

**IBA SPLAT Management Dashboard 1.0**  
Installation and User Guide

## Contents

Introduction .....	3
Installation .....	3
Software requirements .....	3
Network requirements .....	3
Using Installation Wizard .....	3
Initial launch .....	3
Configuration .....	4
Changing preferences .....	4
Licensing .....	4
Adding managed devices .....	4
Migration .....	5
Managing your Check Point SecurePlatform devices .....	5
Software inventory .....	5
Process list .....	6
File Operations .....	6
Launch PuTTY .....	6
Upload file .....	6
Export Configuration .....	6
Web UI Operations .....	7
Hardware Inventory .....	7
Network -> Interface Information .....	7
Network -> Route Information .....	7
Network -> Netstat .....	7
Network -> Arp Table .....	7
Statistics -> FW Statistics .....	7
Statistics -> Memory and Misc .....	7
Statistics -> Disk Usage .....	7
Statistics -> Internal Host Counter .....	7
Debug -> VPN Debug .....	7
Debug -> Certificate Authority .....	7
Debug -> FW-1 Daemons .....	8
Troubleshooting .....	8
Trademarks .....	8

# Introduction

Thank you for using SPLAT Management Dashboard (SPLAT.MD). This document describes how to install, configure and use SPLAT.MD.

SecurePlatform is a very robust and secure operating system which provides best performance for Check Point software products.

SPLAT.MD was created to simplify management of Check Point SecurePlatform-based devices thus reducing TCO in large deployments.

Easy-to-use SPLAT.MD GUI provides:

- SecurePlatform file system operations,
- convenient export of device configuration,
- point-and-click debug,
- simultaneous access to devices managed by different SmartCenters,
- and more.

# Installation

## Software requirements

SPLAT.MD can run on any Windows operating system supported by:

- Java Runtime Environment (JRE) Sun 1.4.2 or higher
- Java Runtime Environment (JRE) IBM 1.4.2 or higher

JRE can be downloaded:

<http://www.java.com/>

<http://www-128.ibm.com/developerworks/java/jdk/>

JRE must be installed prior installing SPLAT.MD.

## Network requirements

SPLAT.MD utilizes SSH protocol only to manage SecurePlatform devices.

So, please, verify that firewall rules, ACLs, etc. permit SSH connections (TCP port 22) from SPLAT.MD management station to every managed device and that SSH server is enabled on managed devices (it is enabled by default).

## Using Installation Wizard

To start installation run *SplatMDsetup.exe*. Please follow installation instructions.

After you have completed the Installation Wizard you can run SPLAT.MD.

## Initial launch

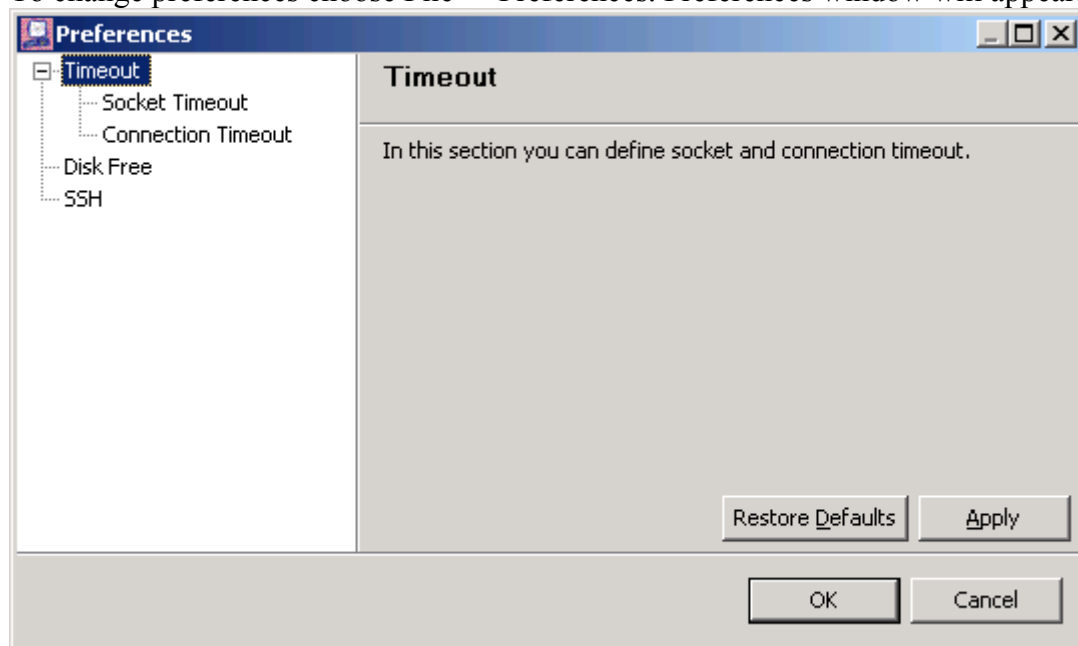
Running SPLAT.MD for the first time you will be asked for a password. It is highly recommended to choose strong password because it is used to protect *%HOMEDIR%\devices.enc* file that contains in encrypted form all configuration information including passwords to your managed devices!

