Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for CA Top Secret Security for z/OS File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for CA Top Secret Security for z/OS File

October 17, 2017

Warranty

Restricted Rights Legend

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.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/16/2015	Updated Device Event Class ID mapping in TSS UTIL mappings.
11/14/2014	Updated TSS UTIL (Short Version) mappings.
05/15/2014	Added support for r15.
05/15/2012	Added new installation procedure.
09/24/2010	Support for r12 tss_audit_track events has been added.
05/26/2010	General availability of support for Top Secret r12.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
08/21/2009	Added Beta support for Top Secret r12.
06/30/2009	Added global update to installation procedure.
02/11/2009	Added configuration information.

SmartConnector for CA Top Secret Security for z/OS File

This guide provides information for installing the SmartConnector for CA Top Secret Security for z/OS File and configuring the device for log file event collection. CA Top Secret Security for z/OS releases 9, 12, and 15 are supported.

Product Overview

CA Top Secret Security for z/OS provides comprehensive security for the z/OS, z/VM, and z/VSE environments, including z/OS UNIX and Linux for zSeries. Built-in administrative and reporting tools and detailed event logging capabilities simplify management of users and their access rights.

Logging Security Events

For complete logging information, see the following eTrust CA-Top Secret product documentation, available with your product:

CA-Top Secret User Guide
CA-Top Secret Report and Tracking Guide
CA-Top Secret Command Functions Guide
CA-Top Secret Control Options Guide

An important prerequisite to the reporting and tracking of security events is the correct specification of log options. TSSUTIL and TSSTRACK can be used to build reports, but only based upon data stored in the System Management Facility (SMF) and Audit/Tracking File (ATF). See the *eTrust CA-Top Secret Report and Tracking Guide* for complete information. ArcSight recommends you log violations and activity to the Audit/Tracking File instead of, or in addition to, SMF. Security events that are logged can be selectively extracted to produce reports using the TSSUTIL batch utility.

TSSUTIL is a flexible report generator/extract utility used to provide batch reports of any security-related events logged to the Audit/Tracking file and SMF. All security events should be logged via the TSS LOG option in order to use the full range of options available with TSSUTIL. The LOG control option lets you request the type of events to be logged, specify where logging information is recorded, and choose where violation notification is to be made. The following logging options are required to record the related security information for later reporting via TSSUTIL:

`LOG(INIT,...)` requests logging of all job/session initiations and terminations
`LOG(SMF,...)` requests SMF recording of selected events.
`LOG(ACCESS,...)` requests logging of all resource access.

Logging options can be set globally by the LOG control option or by facility using the LOG sub-option of the FACILITY control options. See the *eTrust CA-Top Secret Control Options Guide* for complete information about the LOG and FACILITY control options.

Report Authority

To use TSSUTIL, an ACID must possess REPORT authority. This administrative authority might be given by anyone who has REPORT authority be entering the following command:

```
TSS ADMIN(acide) ACID(REPORT) RESOURCE(REPORT)
```

You can extract only those incidents generated for ACIDs within the scope of your authority.

Security violations always are reported in the EVENT(AUDIT) report. To obtain audited events other than security violations, you must run the EVENT(AUDIT) report and have events being audited for resources or user activity using one of the following:

```
TSS ADDTO(acid) AUDIT
TSS PERMIT(acid) resclass(resource) ACTION(AUDIT)
TSS ADDTO(AUDIT) resclass(resourcename)
TSS MODIFY FACILITY(facilityname=AUDIT)
```

The LOG Control Option

LOG identifies the types of events that eTrust CA-Top Secret will log and specifies whether the events are logged onto the ATF (Audit Tracking File), onto the SMF files (System Management Facility), or both.

The LOG option affects all facilities. A Global LOG command can be overridden by a LOG operand entered as a sub-option for a specific facility. See the *eTrust CA-Top Secret Control Options Guide* for complete information.

