Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.3.0

SmartConnector for Sybase Adaptive Server Enterprise DB

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

SmartConnector for Sybase Adaptive Server Enterprise DB

SmartConnector for Sybase Adaptive Server Enterprise DB

This guide provides information for installing the SmartConnector for Sybase Adaptive Server Enterprise Database (ASE) and configuring the device for audit event collection.

This document discusses operating system, appliance, browser, and other support details for ArcSight SmartConnector and select your ArcSight product from the list presented.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Configuration Guide for ArcSight SmartConnector Load Balancer*, which provides detailed information about installing Load Balancer.
- *Release Notes for ArcSight SmartConnectors and ArcSight SmartConnector Load Balancer*, which provides information about the latest release.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

Sybase Adaptive Server Enterprise (ASE) is a high-performance, mission-critical database management system that gives Sybase customers an operational advantage by lowering costs and risks.

Adaptive Server includes a comprehensive audit system. The audit system consists of a system database called `sybsecurity`, configuration parameters for managing auditing, a system procedure, `sp_audit`, to set all auditing options, and a system procedure, `sp_addauditrecord`, to add user-defined records to the audit trail.

Data auditing provides insight into how database systems are used, with a continuous and permanent audit trail of access and changes to data, and to database structure, storing this information in a centralized repository.

Configuration

For complete information about Sybase Adaptive Server Enterprise auditing and configuration, see Sybase's *System Administration Guide for Adaptive Server Enterprise*.

The System Security Officer is the only user who can start and stop auditing, set up auditing options, and process the audit data.

The Audit System

The audit system includes:

- The **sybsecurity** database, which contains global auditing options and the audit trail.
- The in-memory audit queue, to which audit records are sent before they are written to the audit trail.
- Configuration parameters for managing auditing.
- System procedures for managing auditing.

The sybsecurity Database

The **sybsecurity** database is created during the auditing installation process. In addition to all the system tables found in the model database, it contains **sysauditoptions**, a system table for keeping track of server-wide auditing options, and system tables for the audit trail.

sysauditoptions contains the current setting of global auditing options, such as whether auditing is enabled for disk commands, remote procedure calls, ad hoc user-defined auditing records, or all security-relevant events. These options affect the entire Adaptive Server.

The Audit Trail

Adaptive Server stores the audit trail in system tables named **sysaudits_01** through **sysaudits_08**. When you install auditing, you determine the number of audit tables for your installation. For example, if you choose to have two audit tables, they are named **sysaudits_01** and **sysaudits_02**. At any given time, only one audit table is current.

Adaptive Server writes all audit data to the current audit table. A System Security Officer can use sp_configure to set, or change, which audit table is current.

Sybase recommends the number of tables be two or more with each table on a separate audit device. This lets you set up a smoothly running auditing process in which audit tables are archived and processed with no loss of audit records and no manual intervention.

Important: Sybase strongly recommends against using a single audit table on production systems. If you use only a single audit table, you may lose audit records.

The auditing system writes audit records from the in-memory audit queue to the current audit table. When the current table is nearly full, a threshold procedure can automatically archive the table to another database.

Installing and Setting Up Auditing

The overall steps involved in installing and setting up auditing include:

1. Install auditing. Set the number of audit tables and assign devices for the audit trail and the syslogs transaction log in the sybsecurity database. For detailed information, refer to "Installing the audit system" in the *Adaptive Server Enterprise System Administration Guide* and the Adaptive Server installation and configuration.
2. Set up audit trail management. Write and establish a threshold procedure that receives control when the current audit table is nearly full. The procedure automatically switches to a new audit table and archives the contents of the current table. In addition, this step involves setting the audit queue size and the suspend audit when device full configuration parameters. Refer to "Setting up audit trail management" and "Single-table auditing" in the *Adaptive Server Enterprise System Administration Guide*.
3. Set up transaction log management in the sybsecurity database: Determine how to handle the syslogs transaction log, how to set the **trunc log on chkpt** database option, and establish a last-chance threshold procedure for syslogs if **trunc log on chkpt** is **off**. Refer to "Setting up transaction log management" in the *Adaptive Server Enterprise System Administration Guide*.
4. Set auditing options, using **sp_audit** to establish the events to be audited. Refer to "Setting global auditing options" in the *Adaptive Server Enterprise System Administration Guide*.
5. Enable auditing, using **sp_configure** to turn on the auditing configuration parameter. Adaptive Server begins writing audit records to the current audit table.

To enable or disable auditing, use **sp_configure** with the auditing configuration parameter.