Note: there is no way to decrypt *devices.enc* file in case your password is lost.

# Configuration

## Changing preferences

To change preferences choose File -> Preferences. Preferences window will appear.



Here you can change next settings:

**Socket timeout** – seconds to wait for connection to be established.

**Connection timeout** – seconds to wait for data within established connection.

**Disk free** – high disk usage watermark.

**SSH Enable Strict Host Key Checking** – show SSH host fingerprint for newly added devices as well as alerts when fingerprint changed.

Host keys are stored at `%HOMEPATH%\ssh_known_hosts\known_hosts` file.

## Licensing

Without license you can manage only one device. There are no other restrictions.

To add purchased license go to “Help -> License -> Activate License” and point to a *license.lic* file.

To verify that license was added successfully go to “Help -> License -> License” Information.

## Adding managed devices

With SPLAT.MD you can manage any type of SecurePlatform-based devices regardless of what type they are - SmartCenter, gateways, Log servers, etc. However, please note that not all actions make sense for all device types. For example you can run “Process List” against any SecurePlatform devices while it makes absolutely no sense to run HTTP Security Server debug on pure SmartCenter server.

There are several ways to add managed devices:

- Right click on “Devices” tab
- Using menu item: “Device -> Add Device”
- Click “Add Device” button on toolbar

Provide all required information:



**Add new SPLAT device to manage**  
Enter information for new device

Device Information

Name: gate3  
IP Address: 10.1.1.3  
Device Type: R61  
User: admin  
Password: .....

Finish Cancel

Please note that Check Point software release version must be specified correctly.

User with credentials entered here must be valid SecurePlatform user with *bash* shell.

Please note that user created by *adduser* command on SecurePlatform has *cpshell* as shell by default. It is necessary to manually edit */etc/passwd* file to change *cpshell* to *bash*.

*/etc/passwd* file should look like this:

```
root:x:0:0:root:/root:/bin/cpshell
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
rpm:x:37:37:/:var/lib/rpm:/sbin/nologin
pcap:x:77:77:/:var/arpwatch:/sbin/nologin
admin:x:0:0:/:home/admin:/bin/bash
```

### Migration

In order to backup SPLAT.MD managed devices list along with their properties just make a copy of *%HOMEDIR%\devices.enc* file.

## Managing your Check Point SecurePlatform devices

Select device and select desired task using:

- Right-click menu,
- “Task-> Menu,”
- Toolbar button

### Software inventory

Select this task to see rpm’s installed on the target device.

## Process list

Select this task to see process list.

Click any column title to change sort order.

