Micro Focus Security ESM IdentityView

Software Version: 2.60

Release Notes

Document Release Date: January 31, 2019
Software Release Date: January, 2019

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

Follow this link to see a complete statement of copyrights and acknowledgements:
https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

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

Contents

IdentityView 2.60 Release Notes

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 this Release

IdentityView 2.60 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.

System Requirements

For instructions on installation, upgrade, and operation of IdentityView, consult the ESM IdentityView 2.60 Solutions Guide.

ESM Requirements

IdentityView 2.60 is supported on:

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

Connector Requirements

IdentityView 2.60 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 2.60 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.

Requirements for Large Number of Actors

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.

Files in this Release

ESM_IdentityView_RelNotes_2.60.pdf	IdentityView 2.60 Release Notes— Product description and open issues (this document).
ESM_IDView_SolutionGuide_2.60.pdf	IdentityView 2.60 Solution Guide— Product architecture, installation, configuration, and operation instructions.
ArcSight-SolutionPackage-IdentityView.2.6.0.arb	The installation package bundle for all operating systems. Contains all the resources for the IdentityView content package. The IdentityView content package has not been updated for this release. 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

Known Limitations

- 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

Open Issues

This release contains the following open issues.

Issue	Description
ESM-47612	Queries that have selects or conditions on actor roles report duplicate rows and incorrect event counts if the actor has more than one role. Workaround: Select distinct rows in the queries to eliminate duplicate rows. To get the number of events, count the number of distinct event IDs.
SOL-2232	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. Workaround: None. For more information about this issue, see the release notes for your SmartConnector for Actor Model Import.
SOL-2439	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. Workaround: Run the report multiple times and enter a single value.
SOL-3538	The following query viewer does not return data. Do not run the query viewer; it creates an unnecessary load on the system. /All Query Viewers/ArcSight Solutions/IdentityView 2.60/Actor Attribution by IP Address/Source and Destination Subnets for Actor Logins
SOL-3526	On high EPS systems, some query viewers might not return data when running for over 24 hours. 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.
SOL-3515	Some query viewer drilldowns fail with the error Cannot perform drilldown because drill down columns are removed from dependent resources. Workaround: Select all of the fields in the query viewer row before using the drilldown.

Open Issues for Systems with a Large Number of Actors

This release contains the following open issues for ArcSight ESM systems with a large number of actors.

Key	Description

SOL-3525	Deleting the entire IdentityView Actor group from the ArcSight Console takes a long time, locks the console, and might never complete. Workaround: Delete the actors manually, as follows:
	1. SSH to the ArcSight Manager as the arcsight user.
	2. Add the following line to the server.properties file in `/opt/arcsight/manager/config:`
	`dbconmanager.provider.logger.pool.maxcheckout=36000`
	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 `/opt/arcsight/logger/current/arcsight/bin:`
	`. /mysql -u <username> -p<password>`
	<username> and <password> 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 -p and the password.
	In the resulting MySQL prompt, enter the following MySQL instructions:
	`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;`
	If any of the delete commands fail with the SQL message
	ERROR 1205 (HY000): Lock wait timeout exceeded;
	try restarting transaction, retry the delete command after a few seconds.
	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 `/user/agent/agentdata`:
	`*.ps files`
	`*status.init files`
	9. Restart the Actor Model Import Connector for Microsoft Active Directory.

SOL-3519	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. Workaround: Use query viewers to search for actors or other resources

Key	Description
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.

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 Release Notes (IdentityView 2.60)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!