Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for IBM Lotus Domino DB

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for IBM Lotus Domino DB

November 30, 2016

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/17/2015	End of support for Lotus Domino version 6.5.
02/14/2014	Updated parameter screen image.
05/15/2012	Added new installation procedure. Added troubleshooting information.
11/15/2011	Fixed version conflicts within guide.
06/30/2011	Updated user name information under "Add a Domino DB Data Source."
02/15/2011	Updated supported versions and removed from legacy status. Added information to Troubleshooting section.

SmartConnector for IBM Lotus Domino DB

This guide provides information for installing the SmartConnector for IBM Lotus Domino DB and configuring the device for event collection. This SmartConnector is supported for installation on Microsoft Windows 2000 Advanced Server and Windows 2003 Server. IBM Lotus Domino versions 7.0, 8.0, 8.5, Lotus Notes SQL ODBC Driver 8.0, and Lotus Notes SQL 3.0 versions are supported.

Because Notes SQL client is not available on 64-bit platforms, only Windows 32-bit platforms are supported by this connector.

In cases where the Domino database is extremely large, this connector may not perform as expected. A new connector – SmartConnector for IBM Lotus Domino SNMP – is now available for such cases.

Product Overview

Lotus Domino is an IBM server product that provides enterprise-grade e-mail, collaboration capabilities, and a custom application platform. Domino began life as Lotus Notes Server, the server component of Lotus Development Corporation's client-server messaging technology. It can be used as an application server for Lotus Notes applications and as a web server. It also has a built-in database system in the format of NSF. From release 7, Domino server can use IBM DB2 system as its backend database.

Tables Supported

This connector only retrieves events from the Events and the Mail_Routing tables.

The Events table schema has the following columns (not in order)

- StartTime
- FinishTime
- EventsR6
- Server
- Header
- Body
- Hyphen

The Mail_Routing table schema has the following columns (not in order)

- StartTime
- FinishTime
- EventsR6
- Server

- Header
- Body
- Hyphen

What is NotesSQL?

NotesSQL is an ODBC (Open Database Connectivity) driver for Notes and Lotus Domino. It lets ODBC-enabled data reporting tools, database tools, and application development tools read, report, and update information that is stored in Lotus Domino databases (.nsf files).

A Lotus Domino database is not relational, but with NotesSQL a Lotus Domino database looks like a relational data source to an OBDC-enabled tool. This lets relational database management systems (RDBMS) such as Oracle or DB2 issue SQL (Structured Query Language) statements to Lotus Domino.

What is a Notes Database?

A Notes database is a single file that contains multiple documents. Documents in Notes databases can contain rich text, pictures, objects, and many other types of information. Notes comes with templates you can use to create your own databases. These templates have the file extension NTF. The Notes databases have the extension NSF.

Notes databases also have access control lists (ACLs) that control the actions people, groups, and servers can perform in the database. For example, one person may be able to create and read documents in a database, where another person may be allowed only to read documents in the same database.

Events on the Lotus Domino System

Configure events you want to know about based upon the type of information that is important to you. To configure an event, you determine three critical pieces of information: what type of event it is, what the severity level is, and how the event is to be handled.

Configure your events using Event Generator and Event Handler documents. Event generators describe the condition that must be met for an event to be generated; event handlers describe what happens when the event occurs.

After deciding which events you want to know about, decide what will happen when the event occurs. You have several choices. You can log the event to the log file (LOG.NSF); you can mail a notification of the event to a file or an administrator; or mail the event to another application for further processing.

You create an Event Handler document to specify to log the event to a specified destination, and simultaneously receive notification of the event's occurrence and run a program for additional processing. You can also prevent the event from being logged or handled at all. However, if you want to know about an event, you must have an Event Handler document. Otherwise the event is not recorded.

There is no default way of handling an event. So if you do not create event handlers, events are not logged or stored anywhere (except for server or add-in task events, which are stored in the log). After an event is passed to the Event Monitor task, it can invoke one or more configured Event Handlers.

