CHECK POINT
Support Center

Support Center / Search Results / Secureknowledge Details

My Favorites

Search questions, keywords or topics you need information about.

Solution ID: **sk164253**

Technical Level: **Basic**

Email

ATRG: Endpoint Security Firewall and Application Control Blade

Product
Endpoint Security Client

Version
E81.x (EOL), E82.x (EOL), E83.x (EOL), E84.x (EOL)

Last Modified
2023-06-14

Solution

Table of Contents:

- Introduction
- Firewall and Application Control Blade Overview
  - Client-Server Architecture
  - Client Architecture
  - Firewall and Application Control Client UI
  - Viewing Logs
- Managing Firewall and Application Control Blade
  - Defining Firewall Policy
  - Defining Access Zones Policy
  - Defining Application Control Policy

- Known problems and solutions for them
- General troubleshooting Approaches
- Collecting Debug Information

Note: Relevant for R81.

New in R81

- **Application Control** - Support of multiple versions per product / application to be added to the list of applications being imported using the AppScan tool. Refer to the R81 Endpoint Security Administration Guide.
- **Application Control** - Developer Protection. Helps prevent leakage of sensitive information (such as API keys), protects against the usage of vulnerable packages and updates the known vulnerabilities database regularly. Refer to the R81 Endpoint Security Administration Guide.
- **Application Control** - Disabling or enabling Windows Subsystem for Linux (WSL). Refer to the R81 Endpoint Security Administration Guide.
- **Firewall Blade** - Endpoint Host Isolation via Push Operations. Refer to sk169758 - Endpoint Host Isolation.

Introduction

This article describes the main aspects of the Endpoint Security Firewall and Application Control Blade.

Both Firewall and Application Control are protecting computers from Internet threats. Firewall is focused on Connections, while Application Control is focused on Applications.

Understanding Firewall Protection

The firewall guards the "doors" to computers, that is, the ports through which Internet traffic comes in and goes out. It examines all the network traffic and application traffic arriving at your computer, and asks these questions:

- Where did the traffic come from and what port is it addressed to?
- Do the firewall rules allow traffic through that port?
- Does the traffic violate any global rules?

The answers to these questions determine whether the traffic is allowed or blocked.

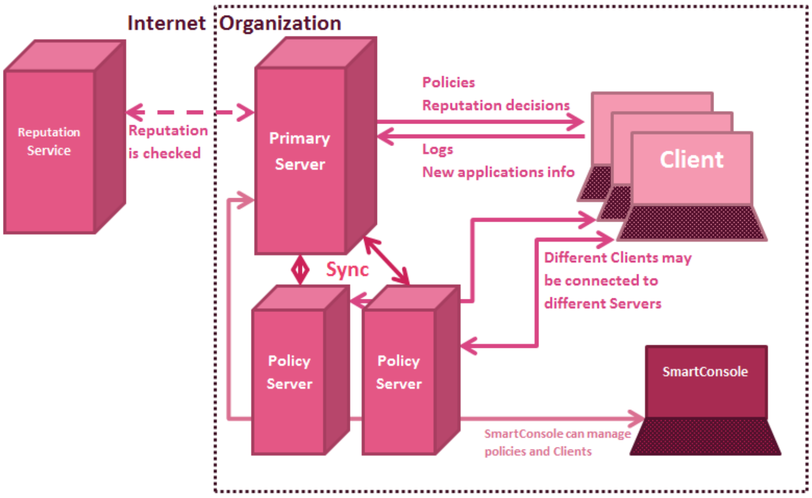
Understanding Application Control

Application Control restricts network access for specified applications. These applications are defined in the Policy that is set by the administrator.

Firewall and Application Control Blade Overview

This section gives the architectural and functional overview of the Firewall and Application Control Blade and describes its common flows.

Client-Server Architecture



From the Firewall and Application Control perspective, the Endpoint Security Client gets the following information from the Endpoint Security Server:

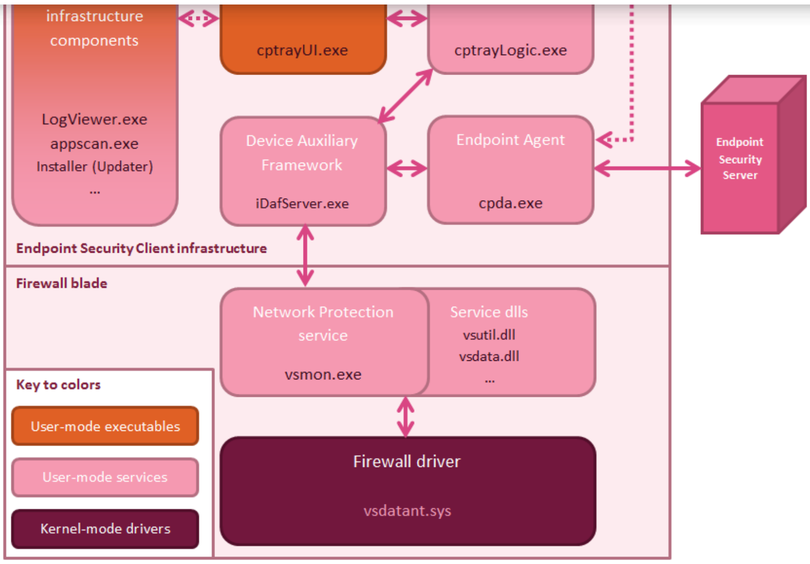
- Policy definitions
- Applications Reputation Updates (on demand, when an unknown application is first discovered)

The Endpoint Security Client sends the following Firewall-related information to the Endpoint Security Server:

- Logs (from the other blades as well). Log upload process can be customized in the Client Settings policy
- Information about new discovered applications

To reduce the load to the Endpoint Security Server, additional servers can be deployed. These servers are called Policy Servers. Policy Servers provide the same functionality to Clients. However, they cannot be used to manage policies with SmartConsole.

Client Architecture



On the client-side, there are several important components that communicate one with another, as described in the figure above.

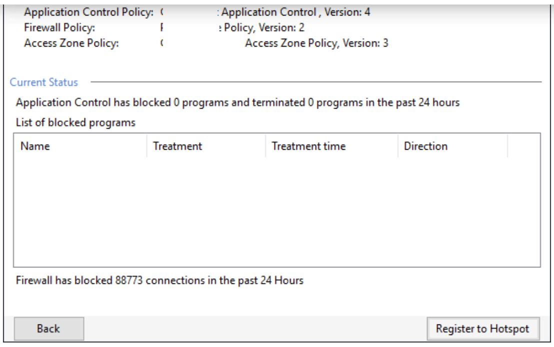
These components are:

- **Check Point Endpoint Agent service:** performs all communications with the Endpoint Security Server, including Policies download, log upload, etc.
- **Check Point Device Auxiliary Framework service:** performs all communications with the installed Endpoint Security Blades and UI.
- **Check Point Client UI service and Client UI process:** perform user actions handling, and show blades status and messages.
- **Check Point Network Protection service:** performs Firewall, Access Zones and Application Control policy maintenance and execution.
- **Service DLLs:** subcomponents of Network Protection service needed for it to run properly
- **Firewall driver:** low-level kernel driver that performs actual packet processing.
- Other infrastructure components: other modules, for example, *appscan* utility and Log Viewer utility.

Firewall and Application Control Client UI

Firewall and Application Control Client UI allows viewing Policies and their information and seeing the current status of the blade.

It shows a summary of the Firewall and Application Control activity and the list of blocked programs with details.



