

**BOMGAR™**

**Splunk Integration Guide**

## Table of Contents

---

<b>Bomgar Remote Support Integration with Splunk</b> .....	<b>3</b>
<b>Prerequisites for the Bomgar Remote Support Integration with Splunk</b> .....	<b>4</b>
Applicable Versions .....	4
Network Considerations .....	4
Prerequisite Installation and Configuration .....	4
<b>Configure Splunk for Integration with Bomgar Remote Support</b> .....	<b>5</b>
<b>Configure Bomgar Remote Support for Integration with Splunk</b> .....	<b>6</b>
<b>Configure the SIEM Tool Plugin for Integration between Splunk and Bomgar Remote Support</b> .....	<b>7</b>
Bomgar Appliance .....	7
Splunk Instance .....	7

## Bomgar Remote Support Integration with Splunk

IT administrators using Splunk can now integrate Bomgar Remote Support (RS) to strengthen access control, identify and prioritize threats seamlessly in real time, and remediate incidents proactively.

The Bomgar Remote Support 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 RS's rich logging capability is populated into Splunk's platform and reports are provided for security review.

# Prerequisites for the Bomgar Remote Support Integration with Splunk

## Applicable Versions

- Bomgar Remote Support: 14.x and newer
- Splunk on-premise: 6.3.0 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	Splunk Server	1514	Session event data is pushed as specially formatted syslog messages into Splunk
Bomgar Appliance	Splunk Server	514	Syslog event information from the appliance

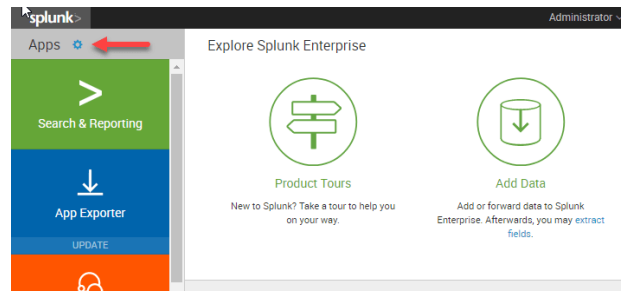
## Prerequisite Installation and Configuration

The Splunk 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](http://www.bomgar.com/docs/integrations/middleware-engine).

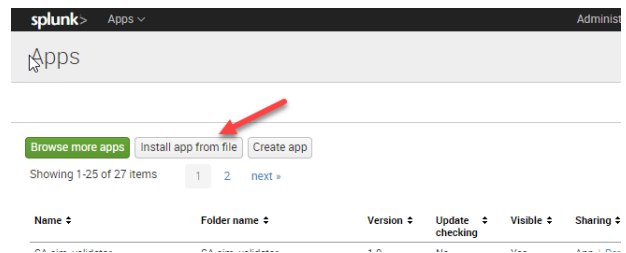
# Configure Splunk for Integration with Bomgar Remote Support

To install the integration, follow the steps below to import an item into Splunk.

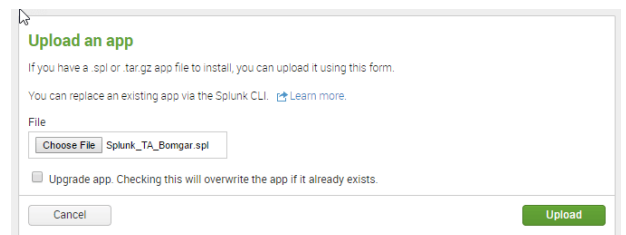
1. Log into Splunk as a user with administrative rights.
2. From the main home page, **/app/launcher/home**, click on the gear icon in the upper-left corner and go to **Manage Apps**.



3. On the **Apps** page, click **Install app from file**.



4. Browse to the location of the **Splunk\_TA\_BomgarPAM.spl** file and install the **Splunk Technology Add-on**.



## Other Considerations

For manual installation not completed through the web user interface, you must determine your deployment method, standalone or distributed. If distributed, your Bomgar technical account manager must go to the **Splunk Indexer** or **Forwarder**.

# Configure Bomgar Remote Support for Integration with Splunk

In addition to the steps outlined in the [Bomgar SIEM Tool Plugin Installation and Administration](http://www.bomgar.com/docs/remote-support/how-to/integrations/plugin/index) at [www.bomgar.com/docs/remote-support/how-to/integrations/plugin/index](http://www.bomgar.com/docs/remote-support/how-to/integrations/plugin/index), the Splunk integration also supports consumption of syslog output directly from the Bomgar Appliance.

All of the steps in this section take place in the Bomgar **/appliance** administrative interface.

1. Access your Bomgar interface by going to the hostname of your Bomgar Appliance followed by **/appliance** (e.g., **https://support.example.com/appliance**).
2. Go to **/appliance >Security > Appliance Administration** and locate the **Syslog** section.
3. Enter the hostname or IP address for your remote syslog server.
4. Select a message format.
5. Click **Submit**.

# Configure the SIEM Tool Plugin for Integration between Splunk and Bomgar Remote Support

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](http://www.bomgar.com/docs/remote-support/how-to/integrations/siem-tool/index) at [www.bomgar.com/docs/remote-support/how-to/integrations/siem-tool/index](http://www.bomgar.com/docs/remote-support/how-to/integrations/siem-tool/index).

## Splunk Instance

1. **Target SIEM System:** Select Splunk from the list.
2. **SIEM Syslog Host:** Enter the hostname or IP address of the Splunk instance that should receive messages.
3. **SIEM Syslog Port:** Enter the port used by the Splunk 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 Splunk. Events matching unchecked event types are ignored.