Event Generators

Event generators gather information by monitoring a task or a statistic or by probing a server for access or connectivity. Each event generator has a specified threshold or condition, which, when met, causes an event to be created. The event is passed to the Event Monitor task, which checks whether an associated event handler has been defined. If an event handler has not been defined, the Event Monitor task does nothing. If an event handler has been defined, the Event Monitor carries out the instructions in the event handler. The Event Monitor task, formerly know as the Event task, starts automatically when you start the server and must run on all servers that you want to monitor.

The Lotus Domino Administrator includes a set of default event generators, which are listed in the Event Generators view of the Monitoring Configuration database (EVENTS4.NSF). To monitor other events that are important to you, you must create an event generator and define the type and severity of the event. The following table lists the types of event generators you can create.

If you purchased an add-in product designed to work with server-management programs, you may see additional types of events listed.

Event Generator	Description
Database	Monitors database activity and free space, monitors frequency and success of database replication, and reports on ACL changes, including those made by replication or an API program
Domino server response	Checks connectivity and port status of designated servers in a network
Mail routing	Sends a mail-trace message to a particular user's mail server and gathers tatistics indicating the amount of time, in seconds, it takes to deliver the message
Statistic	Monitors a specific Lotus Domino or platform statistic
Task status	Monitors the status of Lotus Domino server and add-in tasks
TCP server	Verifies the availability of Internet ports (TCP services) on servers and generates a statistic indicating the amount of time, in milliseconds, it takes to verify that the server is responding on the specified port

Event Severity Levels

The severity of an event indicates the level of required action.

Severity	Meaning
Fatal	Imminent system crash
Failure	Severe failure that does not cause a system crash
Warning(high)	Loss of function requiring intervention
Warning(low)	Performance degradation
Normal	Status messages

Event Handlers

An event handler defines the action that Domino takes when a specific event occurs. You can define an event handler to do one or more of the following:

- Log the event to a configured destination
- Notify you that the event occurred and specify the method of notification

- Forward the event to another program for additional processing
- Prevent the event from being logged to the server console or to a specified destination

The Monitoring Configuration database (EVENTS4.NSF) includes default event handlers for server tasks. However, to customize how events are handled, you may want to create a custom event handlers. You can enable or disable an event handler, so you can easily disable a default event handler and replace it with a custom one.

When you create an event handler, you specify the condition (for example, when an event meets or exceeds a threshold or meets a specified severity level) that triggers it. To specify event handler conditions, you define a set of criteria, specify a task, or select a custom event generator that triggers the event handler.

The ArcSight SmartConnector lets you import events generated by the SmartConnector for IBM Lotus Domino DB device into the ArcSight System. See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.

Before Installing the SmartConnector

Before installing the SmartConnector for IBM Lotus Domino DB:

1 **Install Lotus Notes Client.** Lotus Notes Client is required by NotesSQL. Based upon IBM's corporate Internet site, the following clients are supported: Lotus Notes Client Release 5.0 or later, Lotus Domino Release 5.0 or later, Lotus Notes Designer Release 5.0 or later, Lotus Domino Off-Line Services Release 1.01 or later.

2 **Install Lotus NotesSQL 3.0 or Lotus NotesSQL ODBC Driver 8.0.** Download and install either Lotus NotesSQL 3.0 or Lotus NotesSQL ODBC Driver 8.0 after you install Lotus Notes Client. Both Lotus NotesSQL 3.0 and Lotus NotesSQL ODBC Driver 8.0 have an ODBC driver for Notes and Domino. Install the ODBC driver on the machine where the connector will run.

3 **Add a System Data Source for the Domino DB.**

Add a Domino DB Data Source

Data sources (or DSNs) are one way to connect to a Lotus Domino database with NotesSQL. You can change or delete a data source at any time. You can use as many data sources as you like with a particular driver, provided no two data sources have the same name.

