Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for CA SiteMinder Single Sign-on File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for CA SiteMinder Single Sign-on 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.
03/31/2016	First edition of this Configuration Guide.

Contents

SmartConnector for CA SiteMinder Single Sign-on File

This guide provides information for installing the SmartConnectors for CA SiteMinder Single Sign-on File and configuring the device for log event collection. CA Single Sign-on versions 12 and 12.5 are supported.

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 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.

Configure 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.

Report 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 when objects are created, updated, or deleted. Any exceptions occurred while preparing or executing Single Sign-on obj audit logs 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.

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.

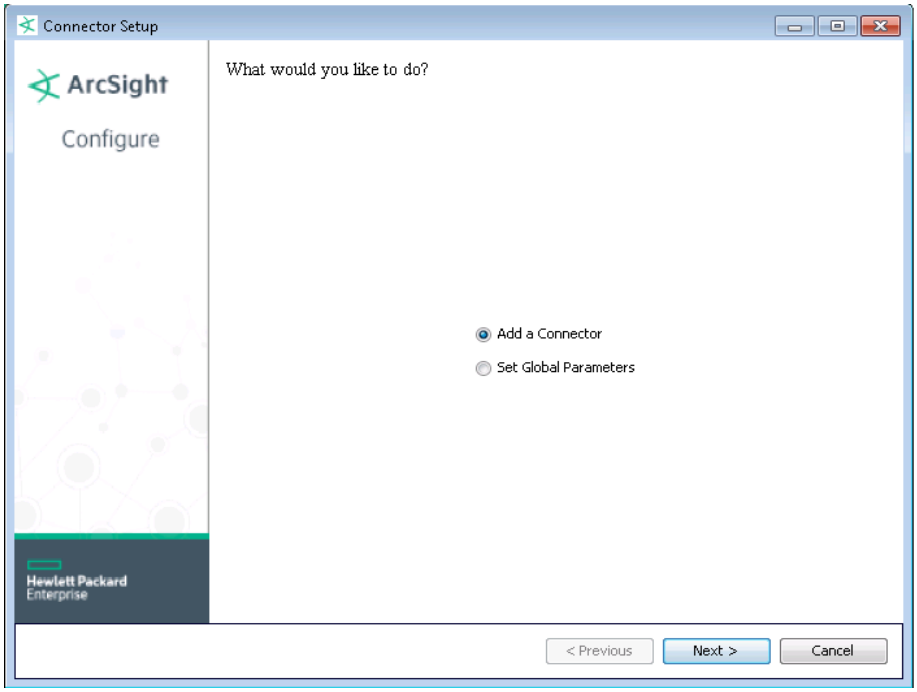
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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'.

Parameter	Setting
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.

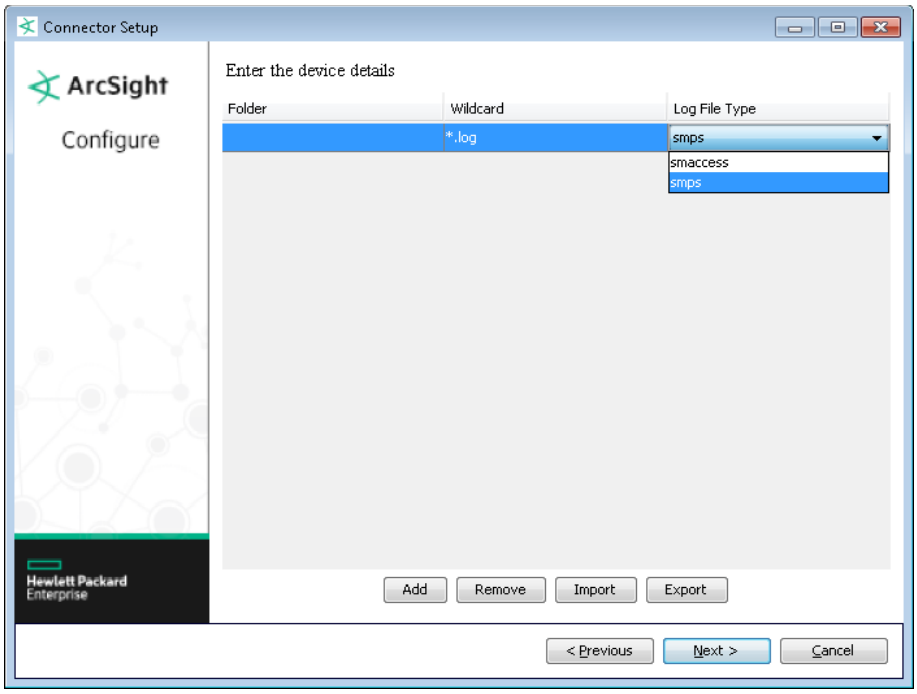
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

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 SiteMinder Single Sign-on File** and click **Next**.
3. 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

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.

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
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
Name	Msg
Source Host Name	sm-Server
Source Process ID	Pid