The syntax is:

```
sp_configure "auditing",[0|1]
```

where `1` enables auditing and `0` disables auditing.
For example, to enable auditing, enter: `sp_configure "auditing", 1`

For complete information, refer to "Enabling and disabling auditing" in the *Adaptive Server Enterprise System Administration Guide*.

Note: When you enable or disable auditing, Adaptive Server automatically generates an audit record.

Installing sybsecurity and Configuring Auditing

To install **sybsecurity** and configure auditing:

1. To install **sybsecurity**, enter the following commands from isql:

   ```
   disk init name = "auditdev",
   physname = "C:\downloads\sybase\data\auditdev.dat",
   vdevno = 3, size = 5120
   disk init name = "auditlogdev",
   physname = "C:\downloads\sybase\data\auditlogdev.dat",
   vdevno = 4, size = 1024
   create database sybsecurity on auditdev
   log on auditlogdev
   ```

2. From the **scripts** directory, run the following commands:

   ```
   set DSQUERY=server_name
   isql -Usa -Ppassword -Sserver_name < installsecurity
   ```

3. Restart the machine.

4. To enable auditing:

   ```
   isql -Usa _ppassword -Sserver
   use sybsecurity
   go
   sp_configure "auditing"
   go
   sp_configure "auditing",1
   go
   sp_configure "allow updates", 1
   go
   sp_configure "suspend audit when device full", 0
   go
   ```

   To add another audit table (there are eight audit tables that change dynamically):

   ```
   sp_addauditttable 'default'
   ```

   To manually switch to the next audit table:

   ```
   sp_configure "current audit table",1,"with truncate"
   ```

Configuring Sybase Audit DB Error Log Path

Each time Adaptive Server starts, it begins to write information to a local error log file, called the Adaptive Server error log. This file logs error and informational messages

generated by the server during its operations, as well as stores information about the success or failure of each start-up event.

Note: When you want to make more memory available by reducing the size of the error log, stop Adaptive Server before deleting logged messages. The log file cannot release its memory space until Adaptive Server has stopped.

The location of the error log in the Sybase installation directory is set when you configure a new Adaptive Server, Backup Server, and Monitor Server. Each have their own error logs. The default location for the Adaptive Server's error log is *$SYBASE/ASE-12_5/install/error.log*.

Note: Multiple Adaptive Servers cannot share the same error log. If you install multiple Adaptive Servers, specify a unique error log file name for each server.

You can change the error log path by editing the `$SYBASE/ASE-12_5/install/RUN_server_name` file. For example, to change the error log path from the following:

```
$SYBASE/ASE-12_5/bin/dataserver -d/Devices/ASE_2K.dat -sASE_2K -i/ASE_125
-e/$SYBASE/ASE -12_5/install/ASE_2K.log-M/ASE_125
```

to the `$SYBASE` directory, enter:

```
$SYBASE/ASE-12_5/bin/dataserver -d/Devices/ASE_2K.dat -sASE_2K-i/ASE_125 -
e/$SYBASE/ASE_2K.LOG -M/ASE_125
```

By default, Adaptive Server does not log auditing events. However, you can use **sp_configure** parameters to specify whether Adaptive Server is to log auditing events, such as logins, to the Adaptive Server Error Log.

You can use the following parameters and values:

- Log audit logon success at 1 - to enable logging of successful Adaptive Server logins.

  ```
  sp_configure "log audit logon success", 1
  ```
- Log audit logon failure at 1 - to enable logging of unsuccessful Adaptive Server logins:

  ```
  sp_configure "log audit logon failure", 1
  ```
- Either parameter at 0 - to disable logging of that message type:

  ```
  sp_configure "log audit logon success", 0
  sp_configure "log audit logon failure", 0
  ```

Installing the SmartConnector

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

Preparing to Install Connector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