LOG(ACCESS), LOG(ACTIVITY), and LOG(ALL) produce a large number of records; dumping such a large volume on the Audit/Tracking File can cause excessive wrapping of the file, which, in turn, means you need a larger file.

A LOG option issued after the startup of eTrust CA-Top Secret resets not only the global LOG options, but also the LOG setting of every facility.

The LOG option is protected by the operator accountability feature. eTrust CA-Top Secret will prompt the person entering the command for the proper ACID/password combination before processing the LOG option. eTrust CA-Top Secret will also create an audit trail identifying the ACID under which the LOG specification was made.

Syntax

```
LOG(ACTIVITY,ACCESS, SMF,SEC9,INIT,MSG)
LOG(NONE)
LOG(ALL)
```

Where:

`ACTIVITY`
Logs all activity for all facilities to the SMF. This is the same as specifying: `LOG(ACCESS,INIT)`.

`ACCESS`
Logs all resource access, except for the following: DBD, FCT, JCT, LCF, OTRAN, PPT, PROGRAM, PSB.

`SMF`
Writes events to the SMF file in addition to the ATF if applicable.

`SEC9`
Routes violation summary messages to the security console.

`INIT`
Logs all job/session initiations and terminations.

`ALL`
Selects all log options for all facilities.

`NONE`
Deactivates all SMF and ATF logging, except for violations and audited events to the ATF.

The default is `LOG(SMF,INIT, SEC9, MSG)`.

Install the SmartConnector

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

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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

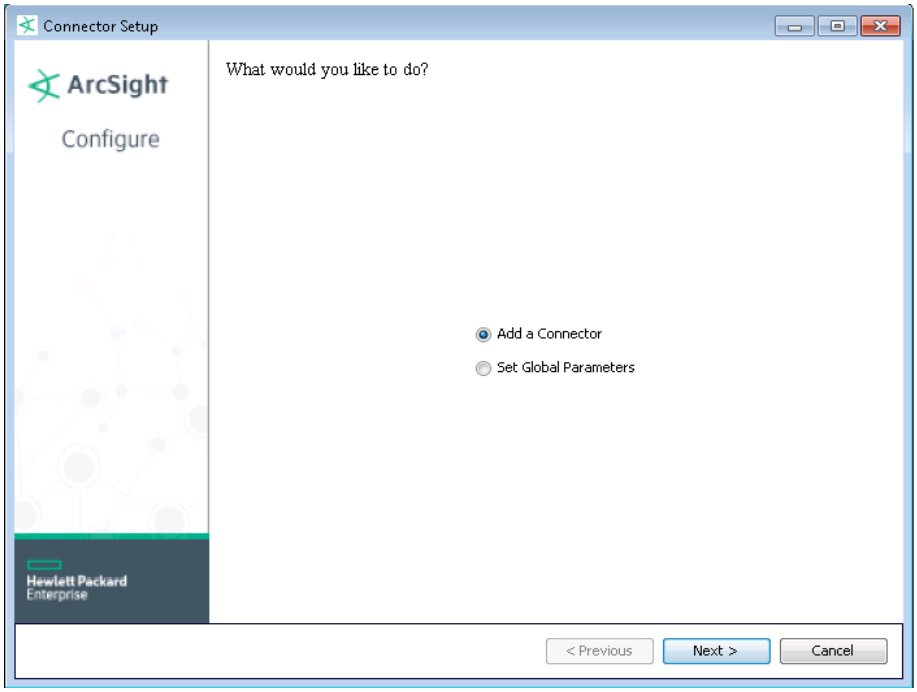
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

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. 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.

