HARMONY ENDPOINT

Endpoint Best Practice & Troubleshooting

Marc Betti | SE

YOU DESERVE THE BEST SECURITY

OBJECTIVES

- Review Top Issue Areas
- Getting issues fixed faster
- Use info for Support KB Lookup - Find the solution
- Use info for internal SE/ Partner lookup – Non approved SKs
- Use info for TAC Support – Escalate the ticket faster

Agenda

- Requirements & Parameters
- Communications & Processes
- Client & Server Error Logging

Requirements & Parameters

Requirements & Parameters

Endpoint Security Home Page - sk117536

- Server Information
- Client Information
- Requirements
- Compatibility

Requirements & Parameters

Client Versions – Home Page

- **Recommended** - Extended QA testing - No new features
- **Latest** - Standard QA testing - Some New fixes & features
- **Custom** - Includes Hotfixes - Not in versions releases

Requirements & Parameters

Supported Configurations – Home page

- Client support per OS version - sk178408
- Server Supported Upgrade Paths - sk109196
- Server versions & Endpoint Security Client versions - sk107255
- OS Versions in development - sk115192

Requirements & Parameters

Tiny Nano Client

- EndpointSetup.exe /CreateMSI
- MAC OS - Now has Initial client
- Linux – Only AV

Requirements & Parameters

