restoring an H2 Database from a Backup"](#) on page 45

Accessing the H2 Web Console

The H2 Web Console is an administrative user interface delivered with the H2 database. Some of the procedures for backing up and restoring an H2 database require accessing this console.

☐ Access the H2 Web Console

- ___ **1** Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___ **2** In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___ **3** On the Grid DB Broker page, click View application configuration.
- ___ **4** On the Applications page, click the H2 Web Console link for the application you want to work with.

Managing Database Drivers for the Grid Database Connectivity Grid Extension

Use these procedures to manage the database drivers used by the Grid Database Connectivity grid extension.

❑ Add a database driver for the Grid Database Connectivity grid extension

The Grid Database Connectivity supports the uploading of new database drivers (type 4 JDBC only). If you have type 4 JDBC drivers you want to use, you can upload them to the GDBC broker.

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___2 In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___3 On the Grid DB Broker page, click Manage Drivers.
- ___4 On the Drivers page, click Add New.
- ___5 Enter a driver name and click Create.
- ___6 On the Driver Details page, click Add file(s).
- ___7 Enter the path and name of the drivers files, or click Browse to navigate to each driver file.
- ___8 Click Add when you have entered or selected all driver files you want to add.

❑ Change the GDBC database driver for an application

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___2 In the Grid Management pages, click the GDBC application link at the bottom of the page.
- ___3 On the Application GDBC page, click Configuration.
- ___4 On the Application: GDBC (GDBC) page, click Edit Properties.
- ___5 Edit the broker.connectionUrl property:
 - ___a Click on the Value link for the broker.connectionUrl property and click Add New Entry.
 - ___b Enter the Grid application name into the Application column, for example, LSO or GDBC.
 - ___c Enter the JDBC driver URL connection string into the Value column.

For example, for a JTDS driver connecting to SQL server, you would use the construct:

```
jdbc:jtds:sqlserver://hostname:port/database_name
```

___d Select the Merge radio button.

___e Click Save.

___6 Edit the broker.driverClassName property.

___a Click on the Value link for the broker.driverClassName property and click Add New Entry.

___b Enter the Grid application name into the Application column, for example, LSO or GDBC.

___c Enter the driver class name into the Value column.

For example, for a JTDS driver, you would use:

`net.sourceforge.jtds.jdbc.Driver`

___d Select the Merge radio button.

___e Click Save.

___7 Edit the broker.userName property.

___a Click on the Value link for the broker.userName property and click Add New Entry.

___b Enter the Grid application name into the Application column, for example, LSO or GDBC.

___c Enter the database user name that should be used for the connection.

___d Select the Merge radio button.

___e Click Save.

___8 Edit the broker.password property.

___a Click on the Value link for the broker.password property and click Add New Entry.

___b Enter the Grid application name into the Application column, for example, LSO or GDBC.

___c Enter the database user's password that should be used for the connection.

___d Select the Merge radio button.

___e Click Save.

___9 Edit the broker.driverDirName property.

___a Click on the Value link for the broker.driverDirName property and click Add New Entry.

___b Enter the Grid application name into the Application column, for example, LSO or GDBC.

___c Enter the driver directory name. This is the Driver Name and can be retrieved from the Drivers page in the GDBC management pages. See "[View database driver file names](#)" on page 41.

___d Select the Merge radio button.

___e Click Save.

- ___10 When you have entered values for the properties, click Save at the top of the Application Properties page and then click Save again on the confirmation dialog box.
- ___11 Restart the application to put the changes into effect.

☐ **View database driver file names**

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___2 In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___3 On the Grid DB Broker page, click Manage Drivers.
- ___4 Click the name of the database driver.

☐ **Remove a database driver from the Grid Database Connectivity grid extension**

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___2 In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___3 On the Grid DB Broker page, click Manage Drivers.
- ___4 Click the red X next to the database driver name.
- ___5 Click Yes to confirm that you want to remove the driver.

Creating and Changing H2 and GDBC Application Users

Use these procedures to create a new user for the H2 database and then change the user for a GDBC application.

☐ **Create a new H2 database user**

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.

- ___2 In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___3 On the Grid DB Broker page, click View application configuration.
- ___4 On the Applications page, click the H2 Web Console link for the application you want to work with.
- ___5 Execute the following SQL statement to create the new user:

```
CREATE USER username PASSWORD 'password'
```

☐ **Change the GDBC application user**

- ___1 Access the Configuration Manager for the grid where the GDBC is installed.
- ___2 Click Applications.
- ___3 Make note of the exact name of the application you want to change the user for (for example, LSO), and then click GDBC.
- ___4 Click Edit Properties.
- ___5 Click the link in the Value column for the broker.userName property.
- ___6 If no entry for the application exists, then click Add New Entry.
- ___7 If this is a new entry, enter the previously noted application name into the Application field and the username into the Value field. Otherwise, simply update the username in the Value field.
- ___8 Click Save.
- ___9 Click the link in the Value column for the broker.password property.
- ___10 If no entry for the application exists, then click Add New Entry.
- ___11 If this is a new entry, enter the previously noted application name into the Application field and the password into the Value field. Otherwise, simply update the password in the Value field.
- ___12 Click Save.
- ___13 Click the Save button at the top of the page and then confirm the save.
- ___14 Restart GDBC and your application.

Changing H2 User and Application User Passwords

Use these procedures to change the password for an H2 database user and to change the password for a GDBC application user.

❑ **Change the H2 user password**

- ___1 Access the management pages for the Grid Database Connectivity grid extension. You can access these pages via the grid's Grid Management Pages, which can be accessed through the LifeCycle Manager, Java Web Start, or HTML. For more information, see the *Infor ION Grid Administration Guide for LifeCycle Manager 10*.
- ___2 In the Grid Management Pages, click the Management Pages link for the Grid Database Connectivity grid extension.
- ___3 On the Grid DB Broker page, click View application configuration.
- ___4 On the Applications page, click the H2 Web Console link for the application you want to work with.
- ___5 Execute the following SQL statement to create the new user:

```
ALTER USER username SET PASSWORD 'password'
```

❑ **Change the GDBC application user password**

- ___1 Access the Configuration Manager for the grid where the GDBC is installed.
- ___2 Click Applications.
- ___3 Make note of the exact name of the application you want to change the user's password for (for example, LSO), and then click GDBC.
- ___4 Click Edit Properties.
- ___5 Click the link in the Value column for the broker.password property.
- ___6 If no entry for the application exists, then click Add New Entry.
- ___7 If this is a new entry, enter the previously noted application name into the Application field and the password into the Value field. Otherwise, simply update the password in the Value field.
- ___8 Click Save.
- ___9 Click the Save button at the top of the page and then confirm the save.
- ___10 Restart GDBC and your application.

Backing Up an H2 Database

Use these procedures to back up an H2 database. You can choose to the back up when the database is running or when it is stopped. You can also perform the backup through a script.

Before you start Be sure to meet the following prerequisites if you are performing the backup from the command line:

- Java 1.6+ must be installed on the machine where commands for backing up the database will run.
- A copy of the H2 jar file must be accessible by the command. This file is delivered with GDBC and is found in `X:\LifeCycle\hostname\grid\gridname\applications\GDBC_application_name\drivers\h2`.
- If you are using the Backup command from the command line, the database must be stopped.

☐ **Back up an H2 database while it is stopped**

This method creates an H2 database with the contents of the backup.

___1 Stop the H2 database.

___2 At a command line, type

```
java -classpath h2-version.jar org.h2.tools.Backup -file fileName.  
zip -dir source_DB_directory -db source_DB_name
```

☐ **Back up an H2 database using the SCRIPT command from the command line**

This method creates a humanly readable SQL script with the contents of the backup. It locks the database objects during the creation of the script.

___1 Access the H2 Web Console and copy the URL at the top of the left pane. It will have a format similar to the following:

```
jdbc:h2:tcp://172.30.73.165:62882/C:\LifeCycle\www.mycorp.com\grid\  
myGrid\applications\GDBC\h2db\GDBC_application_name;MODE=MSSQLSERVER
```

___2 Open a command line window and, at the command line, type

```
java -classpath h2-version.jar org.h2.tools.Script -url DB_JDBC_H2_  
URL_COPIED_FROM_CONSOLE -user db_user -script fileName.zip -options  
compression zip
```

☐ **Back up an H2 database using the SCRIPT command in the H2 Web Console**

This method creates a humanly readable SQL script with the contents of the backup. It locks the database objects during the creation of the script.

___1 Access the H2 Web Console.

___2 Enter the following SQL statement (administrator rights are required to execute this command):

```
SCRIPT TO 'fileName.zip' COMPRESSION ZIP
```

The resulting zipped backup file will be located in

`X:\LifeCycle\hostname\grid\gridname\applications\GDBC_application_name`.

Note: Other switches can be provided, for example, to disable export of passwords. See the H2 reference guide for more information.

❑ Back up an H2 database while it is running

This method creates an H2 database with the contents of the backup. It does not lock the objects during creation, but the backup is transactionally consistent because the transaction log is also copied. Log files are also exported.

___1 Access the H2 Web Console.

___2 Enter the following SQL statement (administrator rights are required to execute this command):

```
BACKUP TO 'fileName.zip'
```

The resulting zipped backup file will be located in

X:\LifeCycle\hostname\grid\gridname\applications\GDBC_application_name.

Restoring an H2 Database from a Backup

Use these procedures to restore an H2 database from a backup.

It may be necessary to drop some or all tables, records, or other database objects prior to commencing a restore. Various SQL commands are available to facilitate partial or total restoration options which are outside the scope of this document.

Before you start Be sure to meet the following prerequisites if you are restoring the database through the command line:

- Java 1.6+ must be installed on the machine where the command will run.
- A copy of the H2 jar file must be accessible by the command. This file is delivered with GDBC and is found in X:\LifeCycle\hostname\grid\gridname\applications\GDBC_application_name\drivers\h2
- If you are using the Restore command at the command line, the database to be restored must be stopped.

❑ Restore an H2 database using the Restore command

___1 Stop the H2 database you want to restore.

___2 At the command line, type

```
java -classpath h2-version.jar org.h2.tools.Restore -file fileName.zip -dir target_DB_directory -db target_DB_name
```

❑ Restore an H2 database using the RUNSCRIPT command in the H2 Web Console

This procedure assumes the backup you are restoring from was created using the SCRIPT command.

- ___1 Place the backup zip file in
X:\LifeCycle\hostname\grid\gridname\applications\GDBC_application_name.
- ___2 Access the H2 Web Console.
- ___3 Enter the following SQL statement (administrator rights are required to execute this command):

```
RUNSCRIPT FROM 'fileName.zip' COMPRESSION ZIP
```

Note: Other switches can be provided. See the H2 reference guide for more information.