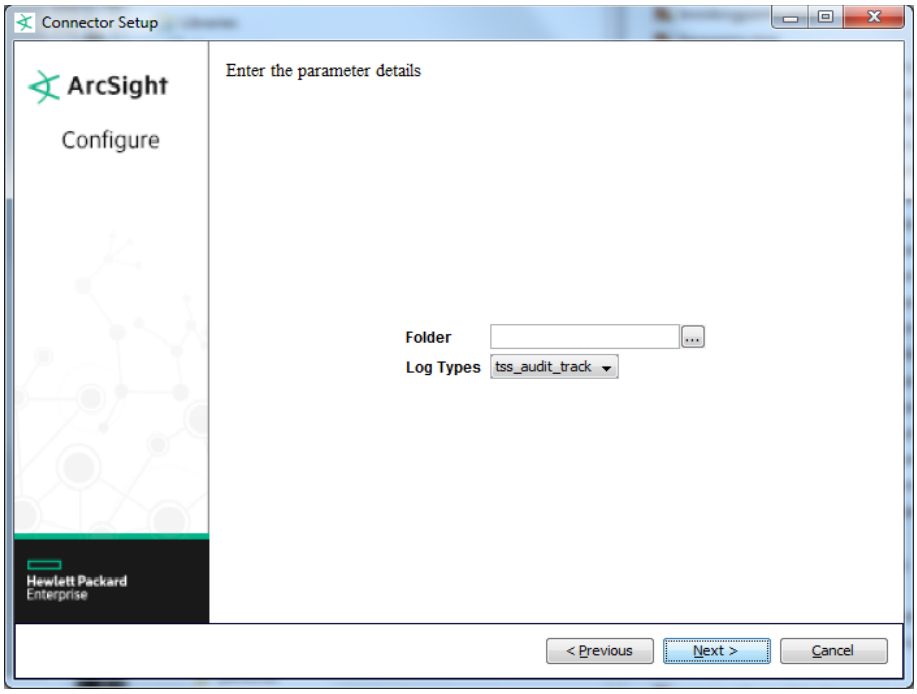
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

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 HPE 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.
Format Preserving Identity	The HPE 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 HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE 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 **CA Top Secret File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	Name of and path to the folder in which the log files are stored. This is the location specified by the LOG control option for the Audit/Tracking File or TSSUTIL Report (Short Version) File.
Log Types	Select 'tss_audit_track' for Top Secret Audit/Tracking log files; select 'tssutil_short' for TSSUTIL (Short Version) log files.

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.

TSS Audit/Tracking Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Escalation Value
Device Custom String 1	Return code or Error code
Device Custom String 2	Terminal
Device Custom String 3	Rule1
Device Custom String 4	Rule2

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Job Name
Device Custom String 6	Keyword or Function or Command
Device Event Category	MsgType
Device External ID	LPAR
Device Product	'Top Secret'
Device Receipt Time	Date
Device Vendor	'Computer Associates'
Message	SubMessage
Name	Message

TSS UTIL (Short Version) Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Process Name	RESOURCE_NAME 'JOB='
Destination User ID	RESOURCE_NAME 'ACID='
Destination User Name	RESOURCE_NAME
Device Custom Number 1	VIOLATION_COUNT
Device Custom String 1	MODE ('D=DORMANT', 'W=WARN', 'F=FAIL', 'I=IMPLEMENT')
Device Custom String 2	RESOURCE_TYPE
Device Custom String 3	RESOURCE_NAME
Device Custom String 4	SRC-DRC
Device Custom String 5	SEC
Device Custom String 6	Both (REQUESTED_ACCESS, ALLOWED_ACCESS)
Device Event Class ID	PROGRAM_NAME
Device Facility	FACILITY
Device Host Name	SYSI
Device Process Name	PROGRAM_NAME
Device Product	'Top Secret'
Device Receipt Time	TIMESTAMP
Device Vendor	'Computer Associates'
External ID	JOBID
File Name	One of (RESOURCE_NAME, RESOURCE_TYPE
File Type	One of (RESOURCE_NAME, SEC)
Name	Both (SEC, RESOURCE_TYPE)
Reason	One of (SRC-DRC, RESOURCE_TYPE, SEC)
Source Host Name	TERMINAL
Source Process Name	JOB_NAME
Source User ID	ACCESSOR