



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Oracle Solaris Basic Security Module Syslog SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2009 – 2023 Open Text.

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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://www.microfocus.com/documentation/arcsight/

Contents

- Configuration Guide for Oracle Solaris Basic Security Module Syslog SmartConnector 4
- Product Overview 6
- Configuration 7
 - BSM Auditing 7
 - Overview of Audit Setup 7
 - Basic Configuration 9
 - Enabling BSM Auditing 9
 - Setting Up Classes and Events 10
 - Audit Startup 11
 - Audit Control 12
 - Audit Log File Rotation 12
 - BSM Caveats 13
 - Configuring for the Syslog SmartConnectors 13
- Installing the SmartConnector 17
 - Preparing to Install SmartConnector 17
 - Installing and Configuring the SmartConnector 17
- Device Event Mapping to ArcSight Fields 21
 - Oracle Solaris 10 and 11 BSM Mappings to ArcSight ESM Fields 21
- Send Documentation Feedback 22

Configuration Guide for Oracle Solaris Basic Security Module Syslog SmartConnector

This guide provides information for installing the SmartConnector for Oracle Solaris Basic Security Module Syslog and configuring the device for event collection.



Solaris versions 8 and 9 are no longer supported for SmartConnector installation and have been removed from connector configuration selections. If you want to continue running these versions with the SmartConnector, do not upgrade the connector. To upgrade, you must be using Solaris version 10 or later.

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:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for 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 SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

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 MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Oracle Solaris Basic Security Module (BSM) provides a security auditing subsystem. The auditing mechanism lets administrators detect potential security breaches. It performs kernel auditing and provides a device allocation mechanism for the Solaris operating system, which lets Solaris meet C2-level criteria.



Note: C2 is a security rating originally defined in the Trusted Computer System Evaluation Criteria (TCSEC), published by the United States National Computer Security Center (NCSC), commonly referred to as the Orange Book.

The BSM audit trail is written to binary files on the local system (or NFS mount). Audit records are initiated from two distinct places in Solaris—privileged user land programs (such as login) and the Solaris kernel. All security-sensitive kernel system calls generate an audit record when BSM auditing is enabled.



Note: Reading or executing privileged audit files requires administrator access.

BSM is not enabled by default under Solaris. The administrator is required to run the `bsmconv` script to set up the initial auditing environment for the system.

Configuration

BSM Auditing

For complete information about BSM auditing, see the *SunSHIELD Basic Security Module Guide*. Additional information includes "Solaris BSM Auditing" by Hal Pomeranz of Deer Run Associates (<http://www.deer-run.com/~hal/sysadmin/SolarisBSMAuditing.html>).

For complete information about the commands mentioned in this section, see Sun Microsystems *man pages section 1M: System Administration Commands*.

The **audit_syslog** plugin module for Solaris Audit, `/usr/lib/security/audit_syslog.so`, provides realtime conversion of Solaris audit data to syslog-formatted (text) data and sends it to a syslog daemon as configured in the `syslog.conf` configuration file. See the **syslog.conf(4)** man page for more information. The plugin's path is specified in the audit configuration file, **audit_control(4)**.

Messages to syslog are written when selected using the plugin option in **audit_control**. Syslog messages are generated with the facility code of LOG_AUDIT (audit in **syslog.conf(4)**) and severity of LOG_NOTICE. Audit syslog messages contain data selected from the tokens described for the binary audit log. See the **audit.log(4)** man page for more information.

Overview of Audit Setup

The following steps provide an overview setting up audit directories and understand the audit classes that need to be audited.

1. Format and partition the disks to create the dedicated audit partitions. You can use any of the following guidance to estimate disc space:
 - Assign 100 MB of space for each machine that is on the distributed system.
 - Estimate the amount of auditing that you perform and the disk space requirements at your site will be greater than this figure per machine.
2. Assign audit file systems to dedicated partitions. Each machine must have a backup audit directory on the local machine that can be used when its NFS-mounted audit file systems are not available.

3. While each machine is in single-user mode, run `tunefs -m 0` on each dedicated audit partition to reduce reserved file system space to 0%.
4. A reserved space percentage called the `minfree` limit is specified for audit partitions in the `audit_control` file. The default is 20%, and this percentage is tunable. Because this value is set by each site in the `audit_control` file, you must remove the automatically reserved file system space that is set aside by default for all file systems.
5. Set the required permissions on each of the audit directories on the audit server and make a subdirectory in each audit directory called **files**. Use `chown` and `chmod` to assign the required permissions to each audit directory and to each `files` subdirectory.
6. If using audit servers, export the audit directories using the `dfstab(4)` file.
7. Create the `audit_control` file entries for all the audit directories in the `audit_control` file on each machine, specifying the `files` subdirectory.
8. On each audit client, create the entries for the audit file systems in the `vfstab(4)` files.
9. On each audit client, create the mount point directories and use `chmod` and `chown` to set the correct permissions.