❑ Restore an H2 database using the RUNSCRIPT command from the command line

- ___1 Access the H2 Web Console and copy the URL at the top of the left pane. It will have a format similar to the following:

```
jdbc:h2:tcp://172.30.73.165:62882/C:\LifeCycle\www.mycorp.com\grid\myGrid\applications\GDBC\h2db\GDBC_application_name;MODE=MSSQLSERVER
```

- ___2 Open a command line window and, at the command line, type

```
java -classpath h2-version.jar org.h2.tools.RunScript -url DB_JDBC_H2_URL_COPIED_FROM_CONSOLE -user db_user -script fileName.zip -options compression zip
```

Event Hub and Event Analytics Grid Extensions

5

This section explains how to install the Event Hub and Event Analytics grid extensions, and provides background details, definitions, and other related information about the Event Hub.

- ["Installing the Event Hub Grid Extension" on page 47](#)
- ["Installing the Event Analytics Grid Extension" on page 48](#)
- ["Introduction" on page 49](#)
- ["Overview" on page 51](#)
- ["Administration" on page 55](#)
- ["Event Hub and Event Analytics Management Pages" on page 59](#)
- ["Event Analytics Rules" on page 69](#)
- ["Code Examples" on page 73](#)
- ["Event Hub Visualization and Recording UI" on page 75](#)
- ["Purging" on page 80](#)

Installing the Event Hub Grid Extension

Note: The Grid Database Connectivity Grid Extension (GDBC) must be configured on the Grid which the application Event Hub uses. GDBC is mandatory which means Event Hub is dependent on GDBC for backend storage. See ["Installing the Grid Database Connectivity Grid Extension" on page 36](#) for configuration of GDBC.

Use this procedure to install the Event Hub grid extension for versions 2.1.x and later.

☐ Install Event Hub Grid Extension

___1 In LifeCycle Manager, select Actions > Install Product.

-
- ___2 From the list, select the product **Event Hub** <version> with the **Install Event Hub** description.
Click Next.
 - ___3 Select the grid on which the grid extension must be installed.
Click Next.
 - ___4 On the Install window, select the **Event Hub host** and **Event Recorder host**. You can run the recorder node on same host or separate host from the Event hub.
Click Next.
 - ___5 On the Install Event Hub window, specify this information:

Port	Accept the default or specify a unique port.
SSL Port	Accept the default or specify a unique port.
 - ___6 On the Summary window, verify the properties provided.
Click Finish.

Installing the Event Analytics Grid Extension

Use this procedure to install the Event Analytics grid extension.

☐ Install the Event Analytics grid extension

- ___1 In LifeCycle Manager, select Actions > Install Product.
- ___2 From the list, select the product **Event Analytics** version with the **Install Event Analytics** description.
Click Next.
- ___3 On the Install window, select the location for Event Analytics:

Name	Select the grid on which the grid extension should be installed.
-------------	--

Click Next.
- ___4 On the Install Event Analytics window, enter values for the following:

Host	The host for the grid extension.
Analytics Persistence Folder	Browse to a location or set a location relative to the grid application location. Note that this location may need several GB of space. This is where Analytics accesses the rules and stores analytics data.

Click Next.
- ___5 On the Summary window, verify the properties provided.
Click Finish.

Introduction

- ["Event Hub Background" on page 49](#)
- ["What is Event Hub?" on page 49](#)
- ["Highlights of Event Hub" on page 50](#)
- ["What Is Event Analytics?" on page 51](#)

Event Hub Background

Infor provides several applications—including M3, ION Enterprise Search (IES), M3 Enterprise Collaborator (MEC), Infor Process Automation (IPA), and ProcessFlow Integrator (PFI)—that send events to other applications.

Examples:

- M3 database records are sent to IES
- M3 Business Message (MBM) initiator files are sent to MEC
- M3 application messages trigger workflows in IPA/PFI

The event format and communication method is proprietary for each application that receives events:

- Sockets with a proprietary protocol to IES
- SNDSTMF (M3 streamfile socket protocol) + XML to MEC
- Proprietary IPA/PFI client code

This is done point-to-point in a spaghetti solution where the event provider needs to implement different event formats and communication for each event consumer. Each event consumer receives different types of events from the event provider, for example M3 database events to IES, M3 media management events (and more) to MEC, and M3 application messages to IPA/PFI. You cannot, for example, send an M3 database event to MEC.

If you want to send a non-standard event from M3 to IPA/PFI or MEC, you need to add those by custom Java code in M3. At the same time, IES receives many events from M3 without any custom Java code. Events are both sent from an application and received in a generic way. This leads to a hub-and-spoke solution which is exactly what the Event Hub is.

What is Event Hub?

The Event Hub is a generic grid extension for sending events between Infor applications. The Event Hub is a publisher-subscriber framework, that is, an application framework that allows applications to expose historical data to other applications that are interested in receiving this data.

Examples:

- IES receives events on create, update, and delete operations on most M3 database records.
- IPA receives events on create, update, and/or delete operations on some M3 data-base records and also when some batch jobs exit.

Definition of terms

Event	A discrete unit of historical data that an application exposes that may be relevant to other applications.
Publisher	An application that needs to publish events.
Subscriber	An application that needs to receive events that are published by another application.
Subscription	A predicate indicating that a subscriber is to receive a particular event. Subscriptions are given to the Event Hub by the subscribers.
Event Hub	A grid application that receives events from publishers and routes the events to subscribers based on subscriptions.

Highlights of Event Hub

Whenever some kind of business event happens in an application--for example, you create a new customer order, you release an item or print a purchase order, or even when you enter or exit a program or a panel--there should be a possibility to send an event to the Event Hub. To accomplish this you need to use some simple publisher Java classes delivered with the Event Hub. The performance penalty when calling the publisher methods is very low, so this can be implemented without affecting performance for the end user.

Applications that need to receive events also need to use some simple subscriber Java classes. Because the Event Hub is metadata driven by subscriptions (given by the subscribers), the application code of the publisher does not need to be modified for every customer case. This supports "mods-free" applications.

Publishers can dynamically connect to the Event Hub. Subscribers can also dynamically connect to the Event Hub. The Event Hub will persist new event data received while the subscriber is down, if set up to do so. You can, for example, restart an application with a subscriber without losing any event data.

Note: You do not set up the Event Hub. Events are published to the Event Hub through a publisher application. These published events are determined by the subscriptions in the subscriber application.

What Is Event Analytics?

The Event Analytics application allows you to analyze the events processed by the Event Hub. The Event Hub is intentionally kept simple. It guarantees delivery of events to subscribers according to the subscriptions. However, sometimes you may need to analyze the events more thoroughly for more refined routings. A very simple example is to send events to Infor Process Automation only when an M3 item is released, that is, when the M3 MITMAS record is updated from a lower status to status 20.

Event Analytics contains a subscriber and a publisher. In between the subscriber and the publisher, there is a rules engine, Drools Expert by JBoss. Events are received by the subscriber and inserted into the rules engine as facts, and the rules are fired based on matching filter conditions. You create your own rules based on facts such as events, time, or custom-declared fact types. In a rule, you can post received events back to the Event Hub, create and post new events, store data, and so on using standard Java code.

Overview

- ["Events" on page 51](#)
- ["Publisher" on page 52](#)
- ["Subscriber" on page 52](#)
- ["Subscription" on page 52](#)
- ["Persistence" on page 53](#)
- ["Event Hub Schematic Overview" on page 53](#)
- ["Event Analytics Technical Overview" on page 54](#)

Events

An event is something that happens in an application which carries a business value--for example, an item is updated or a batch job has finished. The event data is stored in a "document" and the actual event is the operation on the document. Another way to put it is that the document is the object and the operation is the verb. The event occurs in an application, for example, M3.

An event contains the following data:

- Publisher. For example, M3
- Document name. For example, OOHEAD (order head in M3)
- A list of document elements, each having the following:

- Element name. For example, ORSL (order status)
 - Element value
 - Old element value, if applicable
- Operation on the document: **Create**, **Update**, **Delete**, **Start**, **eXit**, **Fail**, **reQ**uest, or **R**esponse. The operations are hardcoded, but can easily be extended if needed.

Note: The bold and uppercase letters are the operation characters. In subscription strings the operation is given by its operation character.

- Tracking ID
- Sent timestamp

The order of the document elements is maintained through Event Hub and Event Analytics.

Publisher

Applications publishing events need to call a simple publisher. The publisher will "tell" the application if someone wants the event or not, for example, an update of the item master table. Unwanted events are not sent to the Event Hub.

If someone wants the event, then the application needs to create an event containing application specific data. The event is then posted to the Event Hub. The publisher is typically called within the database layer of an application.

Subscriber

Applications subscribing to events need to use some simple subscriber code. The subscriber will receive events from the Event Hub according to the subscriptions given by the subscriber.

Subscription

A subscription contains the following information:

- Publisher. For example, M3
- Document name. For example, OOHEAD
- One or several event operations

A subscription also provides properties for guaranteed event sequence (not implemented yet) and event priority (P1, P2, and P3).

A subscription can be defined by a single string using the following layout (BNF format):

```
<syntax> ::= <publisher> ":" <documentName> [ ":" [ <operation char> ] [ ":" [ ("true" | "false") ] ] [ ":" [ <priority> ] ] ]
```

For example, **M3:OOHEAD:CUD:false:P2**

A subscriber needs to define at least one subscription to receive any events.

Note: All subscriptions of subscribers are merged in the Event Hub and propagated to the publishers. A publisher will not post an unwanted event to the Event Hub.

