Check Point
SOFTWARE TECHNOLOGIES LTD.

03 September 2020

SECURITY MANAGEMENT

R81

Early Availability

Administration Guide

[Classification: Protected]

Check Point Copyright Notice

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.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Latest Version of this Document in English

Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
03 September 2020	First release of this document

Accelerated Install Policy

In This Section:

Introduction 4
Operations that allow Accelerated Install Policy 4
Cases in which Install Policy will not be accelerated 13
Limitations 14

Introduction

R81 introduces the Accelerated Install Policy feature. When the Access Control policy installation is accelerated, the installation duration is decreased significantly.

Policy installation is accelerated depending on the changes that were made to the Access Control policy since the last installation.

This document details the changes that allow an accelerated policy installation, as well as the cases, in which policy installation is not accelerated.

Operations that allow Accelerated Install Policy

Policy installation is accelerated *only if* all changes made since the last installation include objects of the types listed below, and only if all changes to those objects are listed under the relevant types. In any other case, the policy installation is *not* accelerated.

Note - In some cases, even if all the changes are to the objects listed below, policy installation is still not accelerated. For more information, see *"Cases in which Install Policy will not be accelerated" on page 13*.

Access Control Rule

- Creating a rule (without editing it)
- Editing the **Name** column
- Editing the **Track** column
- Editing the **Time** column
- Editing the **VPN** column
- Editing the **Content** column
- Editing the **Action** column
  - Action (before and after the edit) is *not* an **Inline Layer**, **User Auth**, or **Client Auth**
- Editing the **Source** or **Destination** columns
  - Adding or removing objects that appear in *"Supported objects for use in the 'Source' and 'Destination' columns" on page 11*
- Editing the **Services & Applications** column
  - Adding or removing objects that appear in *"Supported objects for use in the 'Services & Applications' column" on page 12*
- Deleting, enabling, or disabling a rule
  - Rule's **Action** is *not* an **Inline Layer**, **User Auth**, or **Client Auth**
  - All objects used in the **Source** or **Destination** columns appear in *"Supported objects for use in the 'Source' and 'Destination' columns" on page 11*
  - All objects used in the **Services & Applications** column appear in *"Supported objects for use in the 'Services & Applications' column" on page 12*
  - Rule does not contain a **Service with Resource**

Access Control Layer

- Creating a layer
- Editing layer properties

Host

- Creating a Host object
  - Object does not contain **NAT** settings
  - Object does not contain **Servers Configuration**
- Editing a Host
  - Modified fields or sections:
    - **Name**
    - **IPv4 address**
    - **IPv6 address**
    - **Network Management**
  - Object does not contain **NAT** settings
  - Object does not contain **Servers Configuration**
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions
- Deleting a Host
  - Object does not contain **NAT** settings
  - Object does not contain **Servers Configuration**
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions

Network

- Creating a Network object
  - Object does not contain **NAT** settings
- Editing a Network object
  - Modified fields:
    - Name
    - IPv4 -> **Network address**
    - IPv4 -> **Net mask**
    - IPv4 -> **Broadcast address**
    - IPv6 -> **Network address**
    - IPv6 -> **Prefix**
  - Object does not contain **NAT** settings
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions
- Deleting a Network object
  - Object does not contain **NAT** settings
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions

Address Range

- Creating an Address Range object
  - Object does not contain **NAT** settings
- Editing an Address Range object
  - Modified fields:
    - **Name**
    - IPv4 -> **First IP address**
    - IPv4 -> **Last IP address**
    - IPv6 -> **First IP address**
    - IPv6 -> **Last IP address**
  - Object does not contain **NAT** settings
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions
- Deleting an Address Range object
  - Object does not contain **NAT** settings
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions

Multicast Address Range

- Creating a Multicast Address Range object
- Editing or deleting a Multicast Address Range object
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions

Dynamic Object

- Creating a Dynamic Object
- Editing or deleting a Dynamic Object
  - Object is used only in an Access Control rule, a Threat Prevention rule, or a Network Group

Domain

- Creating a Domain object
- Editing or deleting a Domain object
  - Object is used only in an Access Control rule, a Threat Prevention rule, or a Network Group

Security Zone

- Creating a Security Zone object
- Editing or deleting a Security Zone object
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or Topology Settings

Network Group

- Creating a Network Group object
- Editing a Network Group object
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions
  - All objects added to this group appear in *"Supported objects for use in the 'Source' and 'Destination' columns" on page 11*
  - All objects removed from this group appear in *"Supported objects for use in the 'Source' and 'Destination' columns" on page 11*
- Deleting a Network Group object
  - Object is used only in an Access Control rule, a Threat Prevention rule, a Network Group, or a Group with Exclusions
  - All group members appear in *"Supported objects for use in the 'Source' and 'Destination' columns" on page 11*