Use the following commands to configure auditing:

Utility	Task
<code>allocate(1M)</code>	Allocate a device
<code>audit(1M)</code>	Control the audit daemon
<code>audit_startup(1M)</code>	Initialize the audit subsystem
<code>audit_warn(1M)</code>	Run the audit daemon warning script
<code>auditconfig(1M)</code>	Configure auditing
<code>auditd(1M)</code>	Control audit trail files
<code>auditreduce(1M)</code>	Merge and select audit records from audit trail files
<code>auditstat(1M)</code>	Display kernel audit statistics
<code>bsmconv(1M)</code>	Enable a Solaris system to use the Basic Security Module
<code>bsmunconv(1M)</code>	Disable the Basic Security Module and return to Solaris
<code>deallocate(1M)</code>	Deallocate a device
<code>auditon(2)</code>	Manipulate auditing
<code>auditsvc(2)</code>	Write audit log to specified file descriptor
<code>sudo(1M)</code>	Generate audit log files (<code>/var/audit</code>)

Basic Configuration

1. Enable BSM and ensure that auditd is started at boot time.
 - a. Run `/etc/security/bsmconv` as root to enable auditing. See [Enabling BSM Auditing](#) for more detailed information.
 - b. Set up the `/etc/security/audit_control` file to indicate the type of auditing to be performed. See [Audit Control](#) for more information.
 - c. Reboot the system so the `c2audit` module is properly loaded and the internal audit settings are configured.
2. Set up the classes of events for which you want to generate audit records and where those records are to go. These are defined in `/etc/security/audit_control`. See [Setting up Class and Events](#) for more information

For example, to record the login events for all users, add the class `lo` to the flags: line of `/etc/security/audit_control`. The `dir:` line specifies the directory into which audit records are to be written. This is the directory name you must enter for the **praudit Output File** parameter during SmartConnector installation.



The default path for `praudit` is `/usr/sbin`. If you use another path for `praudit`, make sure that you add the location to the system `PATH` variable.

```
dir: /var/audit
flags: lo
minfree: 20
naflags: lo
```

`flags: lo` logs events regardless of whether the event was a success or a failure.

To log only failures, add a hyphen (-) in front of the class name.

Enabling BSM Auditing

Select one of the following procedures depending on your Operating System:

Enabling BSM Auditing in Solaris 10



Note: Enabling BSM on a server automatically enables the BSM feature on all of that server's clients.

1. Log in as root.
2. Bring the system into the single-user mode:

```
# /etc/telinit 1
```

3. Change to the /etc/security directory and execute the bsmconv script

```
# cd /etc/security  
# ./bsmconv
```

The script sets up a standard Solaris machine to run BSM after a reboot.

4. After the script finishes, halt the system with the telinit command.

```
# /etc/telinit 6
```

5. Reboot the system to bring it up as a multi-user BSM system.



Note: Reboot the server to restart the BSM service.

Enabling BSM Auditing in Solaris 11

Auditing is enabled by default on Solaris 11, but only user login/logout events are monitored by default. To monitor both the OS File change events and OS USER logins/logout events, you can execute the following command with root privilege:

```
# /usr/sbin/auditconfig -setflags fw,fd,fc,fm,fr,lo
```



The bsmconv command has been removed on Solaris 11. Use the audit -s command to enable the auditing feature, when required.

Setting Up Classes and Events

bsmconv creates a number of files in the /etc/security directory, including:

- The `audit_startup` script is invoked at boot time and sets a number of different audit policies for the system.
- The `audit_control` file is the primary configuration file for BSM.
- The `audit_class` and `audit_event` files can be used when more fine-grained control of the audit configuration is required.

The following sections describe the `audit_startup` and `audit_control` files, audit classes and events, and custom audit classes you might access when setting up auditing.

Audit Startup

The existence of a file with the path name `/etc/security/audit_startup` causes the audit daemon to be run automatically when the system enters multi-user mode. A default `audit_startup` script that automatically configures the event to class mappings and sets the audit policies is set up during the BSM package installation.

The `audit_startup` script is a series of `auditconfig` commands to initialize the system auditing policy:

```
#!/bin/sh
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy none
/usr/sbin/auditconfig -setpolicy +cnt
/usr/sbin/auditconfig -setpolicy +argv,arge
```

The first two lines pull configuration information out of the `audit_control` file and set up the basic events the system audits. The remaining lines set other special auditing policy options:

`-setpolicy none`

Clears audit policy so that the system starts fresh.

`setpolicy +cnt`

Indicates the system to continue running even if the auditing partition on the machine fills up. High security sites are required to have the machine shut down if auditing becomes impossible.