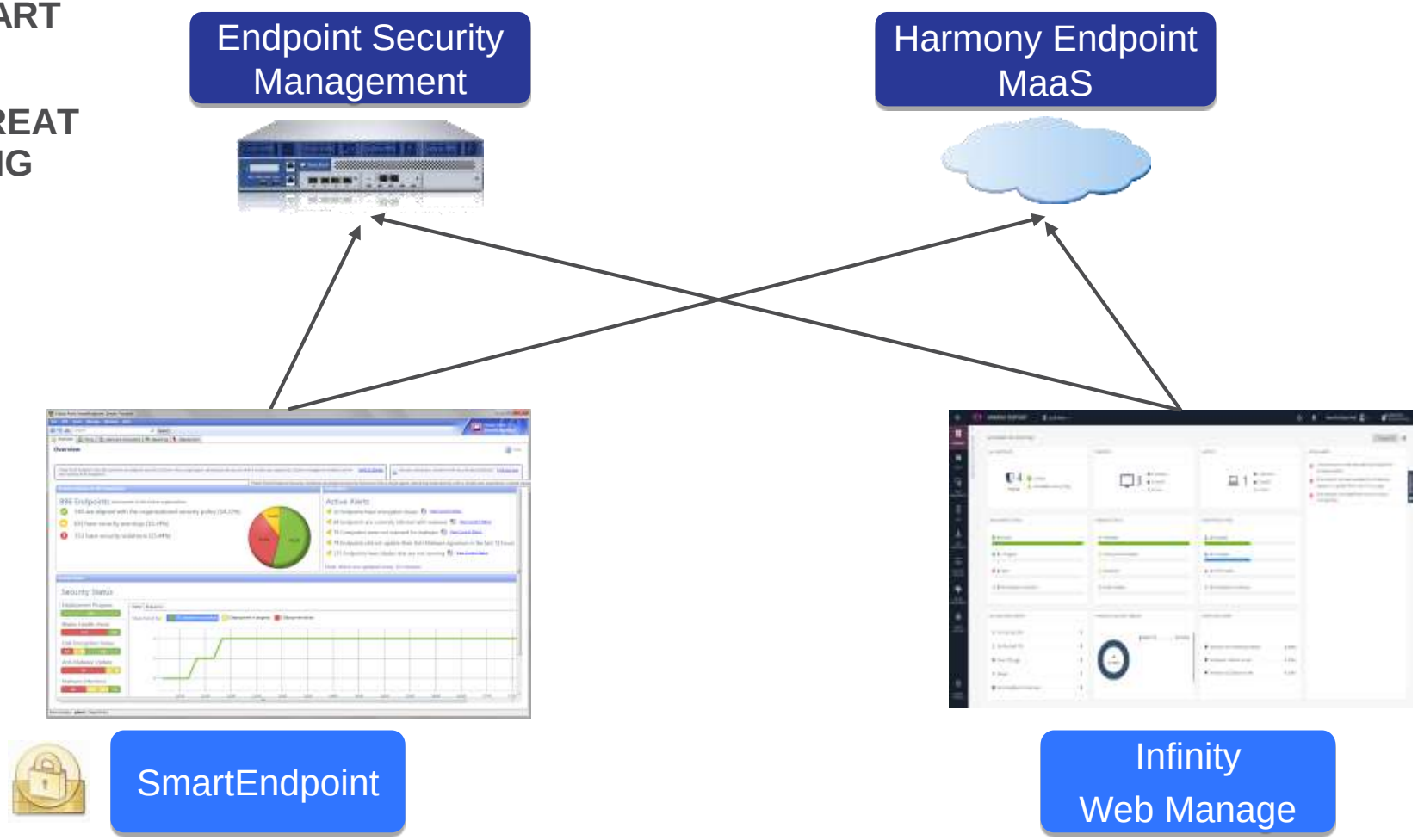
Compliance Enforcing all policies. No rules violated.	Enforce security policy to protect enterprise network
Anti-Malware No infections found	Protects your endpoint from unsecure, malicious and unwanted applications
Media Encryption and Port Protection No devices detected	Centrally enforce encryption of removable media and port control
Firewall and Application Control 0 Programs and 842 connections were blocked in the past 24 hours	Stop unwanted traffic, block targeted attacks
Full Disk Encryption 2 devices encrypted.	Automatically and transparently secure all information on endpoint HDD\SSD
Remote Access VPN Default gateway is il-cp.checkpoint.com	Provide secure, seamless access to corporate networks remotely
Capsule Docs Capsule Docs is externally managed	Secure your data with per-document encryption
URL Filtering Reason for Disable: Disabled by Endpoint Policy	(Legacy) Control access to web sites
Anti-Bot Monitoring	Prevent bot-related communication
Anti-Ransomware, Behavioral Guard and Forensics Monitoring	Stop Anti-Ransomware, unknown threats and view incident reports
Threat Emulation and Anti-Exploit 1 infection found	Protect against drive-by downloads, phishing sites, zero-day and memory attacks
Threat Hunting	Detailed threats overview