Application Control Policy: (: Application Control , Version: 4
Firewall Policy: F : Policy, Version: 2
Access Zone Policy: (Access Zone Policy, Version: 3

Current Status

Application Control has blocked 0 programs and terminated 0 programs in the past 24 hours

List of blocked programs

Name	Treatment	Treatment time	Direction

Firewall has blocked 88773 connections in the past 24 Hours

Viewing Logs

An Endpoint Security activity, including Firewall and Application Control events, is recorded in logs. This information is uploaded to the Server and can be viewed by administrators. Upload is configured in Client Policy.

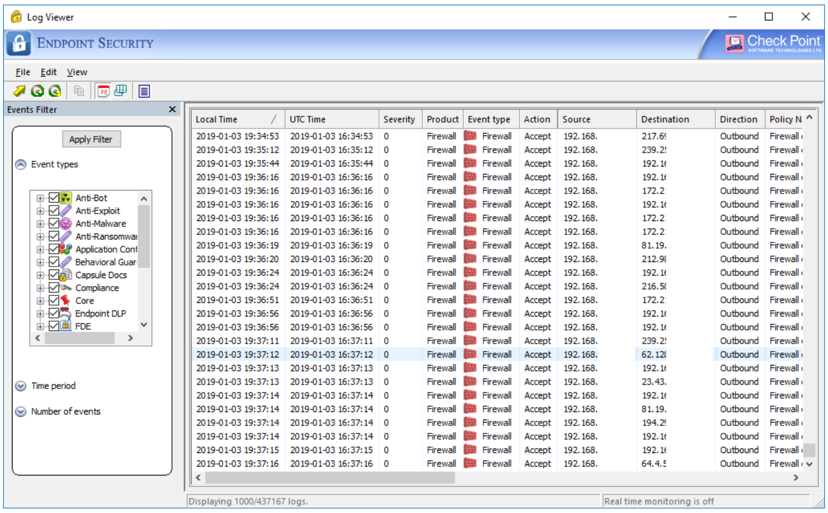
This information can be useful in the following cases:

- To identify the cause of technical problems.
- To monitor traffic more closely.
- To make sure that all features function as they should

Log Viewer is installed together with the client. It can be opened by navigating to 'Endpoint Security Client UI Main Page > Advanced > View Logs'.

Working with Log Viewer

Log Viewer can show details for each log entry (log entry should be double-clicked). It also supports filtering logs, exporting them to some file, sorting them and other operations.



Local Time	UTC Time	Severity	Product	Event type	Action	Source	Destination	Direction	Policy N
2019-01-03 19:34:53	2019-01-03 16:34:53	0	Firewall	Firewall	Accept	192.168.	217.6	Outbound	Firewall
2019-01-03 19:35:12	2019-01-03 16:35:12	0	Firewall	Firewall	Accept	192.168.	239.2	Outbound	Firewall
2019-01-03 19:35:44	2019-01-03 16:35:44	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:36:16	2019-01-03 16:36:16	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:36:16	2019-01-03 16:36:16	0	Firewall	Firewall	Accept	192.168.	172.2	Outbound	Firewall
2019-01-03 19:36:16	2019-01-03 16:36:16	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:36:16	2019-01-03 16:36:16	0	Firewall	Firewall	Accept	192.168.	172.2	Outbound	Firewall
2019-01-03 19:36:16	2019-01-03 16:36:16	0	Firewall	Firewall	Accept	192.168.	172.2	Outbound	Firewall
2019-01-03 19:36:19	2019-01-03 16:36:19	0	Firewall	Firewall	Accept	192.168.	81.19.	Outbound	Firewall
2019-01-03 19:36:20	2019-01-03 16:36:20	0	Firewall	Firewall	Accept	192.168.	212.9	Outbound	Firewall
2019-01-03 19:36:24	2019-01-03 16:36:24	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:36:24	2019-01-03 16:36:24	0	Firewall	Firewall	Accept	192.168.	216.5	Outbound	Firewall
2019-01-03 19:36:51	2019-01-03 16:36:51	0	Firewall	Firewall	Accept	192.168.	172.2	Outbound	Firewall
2019-01-03 19:36:56	2019-01-03 16:36:56	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:36:56	2019-01-03 16:36:56	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:37:11	2019-01-03 16:37:11	0	Firewall	Firewall	Accept	192.168.	239.2	Outbound	Firewall
2019-01-03 19:37:12	2019-01-03 16:37:12	0	Firewall	Firewall	Accept	192.168.	62.12	Outbound	Firewall
2019-01-03 19:37:13	2019-01-03 16:37:13	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:37:13	2019-01-03 16:37:13	0	Firewall	Firewall	Accept	192.168.	23.43.	Outbound	Firewall
2019-01-03 19:37:14	2019-01-03 16:37:14	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:37:14	2019-01-03 16:37:14	0	Firewall	Firewall	Accept	192.168.	81.19.	Outbound	Firewall
2019-01-03 19:37:14	2019-01-03 16:37:14	0	Firewall	Firewall	Accept	192.168.	194.2	Outbound	Firewall
2019-01-03 19:37:14	2019-01-03 16:37:14	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:37:15	2019-01-03 16:37:15	0	Firewall	Firewall	Accept	192.168.	192.1	Outbound	Firewall
2019-01-03 19:37:16	2019-01-03 16:37:16	0	Firewall	Firewall	Accept	192.168.	64.4.5	Outbound	Firewall

Displaying 1000/437167 logs.

Real time monitoring is off

Using the Event Filter

The Event Filter lets you filter the logs to see the information that is relevant to you.

You can filter by:

- **Event types:** Select or clear the checkboxes that relate to the different Endpoint Security features.

- Show Newest or Oldest first: Select which logs should be at the top of the list.

To use the Event Filter:

1. Open the Event Filter pane: Click the "View Event Filter" window icon and select 'View > Event Filter'.
2. Click the black arrows to open and close the sections of the Events Filter pane.
3. Make selections to filter the log results.
4. Click "Filter". The results of the filter are displayed in the Log Viewer.

To export the logs:

1. From the Log Viewer window: Click the "Export" icon and select 'Edit > Export to File'.
2. In the "Save As" window, select the location where you want the file to be saved, enter a File name, and click "Save". The logs are saved in a text file.

Managing Firewall and Application Control Blade

This section describes the SmartEndpoint Policy Rules that are related to the Firewall and Application Control Blade and gives recommendations about configuring them.

There are three main Rules related to the Firewall and Application Control Blade, together with some additional settings controlled in the Common Client Settings Rule:

- **Access Zones:** Defines the topology of the organizational network, separating it into Trusted and Internet domains. This rule affects Windows and MacOS machines with the Firewall Blade installed.
- **Firewall:** Blocks or allows network traffic, based on attributes of network connections. This rule also affects Windows and MacOS machines.
- **Application Control:** Controls network access on a per-application basis, letting you restrict application network access. **This blade is supported only on Windows workstation** (It is not supported on MacOS and on Windows Servers).
- **Client Settings:** Controls common client behavior. There are settings related to the Firewall Blade - log upload and the possibility to disable network protection on demand.

Defining Firewall Policy

Firewall rules allow or block network traffic to endpoint computers, based on connection information, such as IP addresses, ports, and protocols. There are two types of firewall rules:

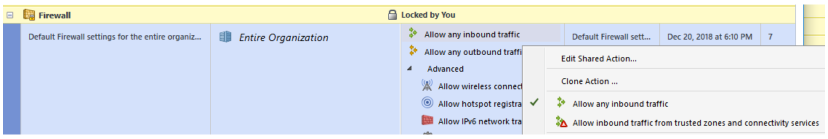
- **Inbound rules:** Rules that allow or block incoming network traffic **to** the endpoint computer.
- **Outbound rules:** Rules that allow or block outgoing network traffic **from** the endpoint computer.

Planning Firewall Policy

third parties.