To add a system data source for the Domino DB:

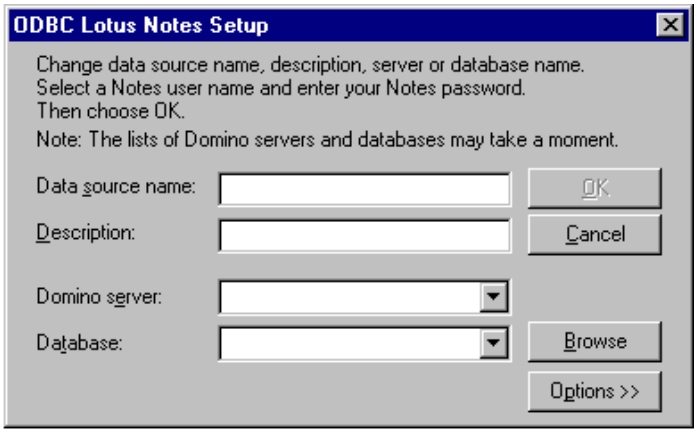
1 From the **Start** menu, select **Control Panel -> Administrative Tools -> Data Sources (ODBC)**.

2 Click the **System DSN** tab.

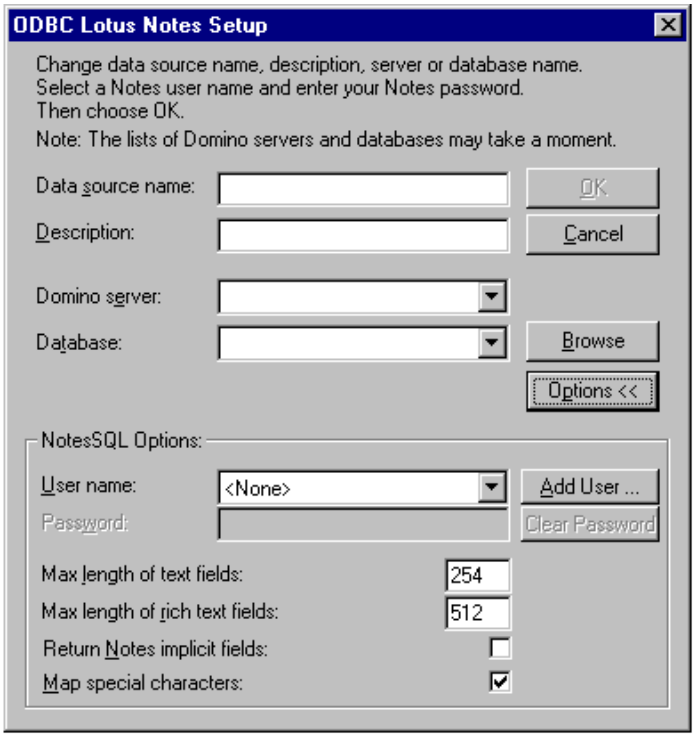
3 Click **Add**.

4 From the list, select the Lotus Notes ODBC driver (such as **Lotus NotesSQL**) from the list of installed ODBC drivers.

5 Click **Finish**; the **ODBC Lotus Notes Setup** dialog box is displayed:



6 Click **Options>>** to access the **NotesSQL Options**.



7 Enter values for the following fields:

- **Data source name:** Enter a name that identifies the data source. For example, add the name "Employee" to identify the ODBC connection to an employee database.
- **Description:**Enter a description of the data source. For example, add the description "Hire data, salary history, and current review of all employees" to describe the contents of the employee database.
- **Domino server:** (Required) Enter the name of the server that contains the database you want to open. Leave the field blank if the database is on the local machine.