*Behavioral Guard and Anti-Exploit are not available for macOS

Requirements & Parameters

Management Architecture

- NO SMART EVENT
- NO THREAT HUNTING



- NO WEB FILTERING

Requirements & Parameters

- **Policies &**
- **Policy Mode**

	User/Computer	Computer
Threat Prevention	Anti-Malware Anti-Bot and URL Filtering Anti-Exploit Threat Emulation Anti-Ransomware Behavioral Guard Forensics	Anti-Malware Anti-Bot and URL Filtering Anti-Exploit Threat Emulation Anti-Ransomware Behavioral Guard Forensics
Access	Firewall Application Control Compliance	Firewall Application Control Compliance
Data Protection	Media Encryption Port Protection Full Disk Encryption OneCheck	Media Encryption Port Protection Full Disk Encryption OneCheck
Client Settings	Client Settings	Client Settings

Requirements & Parameters

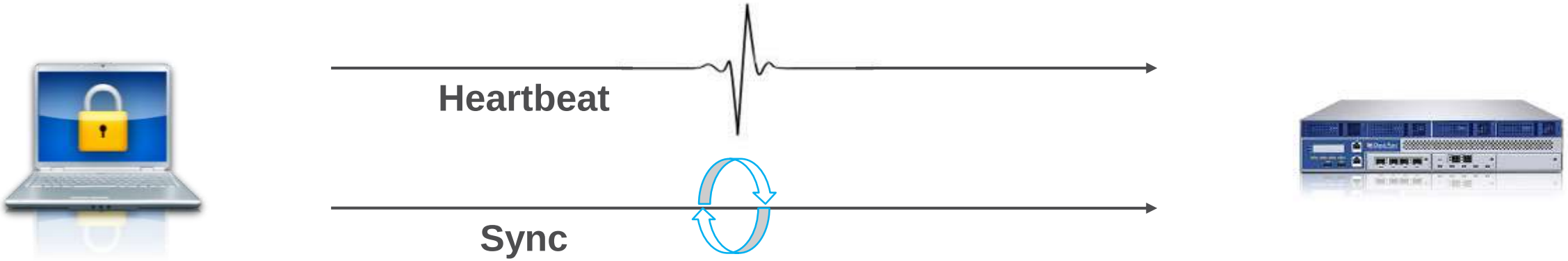
Component	Rule Type	Connected	Disconnected	Restricted
Full Disk Encryption	Computer	✓		
Media Encryption & Port Protection	User	✓	✓	✓
OneCheck User Settings	User	✓		
Capsule Docs	User	✓		
Anti-Malware	User	✓	✓	
SandBlast Agent Anti-Ransomware, Behavioral Guard and Forensics	Computer	✓		
SandBlast Agent Anti-Bot	User	✓	✓	
SandBlast Agent Threat Extraction, Emulation and Anti-Exploit	User	✓	✓	
Compliance	User	✓	✓	
URL Filtering	Computer	✓		
Firewall	User	✓	✓	✓
Access Zones	User	✓	✓	✓
Application Control	User	✓	✓	✓
Client Settings	User	✓		

State Policies

- Connected - SYNC Succeeded
- Disconnected - 5 HB failed
- Restricted - According to compliance

Communications & Processes

Communications & Processes



- Protocols used for client-server communication
- Heartbeat - periodic keep alive session for the Synchronization process
- Synchronization - Updates polices, blades, logs & Status to the server
- For POC or testing minimize for faster response and staging changes **

Communications & Processes

- Connectivity Tool - sk116590 - *CheckConnectivity.exe* **
- How to verify that Harmony Endpoint can access servers

Index	Hostname/URL	Protocol	From	Used For (Version)	Verifying Connectivity (Run command listed below. You will get a response if connectivity is OK.)
Harmony Endpoint Management - Infinity Portal					
1	storage.googleapis.com/datatube-data-eu	https	Threat Hunting	Threat Hunting data upload	curl -v -k -X GET https://datatube-prod.azurewebsites.net/health
2	storage.googleapis.com/datatube-data-us				
3	storage.googleapis.com/datatube-data-uk				
4	europe-west1-datatube-240519.cloudfunctions.net				
5	proddatatubedataeu.blob.core.windows.net				
6	proddatatubedataeastus2.blob.core.windows.net				
7	proddatatubedataaustraliaea.blob.core.windows.net				
8	datatube-prod.azurewebsites.net				
9	datatubeprodwesteurope.blob.core.windows.net				
10	us-east4-chkp-gcp-rnd-threat-hunt-box.cloudfunctions.net/prod-gcp-contractprovider	https	Threat Hunting	Threat Hunting cloud function domain	curl -v -k -X GET https://us-east4-chkp-gcp-rnd-threat-hunt-box.cloudfunctions.net/prod-gcp-contractprovider/health
11	<Connection Token>.epmgmt.checkpoint.com For example: HEPDemo-d9e265f1-hap2.epmgmt.checkpoint.com	https	Harmony Endpoint Management Platform	Client-Server communication	
12	s3-fips-r-w.us-east-1.amazonaws.com	https	Harmony Endpoint Management Platform	Client-Server communication	

Communications & Processes

Server Config Locations	Description
%UEPMDIR%\apache22	Apache core and configuration files
%UEPMDIR%\cpADScanner	Directory Scanner configuration files
%UEPMDIR%\engine\conf	Management Server configuration files **(cp3dlogd)**
%UEPMDIR%\engine\conf\epsNetwork	Defines messages and protocols between the server and endpoints
%UEPMDIR%\engine\conf\local.properties	Connection properties **(purge.max.days) ****
%UEPMDIR%\engine\conf\global.properties	Connections properties **(policy.heartbeat.interval=60) ****

