



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for CA SiteMinder Single Sign-on File 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 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>

Contents

- Configuration Guide for CA SiteMinder Single Sign-on File SmartConnector 4
 - Product Overview 5
 - Configuration 5
 - Configuring the Policy Server Logs 5
 - Reporting Policy Server Logging Problems to the System Log 6
 - Installing the SmartConnector 6
 - Preparing to Install the SmartConnector 7
 - Installing and Configuring the SmartConnector 7
 - Device Event Mapping to ArcSight Fields 8
 - Single Sign-on General Mappings 8
 - Single Sign-on smaccess Multiple Line Event Mappings 9
 - Single Sign-on smaccess Single Line Event Mappings 9
 - Single Sign-on smps Event Mappings10
- Send Documentation Feedback 12

Configuration Guide for CA SiteMinder Single Sign-on File SmartConnector

This guide provides information for installing the SmartConnectors for CA SiteMinder Single Sign-on File and configuring the device for log event collection.

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

CA Single Sign-On provides enterprise-class secure single sign-on (SSO) and flexible identity access management to authenticate users and control access to Web applications and portals. Across Internet, intranet and cloud applications, it helps to enable the secure delivery of essential information and applications through secure single sign-on.

Policy Server provides authentication, authorization, auditing and health monitoring. Authentication can be based on user names and passwords, using tokens, using forms based authentication, and through public-key certificates. Policy server provides authorization by managing and enforcing access control rules established by Policy Server administrators. These rules define the operations that are allowed for each protected resource. Policy Server generates log files that contain auditing information about the events that occur within the system. Policy Server provides health monitoring components.

Configuration

This section tells you how to configure the Policy Server logs and how to report Policy Server logging problems to the system log.

For complete information about CA Single Sign-on, see the technical documentation (CA Single Sign-On - Home (CA Single Sign-On - 12.52 SP1)) at <http://www.ca.com/us/collateral/technical-documents/na/ca-single-sign-on.aspx>. Under "Administrating," select Policy Server Management -> Policy Server Management Console -> Configure the Policy Server Logs. The following sections are derived from the CA Single Sign-on documentation.

Configuring the Policy Server Logs

The Policy Server log file records information about the status of the Policy Server and auditing information about authentication, authorization, and other events that can be configured in the Policy Server log file. These logs can be configured from the Management Console **Logs** tab.

- 1 Start the Policy Server Management Console.
- 2 Click the **Logs** tab.

- 3 Configure the location, roll-over characteristics, and required level of audit logging for the Policy Server log in the **Policy Server Log** and **Policy Server Audit Log** group boxes.
- 4 If the Policy Server is configured as a RADIUS server, configure the settings presented in the **RADIUS Log** group box.
- 5 Click **Apply** to save your changes.

Reporting Policy Server Logging Problems to the System Log

To prevent missing information in a production environment where debug logs are disabled, you can configure Policy Server to log information about exceptions that might occur while preparing or executing audit logs to the Unix syslog file.

To configure Policy Server for this feature, set the value of the **CategoryCount** registry key to **7**. This key is found in the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\SiteMinder
```

These events are logged under the event log categories ObjAuditLog and AccessAuditLog.

Single Sign-on calls object events are those where objects are created, updated, or deleted. Any exceptions can occur while preparing or executing Single Sign-on obj audit logs which are logged to Unix system logs under the ObjAuditLog category.

Access events result from authentication, authorization, administration, and affiliate user-related activities. Any exceptions occurred while preparing or executing Single Sign-on access audit logs are logged to Unix system logs under the AccessAuditLog category.

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 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. Select **CA SiteMinder Single Sign-on File** and click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**

Parameter	Description
Folder	Specify the folder where the log files are stored.
Wildcard	Enter a wildcard that identifies the files to process. For example, if the access log file is 'access1003o21405.log', use wildcard 'access*.log'.
Log File Type	Enter the type of log file: smps or smaccess

- 6. Select a [destination and configure parameters](#).
- 7. Specify a name for the connector.
- 8. (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.

- 9. Select whether you want to install 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 [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.

Single Sign-on General Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	RawLog
Device Product	'Single Sign-On'
Device Vendor	'Computer Associates'

Single Sign-on smaccess Multiple Line Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination FQDN	ObjectPath
Destination User Name	ObjectName
Device Action	Description
Device Custom String 1	DirectoryName
Device Custom String 2	Role
Device Custom String 3	ObjectClass
Device Custom String 4	Organization
Device Custom String 5	SessionID
Device Event Category	Category
Device Event Class ID	EventID
Device Receipt Time	Time
Message	Status
Name	EventName
Reason	StatusID
Source User Name	Username

Single Sign-on smaccess Single Line Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	AdminReject = High; AuthReject, AzReject, ValidateReject, AdminAuth, AdminChange = Medium; AuthAccept, AuthAttempt, AuthChallenge, AzAccept, AdminLogin, AdminLogout, AuthLogout, ValidateAccept, Visit, AzUnresolved, ManagementCommand = Low
Destination Host Name	HostName
Device Custom IPv6 Address 2	Source IPv6 Address
Device Event Category	Category
Device Event Class ID	EventType

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	Time
Device Severity	EventType
Name	EventType
Reason	Reason (0 = None, 1 = PwMustChange, 2 = InvalidSession, 3 = RevokedSession, 4 = ExpiredSession, 5 = AuthLevelTooLow, 6 = UnknownUser, 7 = UserDisabled, 8 = InvalidSessionId, 9 = InvalidSessionIp, 10 = CertificateRevoked, 11 = CRLOutOfDate, 12 = CertRevokedKeyCompromised, 13 = CertRevokedAffiliationChange, 14 = CertOnHold, 15 = TokenCardChallenge, 16 = ImpersonatedUserNotInDi, 17 = Anonymous, 18 = PwWillExpire, 19 = PwExpired, 20 = ImmedPWChangeRequired, 21 = PWChangeFailed, 22 = BadPWChange, 23 = PWChangeAccepted, 24 = ExcessiveFailedLoginAttempts, 25 = AccountInactivity, 26 = NoRedirectConfigured, 27 = ErrorMessageIsRedirect, 28 = Tokencode, 29 = New_PIN_Select, 30 = New_PIN_Sys_Tokencode, 31 = New_User_PIN_Tokencode, 32 = New_PIN_Accepted, 33 = Guest, 34 = PWSelfChange, 35 = ServerException, 36 = UnknownScheme, 37 = UnsupportedScheme, 38 = Misconfigured, 39 = BufferOverflow)

Single Sign-on smps Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	ERROR = Medium; INFO, DEBUG = Low
Device Custom Number 1	Tid (Transaction ID)
Device Custom Number 2	Session
Device Custom String 5	Object Type
Device Custom String 6	Object Name
Device Event Class ID	SourceFile
Device Product	'Single Sign-On'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'Computer Associates'
File Name	SourceFile

ArcSight ESM Field	Device-Specific Field
Name	Msg
Source Host Name	sm-Server
Source Process ID	Pid

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 CA SiteMinder Single Sign-on File 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!