



Hewlett Packard
Enterprise

Release Notes

HPE IdentityView 2.52

ArcSight ESM and ArcSight Express

January 22, 2015

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HPE 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

© Copyright 2015 Hewlett Packard Enterprise Development LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

Contact Information

Phone	A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page: www.hpe.com/software/support/contact_list
Support Web Site	www.hpe.com/software/support
Protect 724 Community	https://www.protect724.hpe.com

Contents

- IdentityView 2.52 5**
 - What's New in IdentityView 5
 - Requirements 5
 - Connector Requirements 6
 - Large Number of Actors Requirements 6
 - Release Contents 6
 - Limitations 7
 - Installing IdentityView 7
 - Performance Impact of IdentityView 8
 - Open Issues in this Release 8
 - Open Issues for Systems with a Large Number of Actors 9

IdentityView 2.52

These release notes discuss the following topics.

["What's New in IdentityView" on page 5](#)

["Requirements" on page 5](#)

["Release Contents" on page 6](#)

["Limitations" on page 7](#)

["Installing IdentityView" on page 7](#)

["Performance Impact of IdentityView" on page 8](#)

["Open Issues in this Release" on page 8](#)

In the past, IT security professionals were predominantly concerned with protecting their assets by keeping unauthorized individuals out of their networks. Today, they must continue to protect their assets while granting access to a wide range of different individuals. Full-time and part-time employees, contractors, partners, and customers all require varying levels of access to resources. Managing the proper level of access for all individuals is challenging even in the simplest network environments.

The ArcSight IdentityView solution provides the ability to correlate identity information maintained in your Identity Management System with the events generated in your network.

What's New in IdentityView

IdentityView 2.52 provides support for updated versions of the following connectors:

- Actor Model Import FlexConnector
- Actor Model Import Connector for Microsoft Active Directory

The IdentityView solution content has **not** been updated for this release.

Requirements

IdentityView 2.52 is supported on:

- ArcSight ESM 5.2 or later
- ArcSight Express 4.0 with CORR-Engine or later

Connector Requirements

IdentityView 2.52 requires at least one of the following:

- Actor Model Import Connector for Microsoft Active Directory, version 7.0.7.7288.0 or later.
- Actor Model Import FlexConnector, version 7.0.7.7289.0 or later.

Support for Windows events in IdentityView 2.52 is provided by the Microsoft Windows Event Log – Unified SmartConnector. All of these connectors must be version 5.2.4.6326 or later, and be configured to use parser version 1. If you need to use parser version 0, you will need to install (or continue to use) IdentityView 2.0 SP1. For information about reconfiguring the connector to use a different parser version, see the Security Event Mappings - SmartConnectors for Microsoft Windows Event Log - Unified With Parser Version 1 Guide.

Large Number of Actors Requirements

ArcSight ESM systems with a large number of actors require more than the minimum system requirements described in the *ESM Installation and Configuration Guide*. 500,000 actors introduces a significant load on ESM. Use only high-level, enterprise grade hardware for ESM systems with a large number of actors.

Release Contents

The files included in this release are:

File name	Description
IdentityView Solution Content:	
ESM_IDView_RelNotes_2.52.pdf	IdentityView 2.52 Release Notes—Product description and open issues (this document).
ESM_IDView_SolutionGuide_2.5.pdf	IdentityView 2.5 Solution Guide—Product architecture, installation, configuration, and operation instructions.
ArcSight-SolutionPackage-IdentityView.2.5.1269.0.arb	<p>The installation package bundle for all operating systems. Contains all the resources for the IdentityView content package.</p> <p>The IdentityView content package has not been updated for this release.</p> <p>Note: If you use Internet Explorer to download the ARB file, it might convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing into ESM.</p>

File name	Description
Actor Model Import Connector for Microsoft Active Directory:	
ActiveDirectory_MICRelNotes_7.0.7.7288.pdf	Actor Model Import Connector for Microsoft Active Directory Release Notes—Product description and open issues.
ActiveDirectory_ActorModelConfig_7.0.7.7288.pdf	Actor Model Import Connector for Microsoft Active Directory Installation and Configuration Guide.
ArcSight-7.0.7.7288.0-ADActorModelConnector-Linux64.bin	Installer for Linux 64-bit systems.
ArcSight-7.0.7.7288.0-ADActorModelConnector-Win64.exe	Installer for Windows 64-bit systems.
Actor Model Import FlexConnector:	
FlexDbActor_RelNotes_7.0.7.7289.pdf	Actor Model Import FlexConnector Release Notes—Product description and open issues.
FlexDbActor_Config_7.0.7.7289.pdf	Actor Model Import FlexConnector Developer's Guide—Overview, installation, configuration, and parser template information.
ArcSight-7.0.7.7289.0-FlexDBActorModelConnector-Linux64.bin	Installer for Linux 64-bit systems.
ArcSight-7.0.7.7289.0-FlexDBActorModelConnector-Win64.exe	Installer for Windows 64-bit systems.

Limitations

IdentityView is limited to:

- 500,000 actors per ArcSight Manager on ArcSight ESM 6.0c or later, using the Actor Model Import Connector for Microsoft Active Directory version 7.0.7.7288 or later, with an average of 10 roles and 10 accounts for each actor.

Systems under a high load will experience slow performance in channels, query viewers, and reports, and in some cases, a reduced EPS rate. The ArcSight Console might also become unresponsive. To resolve these issues, close all open active channels, query viewers, and dashboards, and restart the consoles that are not responding. If the issues persists, consider upgrading the underlying hardware.