Communications & Processes

- **Server Processes**

- All below should be “E” for Status **execute #*cpwd_admin list*** **
- CPM - execute #***watch api status*** Look for "running & ready" & "Started"
- EPM - TOMCAT - Needed to run main services
- CP3DLOGD - Getting client logs to **$UEPMDIR/logs/cp3dlogd.elg** >> SmartLog
- SICTUNNEL - Policy & SMS sync (Client.msi, Policy Updates & Logs) - $CPDIR/log/cptnl.elg
- APACHE - httpd - Client connection / Web UI - apache_error.log - ***#ps aux | grep hppd***
- POSTGRES - DB - ***#ps aux | grep postgres***
- ***CPVIEW - RAM & Disk Space***

Communications & Processes

LmGuardSvc	4344	Check Point Capsule Docs Client Service	Running
Check Point Device Auxiliary Framework	5072	Check Point Device Auxiliary Framework	Running
CPDA	4216	Check Point Endpoint Agent	Running
EPWD	5696	Check Point Endpoint Client Watchdog	Running
TracSrvWrapper	5768	Check Point Endpoint Connect	Running
CPEFR	3472	Check Point Endpoint EFR	Running
RemediationService	5544	Check Point Endpoint Remediation	Running
EpabService	5560	Check Point Endpoint Security AntiBot	Running
Check Point Bitlocker Management		Check Point Endpoint Security Bitlocker Management	Stopped
EPClientUIService	5312	Check Point Endpoint Security Client UI	Running
CPCompliance	5116	Check Point Endpoint Security Compliance	Running
vsmon	11192	Check Point Endpoint Security Network Protection	Running
TESvc	5612	Check Point Endpoint Threat Emulation	Running
DisknetClient	4572	Check Point ESME Client	Running
Full Disk Encryption	3536	Check Point Full Disk Encryption	Running

- CPTrayUI – System Tray
- Vsdant.sys – Hidden Self Protection

Communications & Processes

Self Protection Mode Obfuscated - sk65071

- Purpose – protecting our product from malicious applications
- Part of Endpoint since Rxx Secure Access or earlier
- Most obvious are write-protection for our files and registry entries
- (HKLM\System\CurrentControlSet\services\vsdatant\Parameters)**
- Disable tool from TAC for logging and troubleshooting

Client & Server Error Logging

Client & Server Error Logging

CPInfo

- Endpoint Client CPInfo - sk90445 – InfoView Tool
- Endpoint Server CPInfo - sk158572 – Web Viewer **
- Endpoint VPN Logging - sk169258
- Endpoint Preboot – WinPE / Preboot - sk103837
- MSInfo32

Client & Server Error Logging

Client Log Locations	Description
C:\Program Files (x86)\CheckPoint\CPInstlog	Client Initial Install log
C:\Program Files (x86)\CheckPoint	Main Program Directory
C:\ProgramData\CheckPoint\Logs	Main Logs Directory**
C:\ProgramData\CheckPoint\Endpoint Security\Full Disk	Full Disk Encryption events
C:\ProgramData\CheckPoint\Log_cfg	Log Config file **
C:\ProgramData\CheckPoint	Main Program Data Directory
C:\ProgramData\CheckPoint\Endpoint Security\Logs	User event logs (epslogs)
C:\ProgramData\CheckPoint\Endpoint Security\Common\Storage	Downloaded Polices
HKLM\SOFTWARE\Wow6432Node\CheckPoint\	Most reg entries location
HKLM\SOFTWARE\Wow6432Node\CheckPoint\ Endpoint Security	DeviceAuxiliaryFramework\EnableDebugLogs=1
$FWDIR/conf/SMC_Files/uepm/DA/config.dat	Server list now encrypted on client

Client & Server Error Logging

Server Log Locations	Description
%UEPMDIR%\logs\apache*	Apache events
%UEPMDIR%\logs\apache_access.log	User logs upload events
%UEPMDIR%\logs\Authentication.log	Authentication events
%UEPMDIR%\logs\cpADScanner.log	Active Directory Scanner logs
%UEPMDIR%\logs\server_messages.log	Endpoint Server log file
$UEPMDIR/logs/TmpStdOutErr.log	
%UEPMDIR%\logs\.cp3dlogd.elg	Client user log uploads (TDERROR_CP3DLOGD_ALL=5)