- **Database:** (Required) Enter the path and name for the .NSF file you want to open. You can use any of three formats:

  full path (for example: C:\PERSONNEL\EMPLOYEE.NSF)

  relative path (specifies the path relative to the Notes data directory on that machine, whether the data is local or on a server; the Notes data directory is stored in the Windows registry as HKEY_LOCAL_MACHINE\Software\Lotus\ Notes\DataPath) (for example, PERSONNEL\EMPLOYEE.NSF)

  Universal Naming Convention (UNC) (for example, \\netname\netdir\netsubdir\EMPLOYEE.NSF)

- **User name:** Specify the NotesSQL Client user name, which comes from the Domino Server's `user.id` file. This file is normally stored under the directory where the Notes Client files are stored, for example, `\Documents and Settings\User\Local Settings\Application Data\Lotus\Notes\Data`. This name is used as the ODBC user name in the connector's ODBC configuration.

  To add a user name, click **Add User**. A wizard prompts you for the path to the user.id file and displays the hierarchical user name from the ID in the field.

  To use an existing user name (spoecified earlier for a DSN or added using the NotesSQL Authentication List Manager), select the user name from the drop-down list.

  Existing user names already are associcated with Notes user IDs. If you do not specify a user name, NotesSQL uses the ID of the last user who opened Notes when making the connection. Note that this ID may be password-protected, meaning you will receive a password prompt when NotesSQL connects to the database.

- **Notes Password:** Enter a password for authentication. This password is required if the Notes user ID used to make the connection is password-protected. The password you specify must match the password in the ID. You cannot specify a password without also specifying a Notes user name.

- **Max length of text fields:** Enter `15360`.

- **Max length of rich text fields:** Enter `15360`.

This number is the maximum possible value accepted by the Domino driver. If a larger number is entered, the Domino driver will change the value to 15360.

Specify Required Privilege

Required for SmartConnector log event collection are database read, replicate, write, and create privileges. To authorize this privilege:

1. From the Domino Administrator, click the **Configuration** tab and open the **Server** document.
2. Click the **Security** tab.
3. In the **Database administrators** field, enter the name of the user specified when creating the Domino DB data source and then save the document.

Create an Event Handler

To create an Event Handler document in the Monitoring Configuration database (EVENTS4.NSF):

1 From the Domino Administrator, click the **Configuration** tab, and open the **Monitoring Configuration** view.

2 Open the **Event Handlers - All** view, and click **New Event Handler**.

3 On the **Basics** tab in the **Server(s) to monitor** field, select one:

- Notify of the event on any server in the domain
- Notify of the event only on the following servers. Then select the server from a list.

4 Under **Notification trigger**, select one:

- Any event that matches a criteria. Then complete these fields on the Event tab:

Field	Action
Event type	Select one: "Events can be any type" or "Events must be this type" (then select the type from the list).
Event severity	Select one: "Events can be any severity" or "Events must be one of these severities" (then select a severity level from the list).
Message text	Select one: "Events can have any message" or "Events must have this text in the event message" (then type the message text)

- A built-in or add-in task event. Then click **Select Event**, select the event from the list, and select one: "Events can have any message" or "Events must have this text in the event message" (then enter the message text).
- A custom event generator. Then select it from the list or click **New** to create a new custom event generator.

5 Click the **Action** tab and select the notification method.

6 Select one enablement option:

- Enable this notification; to enable the notification during all hours.
- Enabled only during these times; then click the clock and move the slider to select the start and end time during which this event handler is enabled.

7 Click **Save & Close**.

Create Log Filters

By default, Lotus Domino logs all events to the log file (LOG.NSF), which can become quite large, depending upon the log level set for each event. To prevent events from being logged either to the log file or to the server console, create a log filter that specifies both the type and severity of the event to filter. Then only events that meet the specified criteria appear in the log file.

To create a log filter:

1. From the Lotus Domino Administrator, click the **Configuration** tab and then open the **Monitoring Configuration - Log Filters** view.
2. Click **New Event Filter**.
3. On the **Basics** tab, select the name of the server on which you want to set log filters.
4. Click the **Database** tab. For the field "Log unknown types/severities?" select **Yes** or **No** to filter events from the log file.
5. Select one:
   - Log All Types; then specify a severity level.
   - Select types; then check each type of event to log.
6. Click the **Console** tab. For the field "Log unknown types/severities?" select **Yes** or **No** to filter events from the console.
7. Select one, and then **Save & Close**:
   - Log All Types; then specify a severity level.
   - Select types; then check each type of event to log.