The defined Actions in the Firewall rules make it easy to create the Firewall policy that you choose. Select an Action for Inbound traffic and an Action for Outbound traffic. The required rules are automatically added to the Firewall Inbound and Outbound Rule Bases.

You can add more rules to each Rule Base, and edit rules, as necessary.



Firewall | Locked by You

Default Firewall settings for the entire organiz... | Entire Organization | Allow any inbound traffic | Default Firewall sett... | Dec 20, 2018 at 6:10 PM | 7

Allow any outbound traffi

Advanced

Allow wireless connect

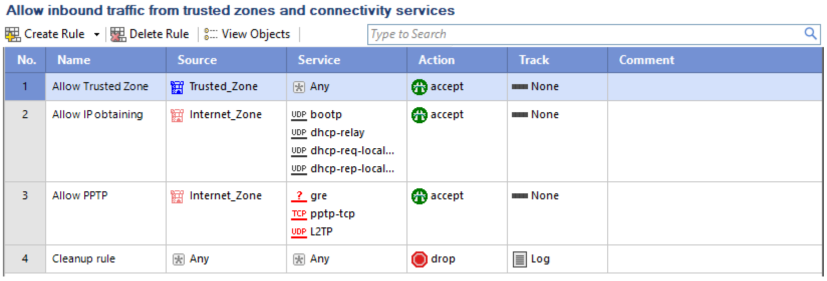
Allow hotspot registra

Allow IPv6 network tra

Edit Shared Action...
Clone Action ...
✓ Allow any inbound traffic
Allow inbound traffic from trusted zones and connectivity services

On the client, the Firewall rules are evaluated in the same order as they are defined in the Firewall Policy. **If two rules match the same traffic, the first one will be applied.**

Therefore, typically, the last rule is the "Cleanup" rule that matches to all traffic, and applies a default action (blocks or allows) all traffic that was not matched to the previous rules.



Allow inbound traffic from trusted zones and connectivity services

No.	Name	Source	Service	Action	Track	Comment
1	Allow Trusted Zone	Trusted_Zone	Any	accept	None	
2	Allow IP obtaining	Internet_Zone	UDP bootp UDP dhcp-relay UDP dhcp-req-local... UDP dhcp-rep-local...	accept	None	
3	Allow PPTP	Internet_Zone	? gre TCP pptp-tcp UDP L2TP	accept	None	
4	Cleanup rule	Any	Any	drop	Log	

Changes are enforced after the Policy is installed.

Inbound Traffic Rules

Inbound traffic rules define which network traffic can reach endpoint computers (known as localhost).

There are two default actions:

- **Allow inbound traffic:** Allows all incoming traffic to the endpoint computer.
- **Allow inbound traffic from trusted zones and connectivity services:** Allows all incoming traffic from trusted zones and IP address obtaining traffic from the internet. **All other traffic is blocked.**

The rules required for the selected Action are automatically added to the "Inbound Firewall Rules" Rule Base.

Right-click an Action to see the "Inbound Firewall Rules" Rule Base. You can add, delete, and change rules, as necessary.

Note that there is no Destination column in the Inbound Rule Base because the destination of all traffic is the endpoint computer.

Outbound Traffic Rules

Outbound traffic rules define which outgoing network traffic is allowed from endpoint computers.

There are two default actions:

- **Allow outbound traffic to trusted zones and common internet protocols:** Allow all traffic to trusted zones and traffic of common Internet protocols to the Internet.

The rules required for the selected Action are automatically added to the "Outbound Firewall Rules" Rule Base.

Right-click an Action to see the "Outbound Firewall Rules" Rule Base. You can add, delete, and change rules, as necessary.

Note that there is no Source column in an Outbound Rule Base because the source of all traffic is the endpoint computer.

Creating Firewall Rules

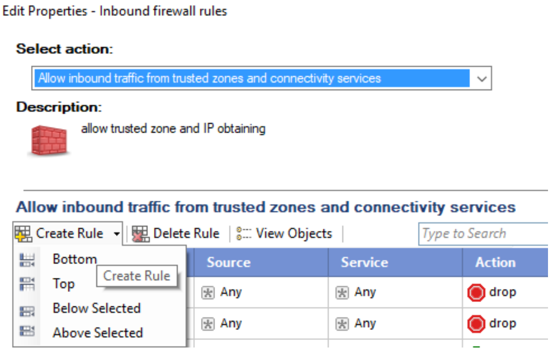
Create Firewall rules that relate to inbound traffic in the "Inbound Firewall Rules" Rule Base and rules that relate to outbound traffic in the "Outbound Firewall Rules" Rule Base.

To create a Firewall rule:

1. In the Firewall rule in the Policy tab, right-click the inbound or outbound traffic Action and select "Edit Properties".
2. Click one of the "Add Rule" icons from above the Rule Base.
3. Fill in the columns of the rule. Right-click the column to select an option.

Column	Description
NO	Rule priority number. Rule priority is important because a client checks firewall rules based on its sequence in the Rule Base. Rules are enforced from the top to the bottom. The last rule is usually a Cleanup Rule that says to drop traffic that does not match any of the previous rules.
Name	Name of the Firewall Rule.
Source/ Destination	• **Source:** Source location of the network traffic. For an outbound rule, the source is always the local computer. • **Destination:** Destination location of network traffic. For an inbound rule, the destination is always the local computer. Source and Destination can be any of the Network Objects defined in the Access Zones policy, or the Trusted/Internet Zone.
Service	Network protocol or service used by traffic.
Action	What is done to traffic that matches the rule: **Accept** or **Drop**.
Track	Tracking when the rule is enforced: • **Log:** Record rule enforcement in the Endpoint Security Client Log Viewer.

	• **None:** Log and alert messages are not created.



Edit Properties - Inbound firewall rules

Select action: Allow inbound traffic from trusted zones and connectivity services

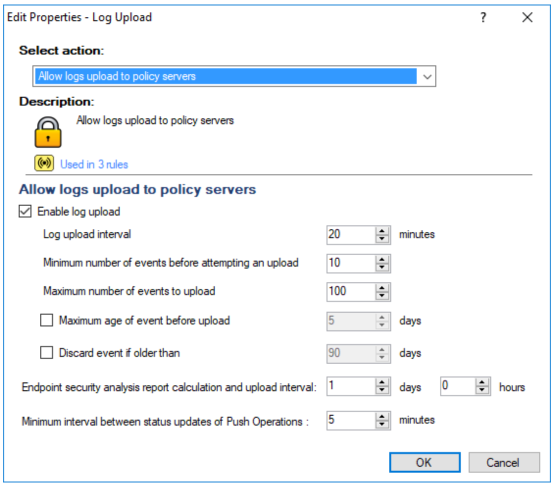
Description: allow trusted zone and IP obtaining

Allow inbound traffic from trusted zones and connectivity services

Source	Service	Action
Any	Any	drop
Any	Any	drop

Notes on configuring Tracking:

- If you have a rule that drops or accepts all traffic, do not enable logging.
- To use logs and alerts, you must configure options in the "Client Settings" rules:
  - In the Log Upload action, "Enable log upload" must be selected.
  - In the "Users Disabling Network Protection" action, under "Network Protection Alerts", in the "Firewall" row, select "Allow Alert".



