
Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.3.0

SmartConnector for CA Top Secret Security for z/OS File

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

© Copyright 2022 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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.

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.

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to [ArcSight Product Documentation Community on the Micro Focus Security Community](#).

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

SmartConnector for CA Top Secret Security for z/OS File	6
Product Overview	6
Logging Security Events	6
Report Authority	7
The LOG Control Option	7
Installing the SmartConnector	8
Preparing to Install the SmartConnector	9
Installing and Configuring the SmartConnector	9
	10
Device Event Mapping to ArcSight Fields	10
TSS Audit/Tracking Mappings to ArcSight ESM Fields	10
TSS UTIL (Short Version) Mappings to ArcSight ESM Fields	11
Send Documentation Feedback	12

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 logging file and event collection.

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 simplifies management of users and accessing their 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 the 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/ extractor utility which is used to provide batch reports for 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, specifically where logging information is recorded and, chosen where violation notification is to be made. The following logging options are required to record the related security information for reporting it later 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 the REPORT authority, and should be entering the following command:

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

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

Security violations are always 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 by 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) produces a large number of records; and dumping such a large volume on the Audit/ Tracking File can cause excessive wrapping of the file, which in turn means requirement of 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 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).

Installing 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.

Preparing to Install the SmartConnector

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

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 **CA Top Secret File** from the **Type** drop-down and click **Next**.
5. Enter the following parameters to configure the SmartConnector, then click **Next**
6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run the connector as a service or in the standalone mode.

10. Complete the installation.

11. 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.

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
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

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 CA Top Secret Security for z/OS File (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!