Persistence

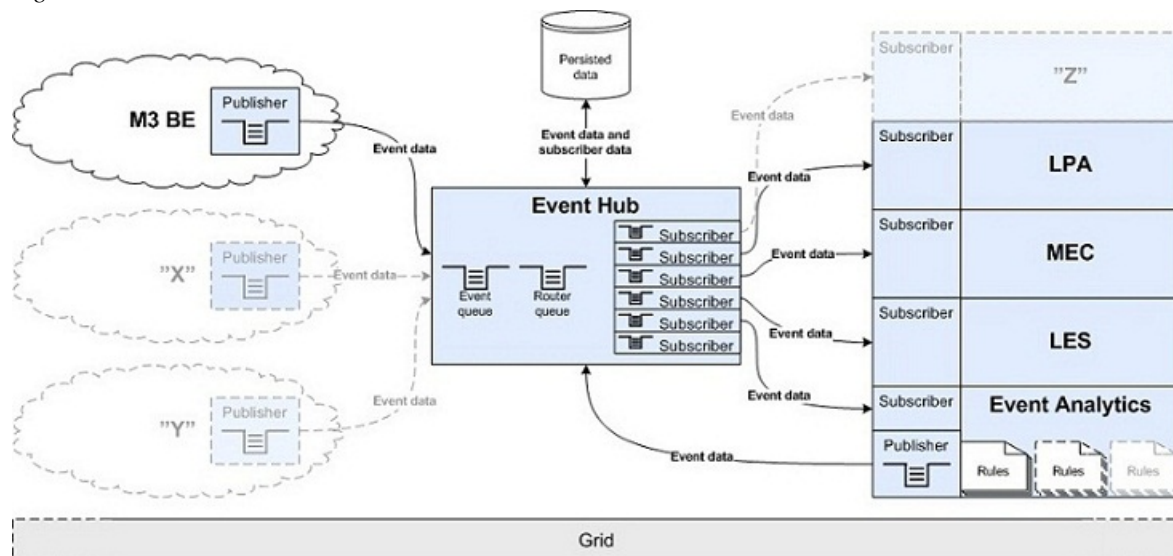
The Event Hub secures event data and event data delivery by persistence. Incoming event data is persisted as well as outgoing event status, that is, if the event has been sent to a subscriber. When an event has been sent to all subscribers, it is removed from the persistence. If a subscriber is busy, the events will be persisted by the Event Hub until they can be processed.

Note: The events should only be persisted for a limited time. The Event Hub is not an archive.

Event Hub Schematic Overview

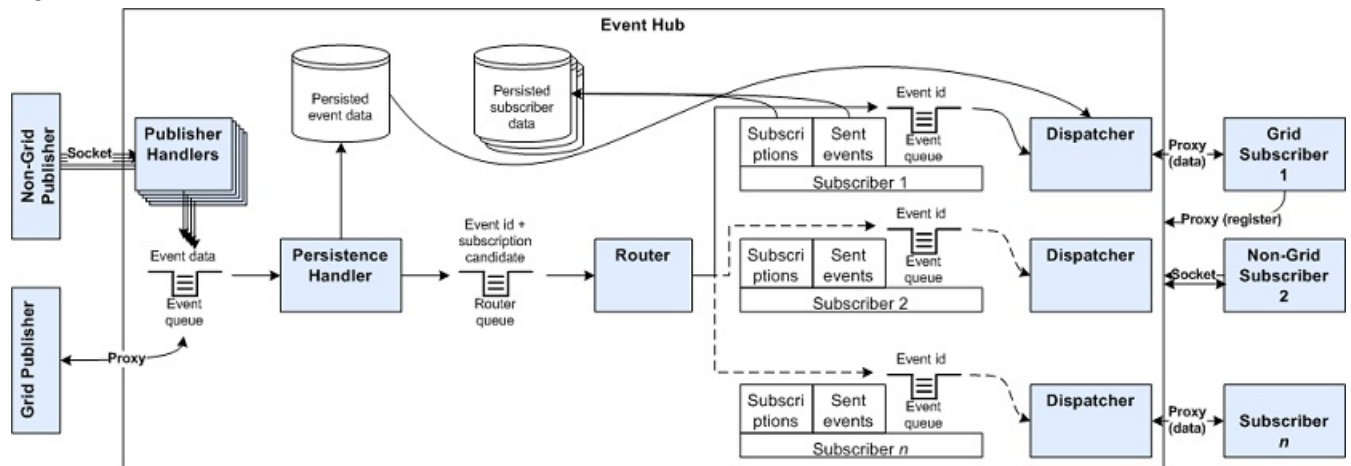
This is a schematic overview of the Event Hub:

Figure 1. Process overview: Event Hub



The following figure is a more detailed overview inside the Event Hub:

Figure 2. Process overview: Event Hub (detailed)



Event Analytics Technical Overview

An event received by the subscriber of Event Analytics is inserted as a fact object (using the class `HubEvent`) into a stateful knowledge base. You can set up several independent stateful sessions in Event Analytics running in separate threads. Then, all rules are fired. Lastly, the inserted fact object is retracted. Session Start, Session Stop and Time (every minute) fact objects are inserted (and rules are fired) automatically.

In the rules, you can analyze the event data and post events using the publisher of Event Analytics, for example, post an event only when the old status is 10 and the new status is 20. You can also create new (meta-)events, for example, count number of new customer orders per customer and day. Stateful sessions' fact objects are persisted automatically. Hence, you can restart Event Analytics without losing counter values.

You can put custom jar files into the "lib" subfolder in the session directory. These are loaded automatically when starting the session.

Subscriptions for Event Analytics are defined as metadata attributes for rules in the following format:

```
@subscription(subscription string)
```

When you (re-)load a session all subscriptions are merged and sent to the Event Hub.

Rule example:

```
rule "OOHEAD_20"
@subscription(M3:OOHEAD:U)
no-loop
when
  event: HubEvent(publisher == "M3", documentName == "OOHEAD", operation == EventOperation.UPDATE,
    elementValues["ORSL"] == "20", elementOldValues["ORSL"] == "10")
then
  event.postEvent("OOHEAD_20");
end
```

You can also declare your own fact types, for example, counters.

Important: You must not store too much data for a session, because all stored fact objects for a session have to be handled as one unit when serializing and deserializing for persistence. If a large amount of data needs to be stored, you should use an external storage method instead.

Administration

- ["Event Hub Grid Application Properties" on page 55](#)
- ["Event Analytics Grid Application Properties" on page 57](#)
- ["Starting and Stopping the Event Hub" on page 57](#)
- ["Starting and Stopping Event Analytics" on page 58](#)
- ["Multiple Nodes for Event Hub" on page 58](#)

Event Hub Grid Application Properties

The following is a list of the properties for the Event Hub grid application:

Property	Type	Default value	Name	Description
Host	String		host	The local address to bind to.
Port	Port		port	The port to use for standard communication.
ID Cache Size	Integer		id-cache-size	The size of the cache for pre-creating message ID.
Bindings Directory	Path		bindings-directory	The file system directory used to store bindings.
Journal Directory	Path		journal-directory	The file system directory used to store journal log.
Large Messages Directory	Path		large-messages-directory	The file system directory used to store large messages.
Paging Directory	Path		paging-directory	The file system directory used to store paging files.
Enable TLS / SSL	Boolean	true	ssl-enabled	

Property	Type	Default value	Name	Description
Only Allow TLS / SSL Connections	Boolean	false	ssl-only	
TLS / SSL Port	Port	61491	ssl-port	The port to use for communication over TLS / SSL
Authenticate Clients	Boolean		ssl-authenticate-clients	Authenticate clients before they can connect.
Key Store Path	Path		key-store-path	
Key Store Password	Password		key-store-password	
Key Password	Password		key-password	
Trust Store Path	Path		trust-store-path	
Trust Store Password	Password		trust-store-password	
Run Server In Backup Mode	Boolean		backup	
Use Shared Store As HA Mode	Boolean		shared-store	
The Multicast Address To Broadcast Connection Data On	String		group-address	
The UDP Port Number Used For Broadcasting	Port	61492	group-port	
The Local Port To Bind The Datagram Socket To	Port		broadcast-port	
Data Access Object Class	String		subscriptions-dao-class-name	

Property	Type	Default value	Name	Description
Driver	String		db-subscriptions-dao-driver	
URL	String		db-subscriptions-dao-url	
User	String		db-subscriptions-dao-user	
Password	Password		db-subscriptions-dao-password	

Event Analytics Grid Application Properties

The following is a list of the properties for the Event Analytics grid application:

Property	Type	Default value	Description
eventhub.analytics.directory	path	analytics	Required. This is the path where the Analytics application accesses the rules and can store analytics data.
eventhub.analytics.persistence.class	string	com.lawson.eventhub.analytics.persistence.FilePersistence	Class for persisting fact objects in Event Analytics. Important: Do not change.
eventhub.analytics.persistence.interval	integer	20	Interval in seconds for persisting fact objects in Event Analytics.

Starting and Stopping the Event Hub

The Event Hub grid application is started and stopped just as any other grid module.

When you start the EventHub module, persisted events are routed to any subscriber that has not already received the event. Thus the state of the Event Hub is preserved. If an event has been received by all subscribers, it will be removed from persistence. Events are continuously persisted. For each subscriber the subscriber name, subscriptions, and internal IDs for sent events are also continuously persisted.

Starting and Stopping Event Analytics

When you start the EventAnalytics module, all enabled sessions start. For each session, all persisted fact objects are inserted into the stateful knowledge session to preserve the state when the session was stopped. No rules are fired when inserting these objects.

Important: The EventAnalytics module will not start if there is an error in a Drools Rules Language (drl) file. Hence, you must not stop EventAnalytics when there is an error in a drl file that is active in a started session.

If you get strange Drools errors when starting EventAnalytics even though the drl files are okay, try to restart EventAnalytics. There is a bug in Drools Expert 5 when running several sessions in parallel.

Multiple Nodes for Event Hub

Publishers

You can run multiple publishers having the same name. A typical example is the M3 publisher. In M3 you run several subsystems in separate JVMs. Each subsystem (JVM) contains its own M3 publisher instance. All M3 publishers can post events to the Event Hub simultaneously.

Subscribers

You can also run multiple subscribers having the same name. However, whereas multiple publisher instances having the same name will post events to the Event Hub simultaneously, the Event Hub will send events to multiple subscribers having the same name one at a time. A subscriber node needs to return true before the next event is sent to another or the same subscriber node. If you have multiple subscribers, an event will be once to each subscriber.

Subscriptions

When a subscriber is registered, its subscriptions are sent to the Event Hub. When several subscriber instances having the same name are registered, all instances will send their respective subscriptions to the Event Hub. This will work if all subscriber instances are set up to use exactly the same subscriptions. However, if the different subscriber instances, all having the same name, use different subscriptions, the subscriptions for the latest registered subscriber will be used for all subscriber instances. This behavior may be changed in future releases of the Event Hub so that there will only be

one "master" subscriber instance (the first). The proper way to use this functionality is to use the same subscriptions for all subscriber instances having the same name.

If you need to alter the subscriptions after the subscribers are registered, you can do so using the `Subscriber.add(Subscription subscription)`, `Subscriber.remove(Subscription subscription)`, or `Subscriber.replaceAll(List<Subscription> subscriptions)` on any subscriber instance. You do not need to do this for every subscriber instance. Be sure to use the updated set of subscriptions for additional subscriber instances though. Remember that the Event Hub only "sees" one subscriber with one set of subscriptions.

Event Hub and Event Analytics Management Pages

This chapter describes the management pages for the Event Hub and Event Analytics applications.

