HP Operations Orchestration

For the Windows and Linux operating systems

Software Version: CP14 (9.x)

HP ArcSight Integration Guide

Document Release Date: May 2014

Software Release Date: May 2014

Legal Notices

Warranty

The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

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, which indicates the software version.
- 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: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Introduction

This chapter includes:

About the HP ArcSight Integration

This integration enables administrators to create HP Operations Orchestration (OO) flows that are integrated with ArcSight. To learn how to create OO flows, see the Studio Guide to Authoring Operations Orchestration Flows in the documentation set for the current OO release. The HP ArcSight integration uses the ArcSight ESM REST API to integrate with OO. The API is accessed through the generic **Retrieve ArcSight Information** operation, by executing HTTP GET methods according to the specifications in the HP ArcSight documentation.

Audience

This guide is intended for system administrators who establish and maintain the implementation of integration between HP ArcSight and HP OO. This guide assumes that you have administrative access to OO, and user access to an ArcSight system.

Prerequisites

To use this integration successfully, you should have basic knowledge of the ArcSight Enterprise Security Management (ESM), the ESM REST API used by the integration, and consuming REST Services.

Supported Versions

Operations Orchestration Version	ArcSight Version
OO Content Pack 14	6.0c, 6.5c

Downloading OO Releases and Documents on HP Live Network

HP Live Network provides an Operations Orchestration Community page where you can find and download supported releases of OO and associated documents.

Note: The Community page requires that you register for an HP Passport and sign-in.

To register for an HP Passport ID:

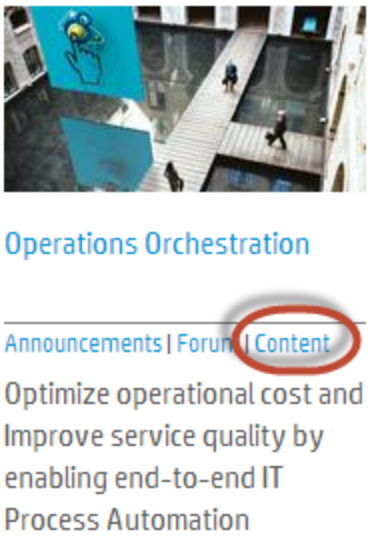
Go to: http://h20229.www2.hp.com/passport-registration.html

Or

Click the **New users - please register** link on the HP Passport login page

To download OO releases and documents:

1. Go to the HPLN site: https://hpln.hp.com/. Page 1 of HP Live Network page opens.
2. Go to page 2 and click the **Content** link under **Operations Orchestration**.



3. From the **Content Catalog** tab, select **Operations Orchestration Content Packs**.
4. Select the Downloads link.

5. Click **Downloads > HP Operations Orchestration 9.00**.
6. Click on HP Operations Orchestration Content Pack 14.

Getting Started

This chapter includes:

What You Need to Know About ArcSight Before Using the Integration

HP ArcSight Enterprise Security Manager (ESM) is the premiere security event manager that analyzes and correlates every login, logoff, file access, database query, or other event in order to support your IT team in every aspect of security event monitoring, from compliance and risk management to security intelligence and operations. The ArcSight ESM event log monitor sifts through millions of log records to find the critical events that matter, and presents them in real time via dashboards, notifications, and reports, so you can accurately prioritize security risks and compliance violations.

To gather information from an available ArcSight server, the generic **Retrieve ArcSight Information** operation can be used and adapted to address specific needs. The operation enables executing a REST HTTP GET request to the specified ArcSight server, to retrieve information in either JSON or XML format. The operation requires specifying an ArcSight <module name> (either core-service or manager-service), a <service name> (the name of the service that exposes the operation to execute), and an <operation name> (the actual operation to call).

After setting up your development environment, you will next want to know the services available for consumption. You do this by displaying the **listServices** file provided by a module. To view the **listServices** file:

Open your browser and enter the URL with the following format:
`https://<HOST>:<PORT>/www/<MODULE>/services/listServices`

For example: `https://arcSight.hp.com:8443/www/manager-service/services/listServices`

The list of services also includes the names of operations available for each service. For example, **ConnectorService** exposes the **getAgentByName** method for retrieving the details of the connector resource with the given name.