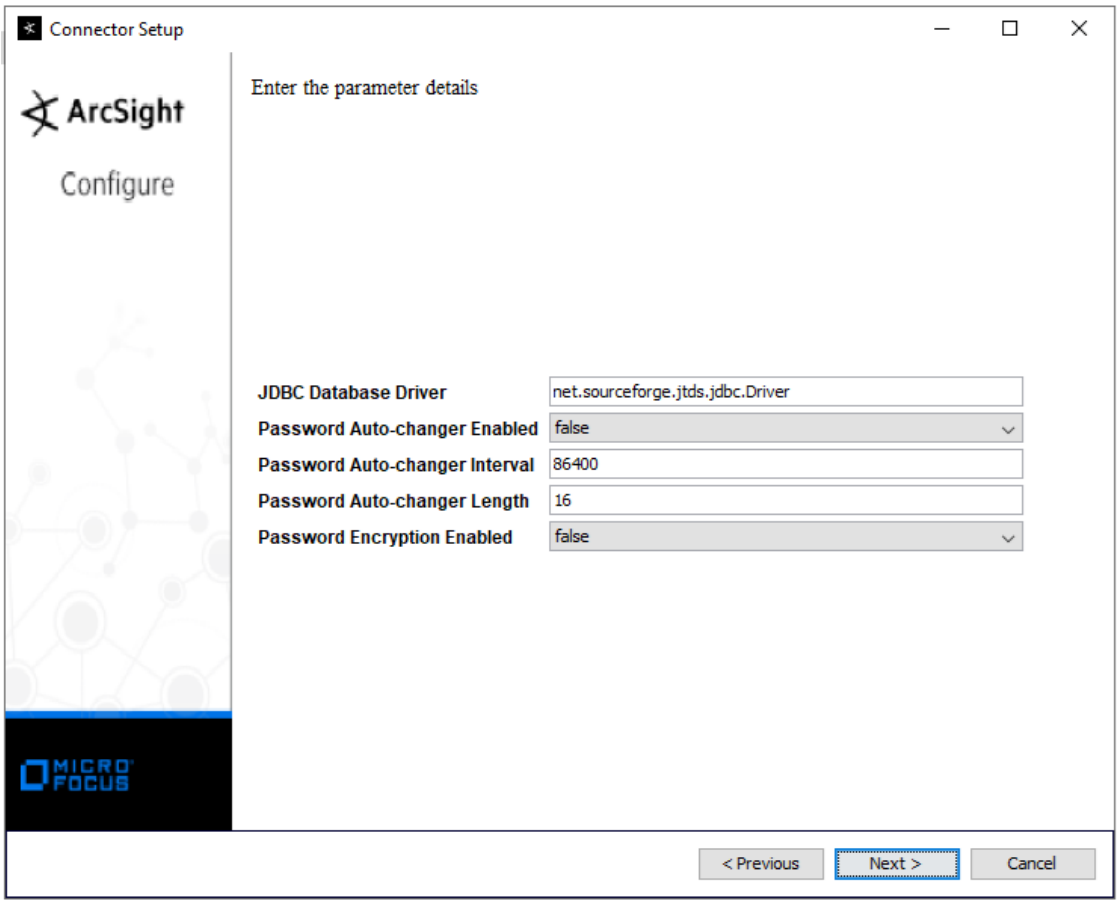
Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Sybase Adaptive Server Enterprise DB Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the Sybase Adaptive Server Enterprise DB Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Select **Sybase Adaptive Server Enterprise DB** from the **Type** drop-down menu, then click **Next**.

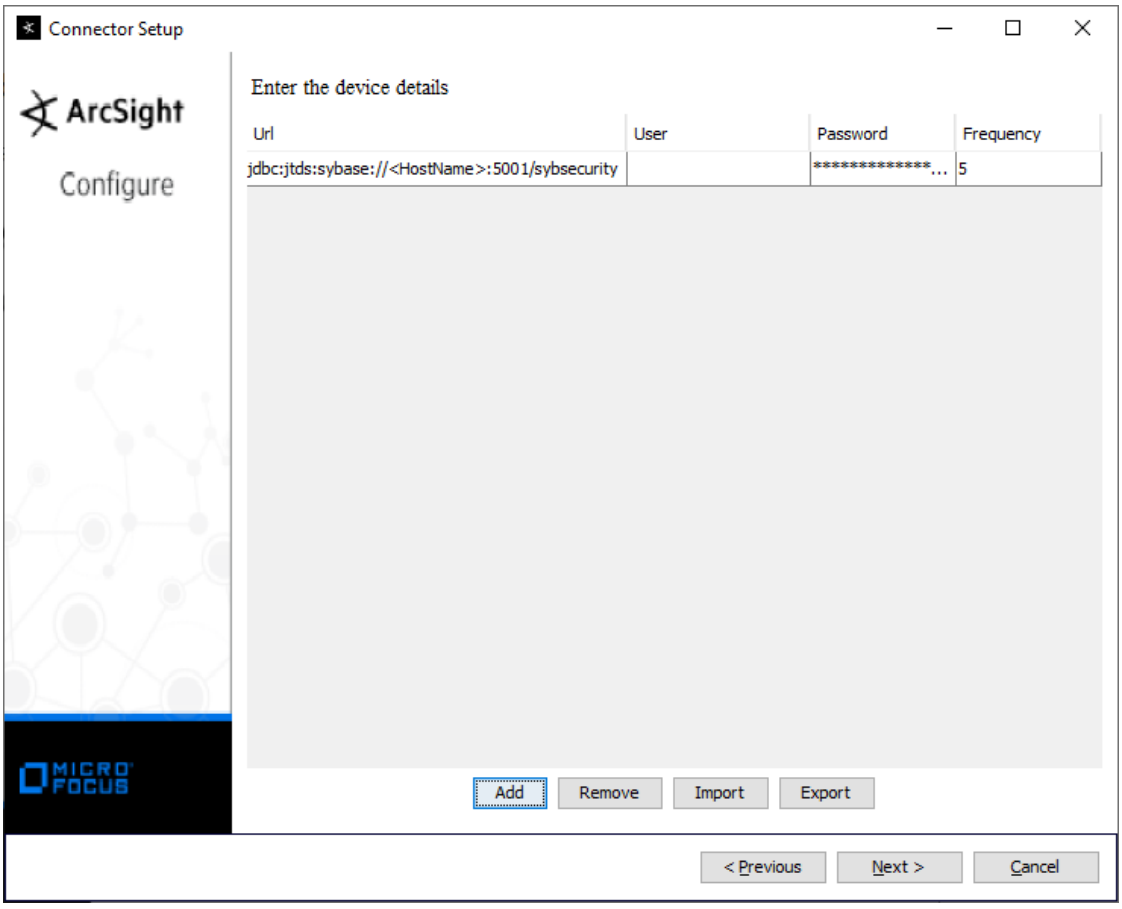
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
JDBC Database Driver	The default value is **net.sourceforge.jtds.jdbc.Driver**.
Password Auto-changer Enabled	The default value is **false**. If you select **true**, then you must specify values for the **Password Auto-changer Interval** and **Password Auto-changer Length** parameters. This feature automatically and periodically changes your password as per the defined password changing interval.