Edit Properties - Log Upload

Select action: Allow logs upload to policy servers

Description: Allow logs upload to policy servers

Used in 3 rules

Allow logs upload to policy servers

☑ Enable log upload

Log upload interval: 20 minutes

Minimum number of events before attempting an upload: 10

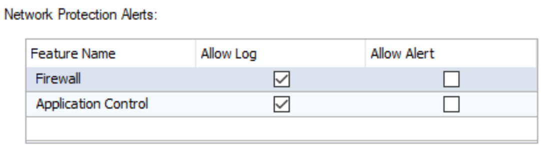
Maximum number of events to upload: 100

☐ Maximum age of event before upload: 5 days

☐ Discard event if older than: 90 days

Endpoint security analysis report calculation and upload interval: 1 days 0 hours

Minimum interval between status updates of Push Operations : 5 minutes



Network Protection Alerts:

Feature Name	Allow Log	Allow Alert
Firewall	☑	☐
Application Control	☑	☐

Firewall Rules and Domain Controllers

When creating Firewall Rules for endpoint clients, create explicit rules that allow all endpoints to connect to all of the domain controllers on the network.

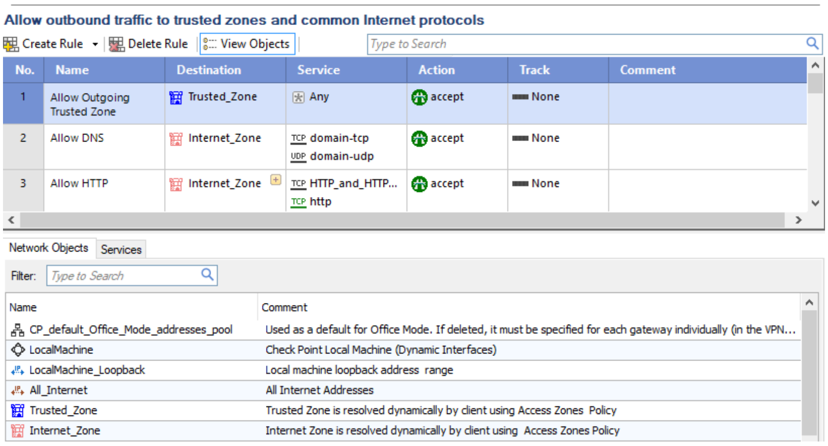
Services and Network Objects

The same Network Objects and Services are used throughout SmartEndpoint and in SmartDashboard. When you create a new object, it is also available in SmartDashboard. **If you change an object in SmartEndpoint or**

1. In the Inbound or Outbound Firewall Rule Base, open the 'Network Objects" tab.
2. Click "New".
3. Select the type of object from the "New Object Type" list.
4. Click "OK".
5. In the Properties window, enter the required information.
6. Click "OK".

To create a Service:

1. In the Inbound or Outbound Firewall Rule Base, open the "Services" tab.
2. Click "New".
3. Select the type of service from the "New Object Type" list.
4. Click "OK".
5. In the Properties window, enter the required information.
6. Optional: If you create a Group, In the Group Properties window, add "Available Services" to a group.
7. Click "OK".



Allow outbound traffic to trusted zones and common Internet protocols

No.	Name	Destination	Service	Action	Track	Comment
1	Allow Outgoing Trusted Zone	Trusted_Zone	Any	accept	None	
2	Allow DNS	Internet_Zone	TCP domain-tcp UDP domain-udp	accept	None	
3	Allow HTTP	Internet_Zone	TCP HTTP_and_HTTP... TCP http	accept	None	

Name	Comment
CP_default_Office_Mode_addresses_pool	Used as a default for Office Mode. If deleted, it must be specified for each gateway individually (in the VPN...
LocalMachine	Check Point Local Machine (Dynamic Interfaces)
LocalMachine_Loopback	Local machine loopback address range
All_Internet	All Internet Addresses
Trusted_Zone	Trusted Zone is resolved dynamically by client using Access Zones Policy
Internet_Zone	Internet Zone is resolved dynamically by client using Access Zones Policy

Disabling and Deleting Rules

When you delete a rule, it is removed from the Rule Base and not enforced in the policy.

When you disable a rule, the rule is not enforced in the policy. The rule stays in the Rule Base with an X showing that it is disabled. **Select "Disable rule" again to make the rule active.**

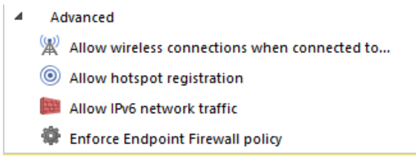
To delete or disable a rule:

1. Right-click in the NO column of a rule.
2. Select "Delete Rule" or "Disable Rule".

The rule is not physically deleted or disabled until you install the policy.

Advanced Firewall Settings

There are other actions besides Firewall Rules that control the network on machines.



- Advanced
  - Allow wireless connections when connected to...
  - Allow hotspot registration
  - Allow IPv6 network traffic
  - Enforce Endpoint Firewall policy

Wireless Connection Settings

These actions define if users can connect to wireless networks while on your organization's LAN.

This protects your network from threats that can come from wireless networks.

- **Allow connecting wireless to LAN:** Users can connect to wireless networks, while connected to the LAN
- **Do not allow connecting wireless to LAN:** Users cannot connect to wireless networks, while connected to the LAN.

Hotspot Settings

These actions define if users can connect to your network from hotspots in public places, such as hotels or airports.

- **Allow hotspot registration:** Bypass the firewall to let users connect to your network from a hotspot.
- **Do not allow hotspot registration:** Do not let users connect to your network from a hotspot.

IPv6 Traffic

You can select one of these actions to allow or block IPv6 traffic to endpoint computers.

- **Allow IPv6 network traffic:** Allows all traffic going through IPv6 protocols.
- **Block IPv6 network traffic:** Blocks all traffic going through IPv6 protocols.

Note: If IPv6 traffic is going through IPv4-based tunnels, service packets encapsulating this tunnel will be evaluated with IPv4 rules.

Choose a Firewall Policy to Enforce

By default, the Firewall policy enforced is the Endpoint Security Firewall Policy.

If your environment used Endpoint Security VPN, and then moved to the complete Endpoint Security solution, you might want to continue to use the Desktop Policy from SmartDashboard.

Select which Firewall policy to enforce:

- **Enforce the above Firewall policy:** Use the Endpoint Security Firewall Policy
- **Enforce Desktop Policy from SmartDashboard:** Use the Desktop Policy from SmartDashboard

1. Select Enforce Desktop Policy from SmartDashboard.
2. Install Policy.
3. Restart all computers included in the rule.

Defining Access Zones Policy

Access Zones lets you create security zones for use in Firewall. **Configure Access Zones before configuring Firewall.**

There are two predefined Access Zones:

- The Internet Zone
- The Trusted Zone

Network locations not placed in the Trusted Zone automatically belong to the Internet Zone.

Note that Access Zones rules are computer-centric (and not user-centric).

Trusted Zone

The Trusted Zone contains network objects that are trusted. Configure the Trusted Zone to include only those network objects with which your programs must interact.

Note: Objects not placed in the Trusted Zone are placed automatically in the Internet Zone.

SmartEndpoint contains an initial Access Zones policy. In the initial policy, these network elements are included in the Trusted Zone:

- **All_Internet**

  This object represents all legal IP addresses. In the initial policy, all IP addresses on the Internet are trusted. However, the Access Zones policy is not a policy that is enforced by itself, but only as a component of the Firewall policy.

- **LocalMachine_Loopback**

  Endpoint computer's loopback address: 127.0.0.1.
  The Endpoint must always have access to its own loopback address.
  Note: Endpoint users must not run software that changes, or hides the local loopback address, for example personal proxies that enable anonymous Internet surfing.

Objects in the Trusted Zone

Think about adding these objects to your Trusted Zone:

- Remote host computers accessed by your programs (if not included in the subnet definitions for the corporate network)
- Corporate WANs accessed by your programs
- Endpoint Security Management Server

- Domain controllers
- File servers and Print servers
- VPN gateway address range
- Internet gateways
- Local subnets
- Security servers (for example, RADIUS, ACE, or TACACS servers)
- Other IP addresses, or IP ranges, to which access is allowed or denied.