Some ArcSight operations may require passing specific parameters, as query parameters in the request URL. To identify the parameters associated to an operation, execute an HTTP OPTIONS request to the following URL:

https://<HOST>:<PORT>/www/<MODULE>/rest/<SERVICE>/<OPERATION>

For example: `https://arcSight.hp.com:8443/www/manager-service/rest/ConnectorService/getAgentByName`

The response to the above request specifies that the **getAgentByName** operation requires a parameter called **name**, besides the **authToken** parameter that is common to all operations and is handled implicitly by the generic operation. The value for the **name** parameter can be passed to the generic operation by adding an extra input with the same name. To call the **getParameterGroups** operation exposed by the same service, perform the following:

1. Identity the names of parameters required by the operation by executing an HTTP OPTIONS request to **https://arcSight.hp.com:8443/www/manager-service/rest/ConnectorService/getParameterGroups**

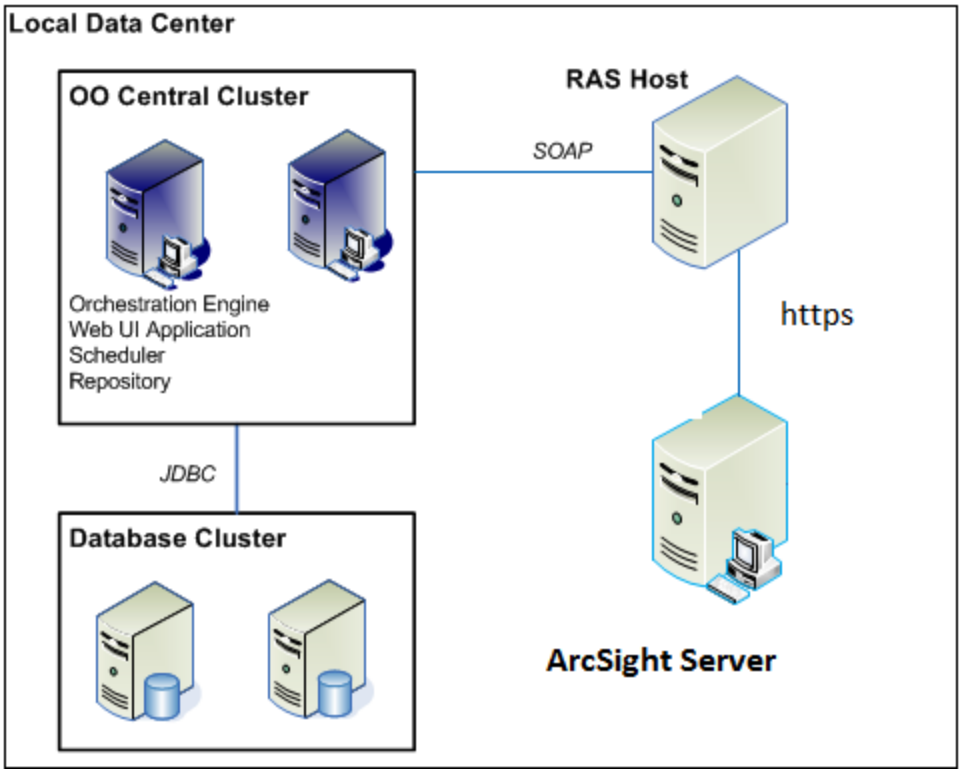
2. In the step(s) using the generic operation to execute the call, add inputs for each of the parameters specific to this operation. For the example function, add an input named **agentId** to pass the value of a connector's ID. Also add a second input, called **agentConfigIndex**, to specify the configuration's index. As explained above, no input is needed for the **authToken** parameter, as this will be obtained and passed in the operation's code.

Use Cases

The following are the major use cases for the ArcSight integration, and the operations that you can use to implement them.

