

12 September 2019

# APPLICATION CONTROL

Self Help Guide



STEP UP TO  
5<sup>TH</sup> GENERATION  
CYBER SECURITY

2019 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

#### RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

#### TRADEMARKS:

Refer to the Copyright page <https://www.checkpoint.com/copyright/> for a list of our trademarks.

Refer to the Third Party copyright notices

<https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/> for a list of relevant copyrights and third-party licenses.

# Important Information



## Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



## Latest Version of this Document

Download the latest version of this document in PDF format  
<http://downloads.checkpoint.com/dc/download.htm?ID=99143>.



## Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments

[mailto:cp\\_techpub\\_feedback@checkpoint.com?subject=Feedback on Application Control Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Application Control Guide).

## Revision History

Date	Description
12 September 2019	First release of this document

# Contents

- Important Information .....3
- Introduction.....5
- Customer Assistance.....5
- Requesting New Application.....6
- False Negative Request .....6
- False Positive Request.....7
- Metadata Change Request.....7
- Custom Application Creation Request.....8
  - Loading a Custom Package (R80.X) .....10
  - Loading a Custom Package (R77.30) .....11

# Introduction

This document helps Application Control users answer the most common questions that arise when dealing with Application Control product issues.

## Customer Assistance

Customer requests can be made in two ways:

- Contact your Sales Engineer (SE).
- Open an RFE (Request for Enhancement).

Every customer request is analyzed. If possible, a new application / fix will be released via the online updates.

When you send a request, please make sure you provide detailed information.

You can report on specific log on the dashboard:

The screenshot shows the Application Control dashboard with a log table and a 'Report Log to Check Point' dialog box.

**Log Table:**

Time	Icon	Source	Destination	Port	Protocol	Application
Today, 9:03:14 AM	[Icons]	ranav_R80.30	4.4.4.3			Bing
Today, 9:03:10 AM	[Icons]	ranav_R80.30	4.4.4.3			HTTP/2 over TLS
Today, 9:03:10 AM	[Icons]	ranav_R80.30	4.4.4.3			Google Services
Today, 9:00:42 AM	[Icons]	ranav_R80.30	4.4.4.3			Google Services
Today, 10:59:20 AM	[Icons]	ranav_R80.30	4.4.4.3			Windows Update
Today, 10:29:32 AM	[Icons]	ranav_R80.30	4.4.4.3			Windows Update
Today, 10:22:26 AM	[Icons]	ranav_R80.30	4.4.4.3			Windows Update
Today, 9:20:53 AM	[Icons]	ranav_R80.30	4.4.4.3			Windows Update
Today, 9:19:42 AM	[Icons]	ranav_R80.30	4.4.4.3			Web Browsing
Today, 9:19:40 AM	[Icons]	ranav_R80.30	4.4.4.3			Web Browsing
Today, 9:19:39 AM	[Icons]	ranav_R80.30	4.4.4.3			OCSP Protocol

**Report Log to Check Point Dialog Box:**

Log Name: Application Control

Additional Information:

Email Address for reply:

☐ Suspected security incident. Please have the Check Point Incident Response Team contact me

Check Point will use this data to improve the product's accuracy. Data will be kept confidential.

[View Privacy Policy](#)

Please add a detailed description about the issue. Include your email address so we can contact you if there are questions about the reports.

To give you the best and quick solution, the following pages detail the information we need about your requests.

## Requesting a New Application

Before you request a new application, check first to see if the application already exists in the Appwiki <https://appwiki.checkpoint.com/appwikisdb/public.htm>.

If the application does not exist, send Check Point the following information:

- Name of the application.
- Application URL / Download link.
- What is the use case?
- Description and justification.
- How is the application identifying today? (you can send a screen shot of the logs).
- Supply Packet capture. Please record the traffic and then open and use the application.

In some cases, additional information may be required.

## False Negative Request

You can suspect a **False Negative** if:

- The application exists in our database, but the traffic is not detected when the application is used.
- You try and fail to block the application.

Please contact Check Point with the following information:

- Name of the application.
- Application URL / Download link.
- What is the use case? Description of the issue
- What is the gateway version? (R77.30 / R80.10)
- What is the platform? (mobile/Web/PC)
- Is the latest JHF installed in the environment?
- What is the client version?
- Is HTTPS inspection turned on?
- Is gateway is up to date?
- Screen shot of the Rule Base. (Make sure User Check is not enabled.)
- Supply Packet capture. Please record the traffic and then open and use the application.

In some cases, additional information may be required.

# False Positive Request

You can suspect a **False Positive** if:

- The traffic is detected under a completely different application.
- When you try to block the application, unrelated traffic is blocked.

Please contact Check Point with the following information:

- Name of the application.
- Application URL / Download link.
- What is the use case? Description of the issue.
- What is the gateway version? (R77.30 / R80.10)
- What is the platform? (mobile/Web/PC).
- Is the latest JHF installed in the environment?
- What is the client version?.
- Is HTTPS inspection on?
- Is the gateway up to date?
- Screen shot of the Rule Base. Make sure User Check is not enabled.
- Supply Packet capture. Please record the traffic and then open and use the application.