- ["Event Hub Management Pages" on page 59](#)
- ["Event Analytics Management Pages" on page 63](#)

Event Hub Management Pages

The Event Hub grid extension has several management pages:

- Main page
- Subscribers page
- Subscriptions page

Main Page

You access the Main management page for Event Hub by double-clicking on the Event Hub application within a grid in the left pane of the LifeCycle Manager and then clicking on the Manage Application link. You can also access it by accessing the Grid Management Pages, clicking the Applications link, and then clicking the Management Pages link for the Event Hub.

The Main page has two sections: Publishers and Subscribers. These sections display the following content:

Publishers Section

Column	Description
Publisher Name	A list of the names of all registered publishers for the Event Hub.

Column	Description
Status	<p>The status of each publisher.</p> <p>The three possible statuses are:</p> <ul style="list-style-type: none">• OK (a green check mark)• WARNING (a yellow exclamation point)• ERROR (red circle with white X) <p>You can hover the mouse over the status to display a tool tip indicating the current state and any warning or error messages.</p>
Last Connected	The last date and time the publisher connected to the Event Hub.
Total Queued Events	The current number of events in the queue. If this number is not 0, then the subscribers are either inactive, disconnected, or slow, and the cause should be investigated.
Subscribers	This column displays a number that indicates the number of subscribers. The number is a link that you can click to go to the Subscriber page, which shows the subscribers for the selected publisher.

Subscribers Section

Column	Description
Subscriber Name	A list of the names of all registered subscribers for the Event Hub. Each name is a link you can click to go to the Subscriber page for that subscriber.
Status	<p>The status of each subscriber</p> <p>The three possible statuses are:</p> <ul style="list-style-type: none">• OK (a green check mark)• WARNING (a yellow exclamation point)• ERROR (red circle with white X) <p>You can hover the mouse over the status to display a tool tip indicating the current state and any warning or error messages.</p>
Last Connected	The last date and time the subscriber connected to the Event Hub.
Total Queued Events	The current number of events in the queue. If this number is not 0, then the subscriber is either inactive, disconnected, or slow, and the cause should be investigated.

Column	Description
Subscriptions	This column displays a number that indicates the number of subscriptions. The number is a link that you can click to go to the Subscriptions page.
Delete link	To delete a subscriber, click the red X (app-admin role required).

Subscribers Page

You access the Subscribers page by clicking a subscriber name link on the Main page. It shows the subscribers specific to the publisher whose subscriber's link you clicked. The following information is shown:

Column	Description
Subscriber Name	A list of the names of all registered subscribers for the publisher. Each name is a link you can click to go to the Subscriber page for that subscriber.
Status	<p>The status of each subscriber</p> <p>The three possible statuses are:</p> <ul style="list-style-type: none">• OK (a green check mark)• WARNING (a yellow exclamation point)• ERROR (red circle with white X) <p>You can hover the mouse over the status to display a tool tip indicating the current state and any warning or error messages.</p>
Last Connected	The last date and time the subscriber connected to the Event Hub.
Total Queued Events	The current number of events in the queue. If this number is not 0, then the subscriber is either inactive, disconnected, or slow, and the cause should be investigated. the following links are available: - Subscriptions - this link takes you to the subscriptions page for the selected subscriber
Subscriptions	This column displays a number that indicates the number of subscriptions. The number is a link that you can click to go to the Subscriptions page.
Purge Events	Click to purge events for the subscriber (app-admin required).
Delete link	To delete a subscriber, click the red X (app-admin role required).

Subscriber Page

The Subscriber page shows information for a single subscriber. You access this page by clicking the name of a subscriber on the Subscribers page.

Column	Description
Publisher Name	The name of the publisher for this subscriber
Status	<p>The status of the subscriber</p> <p>The three possible statuses are:</p> <ul style="list-style-type: none">• OK (a green check mark)• WARNING (a yellow exclamation point)• ERROR (red circle with white X) <p>You can hover the mouse over the status to display a tool time indicating the current state and any warning or error messages.</p>
Queued Events	The current number of events in the queue. If this number is not 0, then the subscribers are either inactive, disconnected, or slow, and the cause should be investigated.
Total Enqueued Events	The number of events sent since the last restart.
Purge Events	Click to purge all undelivered events from publisher for the subscriber (app-admin required).
Subscriptions	This column displays a number that indicates the number of subscriptions. The number is a link that you can click to go to the Subscriptions page, which shows the subscriptions for the this subscriber.

Subscription Page

You access the Subscription page from the Subscriptions link on the Main page. It shows the subscriptions specific to the subscriber for which the link was selected. The following information is shown:

Column	Description
Publisher Name	The publisher for which this subscription is registered.
Document	The name of the event document, for example, MITMAS.
Operation(s)	The operation for the subscription, for example, CUD.
Purge Events	Click to purge all undelivered events matching the document and operation for this subscriber.

Column	Description
Delete link	To delete all subscriptions and all un-delivered events, click the red X (app-admin role required).

Event Analytics Management Pages

The Event Analytics grid extension has several management pages:

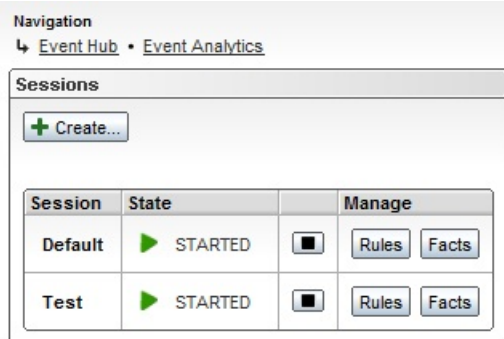
- Main page
- Subscriptions page
- Session Rules page
- Session Facts page

Main Page

The Main management page for Event Analytics contains the following sections:

- Sessions - create, start, stop, manage, and remove sessions
- Menu - link to Subscriptions page for Event Analytics

Figure 3. Screen capture: Event Analytics main page



Subscriptions

[View Subscriptions](#)

When starting Event Analytics for the first time a session named "Default" is automatically created. To create a new session, press + Create... and enter a name for the session. The name can only contain letters, numeric characters, hyphen, and the underscore character. The name must be unique (not case sensitive) and be at least one character long. A directory with the session name is automatically created in the analytics home directory (as defined by the application property `eventhub.analytics.directory`).

Press the start ("play") button to start the session and the stop button to stop the session.

Figure 4. Screen capture: Start session



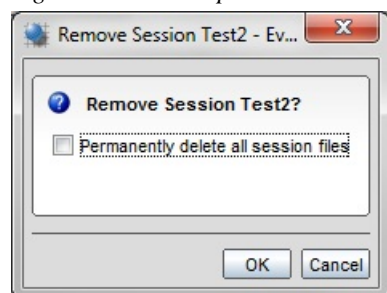
If there is an error in a Drools Rules Language (drl) file for the session, the session cannot be started and gets an error state. You can use the ERRORS link to view the errors.

Figure 5. Screen capture: Session errors



To remove a session, the session must be stopped. When pressing the X (remove) button you get a confirmation dialog with an option to permanently delete all session files, that is, the complete session directory. If you do not select the checkbox, the session directory and its contents will not be deleted, only the session property will be removed. If desired you can create a new session with the same name at a later stage to restore the session set up, including persisted fact objects for the session. If the checkbox is selected, the session directory and all its files and subdirectories will be permanently deleted.

Figure 6. Screen capture: Remove Session confirmation dialog box



Press the Rules button to manage Drools Rules Language (drl) files for the session in the Session Rules page.

Press the Facts button to view fact objects for the session in real time in the Session Facts page.


Event Analytics Subscription Page

In the Event Analytics Subscriptions page you can view all subscriptions for the Event Analytics subscriber. Subscriptions are defined separately for every session and merged into the subscriptions. These subscriptions are sent to the Event Hub, that does not know anything about Event Analytics sessions. Event Analytics is just another subscriber to the Event Hub.

The Event Analytics Subscriptions page shows the Publisher, Document Name, Operations, and Priority (the subscriber is always "EventAnalytics"). You can filter the table on all columns in the same way as in the Event Hub Subscriptions page (no publisher view).

Figure 7. Screen capture: Event Analytics Subscriptions page

Navigation
↳ [Event Hub](#) • [Event Analytics](#) • [Subscriptions](#)

Subscriptions				
Publisher <small>Δ</small>	Document Name <small>Δ</small>	Operations <small>Δ</small>	Priority <small>Δ</small>	
				
M3	MITMAS	U	P2	
M3	MITMAS_34	U	P2	
M3	OOHEAD	U	P1	
M3	MITMAS_33	UD	P1	
M3	MITMAS_32	U	P1	
M3	MITMAS_31	U	P2	
M3	MITMAS_35	U	P2	

Number of subscriptions: 7

Session Rules Page

In the Session Rules page you can create, upload, edit, and remove resources for a session. A resource is a Drools Rules Language (drl) file.

Figure 8. Screen capture: Session Test Rules page for a started session

Navigation

↳ Event Hub • Event Analytics • Session Test Rules

Session: Test

State: STARTED

Drools Rule Language Files

+ Create...

Active	Name	Manage
<input checked="" type="checkbox"/>	Demo	<div>EditUpload</div>
<input checked="" type="checkbox"/>	Test1	<div>EditUpload</div>
<input checked="" type="checkbox"/>	Test2	<div>EditUpload</div>

Rules

Reload

Package	Name
com.lawson.eventhub.analytics.drools	Subscriptions_Demo
com.lawson.eventhub.analytics.drools	MITMAS_20
com.lawson.eventhub.analytics.drools	InsertEventCounterTest1
com.lawson.eventhub.analytics.drools	MITMAS_31Test1
com.lawson.eventhub.analytics.drools	StartTest
com.lawson.eventhub.analytics.drools	TimeTest
com.lawson.eventhub.analytics.drools	StopTest
com.lawson.eventhub.analytics.drools	InsertEventCounterTest2
com.lawson.eventhub.analytics.drools	MITMAS_31Test2

Subscriptions

Publisher	Document Name	Operations	Priority	
M3	MITMAS_34	U	P2	
M3	MITMAS	U	P2	
M3	MITMAS_33	UD	P1	
M3	MITMAS_32	U	P1	
M3	MITMAS_31	U	P2	
M3	MITMAS_35	U	P2	