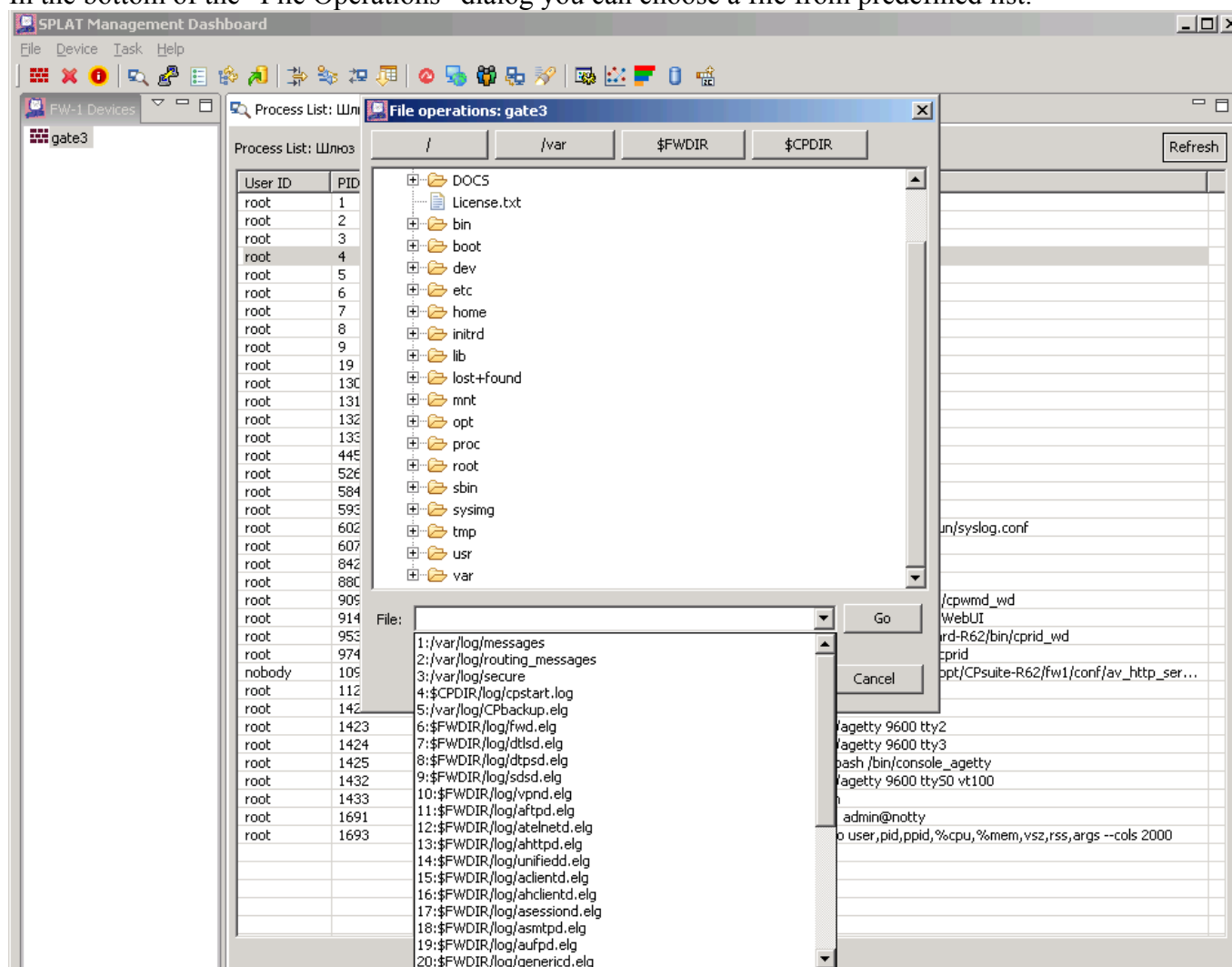
Right click on any process to kill it or to export process list to CSV file.

## File Operations

This task allows:

- walk through target file system,
- open files for viewing,
- open files for editing,
- download files,

In the bottom of the “File Operations” dialog you can choose a file from predefined list.



## Launch PuTTY

This task will launch ssh client PuTTY to connect to selected device.

## Upload file

Use this task to upload file from your workstation to target device.

## Export Configuration

Use this task to run *upgrade\_export* tool on target device and save exported configuration locally.

### **Web UI Operations**

Use this task to enable/disable SecurePlatform HTTPS web server.  
You can also select port to use for Web UI.

### **Hardware Inventory**

Use this task to see basic information about target device hardware.

### **Network -> Interface Information**

Use this task to get information about network interfaces.  
Press “Statistics” or “Advanced” to get more detailed information about particular interface

### **Network -> Route Information**

Use this task get information about routing table.

### **Network -> Netstat**

Use this task to display open sockets.  
Mark checkboxes to filter displayed information

### **Network -> Arp Table**

Use this task to display arp table.  
Click any column title to change sort order

### **Statistics -> FW Statistics**

Use this task to get Firewall-1 statistics

### **Statistics -> Memory and Misc**

Use this task Firewall-1 internal statistics about memory usage and more.

