BOMGAR™

HP ArcSight
with Bomgar Privileged Access

TC:7/11/2017

Table of Contents

Bomgar Privileged Access Integration with HP ArcSight

IT administrators using HP ArcSight can now integrate Bomgar Privileged Access (PA) to strengthen access control, identify and prioritize threats seamlessly in real time, and remediate incidents proactively.

The Bomgar PA integration helps safeguard your business by giving you complete visibility into activity across the IT infrastructure, including external threats such as malware hackers, internal threats such as data breaches and fraud, risks from application flaws and configuration changes, and compliance pressures from failed audits.

Through the integration, session event data captured through Bomgar PA's rich logging capability is populated into HP's platform, and reports are provided for security review.

Prerequisites for the Bomgar Privileged Access Integration with HP ArcSight

To complete this integration, please ensure that you have the necessary software installed and configured as indicated in this guide, accounting for any network considerations.

Applicable Versions

- Bomgar Privileged Access: 15.x and newer
- HP ArcSight: 6.0.0 and newer

Network Considerations

The following network communication channels must be open for the integration to work properly:

Outbound From	Inbound To	TCP Port #	Purpose
Bomgar Middleware Engine Server	HP ArcSight	1514	Middleware pushes CEF formatted syslog messages to HP ArcSight

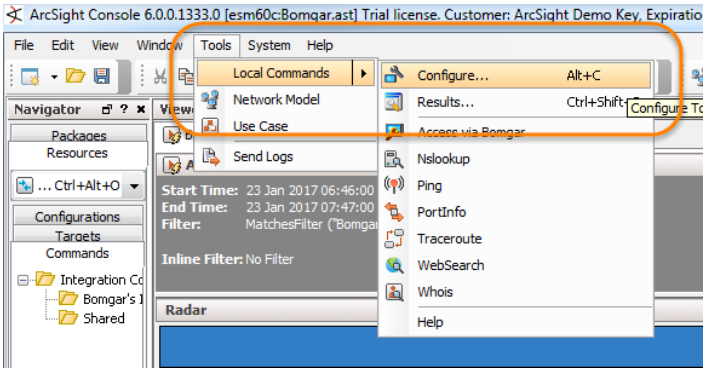
Prerequisite Installation and Configuration

The HP ArcSight integration is a Bomgar Middleware Engine plugin. To install the Bomgar Middleware Engine, follow the instructions in the Bomgar Middleware Engine Configuration document at www.bomgar.com/docs/integrations/middleware-engine.

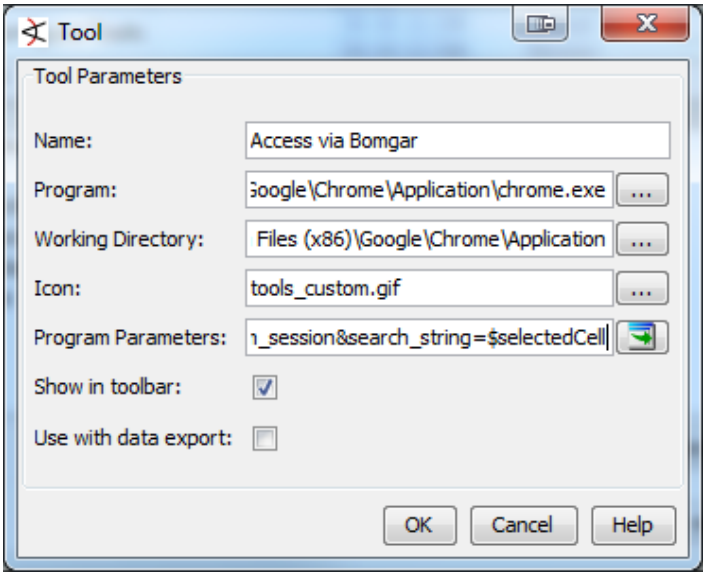
Configure HP ArcSight for Integration with Bomgar Privileged Access

If desired, a custom tool can be created within the ArcSight Console to allow users to Jump directly to an endpoint from an event entry. This approach leverages Bomgar PA's Client Scripting API to construct an open URL in your browser of choice to make sure no additional software is required. The URL instructs the Bomgar Appliance to generate and download a Bomgar console script file run by the access console to initiate the Jump session. To create the tool, follow the steps below.

1. In the **ArcSight Console**, click **Tools > Local Commands > Configure**.



2. Click **New** to create a new **Local Command**.

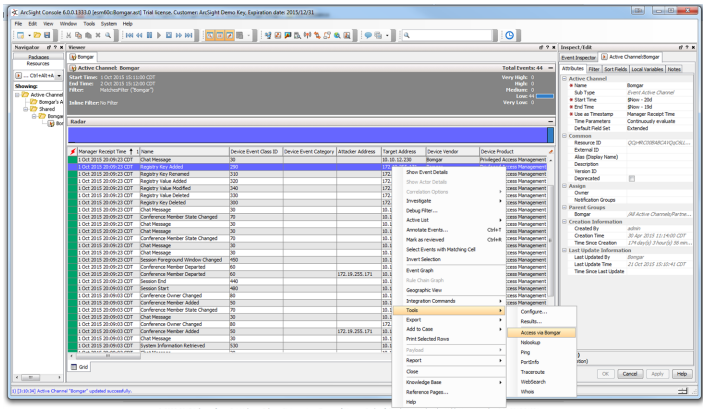


3. In the **Tool** settings dialog, configure the tool as follows:

Field Name	Field Value
Name	Access via Bomgar
Program	[Browse to and select the executable (.exe) for your preferred browser]

Field Name	Field Value
Working Directory	[The directory containing the executable for your preferred browser]
Icon	[Can be the default, tools_custom.gif, or any other image you choose]
Program Parameters	`https://<bomgar-hostname>/api/client_script?type=rep&operation=generate&action=start_jump_item_session&search_string=$selectedCell`
Show in toolbar	[Checked]
Use with data export	[Unchecked

4. Click **OK** to create the tool and close the **Configure Tools** window.
5. You can now right-click on any cell in the grid containing an IP address or hostname that matches an existing endpoint in the rep console to initiate a session.



Note: *The Bomgar Appliance does not require any additional configuration or changes beyond those mentioned in the Bomgar SIEM Tool Plugin Installation and Administration at www.bomgar.com/docs/privileged-access/how-to/integrations/siem-tool/index.*

Configure the SIEM Tool Plugin for Integration between HP ArcSight and Bomgar Privileged Access

To begin configuration, launch the **Middleware Administration Tool** and click on the clipboard icon next to the plugin name.

Bomgar Appliance

The first portion of plugin configuration provides the necessary settings for communication between the plugin and the Bomgar Appliance. These fields are described in the Bomgar SIEM Tool Plugin Installation and Administration at www.bomgar.com/docs/privileged-access/how-to/integrations/siem-tool/index.

HP ArcSight Instance

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the HP ArcSight instance. The configuration settings include:

1. **Target SIEM System:** Select HP ArcSight from the list.
2. **SIEM Syslog Host:** Enter the hostname or IP address of the HP ArcSight instance that should receive messages.
3. **SIEM Syslog Port:** Enter the port used by the HP ArcSight instance to receive syslog messages, usually port 1514.
4. **SIEM Syslog Protocol:** Select the appropriate protocol from the list, usually UDP.
5. **Events to Process:** Bomgar session data may contain many different event types. All types are available; however, only a subset may be desired in the SIEM tool. Select only the events you would like sent to HP ArcSight. Events matching unchecked event types are ignored.