Number of subscriptions: 6

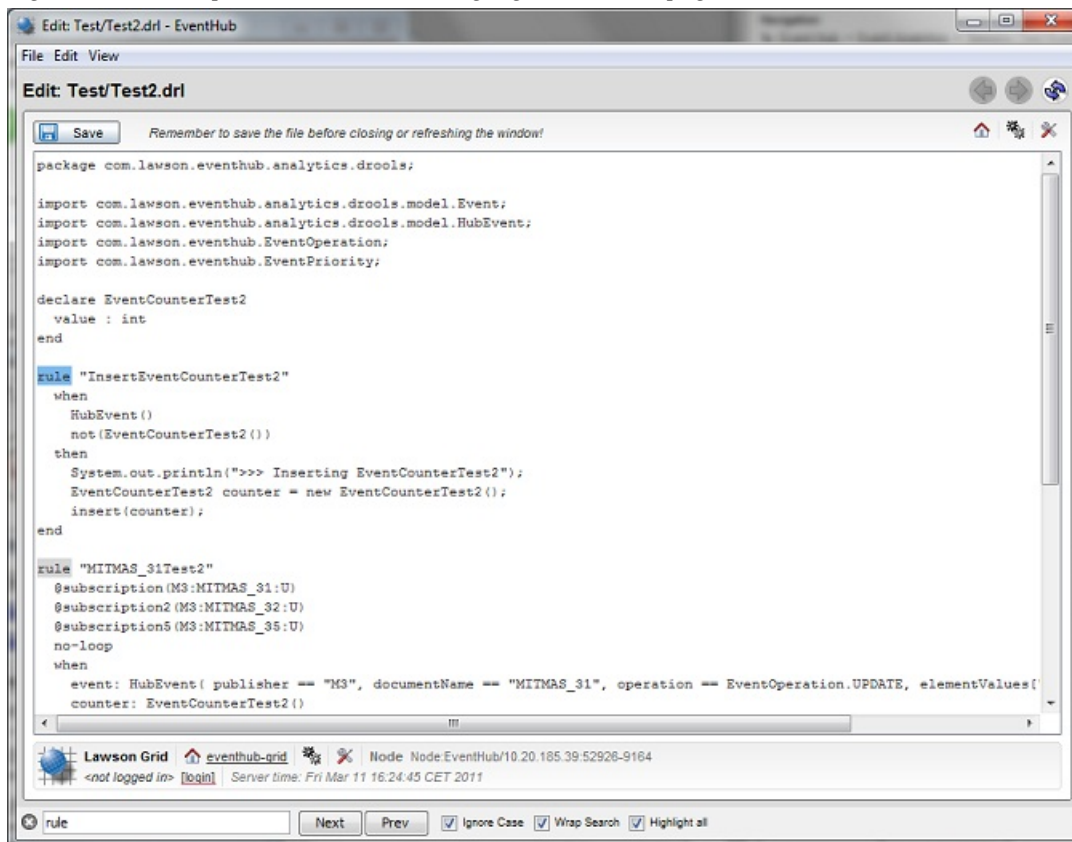
To create a new resource, press + Create... and enter a name for the resource. The name can only contain letters, numeric characters, hyphen, and the underscore character. The name must be unique (not case sensitive) within the session and be at least one character long. A demo drl file with the resource name is automatically created in the session directory. If the drl file already exists, the demo drl file will not be created.

You can edit the drl file in a simple editor by pressing the Edit button. Press Ctrl+F in the editor window to find a string in the file.

Important: Ctrl+S will not save the drl file, you must press the Save button (in upper left corner) to save any changes you have done in the editor. If you close the window or refresh the page, all changes will also be lost.

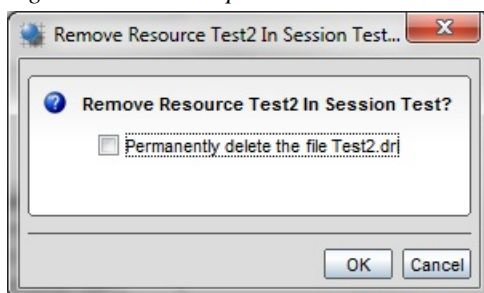
Tip: Open a drl file in the editor page and save it to create Carriage Return / Linefeeds (\r\n) and get correct line numbers in knowledge builder error messages.

Figure 9. Screen capture: Drools Rules Language (drl) editor page



You can upload a drl file by pressing the Upload button. The existing drl file will be replaced by the uploaded file. Press the active checkbox icon to enable or disable the resource.

Figure 10. Screen capture: Remove Resource confirmation dialog box



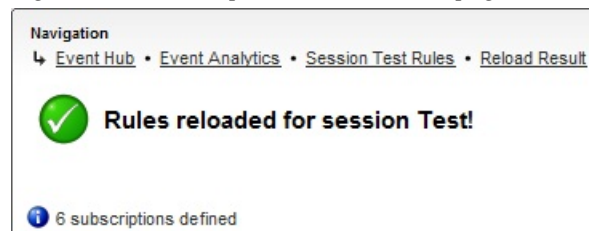
If the session is started you also see the sections Rules and Subscriptions. In the Rules section you can view the package and name for all rules for the session. You can reload the session in runtime by pressing the Reload button. No events are lost, a new knowledge session is created with the same

state as the old one and the old session is replaced. If Event Analytics receives events from the Event Hub while reloading a session, some events will be handled by the old knowledge session. If there is an error in a drl file, the session cannot be reloaded and the old knowledge session will continue to run. You will get to a Reload Result page where the Drools knowledge builder errors are shown. You can also use the ERRORS link to view the errors at a later stage.

Figure 11. Screen capture: Reload Result page with errors



Figure 12. Screen capture: Reload Result page without errors



Note: When creating a session the directory "lib" is created in the session directory. You can put your own jar files into the lib directory and they will be loaded by a custom class loader when starting or reloading a session. If you store an object of a class, defined in a jar file, in the knowledge session you can never remove that class since the persisted object then cannot be deserialized from persistence (since the class is no longer in the classpath).

In the Subscriptions section in the Session Rules page you can view all subscriptions for the session. Subscriptions are defined separately for every resource (drl file) and merged into the subscriptions. These subscriptions are in turn merged into subscriptions for the Event Analytics subscriber as found in the Event Analytics Subscriptions page.

The Session Rules Subscriptions show the Publisher, Document Name, Operations, and Priority. You can filter the table on all columns in the same way as in the Event Analytics Subscriptions page.

Session Facts Page

In the Session Facts page you can view inserted fact objects for a started session in real time. This page shows the following data:

- Type - "Java" for Java objects or "Declared" for declared fact objects.

- Class name - Java class name or the name of the declared fact type.
- Object - A string representation of the object as given by the method toString(). If the type is Declared a built-in toString() method is used.

By refreshing this page you can, for example, watch counter values in real time.

You can filter the table on all columns. If the Reload Page checkbox is selected, you will reload the fact objects for the session when you filter the table. If the Reload Page checkbox is not selected, you can filter the table without reloading the fact objects. Hence, you can filter data on a specific snapshot.

Figure 13. Screen capture: Session Test Facts page

Navigation
Event Hub • Event Analytics • Session Test Facts

Session: Test
State: ▶ STARTED

Snapshot 2011-03-11 16:42:23 ☒ Reload Page

Fact Objects		
Type	Class Name	Object
Declared	EventCounterTest2	com.lawson.eventhub.analytics.drools.EventCounterTest2: value=80329
Declared	EventCounterTest1	com.lawson.eventhub.analytics.drools.EventCounterTest1: value=80329

Number of fact objects: 2

Event Analytics Rules

This section covers the available facts, rule metadata for subscriptions, and some utilities available in Event Analytics.

For documentation on the Drools Rules Language, go to <http://www.jboss.org/drools/drools-expert.html>.

- "Facts" on page 69
- "Subscriptions" on page 71
- "Nonserializable" on page 72
- "Utility Methods" on page 73

Facts

Facts are plain Java classes which rely on the Java Bean pattern. They are asserted into the working memory of the Drools engine. One or more rules may be true and will then be scheduled for execution by the agenda.

HubEvent

When an event is received by the Event Analytics subscriber, it is inserted into the stateful knowledge session as a HubEvent fact. A HubEvent fact cannot be changed in the rules (it is immutable) because several rules may be triggered by the same fact.

After the rules are fired, the HubEvent fact is automatically retracted from working memory by Event Analytics.

There is a convenience method `postEvent()` to post a HubEvent back to the Event Hub albeit with another document name.

The following is an example of a simple rule triggered by a HubEvent fact:

```
rule "MITMAS_20"
    no-loop
    when
        event: HubEvent(publisher == "M3", documentName == "MITMAS", operation ==
EventOperation.UPDATE, elementValues["STAT"] == "20", elementOldValues["STAT"] == "10")
    then
        event.postEvent("MITMAS_20");
    end
```

Event

When you need to create a new event in a rule or when you want to modify a received HubEvent fact, you can use the class `Event`. There are convenience constructors to clone a HubEvent fact into an `Event` and also to clone another `Event`.

The following is an example of a simple rule code to post a new event:

```
Event newEvent = new Event("MyEvent", EventOperation.CREATE);
newEvent.setTrackingId(myTrackingId);
newEvent.addElement("MyElement1", "MyElementValue1");
newEvent.addElement("MyElement2", "MyElementValue2");
newEvent.postEvent();
```

Start

A session `Start` fact is inserted into the stateful knowledge session when the Drools session starts and then all rules are fired. Then, the inserted session `Start` fact is retracted from the stateful knowledge session. A `Start` instance is immutable and cannot be changed.

The following is an example of a simple rule that logs when the session is started:

```
rule "Start"
    when
        start : Start()
    then
        System.out.println("Session " + start.getSessionName() + " started: " + start.toString());
    end
```

Stop

A session `Stop` fact is inserted into the stateful knowledge session when the Drools session stops and then all rules are fired. Then, the inserted session `Stop` fact is retracted from the stateful knowledge session. A `Stop` instance is immutable and cannot be changed.

The following is example of a simple rule that logs when the session is stopped:

```
rule "Stop"
  when
    stop : Stop()
  then
    System.out.println("Session " + stop.getSessionName() + " stopped: " + stop.toString());
  end
```

Time

A Time fact is inserted into the stateful knowledge session every minute and then all rules are fired. Then, the inserted Time fact is retracted from the stateful knowledge session. A Time instance is immutable and cannot be changed.

The following are examples of some simple rules that log birthday greetings:

```
rule "AEBirthday"
  when
    time : Time(month == 3, day == 14, hour == 9, minute == 0)
  then
    System.out.println("Happy birthday Albert!");
  end

rule "ALBirthday"
  when
    time : Time(month == 12, day == 10, hour == 9, minute == 0)
  then
    System.out.println("Happy birthday Ada!");
  end
```

Subscriptions

Subscriptions for Event Analytics are defined as metadata attributes for rules in this format:

```
@subscription(subscription string)
```

Note that the metadata attribute name ("subscription") must be unique within a rule. If you need to specify more than one subscription for a rule, you can add a suffix to the attribute name. All metadata attributes with a name starting with "subscription" are considered to contain subscription strings.

```
@subscription1(subscription string)
@subscription2(subscription string)
@subscription3(subscription string)
```

Another option is to use one metadata attribute having several subscription strings separated by the semicolon character (";") as metadata value.

```
@subscription(subscription string; subscription string; subscription string)
```

This metadata can only exist inside a rule. However several rules may of course need the same subscription. While it works to duplicate the subscriptions (since they are merged), a more organized approach could be to create a "dummy" rule that only contains subscription metadata attributes.