You can also create a log filter from the server console.

NOTES.INI Settings for Log Files

The following table contains the NOTES.INI settings that determine what is reported in the log file and set size limitations

Setting	Description
KeyFileName	Specifies the location of the server ID or user ID file. **The *KeyFileName* field must point to the Lotus Notes userid file**.
Log	Specifies the contents of the log file and controls other logging actions.
Log_AgentManager	Specifies whether or not the start of agent execution is recorded in the log file and shown on the server console.
Log_Console	Enforces logging of server console command output, which can otherwise be prevented if the command is prefixed with an exclamation point (!).
Log_DirCat	Logs information about the Directory Catalog task to the Miscellaneous Events view of the log file (LOG.NSF).
Log_Replication	Specifies the level of logging of replication events performed by the current server.
Log_Sessions	Specifies whether individual sessions are recorded in the log file and displayed on the console.
Log_Tasks	Specifies whether the current status of server tasks is recorded in the log file and displayed on the console.

Setting	Description
Log_Update	Specifies the level of detail of Indexer events displayed at the server console and in the log file.
Log_View_Events	Specifies whether messages generated when views are rebuilt are recorded in the log file.
Mail_Log_To_MiscEvents	Determines whether all mail event messages are displayed in the Miscellaneous Events view of the log file.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

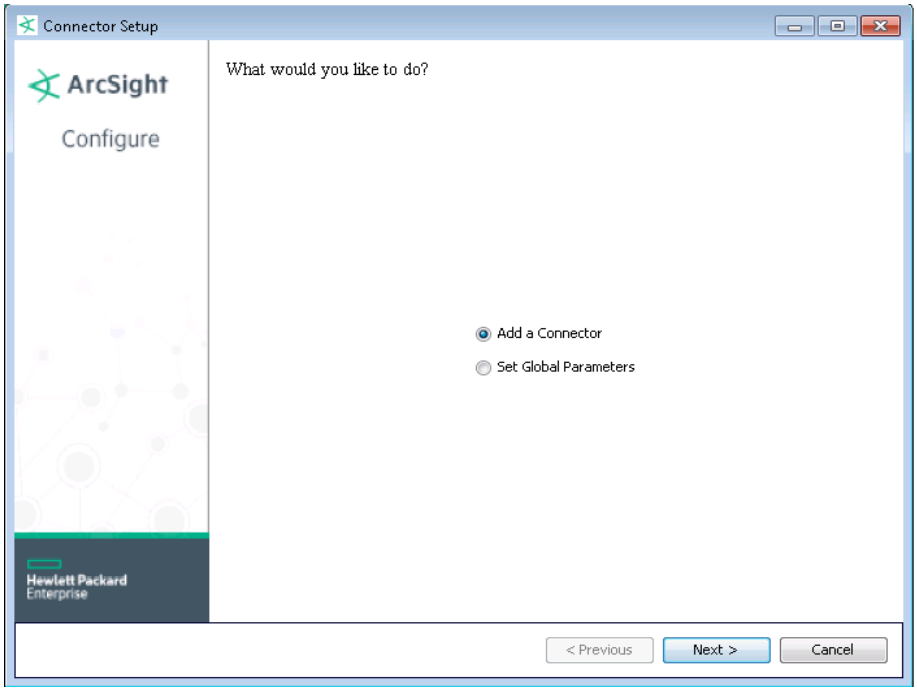
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	If both 'IPv4' and'IPv6' IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is 'IPv4'.