Changing the Access Zones Policy

The main component of the Access Zones policy rule is the definition of the Trusted Zone.

All objects that are not in the Trusted Zone are automatically in the Internet Zone. If necessary, you can create new Trusted Zone objects to use in different policy rules.

You can add and remove network objects from a Trusted Zone.

Note: A computer can have only one Trusted Zone. **This means that if the Access Zones policy has more than one rule, and more than one Trusted Zone applies to a computer, only the last Trusted Zone is enforced.**

To define the Trusted Zone:

1. In the 'Policy tab > Access Zones rule', double-click "Corporate Trusted Zones", or right-click it and select "Edit Shared Action". The Edit Properties - Access Zones window opens.
2. To add an existing object to the Trusted Zone Locations list:

   a. Select a network object from "Available Network Objects".

   b. Click "Add".
3. To remove an existing object:

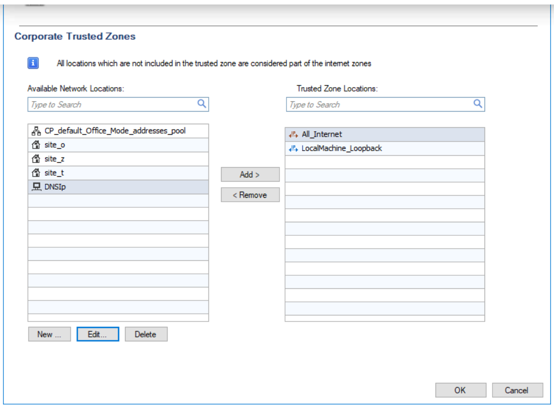
   a. Select the network object from the list.

   b. Click the "Remove" arrow.
4. To delete an existing object, select the object and click "Delete".
5. To create a new Network Object, click "New". The "Select New Object Type" window opens.

   a. Select an object type from the list.

   b. Click "OK". The Properties window for the selected object opens.

   c. Enter the required data.
6. Click "OK".



Corporate Trusted Zones

All locations which are not included in the trusted zone are considered part of the internet zones

Available Network Locations:

- CP_default_Office_Mode_addresses_pool
- site_o
- site_z
- site_t
- DNSIp

Trusted Zone Locations:

- All_Internet
- LocalMachine_Loopback

To create a new Trusted Zone object:

1. In the 'Policy tab > Access Zones rule', double-click "Corporate Trusted Zones", or right-click it and select "Edit Properties". The Properties window opens.
2. In the "Select action" field, select "New".
3. Edit the Name and Description of the Zone.
4. Click "OK".
5. Edit the network locations in the zone, as described in the procedure above.

Network Objects

Access Zones are made up of network objects.

You define network objects by specifying one or more:

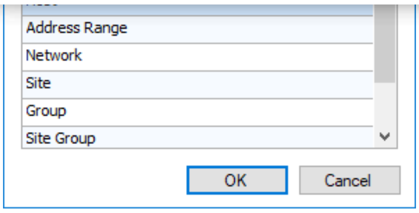
- Host
- IP address range
- Network
- Site

Create network objects for areas that programs must have access to, or areas that programs must be prevented from accessing.

Define objects for each policy, or define objects before you create a policy. After defining an object, the object can be reused in other policies.

The same Network Objects and Services are used throughout SmartEndpoint and in SmartDashboard. When you create a new object, it is also available in SmartDashboard. If you change an object in SmartEndpoint or SmartDashboard, it is changed everywhere that the object is used.

Note: The Trusted Zone and the Internet Zone can also be used as objects in a firewall policy. These objects are resolved dynamically by the client, based on Access Zones policy assignment to the client.

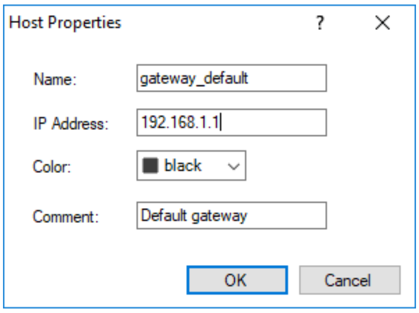


Address Range
Network
Site
Group
Site Group

Configuring a Host as a Network Object

Enter data that defines the network object:

- **Name:** A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
- **IP Address:** The IP address of the host you want to use as a network object.
- **Color:** Select a color to be used for the icon for this network object.
- **Comment:** A description of the network object.



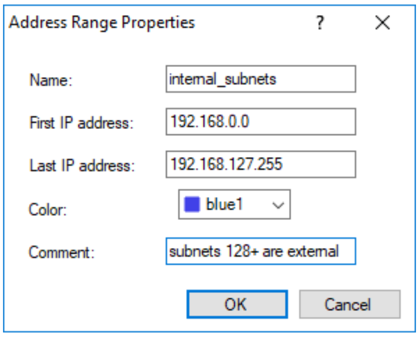
Host Properties

Name: gateway_default
IP Address: 192.168.1.1
Color: ■ black
Comment: Default gateway

Configuring an Address Range as a Network Object

Enter data that defines the network object:

- **Name:** A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
- **First IP Address / Last IP Address:** The first and last IP addresses for the network object.
- **Color:** Select a color to be used for the icon for this network object.
- **Comment:** A description of the network object.



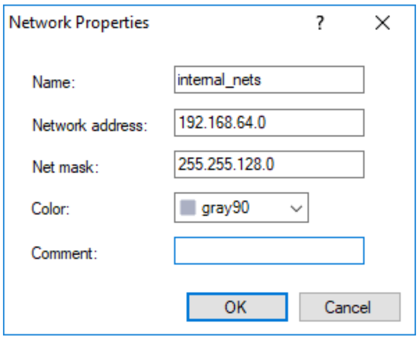
Address Range Properties

Name: internal_subnets
First IP address: 192.168.0.0
Last IP address: 192.168.127.255
Color: ■ blue1
Comment: subnets 128+ are external

Configuring a Network as a Network Object

small letters, numbers and '_'. All other characters are prohibited.

- **Network Address:** The network address you want to use as a network object.
- **Net Mask:** The net mask.
- **Color:** Select a color to be used for the icon for this network object.
- **Comment:** A description of the network object.



Network Properties

Name: internal_nets

Network address: 192.168.64.0

Net mask: 255.255.128.0

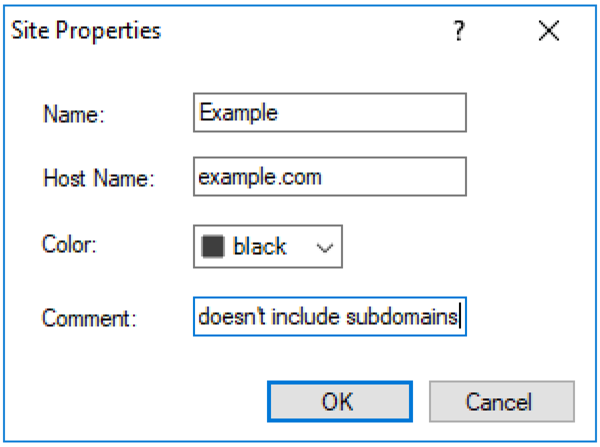
Color: gray90

Comment:

Configuring a Site as a Network Object

Enter data that defines the network object:

- **Name:** A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
- **Host Name:** The full LDAP name of the host of the site you want to use as a network object.
  For example, www.example.com.
  Note: Sub-sites must be added separately, if you want to apply the rule to them, as well. **Wildcard symbols like * are not allowed.**
  Note: www.example.com and example.com may have different IP addresses. In such cases, both domain names should be added.
- **Color:** Select a color to be used for the icon for this network object.
- **Comment:** A description of the network object.