### **Statistics -> Disk Usage**

Use this task to display disk usage information per filesystem

### **Statistics -> Internal Host Counter**

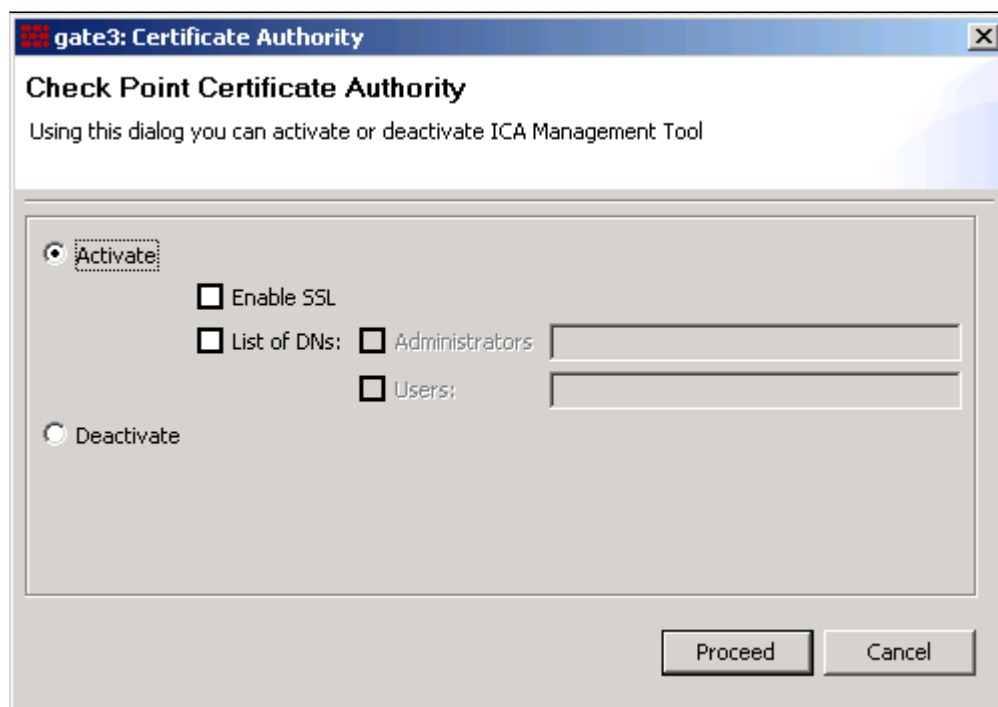
Use this task to display list of internal hosts counted by firewall.  
Please note that list will be empty if target device has Check Point license for unlimited number of hosts

### **Debug -> VPN Debug**

Use this task to switch on/off VPN debugging.  
Select desired item and mark checkbox to open log file.  
Note: do not forget to switch debug off! Otherwise you can get out of disk space on managed device.

### **Debug -> Certificate Authority**

Use this task to activate/deactivate ICA Management Tool.



You can change next settings:

- Enable SSL – when unmarked configures the ICA Management Tool server to use clear http rather than https. (**Use in emergency only! Without SSL anybody can connect to ICA Management Tool without any authentication!**)
- List of DNs – List of users who can connect to ICA Management Tool. Please use Check Point SmartDashboard to obtain users distinguished names.

Go to [http://target\\_ip:18265/](http://target_ip:18265/) or [https://target\\_ip:18265/](https://target_ip:18265/) after activating ICA Management Tool.

If SSL is enabled, please, ensure that you have added administrators using Check Point *cpca\_client* tool.

### Debug -> FW-1 Daemons

Use this task to switch on/off debugging of Firewall-1 daemons (in.ahhttpd, in.aftpd, fwd, etc.)

Note: do not forget to switch debug off! Otherwise you can get out of disk space on managed device.

## Troubleshooting

Before reporting a problem, please take next steps:

1. Check connectivity – verify that SSH port on target device is reachable from SPLAT.MD management station.
2. Check version – verify that Check Point software release version specified correctly in managed device properties.
3. Check target device type – verify that task you are running is applicable to the target device type.
4. Check user shell – verify that user has *bash* shell instead of *cpshell*.

## Trademarks

Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, ConnectControl, Connectra, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Office, SecureClient, SecureKnowledge, SecuRemote, SecurePlatform, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, SiteManager-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter,

## **IBA SPLAT Management Dashboard Installation and User Guide**

---

SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 UTM Edge, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Brand or product names are registered trademarks or trademarks of their respective holders. Eclipse is a trademark of Eclipse Foundation Inc.

Other company, product, and service names may be trademarks or service marks of others.