In some cases, additional information may be required.

# Metadata Change Request

In the Application Database:

- Each application is assigned to one primary category based on its most defining aspect.
- Each application can have multiple tags, which are characteristics of the application. For example, some of the tags of Gmail include: Supports File Transfer, Sends mail, and Instant Chat.

Application risk levels:

Risk	Level
5 - Critical	Can bypass security or hide identities.
4 - High	Can cause data leakage or malware infection without user knowledge.
3 - Medium	Can be misused and cause data leakage or malware infection.
2 - Low	Potentially not business related, but low risk.
1 - Very Low	Usually business related with no or very low risk.

To change a category, tag or risk, contact Check Point with the following information:

- Name of the application.
- Application URL / Download link.
- Justification.

# Custom Application Creation Request

In some cases, you can create a custom application on your own using the Signature Tool:

The screenshot shows two main sections of a web interface. The top section, titled "Application Details", contains fields for "Application Name", "Main Category" (a dropdown menu), "Risk" (a dropdown menu), "Priority" (a numeric input field set to 1000), "Additional Categories" (a dropdown menu with expand/collapse buttons), and a "Description" text area. The bottom section, titled "Application Scenarios", features a table with columns "Scenario Type" and "Scenario Description". A context menu is open over the table, listing options: "HTTP Request", "SSL/TLS", "IP", "Cloud", and "Advanced". At the bottom right of the interface are "Save Application" and "Cancel" buttons.

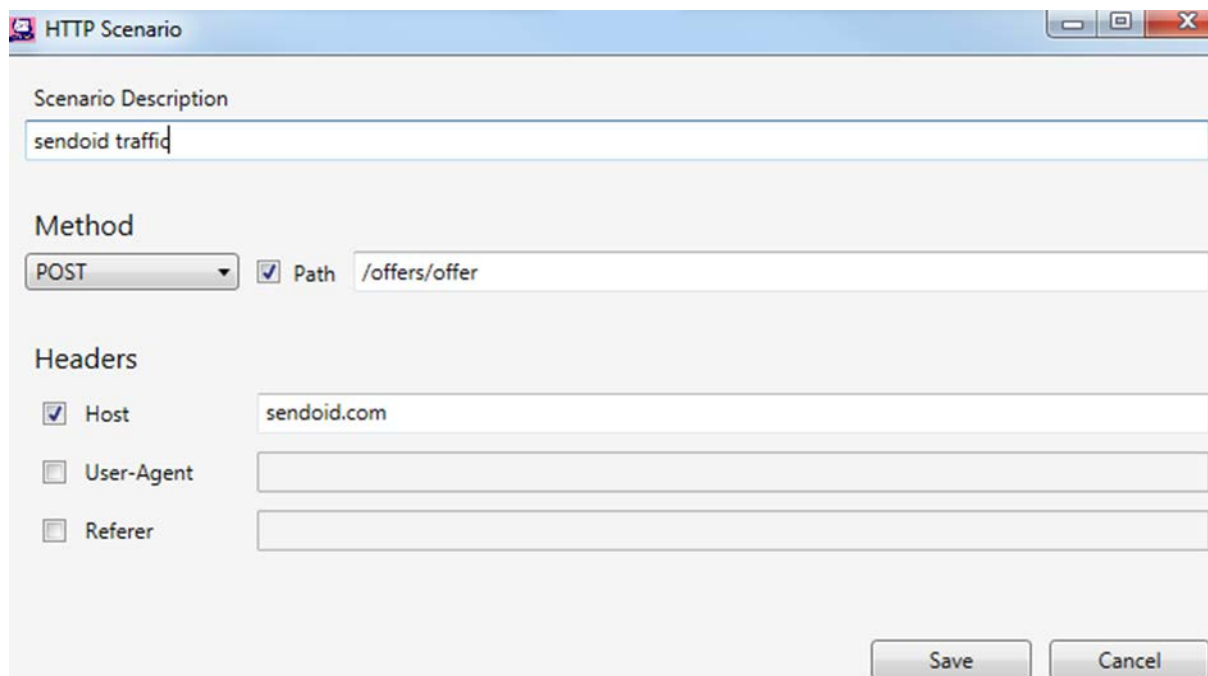
For example:

- SSL/TLS traffic:

The screenshot shows a window titled "SSL/TLS Scenario". It has a "Scenario Description" text area at the top. Below it are two configuration options: "Server Name Indication (C2S)" which is checked and has a text input field containing "facebook.com", and "Common Name (S2C)" which is unchecked and has an empty text input field. An "AND" button is located between the two input fields. At the bottom right are "Save" and "Cancel" buttons.



- HTTP traffic:



The screenshot shows a window titled "HTTP Scenario" with a standard Windows-style title bar. Inside the window, there are three main sections: "Scenario Description", "Method", and "Headers".