The following is an example of some subscription rules:

```
rule "Subscriptions_Item"
  @subscription1(M3:MITMAS:CUD)
  @subscription2(M3:MITBAL:CUD)
  then
end

rule "Subscriptions_Order"
  @subscription(M3:OOHEAD:CUD;M3:OOLINE:CUD)
  then
end
```

Nonserializable

All fact objects that are inserted into a stateful session using the insert(Object) method are serialized to a file for persistence. Declared fact objects are converted into objects of an internal class (DeclaredFact) before serialization. Other Java classes need to implement the Java interface Externalizable or Serializable, otherwise the objects cannot be serialized and you will get errors in the log. If you do not want to serialize, that is, persist objects of a specific Java class, you can define the class name as metadata attribute for rules in this format:

```
@nonserializable(class name)
```

Note: The class name must include the package, for example, "com.lawson.mypackage.MyClass". If you omit the package from the class name the package for the rule will be used.

The metadata attribute name ("nonserializable") must be unique within a rule. If you need to specify more than one nonserializable Java class name for a rule, you can add a suffix to the attribute name. All metadata attributes with a name starting with "nonserializable" are considered to contain nonserializable class names.

```
@nonserializable1(class name)
@nonserializable2(class name)
@nonserializable3(class name)
```

Another option is to use one metadata attribute having several class names separated by the semicolon character (";") as metadata value.

```
@nonserializable(class name;class name;class name)
```

This metadata can only exist inside a rule. You can of course create a "dummy" rule that only contains nonserializable metadata attributes.

Example of some nonserializable rules:

```
rule "Nonserializable_Objects1"
  @nonserializable1(com.lawson.mypackage.MyClass1)
  @nonserializable2(com.lawson.mypackage.MyClass2)
  then
end

rule "Nonserializable_Objects2"
  @nonserializable(com.lawson.mypackage.MyClass3;MyClassInThisDRLFile)
  then
end
```


Note: Objects of classes that are instances of the class `com.lawson.eventhub.analytics.drools.model.AbstractTime`, that is, `Time`, `Start`, and `Stop` will not be persisted.

Utility Methods

Session

The class `Session` contains utility methods to be used in Drools rules to get information about current session. You can get the name of the session, start time, and a list of the subscriptions of a session.

Note: Use the correct package for `Session`: `com.lawson.eventhub.analytics.drools.model`.

Example of a simple rule code that logs all session info:

```
System.out.println("Session info: " + Session.getString());
```

Util

The class `Util` contains some utility methods to be used in Drools rules, for example, left trim, right trim, and a time stamp formatter.

Code Examples

- ["Demo drl File" on page 73](#)
- ["Item Update Counter Rule" on page 74](#)

Demo drl File

The following is the demo drl file generated when creating a new session resource in Event Analytics.

```
package com.lawson.eventhub.analytics.drools;

import com.lawson.eventhub.analytics.drools.model.Event;
import com.lawson.eventhub.analytics.drools.model.HubEvent;
import com.lawson.eventhub.analytics.drools.model.Session;
import com.lawson.eventhub.analytics.drools.model.Start;
import com.lawson.eventhub.analytics.drools.model.Stop;
import com.lawson.eventhub.analytics.drools.model.Time;
import com.lawson.eventhub.analytics.drools.model.Util;
import com.lawson.eventhub.EventOperation;
import com.lawson.eventhub.EventPriority;
```

```
rule "Subscriptions_Demo"
  @subscription1(M3:MITMAS:U)
  then
  end

rule "MITMAS_20_Demo"
  no-loop
  when
    event: HubEvent(publisher == "M3", documentName == "MITMAS", operation == EventOperation.UPDATE,
    elementValues["STAT"] == "20")
  then
    event.postEvent("MITMAS_20");
  end

rule "Start_Demo"
  when
    start : Start()
  then
    System.out.println("Demo: Session " + start.getSessionName() + " started: " + start.toString());

    System.out.println("Demo: Session info: " + Session.getString());
  end

rule "Time_Demo"
  when
    time : Time()
  // time : Time(sessionName == "Test", year == 2010, month == 8, day == 24, weekNumber == 34,
  // dayOfWeek == Calendar.TUESDAY, hour == 10, minute >= 55 )
  then
    System.out.println("Demo: Session " + time.getSessionName() + " got time: " + time.toString());
  end

rule "Stop_Demo"
  when
    stop : Stop()
  then
    System.out.println("Demo: Session " + stop.getSessionName() + " stopped: " + stop.toString());
  end
```

Item Update Counter Rule

The item update counter rule is a rule that counts the number of updates of any M3 item. For every 10th update, an event "10ItemUpdates" is posted to the Event Hub with the current counter value. The actual counter (EventCounterTest) is a declared fact type.

```
package com.lawson.eventhub.analytics.drools;

import com.lawson.eventhub.analytics.drools.model.Event;
import com.lawson.eventhub.analytics.drools.model.HubEvent;
import com.lawson.eventhub.EventOperation;

declare EventCounterTest
  value : int
end

rule "Insert_EventCounterTest"
  when
    HubEvent()
    not(EventCounterTest())
  then
    EventCounterTest counter = new EventCounterTest();
    insert(counter);
  end

rule "MITMAS_Update_Counter"
```

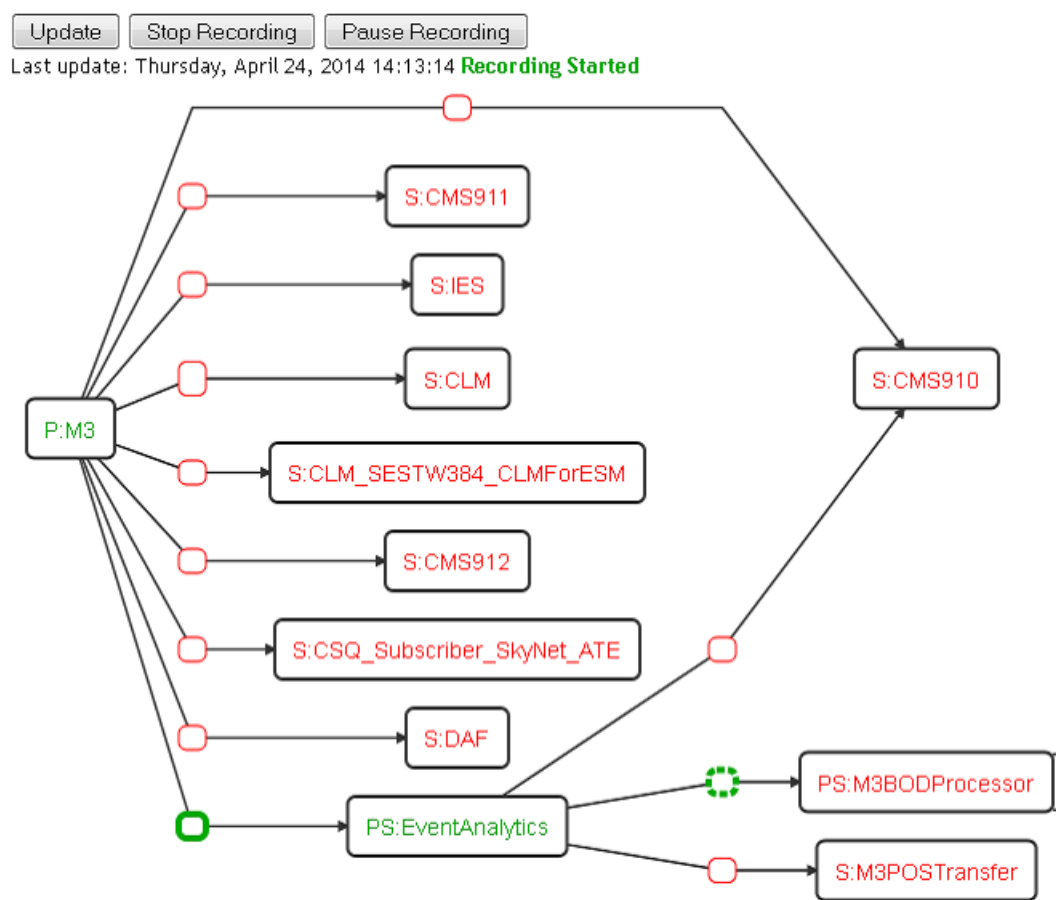
```
@subscription(M3:MITMAS:U)
no-loop
when
  event: HubEvent(publisher == "M3", documentName == "MITMAS", operation == EventOperation.UPDATE)

  counter: EventCounterTest()
then
  counter.setValue(counter.getValue() + 1);
  if (counter.getValue() % 10 == 0) {
    // Post counter event
    Event event2 = new Event();
    event2.setDocumentName("10ItemUpdates");
    event2.setOperation(EventOperation.CREATE);
    event2.setTrackingId(event.getTrackingId());
    event2.addElement("TotalEvents", String.valueOf(counter.getValue()));
    event2.postEvent();
  }
end
```

Event Hub Visualization and Recording UI

Introduction

Event Hub visualization and recording UI is a browser-based tool that provides a graphical overview of the publisher and subscriber topology. The UI provides access to event recording functionality. To access the visualization UI click the "Visualization" link from the main Event Hub management page. This diagram shows the view of the Event Hub topology visualization and recording interface:



Topology visualization provides a graphical overview of the data flow between the publishers and subscribers that are connected to Event Hub and buttons for updating the view or controlling the event recording process.

Topology Visualization

The topology visualization contains a graph that consists of:

- Larger publisher/subscriber nodes with the publisher or subscriber names.
- Arrows that show the data flow between a publisher and a subscriber.
- Connection nodes marking the status of the data flow.

The larger topology nodes containing the names are either subscribers or publishers, for example; applications containing either subscriber or publisher functionality.

The larger topology nodes:

- Publishers are marked with a **P:** prefix.
- Subscribers are marked with an **S:** prefix.

- Certain applications, for example Event Analytics and M3BODProcessor, act both as a publisher and as a subscriber. These are marked with a **PS:** prefix.

The status of the publishers and subscribers is marked with a color.

- The red color marks that the publisher or subscriber is not connected to Event Hub.
- The green color marks that everything is OK with a publisher or a subscriber.
- The yellow color marks that a publisher or a subscriber is paging.

When you click a subscriber or a publisher node, a window containing additional status information is displayed:

- **Subscriber status:** OK, disconnected, paging.
- **Publisher status:** OK, disconnected, paging.
- **Subscriber queued:** Number of events in the queue.
- **Publisher queued:** Number of events in the queue.
- **Subscriber last seen:** The timestamp when the subscriber was last connected to Event Hub.
- **Publisher last seen:** The timestamp when the publisher was last connected to Event Hub.

