SmartConnector™ Configuration Guide for

Mazu Profiler V3 Schema DB

August 15, 2007

ArcSight™

SmartConnector Configuration Guide for

Mazu Profiler V3 Schema DB

August 15, 2007

Revision History

Date	Description
08/15/2007	General content update.
05/15/2007	First release of SmartConnector documentation.

SmartConnector Configuration Guide for Mazu Profiler V3 Schema DB

This guide provides information for installing the SmartConnector for Mazu Profiler V3 Schema DB and configuring the device for event collection. This SmartConnector is supported on Windows and UNIX platforms. Mazu Profiler version 7 with V3 Schema is supported.

Product Overview

Mazu Profiler is a behavior-based, network-security solution designed specifically for protecting internal networks. Profiler analyzes the behavior of hosts in the network rather than threat signatures to detect threats, and is therefore not thrown off by new and zero-day attacks. It can precisely target individual compromised hosts and mitigate attacks with very high speed. It also can assess the impact of policy changes and mitigation actions before they are performed. Profiler leverages routers, switches, and probes already deployed in networks, it provides network-wide protection.

The ArcSight SmartConnector lets you import events generated by the Mazu Profiler V3 Schema 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.

Configuration

Granting Usage

To grant usage to tables containing event information:

1. On the Mazu Profiler appliance, log in as a **root** user or a **postgres** user.
2. Connect to the Mazu database as a **postgres** user:

   psql mazu postgres

3. Execute the following psql commands:

   ```
   GRANT USAGE ON SCHEMA hostscan TO PUBLIC;
   GRANT USAGE ON SCHEMA worm TO PUBLIC;
   GRANT USAGE ON SCHEMA portscan TO PUBLIC;
   GRANT USAGE ON SCHEMA alertrule TO PUBLIC;
   GRANT USAGE ON SCHEMA dos TO PUBLIC;
   GRANT USAGE ON SCHEMA newservice TO PUBLIC;
   GRANT USAGE ON SCHEMA anomalous TO PUBLIC;
   ```

Configuring Mazu Profiler to Send Events

You can use either a **PostgreSQL** or an **ODBC JDBC** driver to configure the device to send events to the SmartConnector. If you are going to use the ODBC driver, you must have a PostgreSQL ODBC driver compatible with your database installed.

When using the PostgreSQL driver, the database URL installation parameter is of the following format:

```
jdbc:postgresql://<HostNameOrIpAddress>:5432/$<Database Name>
```

When using the ODBC driver, the database URL parameter is of the following format:

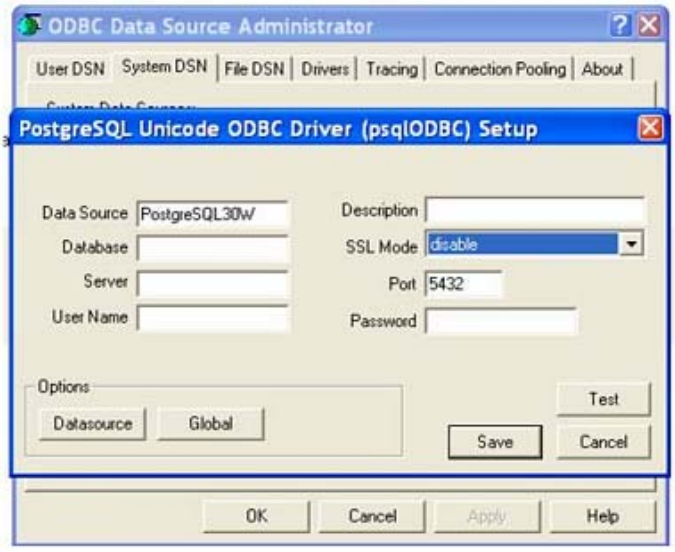
```
jdbc:odbc:<DSN Name>
```

When using the PostgreSQL driver, no further configuration is required. When using the ODBC driver, see "Configuring a PostgreSQL ODBC Data Source."

Configuring a PostgreSQL ODBC Data Source

To create a new DSN ODBC data source that points to the Mazu Profiler's database on the machine on which the SmartConnector is to be installed, follow these steps. Before beginning, make sure you have administrative privileges to create ODBC data sources on the machine.

1. Click **Start**; select **Control Panel -> Administrative Tools -> Data Sources (ODBC)**.
2. Select the **System DSN** tab and click **Add**.
3. Select **PostgreSQL Unicode** from the list of drivers and click **Save**.
4. Enter the parameters for your DSN (Database, Server, User Name, and Password) and, optionally, enter a description.



5 Click **Save**.

6 Click **Next**, then click **Finish**.

7 Test the ODBC data source by clicking **Test Data Source**. If the connection is established successfully, click **OK** to close the ODBC Data Source window.

Remember the ODBC name, username, and password you used in the DSN creation; it will be required when you install the SmartConnector.

Installing the SmartConnector

ArcSight ESM Installation

Before you install any ArcSight SmartConnectors, make sure that ArcSight ESM has already been installed correctly. Also, ArcSight recommends reading the *ArcSight Installation and Configuration Guide* before attempting to install a new ArcSight SmartConnector. For a successful installation of ArcSight ESM, install the components in the following order:

1 Ensure that the ArcSight ESM Manager, Database, and Console are installed correctly.

2 Run the ArcSight ESM Manager; the ArcSight ESM Manager command prompt window or terminal box displays a **Ready** message when the Manager has started successfully. If the ArcSight Manager is being run as a Windows NT/2000 Service, monitor the **server.std.log** file located in `ARCSIGHT_HOME\current\logs`.