- Scenario Description:** A text box containing the text "sendoid traffic".
- Method:** A dropdown menu set to "POST". To its right is a checked checkbox labeled "Path" followed by a text box containing "/offers/offer".
- Headers:** A section with three entries, each with a checkbox and a text box:
  - ☒ Host: sendoid.com
  - ☐ User-Agent: (empty text box)
  - ☐ Referer: (empty text box)

At the bottom right of the window are two buttons: "Save" and "Cancel".

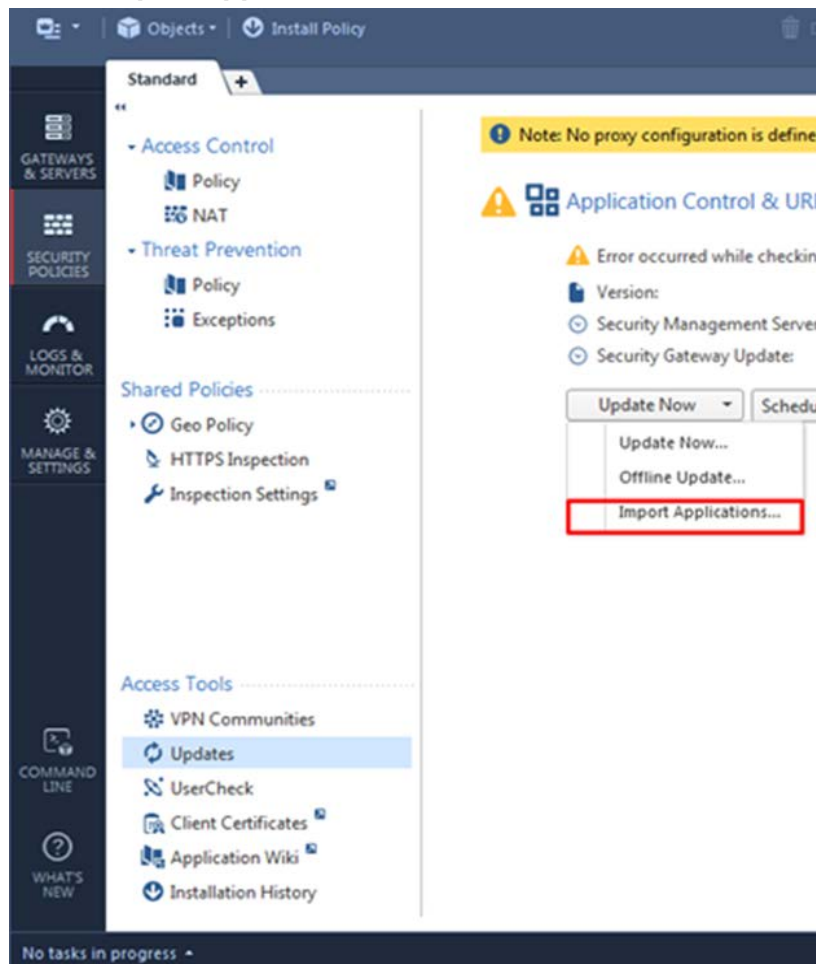
For more information, refer to sk103051

<http://supportcontent.checkpoint.com/solutions?id=sk103051> - Signature Tool for custom Application Control and URL Filtering applications (and the related documentation).

# Loading a Custom Package (R80.X)

To load a custom package to R80.X:

1. Go to **Security Policies > Updates**.
2. Select **Import Applications**.



3. Select the `custom_app_R80.xml` file.
4. Configure the Rule Base.
5. Install the policy.

# Loading a Custom Package (R77.30)

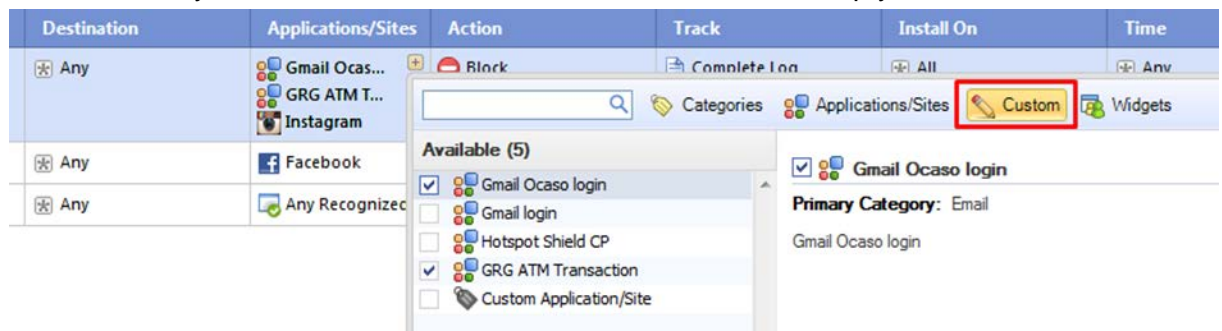
To load a custom package to R77.30:

1. Go to **Application & URL Filtering > Applications/Sites > Actions > Import.**



2. Select the `custom_app.apps` file.
3. Select the application on the Rule Base.

Make sure only **Custom** is selected and leave the search bar empty.



4. Install the policy.