Site Properties

Name: Example

Host Name: example.com

Color: black

Comment: doesn't include subdomains

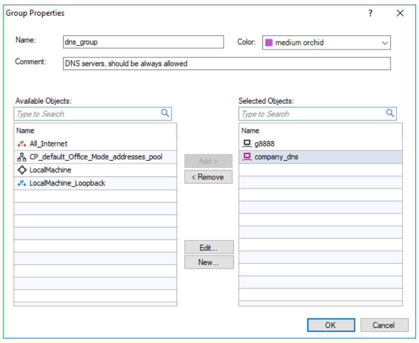
Configuring a Group as a Network Object

- **Name:** A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.

- **Color:** Select a color to be used for the icon for this network object.

- **Comment:** A description of the network object.

After this, select from the "Available Objects" column, or create new objects.



Group Properties

Name: dns_group

Color: medium orchid

Comment: DNS servers, should be always allowed

Available Objects:

- All_Internet
- CP_default_Office_Mode_addresses_pool
- LocalMachine
- LocalMachine_Loopback

Selected Objects:

- g8888
- company_dns

Configuring a Site Group as a Network Object

Enter data that defines the network object:

- **Name:** A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.

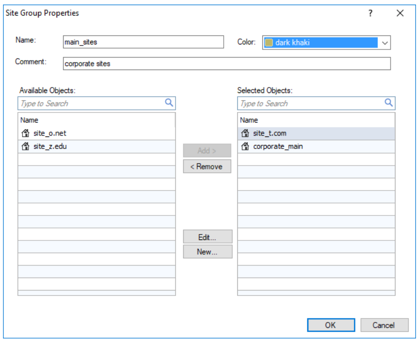
- **Color:** Select a color to be used for the icon for this network object.

- **Comment:** A description of the network object.

After this, select an object from the Available Objects column, or create a new object of the following types:

- Site

- Site Group



Site Group Properties

Name: main_sites

Color: dark khaki

Comment: corporate sites

Available Objects:

- site_o.net
- site_z.edu

Selected Objects:

- site_t.com
- corporate_main

Defining Application Control Policy

The Application Control blade restricts network access for specified applications.

The Endpoint Security administrator defines policies and rules that allow, block, or terminate applications and processes.

If specified in an Application Control rule, an alert shows which application was blocked or terminated.

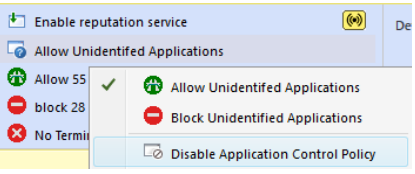
You can also enable the Reputation Service (previously called the Program Advisor) to recommend applications to allow or block.

Firewall Blade can be installed on Windows Server machines in the same way as on workstation. **Application Control is not supported on Windows Server.**

Application Control can be disabled in the policy, or uninstalled from a machine together with the Firewall Blade.

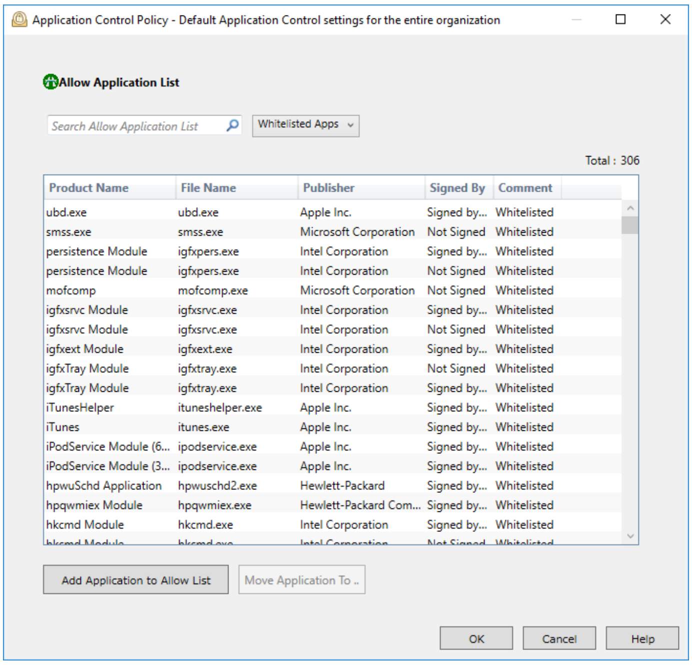
To disable Application Control:

1. In an Application Control Rule, select an action that disables Application Control.
2. Install the policy on all clients that run Windows Server.


Enable reputation service
De
Allow Unidentifed Applications
Allow 55
block 28
No Termi
✓
Allow Unidentifed Applications
Block Unidentified Applications
Disable Application Control Policy

Working with the Application Control Policy

Configure which applications are allowed, blocked, or terminated and what happens when applications are not identified.


Application Control Policy - Default Application Control settings for the entire organization

Allow Application List

Search Allow Application List

Whitelisted Apps

Total : 306

Product Name	File Name	Publisher	Signed By	Comment
ubd.exe	ubd.exe	Apple Inc.	Signed by...	Whitelisted
smss.exe	smss.exe	Microsoft Corporation	Not Signed	Whitelisted
persistence Module	igfxpers.exe	Intel Corporation	Signed by...	Whitelisted
persistence Module	igfxpers.exe	Intel Corporation	Not Signed	Whitelisted
mofcomp	mofcomp.exe	Microsoft Corporation	Not Signed	Whitelisted
igfxsrvc Module	igfxsrvc.exe	Intel Corporation	Signed by...	Whitelisted
igfxsrvc Module	igfxsrvc.exe	Intel Corporation	Not Signed	Whitelisted
igfxext Module	igfxext.exe	Intel Corporation	Signed by...	Whitelisted
igfxTray Module	igfxtray.exe	Intel Corporation	Not Signed	Whitelisted
igfxTray Module	igfxtray.exe	Intel Corporation	Signed by...	Whitelisted
iTunesHelper	ituneshelper.exe	Apple Inc.	Signed by...	Whitelisted
iTunes	itunes.exe	Apple Inc.	Signed by...	Whitelisted
iPodService Module (6...	ipodservice.exe	Apple Inc.	Signed by...	Whitelisted
iPodService Module (3...	ipodservice.exe	Apple Inc.	Signed by...	Whitelisted
hpwuSchd Application	hpwuschd2.exe	Hewlett-Packard	Signed by...	Whitelisted
hpqwmiex Module	hpqwmiex.exe	Hewlett-Packard Com...	Signed by...	Whitelisted
hkcmd Module	hkcmd.exe	Intel Corporation	Signed by...	Whitelisted
hkcmd Module	hkcmd.exe	Intel Corporation	Not Signed	Whitelisted

To configure the allowed applications:

1. In the 'Policy tab > Application Control rule', right-click the "Allowed Apps" Action, and select "Manage Allowed Apps List".
2. To add more applications, click "Add", and select applications from the "Search Applications" window.

To configure the blocked applications:

1. In the 'Policy tab > Application Control rule', right-click the "Block Apps" Action, and select "Manage Blocked Apps List".
2. To add more applications, click "Add", and select applications from the "Search Applications" window.
3. Click "OK".

To configure terminated applications:

1. In the 'Policy tab > Application Control rule', right-click the "Terminated Apps" Action, and select "Manage Terminated Apps List".
2. To add more applications, click "Add", and select applications from the "Search Applications" window.
3. Click "OK".

If you "block unidentified applications", users can only access applications that are included in the "Allowed Apps List".