In addition, detailed error messages are displayed at the bottom of the window.

The arrows that connect subscribers and publishers have a smaller connection node, the color of which marks the status of the data flow between a publisher and a subscriber.

You can click the connection node to see which events are transmitted through the particular connection.

The window provides this information:

- **Document:** The name of the published event.
- **Operations:** Any combination of the operations supported by Event Hub, for example Create, Update. A tool-tip containing the detailed operation names is available when you move the pointer over the operations list.
- **Rule:** A rule name for a rule subscribing for a particular document is available for Event Analytics connections.

Right-click the connection node to access a context menu. The available options are described in "[Event Recording](#)" on page 77.

Event Recording

Event Hub provides a possibility for recording ongoing event traffic in a live environment. The flow of events is saved by the Event Hub. You can review the saved traffic from the Event Hub management interface in Grid.

☐ Start the recording

- ___1 Right-click the connection node and select Change recording paths. A dialog box containing the available event types is displayed.
- ___2 Select the check boxes for the event types to use and click OK. The connection node is marked with a dotted line. This marks that the changes to the recording path are not submitted to the Event Hub. You can add additional recording paths from other nodes. To clear all recording paths select the Clear recording paths option.
- ___3 Click Start Recording. A parameters dialog box is displayed.
- ___4 Specify this information:
 - **Max running time for recording time (min):** The maximum running time for recording.
 - **Max recording size (MB):** The maximum size of the recorded data.If any of these limits is reached, recording is paused automatically.
- ___5 Click OK to start recording.

The connection nodes which had a dotted line become solid. The changes to the recording paths are submitted to Event Hub.

When you modify the recording paths during recording, you must stop and start the recording.

During the recording process you can click Pause Recording to temporarily pause the recording. Examine the recorded events during this time in the main Event Hub management interface. Click Resume Recording to continue recording events.

Click Stop Recording to finish recording events.

Note: When you stop recording all recorded events are discarded.

Viewing Recorded Data

To access active recording sessions, click the Recording Sessions link from the main Event Hub management page.

On the "Recording Sessions" page, you can pause, resume, and stop recordings. To view or search the raw event traffic captured by a recording session, click the name of the session in the session's table.

You can view recorded events whether a session is started or paused. However, viewing live data while a session is started causes a large performance penalty in the server side recording mechanism. Therefore this should generally be avoided when recording high throughput event flows.

The recorded events are displayed in a chronological order based on when the Event Hub received the events. The oldest recorded event is displayed first. If desired, you can slice the event view to only show the events recorded during a certain time period. Specify a start and stop time in the yyyy-mm-dd hh:mm:ss,SSS format, where SSS is milliseconds, and click Search.

Search Query Syntax

In addition to restricting output to a fixed time period, you can search the recorded events using Boolean query expressions. Certain predefined fields are always indexed for each and every event. These predefined fields can always be referenced in search queries. In addition to these predefined fields, all the elements in events are also indexed and can be searched. You can combine both, manually specified search queries and the above-mentioned time period restrictions, to further filter the results.

To search using field names or element names, specify a query expression in this format:

```
<name>=<value>
```

To match the previous value of an element, add the "_old" suffix to the element name:

```
<name>_old=<value>
```

If a value contains whitespaces or colons, you must put the whole name/value pair between double quotation marks:

```
"<name>=this value contains spaces"
```

```
"<name>=abc:xyz"
```

If a value contains double quotation marks, you must use backslashes to manually 'escape' the quotation mark characters:

```
"<name>=this value contains the \" character"
```

To create arbitrarily nested Boolean query expressions, use AND, OR, NOT, and parentheses:

```
<name_a>=x AND (<name_b>=y OR <name_b>=z)
```

```
<name_a>=x NOT <name_b>=y
```

Note: All field names, elements, names, and values are case-sensitive and only complete matches are supported. You cannot use wildcards.

Predefined fields

This table shows the predefined fields:

Predefined field	Description
from	The name of the publisher that posted the event.
to	The name of the subscriber that received the event.
serverTime	The time the Event Hub server received the event.
publisher	The name of the publisher as stated in the event itself.
document	The document name of the event.
operation	The operation of the event.

Predefined field	Description
clientTime	The time the publisher posted the event.
trackingId	The tracking id of the event.
duplicateId	A unique identifier attached to the event when transferring between a publisher and a subscriber.
serverId	A server internal id attached to the event, unique until the server is restarted.

Example

To search for all item master create and update events with status 20 (released) sent from M3 to Event Analytics, specify this expression:

```
from=M3 AND to=EventAnalytics AND document=MITMAS AND (operation=CREATE OR operation=UPDATE) AND STAT=20
```

Event Recorder Node

This node is responsible for recording, persisting, and later providing the actual data for viewing/searching. It is automatically started, if not already running, when a recording session is started, resumed, or viewed/searched. If desired, you can manually start the Event Recorder node ahead of time. It must be running at all times during an ongoing recording session. Once the recording session is paused, you can manually stop the Event Recorder node, if desired. When the last recording session is stopped, the Event Recorder node is automatically stopped.

Purging

Purging provides a mechanism to clear unwanted queues and queued events of a disconnected subscriber. These events take up disk space which can be utilized otherwise.

An example of when purging can be applied.

Two subscribers EventAnalytics and MEC are subscribed to a publisher called M3. MEC has registered to EventHub but is unavailable for a long time. Because MEC is still registered, events are persisted by EventHub and keep queuing up on the disk. When MEC returns, the queued up data is unwanted. Therefore, the user may want to clean up this data. A purge operation can be used in this scenario.

This kind of situation can arise in a test environment where test subscribers are registered and do not return or are intermittently available. If you are sure the subscriber never returns there is an option to delete the subscriber.

These variances of purging are supported in EventHub:

- Manual purging
- Automatic purging

Note: The default behavior is no purging.

Manual purging





The manual purging functionality allows one time purging of queued events. You can start this purging on an ad hoc basis.

To initiate a manual purge request:






- 1 Go to the main EventHub management page subscriber table.
- 2 Click the subscriber name link.
- 3 Click the purge icon next to the publisher for which you want to initiate this request.

A Purging operation is initiated for the above selected subscriber-publisher combination. All undelivered events to that subscriber from this specific publisher are removed.

In this example click the first icon to remove all undelivered events from publisher M3 to subscriber MEC. See this screenshot:

MEC					
Publisher Name	Status	Queued Events	Total Enqueued Events	Purge Events	Subscriptions
M3		3988150	3989843		<u>1</u>
Pub		0	0		<u>1</u>

You can also start with a publisher and choose to remove all queued events and queues for a publisher subscriber combination. See this screenshot:

M3					
Subscriber Name	Status	Last Registered	Total Queued Events	Subscriptions	Purge Events
EventAnalytics		2014-07-01 14:43:06,851	0	<u>34</u>	
MEC		2014-07-02 00:37:28,759	4434085	<u>1</u>	 

You can purge events selectively corresponding to a particular subscription. In the second example clicking the purge event icon on the first row removes all undelivered events matching subscription **M3:CCURRA:Q:false:P2** for subscriber EventAnalytics. See this screenshot:

EventAnalytics			
Publisher Name	Document	Operation(s)	Purge Events
M3	CCURRA	Q	↓
M3	CIDMAS	Q	↓
M3	CMNDIV	Q	↓
M3	CMNUSR	Q	↓
M3	CSYPER	Q	↓
M3	CSYSTS	Q	↓
M3	CSYTAB	Q	↓
M3	DCONSI	Q	↓
M3	FBAKEY	Q	↓
M3	FBUDET	Q	↓
M3	FCHACC	Q	↓
M3	FFASMA	Q	↓
M3	FGLEDG	Q	↓
M3	FPLEDG	Q	↓
M3	FSLEDG	Q	↓
M3	MHDISH	Q	↓
M3	MHEXRH	Q	↓

If there are many events to remove the purge operation can take some time.

Automatic purging

Automated purging functionality allows configurable time period based purging of subscribers. For example, if x days/ a hour and b minutes passed since the last time a subscriber connected then initiate a delete queues and queued events. In this way the system is self-cleansing the test environment at a regular interval if the subscribers remain disconnected.

To schedule an automatic purge for a subscriber:

- ___1 Go to the main EventHub management page subscribers table.
- ___2 Click Add for the specific subscriber.
- ___3 Specify the interval, in hour and minutes, to run the auto purge job. See this screenshot:

Subscribers					
Subscriber Name	Status	Last Seen	Total Queued Events	Auto Purge	Subscriptions
EventAnalytics	✓	2014-07-01 14:43:06	851 0	+ Add...	34
MEC	✗	2014-07-02 00:37:28	759 492	+ Add...	1 ✗

To run the auto purge every 24 hour specify this information:

Edit Auto Purge

Schedule an automatic purge job for subscriber MEC

Enter an interval between automatic deletion of events for a disconnected subscriber.

Hours

24

Minutes

0

OK

Remove

Cancel

Important: This functionality is used for cleanup unwanted events. Do not use this for production data. It can cause permanent loss of undelivered events to the subscribers.

M3 BE Event Hub Publisher



This appendix lists the event types that can be published by M3 BE Grid Foundation. To enable this functionality, you have to enable Event Hub in the M3 BE properties. Remember that it is the subscribers that define, through the subscriptions, which events will be published by M3 BE — there is no configuration available in M3 BE for this.

The publisher name for M3 BE events is hardcoded to "M3". Each M3 BE subsystem hosts its own publisher instance.

Each table below represents an event type.

<M3 Table>

An example of an M3 Table is MITMAS.