Client & Server Error Logging

Smart Console logs

- /smartconsole/r80.xx/programs/endpointmanager.exe.config
- change TechDebugMode=True
- Look in $UEPMDIR/logs/server_messages.log for ERROR CODE in GUI
- Look in %LOCALAPPDATA%\CheckPoint\SmartEndpoint_Logs\R80_XX

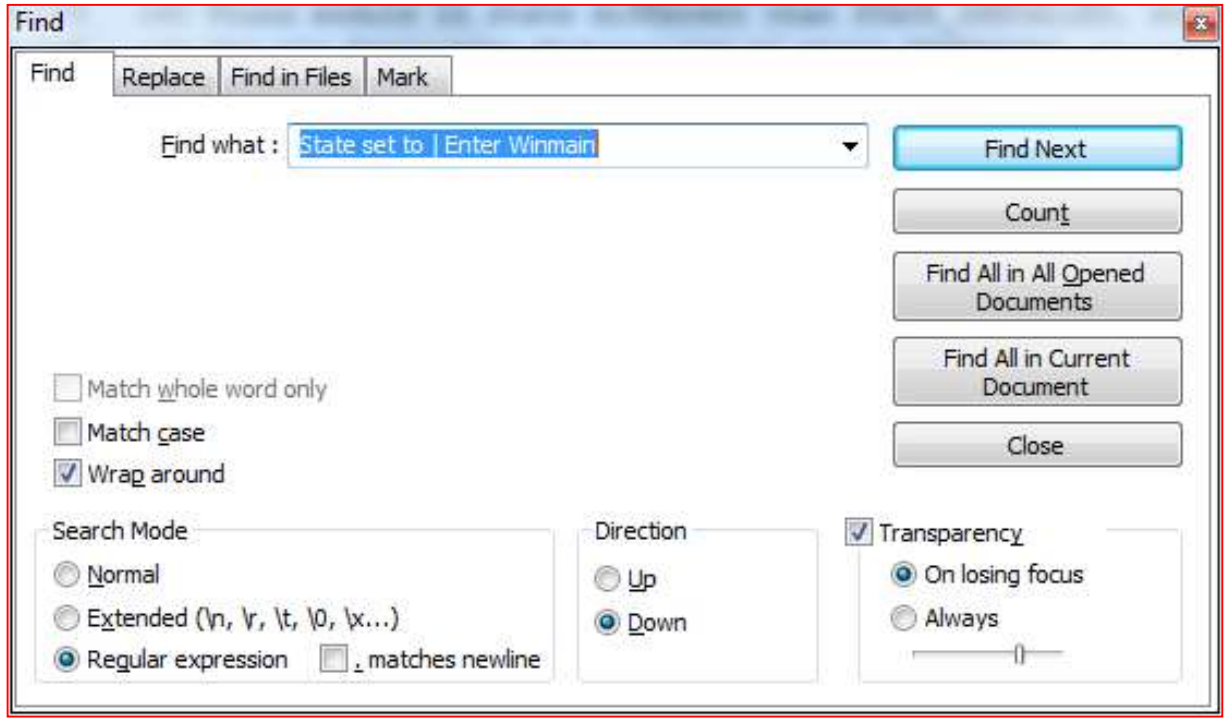
Client & Server Error Logging

LINUX

- Search for “Error” or “Caused by”

- grep 'ERROR' logname
- grep -i 'ERROR' logname
- grep -c ‘CAUSED' logname
- grep -v 'WARNING' logname
- cat logname | grep -i 'ERROR'