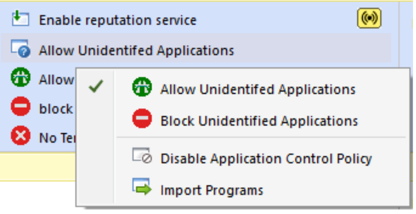
If you "allow unidentified applications", users can access all applications that are not on the "Blocked" or "Terminated" Lists.

If you "allow unidentified applications", make sure your "Blocked" and "Terminated" Lists are complete.

To configure what happens to unidentified applications:

In the 'Policy tab > Application Control rule', select "Block Unidentified Applications", or right-click and select "Allow Unidentified Applications".

Note: Terminated applications are not allowed to pass through the firewall.


Enable reputation service
Allow Unidentifed Applications
Allow
block
No Te
✓ Allow Unidentifed Applications
Block Unidentified Applications
Disable Application Control Policy
Import Programs

Reputation Service

The Check Point Reputation Service is an online service that automatically creates recommended rules that block or allow common applications.

These rules are based on the recommendations of Check Point security experts.

Note: Your Endpoint Security Management Server must have Internet access (on ports 80 and 443) to connect to the Check Point Reputation Service Server.

Note: Make sure that your firewall allows this traffic. It is recommended to add the Reputation Service Server to your Trusted Zone.

To see the recommendations of the Reputation Service for safe applications:

2. In the "Allow Applications List", select "Good Reputation" from the options menu. A list of applications with a good reputation, generated by the "Reputation Service", opens. You can move applications to the "Block" or "Terminate" lists.

To see the recommendations of the Reputation Service for malicious applications:

1. In the "Application Control" rule, right-click the "Terminated Apps" action and select "Manage Terminated Apps List".
2. In the "Terminate Application List", select "Known Malware Apps" from the options menu. A list of malicious applications, generated by the "Reputation Service", opens. You can move applications to the "Block" or "Allow" lists.

Using the Reputation Service with a Proxy

If your environment includes a proxy server for Internet access, perform the configuration steps below to let the Endpoint Security Management Server connect to the Check Point Reputation Service Server via the proxy server. **Note that all configuration entries are case-sensitive.**

If your organization uses a proxy server for HTTP and HTTPS traffic, you must configure the Endpoint Security Management Server to work with the proxy server.

To configure use of a proxy server:

1. From the Endpoint Security Management Server command line, run: *cpstop*.
2. Go to *$UEPMDIR/engine/conf* and open the *local.properties* file in a text editor.
3. Add a line for these properties:
    - The proxy server IP address: *http.proxy.host=<ipaddress>*
    - The proxy server listening port (typically 8080): *http.proxy.port=<port>*
    - If authentication is enabled on the proxy server, add these lines:
        - (Do not add these lines, if authentication is not required.)
        - *http.proxy.user=<username>*
        - *http.proxy.password=<password>*
        - Make sure that you delete (or do not insert) the '#' character at the beginning of these lines.
4. Save *$UEPMDIR/engine/conf/local.properties* and then close the text editor.
5. Run: *cpstart*.

Importing Program References

The Appscan command lets you automatically create Application Control rules for common applications and operating system files on an endpoint computers network.

identifiers for programs that cannot be forged. This prevents malicious programs from masquerading as other, innocuous programs.

Create an Appscan for each disk image used in your environment. You can then create rules that will apply to those applications. You can create Appscan files by running the *appscan.exe* utility on a computer with a tightly-controlled disk image, then importing the file into Endpoint Security.

Creating an Appscan XML File

Before you can use *Appscan*, set up a Windows computer with the typical applications used on protected computers in your organization.

If you have several different configurations, perform these steps for each one.

Important: The computer you scan to create an Appscan must be free of all malware.

To run Appscan from the command line:

1. Download the appscan tool from sk108536 to the root directory (typically c:\) of the baseline reference source computer.
2. From the target computer command prompt, go to the root directory, or to a specific directory to scan (for example, c:\program files).
3. Run *appscan* with the applicable parameters. When the scan is complete, an output file (Default = *scanfile.xml*) is created in the specified directory.

Appscan Command Syntax

The *Appscan* utility scans the host computer and creates an XML file that contains a list of executable programs and their checksums. This XML file is used by the Check Point Reputation Service to create recommended rules to block or allow common applications.

Syntax

appscan [/o <filename>] [/s <target directory>] [/x <extension string>]
[/e] [/a] [/p] [/verbose] [/warnings] [/?] [/help]

Parameters

<filename>: Output file name and path.
/o: Sends output to the specified file name. If no file name is specified, *Appscan* uses the default file name (*scanfile.xml*) in the current folder.
/s: Specifies the directory, including all subdirectories, to scan.

- You must enclose the directory/path string in double quotes.
- If no directory is specified, the scan runs in the current directory only.

/x: Specifies the file extension(s) to include in the scan.

- The extension string can include many extensions, each separated by a semi-colon.

- You must specify a target directory using the **/s** switch.
- If you do not use the **/x** parameter, only *.exe* executable files are included in the scan

/e: Include all executable files in the specified directory regardless of the extension.
Do not use /e together with /x.
/a: Includes additional file properties for each executable.
/p: Shows progress messages during the scan.
/verbose: Shows progress and error messages during the scan.
/warnings: Shows warning messages during the scan.
/? or /help: Shows the command syntax and help text.

Examples

- *appscan /o scan1.xml*

  This scan, by default, includes *.exe* files in the current directory and is saved as *scan1.xml*.

- *appscan /o scan2.xml /x ".exe;.dll" /s "C:\"*

  This scan includes all *.exe* and *.dll* files on drive C and is saved as *scan2.xml*.

- *appscan /o scan3.xml /x ".dll" /s c:\program files*

  This scan included all *.dll* files in *c:\program* files and all its subdirectories. It is saved as *scan3.xml*.

- *appscan /s "C:\program files" /e*

  This scan includes all executable files in *c:\program* files and all its subdirectories. It is saved as the default file name *scanfile.xml*.

Importing Appscan XML Files

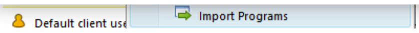
After you generate the Appscan XML file, you can import it to the Endpoint Security Management Server.

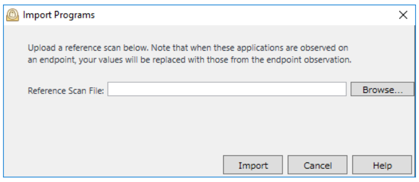
Note: You must remove all special characters, such as trademarks or copyright symbols, from the XML file before importing it.

To import an Appscan XML file:

1. In the 'Policy tab > Application Control rule', right-click the "Allowed Apps List".
2. Select "Import Programs".
3. In the "Import Programs" window, go to and select the applicable Appscan XML file.
4. Click "Import".

Note: When applications, included in the imported file, are found on endpoint computers, they are automatically added to the Allowed or Block applications group.




Import Programs

Upload a reference scan below. Note that when these applications are observed on an endpoint, your values will be replaced with those from the endpoint observation.

Reference Scan File:

Defining Other Firewall and Application Control Settings

Disable Network Protection

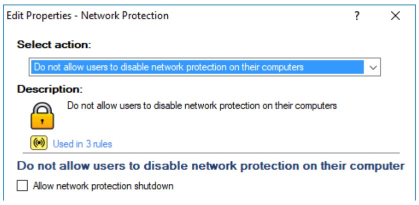
Network Protection is a term meaning Firewall and Application Control Blade.
You can let users disable network protection on their computers.

Warning: If users disable network protection, their computers will be less secure and vulnerable to threats.

Note: If the policy does not allow users to disable network protection, administrators can assign permissive policies to temporarily disable network protection for specified users.

These are the actions in the Client Settings Policy:

- **Allow users to disable network protection on their computers:** New option (Disable Network Protection) shown in the right-click menu of the client icon from the notification area.
- **Do not allow users to disable network protection on their computers:** Only administrators can disable user's network protection.