`-setpolicy -cnt` and `-setpolicy +argv,arge`

Tracks the full command line and all environment settings for any command executed on the system. Note that the `-setpolicy +argv,arge` line is not part of the default BSM configuration set up by the `bsmconv` script.

Audit Control

An `audit_control` file looks similar to the following:

```
dir:/var/audit
minfree:20
flags:lo,ad,pc,fm,fw,-fc,-fd,-fr
naflags:lo,ad,ex
```

`dir`

is the directory into which audit logs will be written on the . This directory must be accessible only by the superuser. You must specify this directory name required during SmartConnector installation. There is no built-in facility to write audit logs to some other system, although some sites have attempted writing to an NFS-mounted directory from some central file server. This configuration requires the client system to have root write privileges into the NFS volume, which has some significant security implications.

`minfree`

Specifies the amount of free space, as a percentage, that must exist in the auditing partition. For example, if `minfree` is set at 20, and the audit partition goes above 80% full, the auditing subsystem starts sending warning messages to the administrator

`flags` and `naflags`

Define to which audit events the system actually is going to pay attention. The `auditconfig -conf` and `auditconfig -aconf` commands in `audit_startup` looks for these flags. The two letter codes are groups or audit classes of related events or system calls defined through the `audit_class` and `audit_events` files.

The `flags` line defines the audit vector for normal user sessions on the machine. The `naflags` line catches all events that are not associated with a particular user's session. Usually, these events are the result of system processes and do not occur often.

Audit Log File Rotation

Audit logs are written to binary files in your audit directory. The file naming convention used is `<start>.<end>.<hostname>`, where `<start>` and `<end>` are time/date stamps in the format `YYYYMMDDhhmmss` and `<hostname>` is the fully-qualified hostname of the local machine. The current audit log that is actively being written is named `<start>.not_terminated.<hostname>` to distinguish it from the other audit logs in the directory.

The command `audit -n` signals the system audit daemon to close its current audit log file and start a new one. Unless told otherwise, the audit daemon will simply continue writing to the current audit log and it will grow without bound until it reaches the file size limit for the machine or fills the partition. To force audit logs to be restarted at the top of every hour:

```
0 8 8 8 8 /usr/sbin/audit -n
```

After the new audit log has been started, the old log can be compressed or moved off of the local system for archival.

BSM Caveats

- Enabling BSM automatically disables the <Stop>-A keyboard sequence on the machine. This enables you to monitor shutdown and reboot events and associate them with a particular user. Disabling <Stop>-A requires someone to log in, become root, and halt the machine, all of which are auditable events.
- Enabling BSM disables auto-mounting of CD-ROMs and floppies using `vo1d`. Again, there is an audit trail issue if a system process spontaneously mounts and dismounts file systems.
- There are known interoperability problems between OpenSSH (particularly with PrivSep enabled) and BSM. The most noticeable issue is that OpenSSH sessions will not appear in the audit logs at all. A patch[4] is available to fix this and some other issues.

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as *messages.log* rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the `/etc/rsyslog.conf` file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

```
mkfifo /var/tmp/syspipe
```

2. Add one of the following lines depending on your OS to the `/etc/rsyslog.conf` file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug | /var/tmp/syspipe
```

3. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the `/etc/rsyslog.conf` file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

3. Restart the syslog daemon in one of the following methods:
 - a. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```


Installing the SmartConnector

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

Preparing to Install SmartConnector

Before you install any SmartConnectors, make sure that the OpenText 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

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. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next**, then specify the following parameters:

Parameters	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .

- b. Click **Next**.
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, then specify the following parameters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> .
File Absolute Path Name	<p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none"> • Solaris: <code>\var\adm\messages</code> • Linux: <code>\var\log\messages</code> <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none"> • Date format log rotation: The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code> • Index log rotation: The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: <code>filename'%d,1,99,true'.log</code>; Specifying <code>true</code> indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of <code>true</code> is optional.

Parameters	Description
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension.

b. Click **Next**.

5. Select a [destination and configure parameters](#).
6. Specify a name for the connector.
7. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

8. Select whether you want to install the connector as a service or in the standalone mode.
9. Complete the installation.
10. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

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.

Oracle Solaris 10 and 11 BSM Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Connector (Agent) Severity	High = alert, Medium = failed, Low = ok
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom String 1	access info
Device Custom String 2	session
Device Custom String 3	user group
Device Custom String 4	zone name
Device Event Class ID	msg
Device Process Name	auditd
Device Product	'solaris'
Device Severity	alert failed ok
Device Vendor	'Oracle'
Device Version	'10/11'
External ID	ID
File Name	filename
File Path	path
Message	msg
Name	Both("solaris BSM",Module)
Source Address	source ip
Source Host Name	source host name
Source User Name	source user name

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 Configuration Guide for Oracle Solaris Basic Security Module Syslog SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!