WINDOWS



Client & Server Error Logging

String	Explanation
###Enter WinMain###	*Start running cpda.log*
Enter sendRegisterEndpoint	*Registering the endpoint client on first connection to server*
Enter sendNewZPDocKey	*Asking for session cookie*
Enter sendHeartbeat	*starting heartbeat*
SortedServerlist	*Available Endpoint Servers after the proximity resaults*
State set to	*Follow states in Software Deployment State Machine, find Installation\Download Errors*
Called createServerProximityTasks	Starting calculation of the closest Policy Server
Sorted Server list	List the reachable Endpoint Servers
Server list is (serverlistis):	to see server list, received by DA
<EDE_SYNC_REQ	SYNC request message
<EDE_SYNC_RESP	SYNC response (receiving only when connected to server)
SyncReason	check why SYNC request was initiated
UpdateModulesState	Decision on performing Software Deployment
Policy downloaded	notifying about new downloaded policy
ConnectionState: Entering	Look in all file to see when client was connected\disconnected\restricted
Running blades mask changed	Changes in running state of blades
Do sync	starting sync
---ERROR---	all errors

Client & Server Error Logging

Blade Name	Binary Mask	Integer Value
DA+DAF	0000000000000001	1
FDE	0000000000000010	2
ME	0000000000000100	4
FW1	0000000000001000	8
Compliance	0000000000010000	16
Program Control	0000000000100000	32
Anti Malware	0000000001000000	64
Web Check	0000000010000000	128
Endpoint Connect	0000000100000000	256
Legacy VPN	0000001000000000	512
URLF	0000010000000000	1024
DocSec	0000100000000000	2048
AntiBot	0001000000000000	4096
DLP	0010000000000000	8192
Forensics	1000000000000000	65536

Client & Server Error Logging

- ################################ Enter WinMain ################################ (WinMain)
- ##### Enter sendRegisterEndpoint (CDAProtocol::sendRegisterEndpoint)
- ##### Enter sendNewZPDocKey (CDAProtocol::sendNewZPDocKey)
- ##### Enter sendSynchronization (CDAProtocol::sendSynchronization)
- ##### Enter sendHeartbeat (CDAProtocol::sendHeartbeat)
- SwMng: State set to Scheduled, try: 1, for module: version: 8.4.152, installBlades: 383, requstedBlades: 383, supportedBlades: 4294967295, packageCode: 2106D983-E49F-4EC4-954E-5A58FF8DC7D6, name: Check Point Endpoint Total Security x64 (CDeplModule::setStateToScheduled)
- bd4 SwMng: State set to Download, try: 1, for module: version: 8.4.152, installBlades: 383, requstedBlades: 383, supportedBlades: 4294967295, packageCode: 2
- bd4 SwMng: State set to Scheduled, try: 1, for module: version: 8.4.152, installBlades: 383, requstedBlades: 383, supportedBlades: 511, packageCode: 2106D983-E49F-4EC4-954E-5A58FF8DC7D6, name: Check Point Endpoint Total Security x64 (CDeplModule::setStateToScheduled)
- bd4 SwMng: State set to Download, try: 1, for module: version: 8.4.152, installBlades: 383, requstedBlades: 383, supportedBlades: 511, packageCode: 2106D983-E49F-4EC4-954E-5A58FF8DC7D6, name: Check Point Endpoint Total Security x64 (CDeplModule::setStateToDownload)
- bd4 SwMng: State set to Installing(Uninstalling), try: 1, for module: version: 8.4.152, installBlades: 383, requstedBlades: 383, supportedBlades: 511, packageCode: 2106D983-E49F-4EC4-954E-5A58FF8DC7D6, productCode: {49D17C44-5750-443D-9098-827D98A2ED6A}, name: Check Point Endpoint Total Security x64 (CDeplModule::setStateToInstalling)
- bd4 SwMng: State set to Installed, try: 1, for module: version: 8.4.152, installBlades: 383, requstedBlades: 383, supportedBlades: 511, packageCode: 2106D983-E49F-4EC4-954E-5A58FF8DC7D6, name: Check Point Endpoint Total Security x64 (CDeplModule::setStateToInstalled)