Parameter	Description
Password Auto-changer Interval	The default value is **86400**seconds. Enter a password changing interval.
Password Auto-changer Length	The default value is **16**. Enter the desired length for generated passwords.
Password Encryption Enabled	The default value is **false**. Select **true** if the password encryption is enabled in the Sybase ASE database, else select **false**. If you select **true**, then you must enter JDBC Databse Driver as **com.sybase.jdbc4.jdbc.SybDriver**. It is mandatory to place the **jconn4.jar** file in the following folder: `current\user\agent\lib`. The **jconn4.jar** file is available in the Sybase ASE database Installation directory. Example: `C:\SAP\jConnect-16_0\classes\jconn4.jar`.

6. Click **Add**. Enter the devices details to configure the connector, then click **Next**.



Parameter	Description
URL	The default value is **jdbc:jtds:sybase://<HostName>:5001/sybsecurity**. Enter the database URL. If you have selected the **Password Encryption Enabled** parameter as **true** and entered the JDBC Databse Driver as **com.sybase.jdbc4.jdbc.SybDriver**, then you must enter URL in the following format: `jdbc:sybase:Tds:[HostName]:[Port]?ServiceName=sybsecurity&ENCRYPT_PASSWORD=true`
User	Enter the database user name (with adequate privilege). Note that a System Security Officer (sso_role) manages the audit system and is the only user who can start and stop auditing, set up auditing options, and process the audit data.
Password	Password for the database user.
Frequency	The default value is **5** seconds. Enter the frequency, in seconds, at which the connector is to check for new events.

7. Select a destination and configure parameters.
8. Specify a name for the connector.
9. If you have selected ArcSight Manager as the destination, 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.
10. Select whether you want to run the connector as a service or in the standalone mode.
11. Complete the installation.
12. Run the SmartConnector.

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

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.

Adaptive Server Enterprise DB Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	_DB_HOST
Destination Host Name	asehostname()
Destination Port	_DB_URL
Device Address	_DB_HOST
Device Custom Number 1	dbid ('Database ID')
Device Custom Number 2	objid ('Accessed Object ID')
Device Custom String 1	extrainfo ('ExtraInfo')
Device Custom String 2	objname ('Object Name')
Device Custom String 3	objowner ('Object Owner')
Device Custom String 4	eventmod ('EventMod')
Device Custom String 5	sequence ('Sequence')
Device Custom String 6	dbname ('Database Name')
Device Event Class ID	Event
Device Host Name	One of (asehostname(), _DB_HOST, _DB_URL)
Device Process Name	servername
Device Product	Adaptive Server Enterprise
Device Receipt Time	eventtime
Device Severity	eventmod
Device Vendor	Sybase
End Time	eventtime

ArcSight ESM Field	Device-Specific Field
Source Host Name	host_name()
Source Process Name	spid
Source User ID	suid
Source User Name	loginname
Start Time	eventtime

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for Sybase Adaptive Server Enterprise DB (Micro Focus Security ArcSight Connectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!