Micro Focus Security ArcSight Real-time Threat Detection

Software Version: 8.0

Administrator's Guide

Document Release Date: March 2023
Software Release Date: March 2023

Legal Notices

Copyright Notice

Trademark Notices

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://www.microfocus.com/documentation/arcsight/

Contents

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Chapter 2: Basic Configuration Tasks

Many configuration options are not available in Real-time Threat Detection for SaaS. For further configuration details, contact your administrator.

Configuring Asset Aging

Note: Configuration options are not available in Real-time Threat Detection for SaaS. For further configuration details, contact your administrator.

The age of an asset is defined as the number of days since it was last scanned or modified. So, for example, if an asset was last modified 29 hours ago, the age of the asset is taken as 1 day and the remaining time (5 hours, in our example) is ignored in the calculation of the asset's age. You can use asset aging to reduce asset confidence level as the time since the last scan increases.

Note: Only the assets belonging to the following categories are considered for aging:

- /Site Asset Categories/Scanned/Open Ports
- /Site Asset Categories/Scanned Vulnerabilities

Customizing Product Image on Login Screen and Navigation Bar in the Real-time Threat Detection Command Center

You can add your own product images to the Real-time Threat Detection Command Center login page (up to four images) and to the top left of the navigation bar.

Note: Customization options are not available in Real-time Threat Detection for SaaS. For further customization details, contact your administrator.

Appendix 3: Troubleshooting

The following information may help solve problems that occur while operating the ArcSight system. In some cases, the solution can be found here or in specific ArcSight documentation, but Customer Support is available if you need it.

If you intend to have Customer Support guide you through a diagnostic process, prepare to provide specific symptoms and configuration information.

ArcSight Console Troubleshooting

Can't log in with any Console

Check that the Manager is up and running. If the Manager is not running, start it.

If the Manager is running, but you still can't log in, suspect any recent network changes, such as the installation of a firewall that affects communication with the Manager host.

Can't log in with a specific Console

If you can log in from some Console machines but not others, focus on any recent network changes and any configuration changes on the Console host in question.

Console cannot connect to the Manager

If you start an ArcSight Console that could previously connect to the Manager with no trouble, but now it can't, see if the error is similar to:

"Couldn't connect to manager - improper authorization setup between client and manager."

If so, it's likely that the manager has been reconfigured in such a way that it now has a new certificate. Especially if the Console asked you to accept a new certificate when you started it. To fix this, find and delete the certificate that the Console was using before, and then manually import another certificate from the Manager.

Console out of memory

If your ArcSight Console is so busy that it runs out of memory, change the memory settings in the `console.bat` or `console.sh` file. This file (for Windows or Linux, respectively) is located in the directory in which you installed the ArcSight Console, in `Console/current/bin/scripts`.

Find the line that starts with `set ARCSIGHT_JVM_OPTIONS=`
Find the parameter `–Xmx512m` (Xmx controls the maximum JVM memory).
Change the value to 1024: `–Xmx1024m`.
Restart the Console for the new setting to take effect.

Acknowledgement button is not enabled

The Acknowledgement button is enabled when there are notifications to be acknowledged and they are associated with a destination that refers to the current user. To enable the button, add the current user to the notification destination.

The grid view of live security events is not visible

To restore the standard grid view of current security events, select **Active Channels** from the Navigator drop-down menu. Double-click **Live**, found at `/Active channels/Shared/All Active channels/ArcSight System/Core/Live`

The Navigator panel is not visible

Press **Ctrl+1** to force the Navigator panel to appear.

The Viewer panel is not visible

Press **Ctrl+2** to force the Viewer panel to appear.

The Inspect/Edit panel is not visible

Press **Ctrl+3** to force the Inspect/Edit panel to appear.

Internal ArcSight events appear

Internal ArcSight events appear to warn users of situations such as low disk space for the ArcSight Database. If you are not sure how to respond to a warning message, contact Customer Support.

The Manager Status Monitor reports an error

The Console monitors the health of the Manager and the ArcSight Database. If a warning or an error occurs, the Console may present sufficient detail for you to solve the problem. If not, report the specific message to Customer Support.

Console logs out by itself

Check the Console log file for any errors. Log in to the Console. If the Console logs out again, report the error to Customer Support.

Duplicate audit events or rule actions after a crash recovery

When you stop Real-time Threat Detection, it takes a checkpoint of the rules engine so that it knows where it stopped. If Real-time Threat Detection crashes in such a way that it cannot take a checkpoint (power failure, for example), it returns to the last checkpoint when it restarts, and replays events from there. Any actions that occurred between that checkpoint and the crash will therefore be repeated. Repeated actions that generate audit events generate duplicate audit events.

You should investigate repeated actions that do not duplicate well. For example, if an action adds an item to an Active List, that item’s counter will be incremented. If the action runs a command, it will run it again, and so on.

You can reduce duplicates by including a rule condition that checks if the relevant entry is already in the active list.

Hostname Shown as IPv6 Address in Dashboard

This can occur due to a mismatch between the system hostname, the network configuration, and your environment's name resolution. Review your system's hosts file and DNS configuration, as well as the addresses found in the DNS for the system hostname.

Appendix 4: Creating Custom Emails Using Velocity Templates

Real-time Threat Detection supports the use of *velocity templates* or scripts as defined by The Apache Velocity Project. Velocity templates are a means of specifying dynamic or variable inputs to, or outputs from, underlying Java code.

Velocity templates have many potential applications in Real-time Threat Detection. This section describes one such application, Email Notification Messages, which you can use Velocity templates on your Manager to create custom email messages to suit your needs.

Note: Velocity templates are an advanced user feature:

- Velocity templates can have wide-ranging effects, so misapplication or inappropriate application is possible. Micro Focus cannot assume responsibility for adverse results caused by user-created Velocity templates.
- Real-time Threat Detection does not provide error checking or error messaging for user-created velocity expressions. Refer to the Apache Velocity Project web page at http://velocity.apache.org/engine/devel/user-guide.html for information.

Note: Modification options are not available in Real-time Threat Detection for SaaS. For more information, contact your administrator.

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 Administrator's Guide (Real-time Threat Detection 8.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!