

Oracle Enterprise Manager 10g Grid Control Getting Started Guide for Check Point Firewall Plug-in

This document provides a brief description about the Check Point Firewall plug-in, details on the versions supported by the plug-in, pre-requisites for installing the plug-in, and step-by-step instructions on how to download, install and use the plug-in.

Description

The Check Point Firewall plug-in extends Oracle Enterprise Manager to add support for managing Check Point Firewalls. The current version of the plug-in has the following features:

- o Monitor Check Point Firewall devices
- o Raise alerts and violations based on thresholds and policies set on monitoring and configuration data
- o Out-of-box UI rich reports based on the gathered data

The plug-in can be deployed to agent that remotely monitors the Check Point firewall. It is not required that Oracle Enterprise Manager agent to be on the same machine as Check Point firewall.

Versions Supported

The plug-in works with Enterprise Manager 10gR2 and higher. It supports the following versions of Check Point Firewall:

1. NG- AI(R54), NG-AI (R55), NG-AI (R60)
2. Future versions of Check Point Firewall provided they are backward compatible

Pre-requisites

This section outlines all the pre-requisite software and hardware setup needed to deploy and use the plug-in.

1. If 'SNMP Community' (other than default community "public") is configured and the same is required to be used for monitoring the Check Point Firewall Target, the EMAgent's IP Address needs to be added for the particular SNMP Community.
2. Specific requirement for Operating Systems:
 - a. **Linux:** Firewall SNMP daemon to be running on the Check Point Firewall Device
 - b. **Windows:**
 - Standard Windows SNMP Agent installed and SnmpService running
 - Firewall SNMP sub-agent /extension agent installed (Please see "[Pre-requisite Installation Steps](#)" section for more details)
 - c. **Check Point SecurePlatform:**
 - SNMP service is enabled

Installation Steps

1. Ensure the pre-requisites (SNMP daemon/service) is installed/running:
2. Download Check Point Firewall Plug-in archive from OTN or OPN website to your desktop or machine on which the browser is launched
3. Please refer to the following sections for deployment and undeployment.

Deployment Steps

1. Log into Enterprise Manager as a user with administrator privilege.
2. Click on setup link on the upper right and management plug-ins link on the left.
3. Click on the import button.
4. Click on the browser button and select the plug-in archive. Click on List Archive button. Select the plug-in and click on OK button.

5. In the management plug-ins page, check the box next to the plug-in name that you want to deploy, click on the icon in the deploy column.
6. Click on Add Agents button. Select the agent you want to deploy the plug-in to and click on next. Click on Finish.
 - If you get error message that says the preferred credential is not set up, go to preferences page and add the preferred credential to the host and agent.

Verification/Validation Steps

1. Locate Check Point Firewall target type under the agent where the archive was deployed. Add the plug-in. The fields that you will need to specify are:
 - a. Name: A Name for the plug-in
 - b. Firewall Host or IPAddress: The name/IPAddress of the Check Point Firewall device.
 - c. Check Point SNMP Daemon port: The port number where the Check Point SNMP daemon is running (default – 260 on UNIX platforms).
 - d. Host SNMP Daemon port: The port number where the native OS SNMP daemon is running (default – 161).
 - e. SNMP community: The community name for which the agent IPAddress is added (default – public)
 - f. SNMP Timeout – Timeout value by when the SNMP call should be terminated (recommended – 5)
2. Locate plug-in under the Targets tab.
3. Ensure metric collection is working without failures
4. Ensure reports can be seen
5. Ensure Configuration data can be seen

Undeployment Steps

1. Log into Enterprise Manager as a user with administrator privilege.
2. Go to All Targets page and select on the target of the plug-in target type. Click on Remove button. You need to do it for all targets of that plug-in target type.
3. Click on setup link on the upper right and management plug-ins link on the left.
4. Check the plug-in target type that you want to undeploy. Click on the icon in Undeploy column.
5. Check all the agents that have that plug-in type deployed and click on OK.
6. Select the plug-in target type and click on Delete button.

Pre-requisite Installation Steps

Following is a summary of the installation steps for the pre-requisites. For more Check Point Firewall specific details, refer to the Check Point documentation.

1. Steps for enabling SNMP Gets on Check Point Firewall device

Changes by platform

 - a. Linux:
 - i. The “snmpd.conf” file is located under ‘/etc/snmp’ or ‘/etc/SnmpAgent.d’. (Please refer [SNMP.CONF](#) under section “Directories Searched” for more details)
 - ii. Edit the snmpd.conf to enable the SNMP calls for the following OIDs
 # Make at least snmpwalk -v 1 localhost -c public system fast again.
 # name incl/excl subtree mask(optional)
 view systemview included .1.3.6.1.2.1.1
 view systemview included .1.3.6.1.2.1.2
 view systemview included .1.3.6.1.4.1.2021.11
 view systemview included .1.3.6.1.4.1.2021.4

view systemview included .1.3.6.1.2.1.25

- iii. Enable the Check Point SNMP Extension via “cpconfig” command. On Unix platforms a special Check Point SNMP daemon called cpsnmpd, is installed. This daemon provides status information on VPN-1 Pro specific objects. This daemon is not run by default. The daemon is enabled or disabled through cpconfig. Once enabled, the daemon listens on port 260.

Note - The standard Unix SNMP daemon loads before the Check Point daemon and binds to port 161. If the regular daemon is not running, cpsnmpd binds to both ports (161 and 260). If both ports are occupied by a previous process, the Check Point daemon will not run. Further, if the Check Point daemon receives a request for an unrecognized OID, it does not forward this to the standard snmp OS daemon.

- b. Windows
 - i. Refer to the Windows User Guides to install and configure the SNMP Service.
 - ii. When the firewall is installed, a special Check Point dynamic link library (DLL) is listed in the window’s registry. The SNMP service running on the Operating System loads this DLL. The SNMP service listens in the standard way on port 161 for incoming SNMP requests from the SNMP Network Management Station. The Check Point DLL extends the Windows NT SNMP service to identify those status requests directed at Check Point products.
- c. Check Point SecurePlatform

Check Point SecurePlatform is a prehardened operating system that can be deployed on Intel- or AMD-based open servers. A net-snmp daemon provides access to OS-MIB-II and a Check Point AgentX daemon provides access to the Check Point product MIB.

 - i. By default the SNMP service is disabled. Enable it with the command “snmp service enable”.
 - ii. Basic configuration can be done using the “snmp” command.”


```
snmp service enable [<portnumber>]
snmp service stat
snmp service disable
snmp user add noauthuser <username> [oidbase <OID>]
snmp user add authuser <username> pass <passphrase> [priv
<privacyphrase>] [oidbase <OID>]
snmp user del <username>
snmp user show [<username>]
```
 - iii. Additional configuration can be done by editing /etc/snmp/snmpd.conf.