1. Samples:
   - Get Connector Commands
   - Get Connector Details
   - List Connectors
2. Retrieve ArcSight Information

ArcSight — OO Architecture



ArcSight Terminology

The following terms are used in the ArcSight Integration Guide.

ESM. ArcSight™ Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

Module. ESM Service Layer groups services in two service modules:

- **Core Service module.** This module provides login services (**loginService**) by returning the authentication token (**authToken**) needed to begin consuming a service. The services are designed to be stateless. You will therefore pass the authentication token every time you consume a service.
- **Manager Service module.** This module provides the ESM functionality, for example, Connector Service.

Authentication Token. An authentication token is the first requirement for accessing ESM Service Layer to obtain service information and then consume the services. The ArcSight-OO integration does not require the user to explicitly handle the authentication token request. This is performed behind the scenes by the generic operation, which only requires providing ArcSight access credentials.

Certificates. SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol (over port 443), allowing secure communication between a web server and a client. Once the organization installs the SSL certificate onto its web server, secure connections can be established over https and traffic between the web server and the client will be secure.

Certificate Authority (CA). An entity which issues digital certificates for use by other parties. It is an example of a trusted third party.

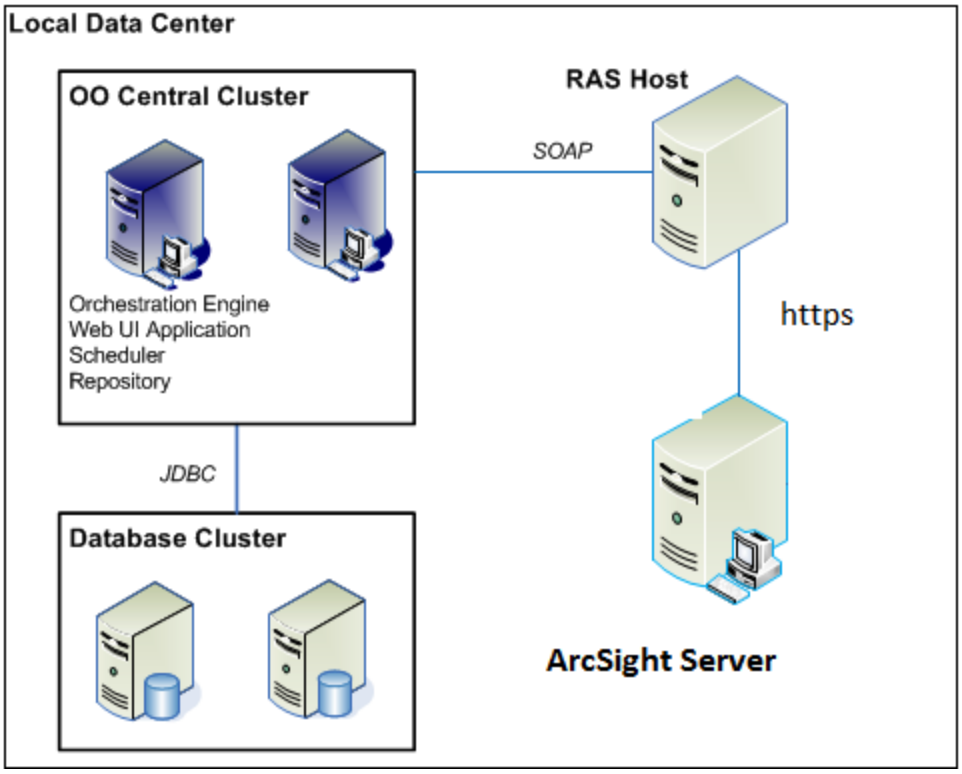
ArcSight Interfaces You May Need to Access

When using the ArcSight - OO integration, you may need to access the following interface: ArcSight ESM REST API.

The ArcSight ESM REST API enables accessing the ESM Web Services. A client application based on the API can retrieve information associated to the existing ESM resources. Without any coding, browsers can also be used as clients to read information from ESM.

