Micro Focus Security ArcSight Connectors

SmartConnector for Sybase Adaptive Server Enterprise DB

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Sybase Adaptive Server Enterprise DB

June, 2018

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2015	Updated Device Host Name mapping.
05/15/2012	Added new installation procedure.
09/30/2011	Reactivated support for this connector.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure for FIPS support.
02/11/2009	Added description of Password Auto-enable parameter; added configuration steps.

SmartConnector for Sybase Adaptive Server Enterprise DB

This guide provides information for installing the SmartConnector for Sybase Adaptive Server Enterprise DB and configuring the device for audit event collection. Sybase Adaptive Server Enterprise versions 12.5 and 15.0 are supported.

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 consists of:

- 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.

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.

Install and Setup 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.

   See "Installing the audit system" in the *Adaptive Server Enterprise System Administration Guide* and the Adaptive Server installation and configuration information for detailed information.

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.

   See "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**.

   See "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.

   See "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
```

See "Enabling and disabling auditing" in the *Adaptive Server Enterprise System Administration Guide* for complete information.

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

Install sybsecurity and Configure 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_addaudittable 'default'
```

To manually switch to the next audit table:

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

Configure 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.

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*.

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.

Possible parameters and values are:

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
```

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).

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

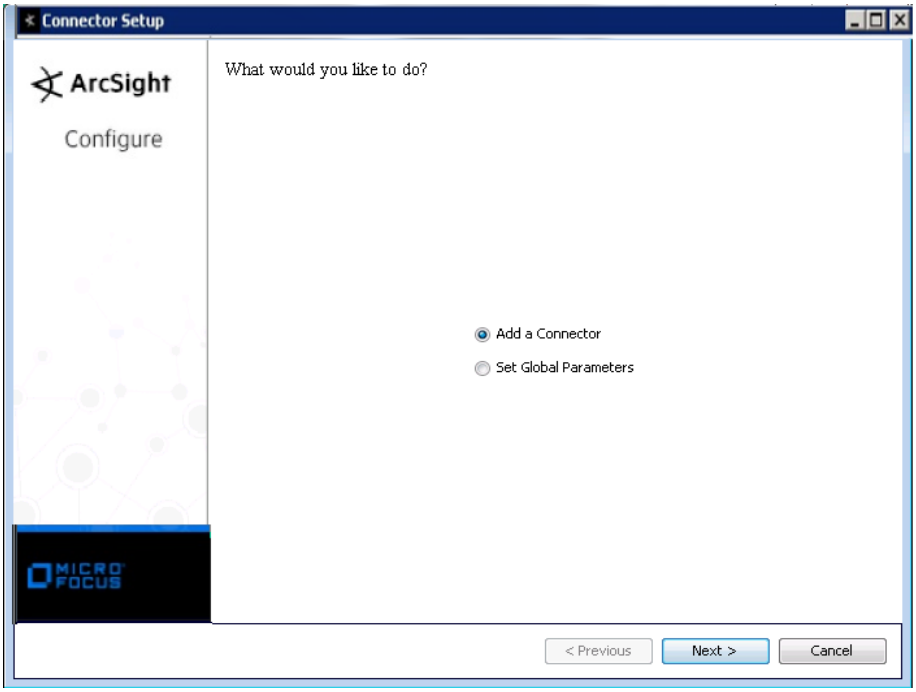
Install Core Software

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 Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus 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. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.
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	When 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. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.

Parameter	Setting
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

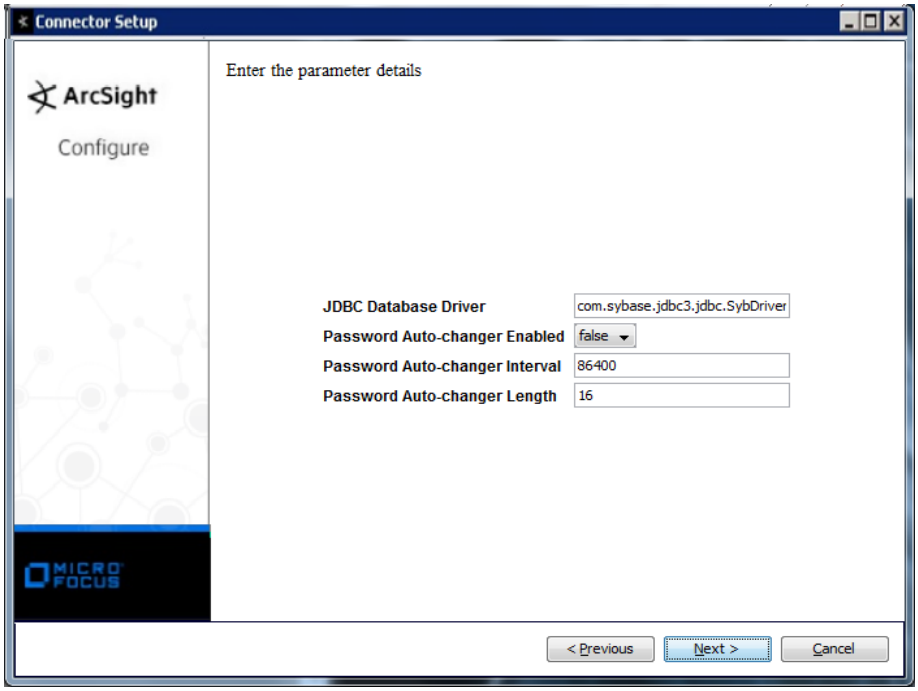
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

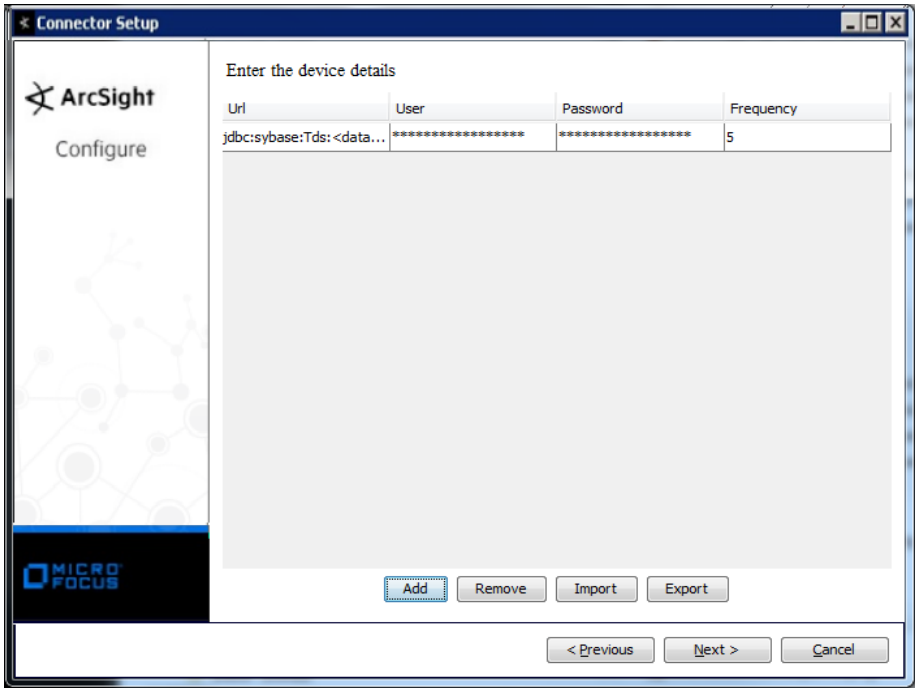
Select Connector and Add Parameter Information

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 **Sybase Adaptive Server Enterprise DB** and click **Next**.

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





Parameter	Description
JDBC Database Driver	com.sybase.jdbc2.jdbc.SybDriver
Password Auto-changer Enabled	The default value is 'false.' This feature automatically changes the password of the user it is using every time the user logs in and also periodically according to a configurable amount of time. If you change this value to 'true,' also enter values for the 'Password Auto-changer Interval' and 'Password Auto-changer Length' parameters.
Password Auto-changer Interval	Enter a password changing interval; the default value is 86400 seconds.
Password Auto-changer Length	Enter the desired length for generated passwords; the default value is 16.
Databases	Enter the parameters for the databases this connector is to query in the following fields.
URL	Enter the database URL.
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	Enter the frequency, in seconds, at which the connector is to check for new events.

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be 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 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.

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 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.

Adaptive Server Enterprise DB Mappings to ArcSight ESM Fields

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