3 Run the ArcSight Console. Though not necessary, it is helpful to have the ArcSight Console running when installing the SmartConnector to verify successful installation.

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

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

SmartConnector Installation

For information regarding operating systems and platforms supported, see SmartConnector Product and Platform Support.

1 Insert the ArcSight Installation CD into your CD-ROM drive or navigate to the location of the ArcSight SmartConnector Installer directory.

2 Start the ArcSight SmartConnector Installer by running the executable for your operating system.

When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

3 When the installation of ArcSight SmartConnector core component software is finished, the ArcSight Installer confirms successful installation and prompts you to continue with the configuration of a specific SmartConnector. On the **Install Complete** window, read the information, then click **Done**.

4 Select **ArcSight Manager** on the next screen and click **Next**.

5 The Wizard first prompts you for Manager certificate information. The default selection is **No**, the ArcSight Manager is not using a demo certificate. Choose **Yes** if ArcSight Manager is using a demo certificate. Then click **Next**.

6 The Wizard prompts for **Manager Host Name** and **Manager Port**. Enter the information and click **Next**.

7 Enter a valid ArcSight **User Name** and **Password**. This is the same user name and password you created during the ArcSight Manager installation. Click **Next**.

8 The Configuration Wizard displays a list of available SmartConnectors you can configure. Select **Mazu Profiler V3 Schema DB** and click **Next**.

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

Parameter	Description
Mazu Profiler V3 Schema Database JDBC Driver	Select the driver from the drop-down list or accept the default value of 'org.postgresql.Driver'
Mazu Profiler V3 Schema Database URL	Enter the URL for the Mazu Profiler Database (in the format: 'jdbc:postgresql://<HostName or Ip Address>:5432/<Database Name>')
Mazu Profiler V3 Schema Database User	Enter the name of the Database User with appropriate authority to access the database.
Mazu Profiler V3 Schema Database Password	Enter the password for the Database User.

10 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**.

11 Read the SmartConnector summary and click **Next**. If the summary is incorrect, click **Back** to make changes.

12 When the SmartConnector completes its configuration, click **Next**. The Wizard now prompts you to choose whether you want to run the SmartConnector stand-alone or as a service. If you choose to run the SmartConnector as a service, the Wizard prompts you to define service parameters for the SmartConnector.

When running any SmartConnector as a service on Windows, specify the file path in UNC (for example, \\10.0.111.4\xyz) and not as a network mapped drive (Z:\xyz).

13 After making your selections, click **Next**. The Wizard displays a dialog confirming the SmartConnector's setup and service configuration.

14 Click **Finish**.

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.

You can now start using the SmartConnector.

For more detailed installation instructions, see the *ArcSight ESM Installation and Configuration Guide*.

Uninstalling a SmartConnector

Before uninstalling a SmartConnector that is running as a service or daemon, first stop the service or daemon. To uninstall on Windows, open the **Start** menu. Run the **Uninstall SmartConnectors** program found under **All Programs, ArcSight SmartConnectors**. If SmartConnectors were not installed on the **Start** menu, locate the **ARCSIGHT_HOME\UninstallerData** folder and run:

```
Uninstall ArcSightAgents.exe
```

To uninstall on UNIX hosts, open a command window on the **ARCSIGHT_HOME/UninstallerData** directory and run the command:

```
./Uninstall_ArcSightAgents
```

Upgrading a SmartConnector

To locally upgrade the connector, stop the running connector and run the ArcSight SmartConnector installer. The installer prompts you for the location to install the connector. Select the location of the SmartConnector that you want to upgrade; you will receive the message "Previous Version Found. Do you want to upgrade?" Select the option to continue and upgrade the connector. The original installation will be renamed by prefacing characters to the original folder name; the upgraded connector will be installed in the location `$ARCSIGHT_HOME\current`.

You can remotely upgrade multiple SmartConnectors from the ArcSight ESM Console. See the *SmartConnector User's Guide* for remote upgrade procedures.

To rollback the connector:

- Stop the upgraded connector, which is under `current`.
- Rename the current folder to a name based upon the build version of the upgraded connector.
- Rename the old connector build folder to `current`.
- Start the connector.

Device Event Mapping to ArcSight Fields

The following table lists the mapping of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Mazu Profiler V3 Schema Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Event
ArcSight Severituy	High when Device Severity = 3; Medium when Device Severity = 2; Low when Device Severity = 1
Destination Address	ipaddr_b
Device Custom Number 1	PORTS
Device Custom Number 2	type (0 = DoS/Bandwidth Surge, 1=Worm, 2=Host Scan, 3=Port Scan, 4=Suspicious Connection, 5=New Host, 9=New Server Port, 11=Rule Based Event)
Device Custom String 1	RULE ID
Device Custom String 2	HOSTS
Device Custom String 3	NOTIFICATION
Device Product	'Profiler'
Device Receipt Time	start_time
Device Severity	alert_level
Device Vendor	'Mazu'
End Time	end_time
External ID	eid
Source Address	ipaddr_a
Start Time	start_time