Location of ArcSight Integration Operations and Flows in OO Studio

The ArcSight integration includes the following operations and flows in the OO Studio Library/Integrations/Hewlett-Packard/ArcSight folder.


Local Data Center
OO Central Cluster
Orchestration Engine
Web UI Application
Scheduler
Repository
JDBC
Database Cluster
RAS Host
SOAP
https
ArcSight Server

Troubleshooting

This chapter includes:

Troubleshooting Overview

This section provides troubleshooting procedures and tools that you can use to solve problems you may encounter while using this integration. It also includes a list of the error messages you may receive while using the integration and offers descriptions and possible fixes for the errors.

General Troubleshooting Procedures and Tools

This section describes the troubleshooting procedures and tools you can use to fix problems that you may experience while using this integration.

The most common problems you may encounter are inadequately requesting ArcSight resource information (by providing incorrect credentials, using invalid certificates, adding invalid inputs used as query parameters to compose the URL, and so on). To eliminate such causes for error, ensure that you do not experience the same behavior by making the request from a browser as client. For example, if the OO flow you are running returns a **FailureMessage** such as

```
java.io.IOException: Server returned HTTP response code: 500 for URL:
https://arcSight.hp.com:8443/www/manager-
service/rest/QueryService/findByUUID?id=%5B%2B9mApQ4BABDUCa64-
xeRwg%3D%3D&authToken=XXPlOIWTLU1phnB-JAi2vt8x46UGWZp99qcOn6772bA.
```

when trying to obtain the details of a query resource having the given ID, try executing an HTTP GET from your browser to the URL returned in the **FailureMessage** output. If you receive the same error code, the resource you requested does not exist, and the behavior of the OO flow is as expected.

Security

This section describes how security is handled by the ArcSight integration.

ArcSight 6.0c servers are accessed via REST over HTTPS. The user provides logon credentials for connecting to ArcSight, through the REST API, and the operation will handle the obtaining of an authentication token that must further be used when executing requests. The services that ArcSight exposes are designed to be stateless, therefore the authentication token will be passed when the operation makes a second request, to actually consume the needed service. The username and password must be defined in the ArcSight system, and represent actual users of ArcSight.

All exposed ESM services are TLS/SSL-secured. Therefore, the following inputs are available for managing the SSL certificates:

- trustAllCertificates
- keyStore
- keyStorePassword
- trustStore
- trustStorePassword

By default, weak security over SSL is disabled due to security reasons. To successfully use the ArcSight operations, either set trustAllCertificates to **true**, or import the ArcSight ESM Manager's certificate into your development/runtime environment. The certificate option was chosen during ArcSight ESM installation. It could be a temporary certificate authority (CA), a self-signed certificate, or a signed certificate from a trusted CA. Ask your ArcSight administrator about which certificate option was chosen during installation and import that certificate (either into your development JRE at **jre/lib/security/cacerts**, or to a different location).

OO Tools You Can Use with the ArcSight – OO Integration

Following are OO tools that you can use with the ArcSight integration:

- **RSFlowInvoke.exe and JRSFlowInvoke.jar**

  RSFlowInvoke (RSFlowInvoke.exe or the Java version, JRSFlowInvoke.jar) is a command-line utility that allows you to start a flow without using Central (although the Central service must be running). RSFlowInvoke is useful when you want to start a flow from an external system, such as a monitoring application that can use a command line to start a flow.

- **Web Services Wizard (wswizard.exe)**

  When you run the Web Services Wizard, you provide it with the WSDL for a given Web service. The WSDL string you provide as a pointer can be a file's location and name or a URL. The Web Services Wizard displays a list of the methods in the API of the Web service that you specify. When you run the wizard, pick the methods you want to use, and with one click for each method you have selected, the wizard creates an HP OO operation that can execute the method. This allows you to use the Web Services Wizard to create operations from your monitoring tool's API.

These tools are available in the Operations Orchestration home folder in **/Studio/tools/**.


Java™
COMPATIBLE