Client & Server Error Logging

```
07:33:54.696   f64 Don't install, wrong version for installation was requested (CDA::needToRunInstaller)
07:33:54.696   f64 needToRunInstaller returned with values: isInstallerRunNeeded: False, useCLIPropsDummy: False, msiAvail: PKG_NOT_PRESENT (CDA::upda
07:33:54.696   f64 UpdateModulesState: Deployment policy contains deployment request that is unknown to DA, however should NOT do SW management: (CDA
07:33:54.696   f64     Deployment version: 8.2.502, blades: 511, packageCode: 9B9E3AA0-2776-4588-95A4-DF8BBFFCEDD4, productCode: B9C999F1-8D66-404D-AI
07:33:54.696   f64 SwMng: No master depl module found in internal structure corresponding to deployment's request, version: 8.2.502 mask: 511, package
07:33:54.696   f64 SwMng: A master depl module with a higher version: 8.2.508 and mask: 1 than of deployment's request, is already installed accordin
```

```
09:55:40.324  2a20 Sorted Server list: (CServerList::doProximityEvaluation)
09:55:40.325  2a20     Server[0]: ip=194.29.34.136 respTime=1279 acceptClients=1 (CServerList::doProximityEvaluation)
09:55:40.326  2a20     Server[1]: ip=194.29.34.62 respTime=1280 acceptClients=1 (CServerList::doProximityEvaluation)
09:55:40.327  2a20     Server[2]: ip=192.168.181.137 respTime=4294967295 acceptClients=1 (CServerList::doProximityEvaluation)
09:55:40.328  2a20     Server[3]: ip=194.29.34.134 respTime=4294967295 acceptClients=1 (CServerList::doProximityEvaluation)
09:55:40.329  2a20 ProximityTimeCalculation: Total time [00:00:21] (CServerList::doProximityEvaluation)
09:55:40.330  2a20 Selecting first CP in server list as current CP (not active yet) (CDAConfig::useFirstCPAsCurrent)
```

Client & Server Error Logging

```
20131220 15:56:58.377  13a4 Old PAT on CP, no action. (CDAProtocol::handleResponse)
20131220 15:56:58.387  13a4 ##### Exit sendSynchronization (CDAProtocol::sendSynchronization)
20131220 15:56:58.388  13a4 ---ERROR--- Old PAT on CP. Last win error: 122 (0x7A) (CDA::doSync)
20131220 15:56:58.400  13a4 ---ERROR--- Sync failed, rc == 70017. Last win error: 122 (0x7A) (CDA::threadMethod)
20131220 15:56:58.410  13a4 Sync response conatins old PAT (CDA::threadMethod)
```

```
8d8 Status OK, all information from DAF_DSM is available (CDA::getDAProviderElement)
8d8 RunningBladesMask: Update succeeded. Received mask: 3(0x3) (CDA::updateRunningBladesMask)
8d8 RunningBladesMask: Installed: 7(0x7), Running: 3(0x3), Non-running: 4(0x4) (CDA::getNotRunningBladesMask)
8d8 Found module in INSTALLED state, adding installed_mask info to DA element (addDeplModules)
```

Client & Server Error Logging

```
Full Disk Encryption - Preboot Customization
(1)   Mouse Support - Enabled
(2)   Highcolor Graphics - Enabled
(3)   USB Support - According to Policy
(4)   PCMCIA Support - Enabled
(5)   Windows Integrated Logon - Enabled
(6)   Boot record to start - Master Boot Record
(7)   HID drivers - Enabled
(8)   Restore boot records - No
(9)   Start Evaluation Recovery - No
(R)   Disable Image Rebranding - No
(D)   Diagnostics log menu
(Esc) Continue
```

Use Double-Shift key to access the preboot customization menu

Disable USB Smartcard reader if suspecting issue with BIOS USB

Use Boot Record to start and select "Partition Boot Record" if OS is not loading

Use Restore Boot Records if pre-boot is not loading at all

SUMMARY

- Review Top Issue Areas
- Getting issues fixed faster
- Use info for internal SE lookup
- Use info for Support KB Lookup
- Use info for TAC Support

CHECK POINT™

THANK YOU

YOU DESERVE THE BEST SECURITY