Group with Exclusions

- Creating a Group with Exclusions object
- Editing or deleting a Group with Exclusions object
  - Object is used only in an Access Control rule, a Threat Prevention rule, or a Network Group

Application Group

- Creating an Application Group object
- Editing an Application Group object
  - Object is used in an Access Control rule, or an Application Group object
  - Object is used in Access Control policy, and all objects added to this group appear in *"Supported objects for use in the 'Services & Applications' column" on page 12*
  - Object is used in Access Control policy, and all objects removed from this group appear in *"Supported objects for use in the 'Services & Applications' column" on page 12*
- Deleting an Application Group object
  - Object is used only in an Access Control rule and an Application Group object
  - Object is used only in Access Control policy, and all group members appear in *"Supported objects for use in the 'Services & Applications' column" on page 12*

Wildcard

- Creating, editing, or deleting a Wildcard object

Time

- Creating a Time object
- Editing a Time object
  - Object is used only in an Access Control rule and a Time Group object
- Deleting a Time object

Time Group

- Creating a Time Group object
- Editing a Time Group object
  - Object is used only in an Access Control rule and a Time Group object
- Deleting a Time Group object

Limit

- Creating, editing, or deleting a Limit object

Data Center

- Creating, editing, or deleting a Data Center object

Additional Modifications

- Creating, editing, or deleting a Threat Prevention rule, a Threat Prevention Layer, a Threat Prevention rule's Section, or Threat Prevention Exceptions
- Changing the **Color** of any object
- Editing the **Comment** of any object
- Creating, editing, or deleting the **Section Title** in an Access Control rule

Supported objects for use in the 'Source' and 'Destination' columns

- Host
- Network
- Address Range
- Multicast Address Range
- Dynamic Object
- Domain
- Wildcard
- Security Zone
- Network Group
  - Supported only if all group members also appear in this list
- Group with Exclusions
- Access Role
- Gateway
- Gateway Node
- Check Point Host
- Gateway Cluster
- Cluster Member
- VSX Gateway
- Virtual System
- VSX Cluster
- Virtual System Cluster
- Internet

Supported objects for use in the 'Services & Applications' column

- Application
  - Supported only if all the services defined for this Application also appear in this list
- Category
  - Supported only if all the services defined for this Category also appear in this list
- Application/Site Group
  - Supported only if all the services defined for this Application/Site Group also appear in this list
- Service Group
- TCP Service
- UDP Service
- RPC Service
- DCE-RPC Service
- ICMP Service
- ICMPv6 Service
- SCTP Service

Cases in which Install Policy will not be accelerated

- All operations that are not explicitly mentioned in the whitelist above do not trigger accelerated policy installation.
- **Changing a policy package**:

  Installing a policy package that is different than the package installed on the Security Gateway does not trigger accelerated policy installation.
- If objects of types **Client Authentication, User Authentication, Logical Server** or **Service with Resource** are used in the policy (can only be used in the first layer), any change that affects a rule in the first layer does not trigger accelerated policy installation.
- **Manual changes on the Security Management Server**:

  When changes are made to configurations files (for example - all inspect files in the $FWDIR/lib/ directory) on the Security Management Server, the next policy installation on the Security Gateway will not be accelerated regardless of the changes that were made.
- **Global Domain assignment**:

  After Assigning/Reassigning Global Domain on the Security Management Server, the next policy installation on the Security Gateways that are part of the Domain that was assigned/reassigned are not accelerated.
- **Reverting the Security Gateway to an older snapshot**:

  If a Security Gateway is reverted to an older snapshot and the policy installation is accelerated (because the changes triggered Accelerated Install Policy), the policy installation fails with this error message:

  ```
  Security Gateway and Security Management policy versions are
  incompatible. Disable Accelerated Install Policy for this Security
  Gateway and install policy again. For more information, see
  sk168055.
  ```

Note - sk168055 is not publicly available yet. Below are the applicable instructions to disable the Accelerated Install Policy before you install it.

- If this Management Server manages several Security Gateway objects:
  1. Click **Install Policy**.
  2. In the **Install Policy** window, right-click on any of the Security Gateway objects.
  3. Select **Do not use Install Policy Acceleration for all gateways**.
  4. Select the applicable Security Gateway objects.
  5. Click **Install**.
- If this Management Server manages only a single Security Gateway object:
  1. Click **Install Policy**.
  2. In the middle of the **Install Policy** window, right-click on the Security Gateway object name.
  3. Select **Do not use Install Policy Acceleration for all targets**.
  4. Click **Install**.

The **Install Policy Details** window shows: `Install Policy Acceleration is disabled for the current installation.`

Limitations

- The Security Management Server and the Security Gateway must run version R81 or above.
- Policy Installation will not be accelerated on the following types of Gateways: Gaia Embedded, LSM Profile, Scalable Platforms 40000 / 60000, and Maestro.