Operation	Elements	Example*
C (Create) When a new record is created	keyValue, startProgram, currentProgram, [Program properties], [Table columns]	<pre>M3:MITMAS:C startProgram=MMS001; currentProgram=MITMASPI; startTimeMillis=1327331743637; owner=M3User; startTime=2012-01-23 16:15:43; jobUUID=533d5c25cecb43b884707ef1bafc4bd5; sessionId=11.22.3.444:63547_0-0; CWUN=PCE; STAT=20; ... ITNO=I012345 ; ... CONO=330; LMDT=20120123; CONC=0; SCGR=0.0; keyValue=MMCONO,330,MMITNO,I012345+++++++; environment=M3BEEEnv; version=1410; application=M3;</pre>

Operation	Elements	Example*
U (Update) When a record is updated	keyValue, startProgram, currentProgram, [Program properties], [Table columns (with old values if they are present)]	<pre> M3:MITMAS:U startProgram=MMS001; currentProgram=MITMASPI; startTimeMillis=1327331743637; owner=M3User; startTime=2012-01-23 16:15:43; jobUUID=533d5c25cecb43b884707ef1bafc4bd5; sessionId=11.22.3.444:63547_0-0; CWUN=PCE(PCE); STAT=20(20); ... ITNO=I012345 (I012345); ... CONO=330(330); LMDT=20120123(20120123); CONC=0(0); SCGR=0.0(0.0); keyValue=MMCONO,330,MMITNO,I012345+++++++; environment=M3BEEEnv; version=1410; application=M3; </pre>
D (Delete) When a record is deleted	keyValue, startProgram, currentProgram, [Program properties]	<pre> M3:MITMAS:D startProgram=MMS001; currentProgram=MWMNGFDE; startTimeMillis=1327331743637; owner=M3User; startTime=2012-01-23 16:15:43; jobUUID=533d5c25cecb43b884707ef1bafc4bd5; sessionId=11.22.3.444:63547_0-0; CWUN=PCE; STAT=90; ... ITNO=I012345 ; ... CONO=330; LMDT=20120123; CONC=0; SCGR=0.0; keyValue=MMCONO,330,MMITNO,I012345+++++++; environment=M3BEEEnv; version=1410; application=M3; </pre>

<M3 Batch Program>

An example of an M3 Batch Program is PPS914.

Operation	Elements	Example*
S (Start) When a batch program is started	call-stack, USID, CONO, DIVI, program-type, BJNO, [Program properties]	M3:PPS914:S callStack=SYS->MMS940CL->MMS940->PPS914CL->PPS914; PGMN=PPS914; USID=M3User ; CONO=330; DIVI= ; programType=Batch; startTimeMillis=1327386739818; jobNo=853290583313539755; owner=M3User ; startTime=2012-01-24 07:32:19; jobUUID=b3bc22d6467b4dbdb9c5b4c3f7ad4116; sessionId=11.22.3.444:64834_25-0; BJNO=853348583340642306; environment=M3BEEEnv; version=1410; application=M3;
X (Exit) When a batch program exits	call-stack, USID, CONO, DIVI, program-type, BJNO, [Program properties], Stop Time	M3:PPS914:X callStack=SYS->MMS940CL->MMS940->PPS914CL->PPS914; PGMN=PPS914; USID=M3User ; CONO=330; DIVI= ; programType=Batch; startTimeMillis=1327386739818; jobNo=853290583313539755; owner=M3User ; startTime=2012-01-24 07:32:19; jobUUID=b3bc22d6467b4dbdb9c5b4c3f7ad4116; sessionId=11.22.3.444:64834_25-0; BJNO=853348583340642384; stopTime=2012-01-24 15:04:02; environment=M3BEEEnv; version=1410; application=M3;
F (Fail) When a batch program fails	call-stack, USID, CONO, DIVI, program-type, BJNO, [Program properties], Fail Time	M3:PPS914:F callStack=SYS->MMS940CL->MMS940->PPS914CL->PPS914; PGMN=PPS914; USID=M3User ; CONO=330; DIVI= ; programType=Batch; startTimeMillis=1327386739818; jobNo=853290583313539755; owner=M3User ; startTime=2012-01-24 07:32:19; jobUUID=b3bc22d6467b4dbdb9c5b4c3f7ad4116; sessionId=11.22.3.444:64834_25-0; BJNO=853348583340642384; stopTime=2012-01-24 15:04:02; environment=M3BEEEnv; version=1410; application=M3;

<M3 Interactive Program>

An example of an M3 Interactive Program is MMS001.

Operation	Elements	Example*
S (Start) When an interactive program is started	call-stack, USID, CONO, DIVI, program-type, [main-table, primary-key, main-table-language-constant (if they are found)], [Program properties]	<pre> M3:MMS001:S callStack=SYS->MMS001; PGMN=MMS001; USID=M3User ; CONO=330; DIVI=AAA; programType=Interactive; startTimeMillis=1327328450551; owner=M3User; startTime=2012-01-23 15:20:50; jobUUID=05d9cacec00843da948e2131d01e4a95; sessionId=11.22.3.444:63547_5-0; OPT2= 2; environment=M3BEEEnv; version=1410; application=M3; </pre>
X (Exit) When an interactive program exits	call-stack, USID, CONO, DIVI, program-type, [main-table, primary-key, main-table-language-constant (if they are found)], [Program properties]	<pre> M3:MMS001:X callStack=SYS->MMS001; PGMN=MMS001; USID=M3User ; CONO=330; DIVI=AAA; programType=Interactive; startTimeMillis=1327328450551; owner=M3User; startTime=2012-01-23 15:20:50; jobUUID=05d9cacec00843da948e2131d01e4a95; sessionId=11.22.3.444:63547_5-0; mainTable=MITMAS; relatedTables=; primaryKey=MMCONO,330,MMITNO,++++++TEST++++; mainTableLanguageConstant=XMI1001; OPT2= 2; stopTime=2012-01-23 15:21:24; environment=M3BEEEnv; version=1410; application=M3; </pre>

Operation	Elements	Example*
F (Fail) When an interactive program fails	call-stack, USID, CONO, DIVI, program-type, [main-table, primary-key, main-table-language-constant (if they are found)], [Program properties]	<pre> M3:MMS001:F callStack=SYS->MMS001; PGMN=MMS001; USID=M3User ; CONO=330; DIVI=AAA; programType=Interactive; startTimeMillis=1327328450551; owner=M3User; startTime=2012-01-23 15:20:50; jobUUID=05d9cacec00843da948e2131d01e4a95; sessionId=11.22.3.444:63547_5-0; mainTable=MITMAS; relatedTables=; primaryKey=MMCONO,330,MMITNO,++++++TEST++++; mainTableLanguageConstant=XMI1001; OPT2= 2; stopTime=2012-01-23 15:21:24; environment=M3BEEEnv; version=1410; application=M3; </pre>

<M3 Interactive Program> "." <Method>

An example of an M3 Interactive Program.Method is MMS001.PEDSP

Operation	Elements	Example*
S (Start) When a standard method in an interactive program is called	call-stack, USID, CONO, DIVI, program-type, [main-table, primary-key, main-table-language-constant (if they are found)], [Program properties]	<pre> M3:MMS001.PEDSP:S callStack=SYS->MMS001; PGMN=MMS001; USID=M3User ; CONO=330; DIVI=AAA; programType=Interactive; startTimeMillis=1327328450551; owner=M3User; startTime=2012-01-23 15:20:50; jobUUID=05d9cacec00843da948e2131d01e4a95; sessionId=11.22.3.444:63547_5-0; mainTable=MITMAS; relatedTables=; primaryKey=MMCONO,330,MMITNO, ++++++TEST++++; mainTableLanguageConstant=XMI1001; OPT2= 2; environment=M3BEEEnv; version=1410; application=M3; </pre>

Operation	Elements	Example*
X (Exit) When a standard method in an interactive program is left	call-stack, USID, CONO, DIVI, program-type, [main-table, primary-key, main-table-language-constant (if they are found)], [Program properties]	<pre> M3:MMS001.PEDSP:X callStack=SYS->MMS001; PGMN=MMS001; USID=M3User ; CONO=330; DIVI=AAA; programType=Interactive; startTimeMillis=1327328450551; owner=M3User; startTime=2012-01-23 15:20:50; jobUUID=05d9cacec00843da948e2131d01e4a95; sessionId=11.22.3.444:63547_5-0; mainTable=MITMAS; relatedTables=; primaryKey=MMCONO,330,MMITNO, ++++++TEST++++; mainTableLanguageConstant=XMI1001; OPT2= 2; stopTime=2012-01-23 15:21:08; environment=M3BEEEnv; version=1410; application=M3; </pre>

<M3 Program>

Any program in M3 BE.

Operation	Elements	Example*
S (Start) When a program is started	call-stack, PGMN, USID, CONO, DIVI, program-type (values: MIBatch, Batch, Interactive, ControlLanguage, Print or Unknown), startTimeMillis, owner, startTime, jobUUID, sessionId, [Interactive only: mainTable, relatedTables, primaryKey, mainTableLanguageConstant, OPT2] [Batch and MIBatch only: BJNO] environment, version, application	<pre> M3:PROGRAM:S callStack=SYS->PMS100->CRRTVIDS; PGMN=CRRTVIDS; USID=M3User ; CONO=330; DIVI=AAA; programType=Batch; startTimeMillis=1327330787842; owner=M3User; startTime=2012-01-23 15:59:47; jobUUID=054f0a55falf4c709fae905ca9ce1586; sessionId=11.22.3.444:63547_18-0; BJNO=850528583257729146; environment=M3BEEEnv; version=1410; application=M3; </pre>

Operation	Elements	Example*
X (Exit) When a program exits	call-stack, PGMN, USID, CONO, DIVI, program-type (values: MIBatch, Batch, Interactive, ControllLanguage, Print or Unknown), startTimeMillis, owner, startTime, jobUUID, sessionID, [Interactive only: mainTable, relatedTables, primaryKey, mainTableLanguageConstant, OPT2] [Batch and MIBatch only: BJNO] stopTime, environment, version, application	M3:PROGRAM:X callStack=SYS->PMS100->CRRTVIDS; PGMN=CRRTVIDS; USID=M3User ; CONO=330; DIVI=AAA; programType=Batch; startTimeMillis=1327330787842; owner=M3User; startTime=2012-01-23 15:59:47; jobUUID=054f0a55falf4c709fae905ca9ce1586; sessionID=11.22.3.444:63547_18-0; BJNO=850528583257729224; stopTime=2012-01-23 16:02:09; environment=M3BEEEnv; version=1410; application=M3;
F (Fail) When a program fails	call-stack, PGMN, USID, CONO, DIVI, program-type (values: MIBatch, Batch, Interactive, ControllLanguage, Print or Unknown), startTimeMillis, owner, startTime, jobUUID, sessionID, [Interactive only: mainTable, relatedTables, primaryKey, mainTableLanguageConstant, OPT2] [Batch and MIBatch only: BJNO] stopTime, environment, version, application	M3:PROGRAM:F callStack=SYS->PMS100->CRRTVIDS; PGMN=CRRTVIDS; USID=M3User ; CONO=330; DIVI=AAA; programType=Batch; startTimeMillis=1327330787842; owner=M3User; startTime=2012-01-23 15:59:47; jobUUID=054f0a55falf4c709fae905ca9ce1586; sessionID=11.22.3.444:63547_18-0; BJNO=850528583257729224; stopTime=2012-01-23 16:02:09; environment=M3BEEEnv; version=1410; application=M3;

* Format

<format> ::= <subscription string><name-value pair> { ";" <name-value pair> }

<name-value pair> ::= <name> "=" <value> ["(" <old value> ")"]