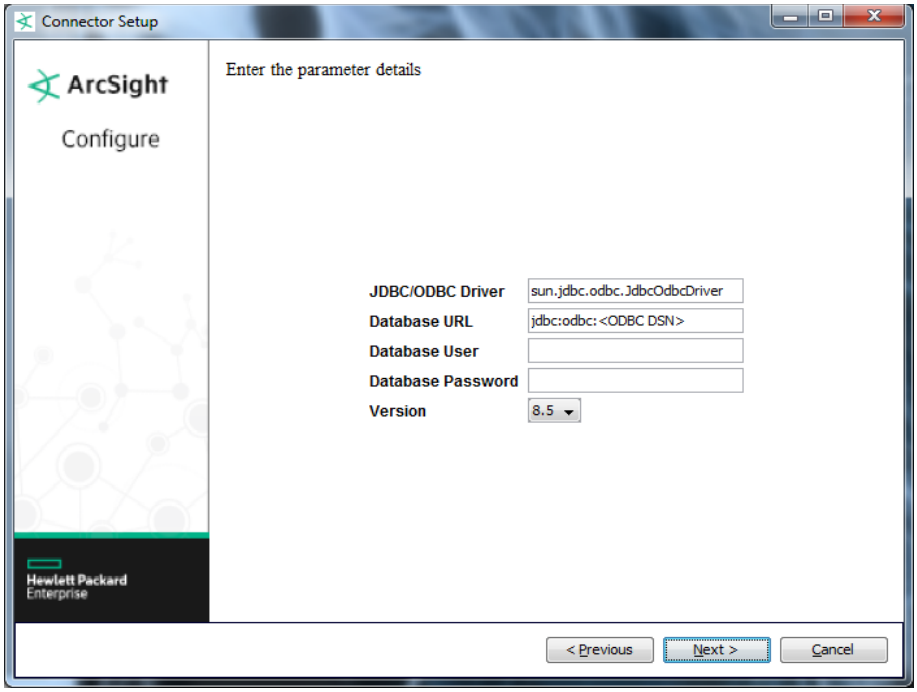
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2 Select **IBM Lotus Domino DB** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
JDBC/ODBC Driver	Enter the name of the JDBC driver. For this Domino SmartConnector, accept the default of sun.jdbc.odbc.JdbcOdbcDriver.
Database URL	Accept the default jdbc:odbc:<DSN NAME> for this Domino SmartConnector (where DSN NAME is the ODBC data source name for the Domino database).
Database User	User name for the Domino database. See the "Configuration" section for more information.
Database Password	User password assigned to access above database. See the "Configuration" section for more information.
Version	Select a version 7.0, 8.0, or 8.5 from the drop-down box.

Select a Destination

1 The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2 Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 The certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

IBM Lotus Domino DB Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	Application Protocol
Connector Severity	High = 0, 1, or 2; Medium = 3 or 4; Low = 5
Destination Address	Destination Address
Destination Dns Domain	Destiantion Dns Domain
Destination Host Name	Destination Host Name
Destination User Name	Destination User Name
Device Custom Number 1	Message size
Device Custom Number 2	Message Count
Device Custom Number 3	Disk Short
Device Custom String 1	Reason
Device Custom String 2	Message IDs
Device Custom String 3	Destination Email Domain
Device Custom String 4	Source Email Domain
Device Custom String 5	File Size
Device Custom String 6	Hop Count
Device Event Class Id	lnEvtType
Device External Id	lnEvtSeq
Device Product	'Domino'
Device Receipt Time	lnEvtWhen
Device Severity	lnEvtSeverity
Device Vendor	'IBM'
External Id	lnEvtSeq
File Name	File Name
File Size	File Size
Message	lnEvtData
Name	lnEvtData
Source Address	Source Address
Source Host Name	Source Host Name
Source User Name	Source User Name
Transport Protocol	Transport Protocol

Troubleshooting

Why can't I shut down the connector using Ctrl-C after a Lotus Notes server restart?

