

## Host Checker Troubleshooting Guide

What is Host Checker?.....	1
HC client side logs.....	1
HC Server side logs.....	2
Reading HC Logs.....	3

### What is Host Checker?

Host Checker is a client-side agent that performs endpoint checks on hosts that connect to the IVE. You can invoke Host Checker before displaying an IVE sign-in page to a user and when evaluating a role mapping rule or resource policy.

The IVE may check hosts for endpoint properties using:

***The Host Checker implementation of a supported endpoint security application (Windows only)*** — The Host Checker client-side agent calls the Host Checker integration function of the specified third-party endpoint security product and examines the return value to see if the product is running in accordance with its configured policies

***Host Checker integration using a custom DLL (Windows only)***—The Host Check Client Interface enables you to integrate a DLL that performs customized client-side checks. You must install this DLL on each client machine.

***Attribute checking*** — On Windows, Macintosh, or Linux, Host Checker looks for the application fingerprints that you specify, including processes or files. On Windows, Host Checker can also checks registry entries.

If the user's computer does not meet any of the Host Checker policy requirements, you can display a remediation page to the user. This custom-made HTML page can contain your specific instructions as well as links to resources to help the user bring his computer into compliance with each Host Checker policy.

### HC Client side logs

1. C:\Documents and Settings\\Application Data\Juniper Networks\Host Checker\dsHostChecker.log
  - a. This log file is useful to isolate the problems related to
    - i. Process idle timeout
    - ii. Show remediation/Hide remediation feature
    - iii. Try Again or any action related to Host checker
2. C:\Documents and Settings\\Application Data\Juniper Networks\Host Checker\dsHostCheckerProxy.log
  - a. This log is generated when Pre-auth tunnel feature is used. Useful to determine the issues related to port-forwarding
3. C:\Documents and Settings\ USERNAME>\Application Data\Juniper Networks\EPCheck\EPCheck.log
  - a. This is the most important log file, this log file contains the policy evaluation results, http Send status.

## HC Server side logs

1. User access logs: Please collect user access logs for every failed case.
2. Also try to get policy traces for the session. Useful for troubleshooting login issues and role-mapping issues.

### **Process Checks**

1. Check if the process is present in the Task manager
2. Use online tools to compute the checksum's for the process (For Ex Ping.exe on win2k)

### File Checks

1. Double check the presence of file and use MD5 checksum
2. Use "SET" command on the dos prompt to determine the environment variables
3. Make sure that environment variables are set using <%Variable%> syntax
4. Wildcards are supported only for leaf node.
  - a. C:\\*\\*.doc is not valid
  - b. C:\Test\\*.doc is valid

### Registry Checks

5. Wildcards are not supported
6. Only HKEY\_CLASSES\_ROOT, HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, HKEY\_USERS, HKEY\_CURRENT\_CONFIG are supported
7. HKEY\_DYN\_KEY is not supported

### Third Party policies

1. Make sure that process idle timeout is relatively large (Especially incase of Sygate Virtual Desktop)
2. If third party (3P) policies are using tunnel definitions, verify the tunnels in the HC admin page after 3P is uploaded
3. If you run into issues related to connectivity, check the following steps:
  - a. Do a netstat -a -n -p tcp and make sure that 0.0.0.0:<port> is not in the listening state Ex: TCP 0.0.0.0:80 0.0.0.0:0 LISTENING TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
  - b. Also make sure that <Loopback IP>:<Port> is not in the listening state
  - c. If you are using XP + SP2 make sure that the hotfix is installed
  - d. Eliminate any Personal firewall related exceptions
  - e. Examine User access logs for IVE connection requests
  - f. Take TCP dump only for issues related to data getting truncated ...etc
4. If customers/vendors complain about connectivity, create a simple tunnel like 127.0.0.1:8000 [www.yahoo.com:80](http://www.yahoo.com) in the manifest file and upload it (Enforce it). Use IE to browse to 127.0.0.1:8000. If this works (if you get to yahoo) then it is something to do with 3P package.

### Connection control policy

1. Remember to enforce the policy after choosing the option in admin page
2. This blocks all incoming TCP connection, UDP packets.
3. There is no option to set the exceptions

4. It allows communications to IVE/Proxy server/DNS/WINS/DHCP and Network Connect (NC) adapter
5. Through NC it allows all incoming and outgoing connections

#### Remediation

1. Make sure that custom instruction checkbox is set, without this remediation will not be shown
2. Check the expression evaluation carefully, default is all AND

#### Remediate Actions

1. Kill Process: Same as Process checks as far as MD5's and wildcards are concerned.
2. Killing of process is best-effort, in other-words it kills only if the user has access to terminate the process
3. Deleting the files, no wildcards are supported
4. Conditional evaluation of policies. The conditional policy is to evaluate only when the primary policy fails.

#### Hosts file modification and potential conflicts with JSAM/WTS

1. If the tunnel definitions are specified using hosts file, then we modify the hosts file to create a loopback dynamically
2. To avoid conflicts with JSAM, we start from 127.0.0.3 (outlook 2000 and JSAM is hard-coded to use 127.0.0.1)
3. HC/WTS creates hosts file backup (hosts\_juniper.bak) and creates a RunOnce registry entry
4. All the entries are added with Prefix #[HC\_Begin] and #[HC\_End]
5. When HC is exiting, it clears only the entries that it made during startup
6. If there are no entries from WTS or JSAM then it copies the backup file to the original location and clears the registry.
7. If HC crashes or reboots then Runonce registry takes care of restoring the hosts file.

## Reading HC Logs

05/20/2005 18:51:23 dsEPChecker.cpp:164 - CdsEPChecker::customFunction():

\*\*\*\*\***Start end point checks**\*\*\*\*\*

→ **This indicates the time at which End point check is started**

\*\*\*\*\*

\*\*\*\*\***05/20/2005 18:54:53 dsEPChecker.cpp:217 -**

**CdsEPChecker::customFunction(): \*\*\*\* Host Checker was ended**

\*\*\*\*\*

\*\*\*\*\*

\*\*\*\*\*

→ **This indicates the time at which Host Checker is about to exit**

Host checker could prevent the user from logging to IVE or could kick user out of session if

- Policies fail
- If client is not able to send the status to the server

To isolate the problems look at the logs related to HTTPSend request

05/20/2005 18:51:24 dsEPChecker.cpp:815 - **CdsEPChecker::httpSend:**

**HttpSendRequest HTTP\_OK**

05/20/2005 18:51:24 dsEPChecker.cpp:779 - CdsEPChecker::sendEPCheckStatus():  
Check http status...0

05/20/2005 18:51:24 dsEPChecker.cpp:793 - CdsEPChecker::sendEPCheckStatus():  
**HTTP\_OK**

- ➔ This indicates that the communication is okay, in case of errors  
HttpSendRequests reports WININET error (Look for Proxy configuration at  
the browser and general connectivity to isolate the problem)

Logs related to Policies :

05/20/2005 18:51:23 dsEPChecker.cpp:703 - CdsEPChecker::HttpSendStatus():

szPost = policy:policy\_4 status:OK

- ➔ The above line says that policy\_4 is ok, if it is not ok then policy failed. Look  
at the admin configuration for all the rules in the policy and check manually to  
make sure that all rules satisfy and look for provider specific error messages  
in the log.
  - Ex: 05/03/2005 14:03:13 dsEPChecker.cpp:646 - [CheckAYT() failed]:  
policy\_2::ping.exe not found
  - Search the log file with file name, process name, registry key, etc... to  
get the exact reason for errors.