- 50,000 actors per ArcSight Manager on ArcSight ESM 5.2 or later (Oracle)
- 2,500 actors per ArcSight Express appliance

IdentityView does not support the Actor Category Model.

Installing IdentityView

For installation, configuration, and upgrade instructions, see the *IdentityView 2.5 Solution Guide*.

Performance Impact of IdentityView

ArcSight solution packages contain data monitors and rules that can place an additional load on the ArcSight Manager, which may impact the ArcSight Manager performance. If your ArcSight system is operating at an average event per second (EPS) rate that has maximized the CPU utilization, you might experience a reduced average EPS rate after installing the IdentityView package. If this performance impact occurs, HP recommends that you disable data monitors and rules in use cases that you do not need to reduce the load on the ArcSight Manager.



If your ArcSight system is not operating at an average event per second (EPS) rate that has maximized the CPU utilization, you should not notice an EPS rate decrease.

For additional performance impact issues, see [“Open Issues for Systems with a Large Number of Actors” on page 9](#).

Open Issues in this Release

The following issues are open in this release.

Number	Description
ESM-47612	<p>Queries that have selects or conditions on actor roles report duplicate rows and incorrect event counts if the actor has more than one role.</p> <p>Workaround: Select distinct rows in the queries to eliminate duplicate rows. To get the number of events, count the number of distinct event IDs.</p>
SOL-2232	<p>If a single user has multiple (identical) accounts on distinct ADs, when these accounts are imported from their Identity Management Systems using multiple Active Model Import connectors, these accounts are not merged into a single actor.</p> <p>Workaround: None. For more information about this issue, see the release notes for your SmartConnector for Actor Model Import.</p>
SOL-2439	<p>When running reports that invoke queries that support multiple parameters, specifying multiple values results in empty reports. For example, when running the Failed Privileged User Logins for Role report, if you specify two roles, the returned report is empty.</p> <p>Workaround: Run the report multiple times and enter a single value.</p>
SOL-3538	<p>The following query viewer does not return data. Do not run the query viewer; it creates an unnecessary load on the system.</p> <p>/All Query Viewers/ArcSight Solutions/IdentityView 2.5/Actor Attribution by IP Address/Source and Destination Subnets for Actor Logins</p>
SOL-3526	<p>On high EPS systems, some query viewers might not return data when running for over 24 hours.</p> <p>Workaround: Edit the query viewer and change the interval to one hour by setting the Start Time and End Time parameters, and set the Query Time Out field to 60 minutes.</p>
SOL-3515	<p>Some query viewer drilldowns fail with the error Cannot perform drilldown because drill down columns are removed from dependent resources.</p> <p>Workaround: Select all of the fields in the query viewer row before using the drilldown.</p>

Open Issues for Systems with a Large Number of Actors

The following issues occur on ArcSight ESM systems with a large number of actors:

Number	Description
SOL-3525	<p>Deleting the entire IdentityView Actor group from the ArcSight Console takes a long time, locks the console, and might never complete.</p> <p>Workaround: Delete the actors manually, as follows:</p> <ol style="list-style-type: none"> 1 SSH to the ArcSight Manager as the <i>arcsight</i> user. 2 Add the following line to the <code>server.properties</code> file in <code>/opt/arcsight/manager/config</code>: <code>dbconmanager.provider.logger.pool.maxcheckout=36000</code> 3 In the ArcSight Console, stop the Actor Model Import Connector for Microsoft Active Directory. Right-click the connector and choose Send Commands > Model Import Connector > Stop. 4 Stop the ArcSight Manager. 5 Delete the actor data from the database. Run the following command in <code>/opt/arcsight/logger/current/arcsight/bin</code>: <code>./mysql -u <username> -p<password></code> <code><username></code> and <code><password></code> are the database user name and password set when you configured the database, typically by using the First Boot Wizard. Per MySQL conventions, omit the space between <code>-p</code> and the password. In the resulting MySQL prompt, enter the following MySQL instructions: <pre>use <ESM database name>; delete from arc_actor; delete from arc_resource where resource_type=56; delete from arc_sld_res56B_DN; delete from arc_sld_res56B_UUID; delete from arc_sld_res56D_BASE; delete from arc_sld_res56D_ROLES; delete from arc_sld_res56B_ACCTS; delete from arc_sld_res56D_ACCTS; commit; quit;</pre> <p>If any of the delete commands fail with the SQL message <code>ERROR 1205 (HY000): Lock wait timeout exceeded; try restarting transaction</code>, retry the delete command after a few seconds.</p> 6 Start the ArcSight Manager. 7 From the ArcSight Console, delete any remaining actors from the IdentityView Actor group. 8 On the machine where the Actor Model Import Connector for Microsoft Active Directory is installed, delete the following files from <code>/user/agent/agentdata</code>: <code>*.ps</code> files <code>*status.init</code> files 9 Restart the Actor Model Import Connector for Microsoft Active Directory.
SOL-3519	<p>The search feature in the ArcSight Console might fail to find specific actors. In systems with more than 300,000 actors, the search might also fail to find other resources.</p> <p>Workaround: Use query viewers to search for actors or other resources.</p>

SOL-3539	Systems with 500,000 actors might experience JVM Full GC (garbage collection) pauses up to 45 seconds every 40 minutes, during which the ESM system might become unresponsive. The length and frequency of these pauses depend on the hardware being used.
----------	--