Because of a Lotus Notes SQL driver limitation, the connector cannot be shut down using Ctrl-C after the Lotus Notes server has restarted. You can end the Java process manually on all platforms; on

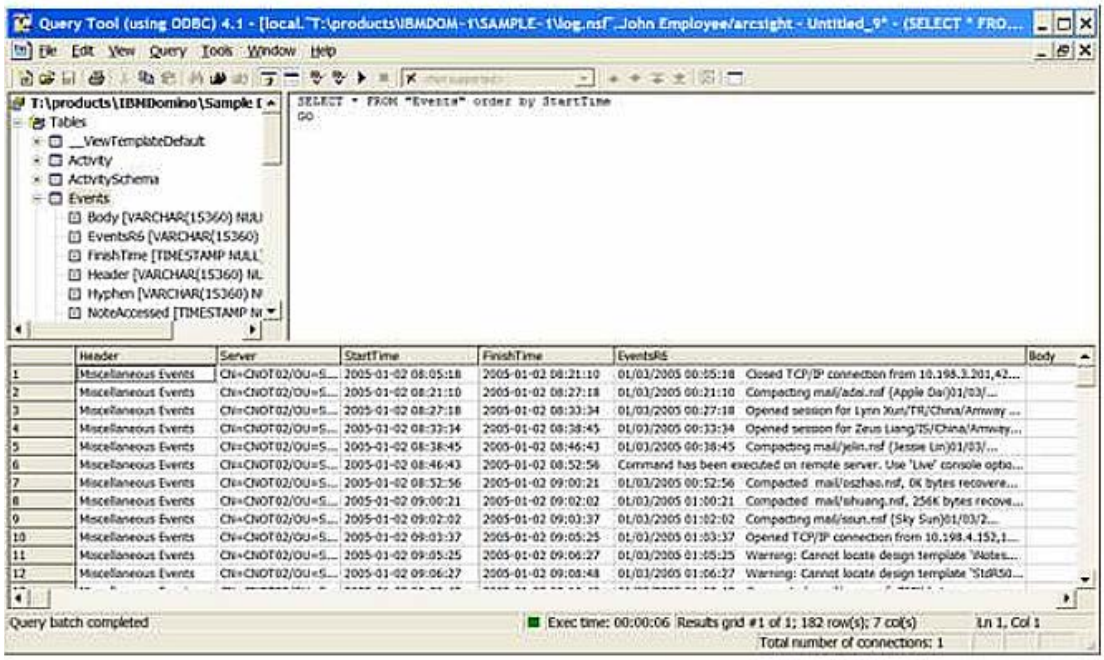
Windows, use the Windows Task Manager. The event process for this connector is not affected by the limitation.

How can I verify query results?

You can use a free Query Tool to verify query results. See the following address to download this tool:

http://gpoulose.home.att.net/Tools/QTODBC61.msi

A sample window of this tool follows.



Why am I receiving duplicate events?

ArcSight has identified a potential problem with the IBM Domino ODBC driver that can cause data duplication when using ArcSight's SmartConnector for IBM Lotus Domino DB. We have been able to reproduce a customer issue in which the Domino connector can inadvertently send duplicate data to the ArcSight ESM Manager or ArcSight Logger. This SmartConnector uses IBM's Domino ODBC driver to retrieve data from the Domino server; ArcSight has traced the issue to an incorrect result set returned by this ODBC driver. Based upon our lab testing, the issue may be related to large log.nsf files (a file size of 1.6Gb in our lab, but size might depend upon Domino's server hardware).

The cause for this data duplication issue has not yet been confirmed with IBM, but we are currently seeking their assistance. In our lab, once the log was cleaned up, reducing its size in the process, the problem disappeared and IBM's Domino ODBC driver started returning correct result sets. Until we receive further information from IBM regarding this issue, customers are advised to periodically monitor the data sent by the connector and, in particular, the size of the log.nsf file to make sure it does not grow too large.

The SmartConnector for IBM Lotus Domino SNMP has been developed for situations in which this known issue occurs.