Edit Properties - Network Protection

Select action: Do not allow users to disable network protection on their computers

Description:

Do not allow users to disable network protection on their computers

Used in 3 rules

Do not allow users to disable network protection on their computer

☐ Allow network protection shutdown

Allow Network Protection Alerts

Alerts are notifications shown to users after some events happen on machines.
Firewall Blade can show alerts, when it identifies some packets according to the Firewall Policy.

To configure the Network Protection Alerts:

1. In the "Policy" tab, "Client Settings" rule, double-click the "Network Protection" Action.
2. Click "Edit Properties".
3. In the "Network Protection" section, select or clear these options for each Software Blade:

-
    - **Allow Log:** Generate logs for events.
    - **Allow Alert:** Generate alerts for events.

You must also set "Alert" in the "Track" column of Firewall rules.

Enforcing Rules According to States

Endpoint Security can enforce policy rules on computers and users, based on their connection and compliance state.

When you create a policy rule, you can select the state or states, during which this policy is enforced. **By default, policies apply when the client is Connected.**

States are not applicable for all blades. For example, **Full Disk Encryption rules always apply and cannot change based on state.** The option to create rules, based on state, is only displayed for applicable blades.

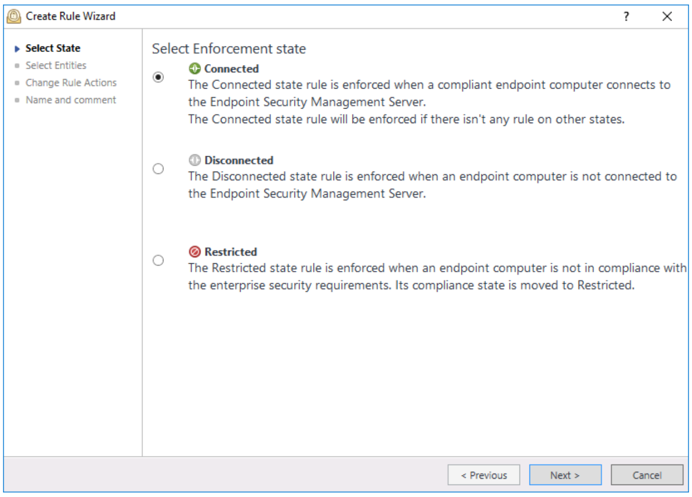
If there is no applicable rule for the "Disconnected" or "Restricted" states, the "Connected" policy applies.

- The "Connected" state policy is enforced, when a compliant endpoint computer connects to the Endpoint Security Management Server.
- The "Disconnected" state policy is enforced, when an endpoint computer is not connected to the Endpoint Security Management Server. For example, you can enforce a more restrictive policy, if users are working from home and are not protected by organizational resources.
- The "Restricted" state policy is enforced, when an endpoint computer is not in compliance with the enterprise security requirements. Its compliance state is moved to "Restricted". **In the "Restricted" state, you usually choose to prevent users from accessing some, if not all, network resources.**

To configure conditions when "Restricted" policy is applied, check the Compliance Policy section in the Endpoint Security Administration Guide.

Restricted state policies can be configured for the following blades:

- Firewall
- Access Zones
- Application Control
- Media Encryption & Port Protection



Select Enforcement state

● Connected
The Connected state rule is enforced when a compliant endpoint computer connects to the Endpoint Security Management Server.
The Connected state rule will be enforced if there isn't any rule on other states.

○ Disconnected
The Disconnected state rule is enforced when an endpoint computer is not connected to the Endpoint Security Management Server.

○ Restricted
The Restricted state rule is enforced when an endpoint computer is not in compliance with the enterprise security requirements. Its compliance state is moved to Restricted.

This section describes known problems and general troubleshooting recommendations.

Known problems and solutions for them

Wireshark is not showing outgoing packets

Other tools can be used: npcap instead of winpcap driver, or Microsoft Network Monitor instead of Wireshark.

Communication between VMWare Host and VM fails

This is a known issue and can be resolved with a special utility. See sk104622 for more information.

No network access when some 3rd party network software is installed

This is a known issue in some specific cases. These cases can be resolved with a special package. See sk99065 for more information.

Wireless adapter is disabled when virtual LAN adapter is enabled

This is a known issue and can be resolved with a special utility. See sk123318 for more information.

General troubleshooting Approaches

Traffic is dropped

Typically, this happens because of some misconfigured rule in the Firewall Rules.

The following actions can be performed:

1. Assigning an all-allowing policy can confirm that traffic is blocked by the Firewall Blade.
2. Firewall Rules can be set up to log blocked actions. After this, Firewall logs in SmartViewTracker, or in Local Log Viewer Utility, can be examined to find the blocking rule.

Contact Check Point Support if the above steps do not help.

Application is blocked

A full list of blocked applications can be found in the Firewall and Application Control Blade Client UI and in Logs.

The Administrator can move the application to the "Allowed Application" List, if it is blocked by policy.

Also note that applications can be blocked by other (3rd party) software, or by other Endpoint Security Software Blades (for example, Anti-Malware, Anti-Bot).

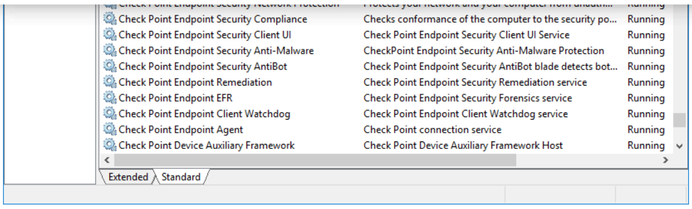
Contact Check Point Support if the above steps do not help.

Firewall and Application Control Blade is not running

Usually, this means that one of the corresponding services is not running.

Examine their status via the Control Panel Services utility.

Try to manually run services, if some of them are not running.



Check Point Endpoint Security Network Protection	Protects your network and your computer from unauth...	Running
Check Point Endpoint Security Compliance	Checks conformance of the computer to the security po...	Running
Check Point Endpoint Security Client UI	Check Point Endpoint Security Client UI Service	Running
Check Point Endpoint Security Anti-Malware	CheckPoint Endpoint Security Anti-Malware Protection	Running
Check Point Endpoint Security AntiBot	Check Point Endpoint Security AntiBot blade detects bot...	Running
Check Point Endpoint Remediation	Check Point Endpoint Security Remediation service	Running
Check Point Endpoint EFR	Check Point Endpoint Security Forensics service	Running
Check Point Endpoint Client Watchdog	Check Point Endpoint Client Watchdog service	Running
Check Point Endpoint Agent	Check Point connection service	Running
Check Point Device Auxiliary Framework	Check Point Device Auxiliary Framework Host	Running

Contact Check Point Support if the above steps do not help.

Collecting Debug Information

CPinfo Utility

On all systems installed with Endpoint Security there is a debug log collector, accessible via the Endpoint Security Client Application. The tool is called CPInfo. Refer tosk90445 for more information.

CPInfo can be executed in Basic, General and Extended modes. For faster investigation, always select Extended mode, as it contains more information.

Other Debugging Tools

In some cases, Check Point Support may use some other debugging tools. It can be common troubleshooting tools like Wireshark or Process Monitor, or can be some Check Point-specific tools.

These Check Point-specific tools either control and check some internal settings, and states of Firewall and Application Control Blade components, or enable additional logging.

Check Point Support will provide explanations about performed tests and used tools, if needed.

Article Properties

Access Level
General

Date Created
2019-12-24

Last Modified
2023-06-14

Was this page helpful? Yes No

Haven't found what you're looking for?

Our customer support team is only a click away and ready to help you 24 hours a day.