# HP Connection Inspector

## Table of contents

# Introduction

**HP Connection Inspector** is a new intelligent embedded security feature created by HP Labs. The technology inspects outbound network connections typically abused by malware, determines what is normal and stop suspicious activity. If the printer is compromised, it will automatically trigger a system restart to initiate HP Sure Start self-healing procedures.

# Theory of Operation

Malware is typically designed to call home to its external server to get further instructions, updates and information on where to send collected data. Early malware used hardcoded IP addresses. Modern malware uses more sophisticated behaviors to establish and maintain contact with its external server. These behaviors can be recognized to detect the presence of malware and block the attackers.

When anomalous behavior on outgoing connection requests is detected, the device enters a protected mode of operation for DNS queries, designed to stop the malware communicating with its external server and preventing the malware from causing additional damage, while allowing the printer to function normally.

If further anomalous connection requests are detected, the device performs a system restart which is designed to clear the malware by taking advantage of the device's Sure Start and Whitelisting features. An IT security alert is generated to communicate a possible attack.

# HP Connection Inspector settings

Settable parameters define how the feature identifies DNS behavior that could indicate anomalous activity. The device enters either of two modes: DNS Protected Mode or a Self-Healing Mode where the device performs a system restart. The settable parameters allow the detection method to be tuned to different customer environments, in terms of typical network behavior and security sensitivity.

Configuration interfaces:

- Embedded Web Server (EWS) supports all configuration settings
- HP Web Jetadmin supports Enable/Disable only in version 10.4sr2 Feature Pack 6
- HP JetAdvantage Security Manager supports all configuration settings in version 3.1

## Feature Enable / Disable

The HP Connection Inspector feature can be disabled for troubleshooting purposes. Disabling and re-enabling the feature resets Protected mode counters and monitoring statistics to their configured values.


Figure 1: HP Connection Inspector Enable/Disable in the Embedded Web Server (EWS)

**EWS Path:** Networking Tab -> TCP/IP Menu –> Network Identification Page

## Threshold and Duration Settings

**DNS Failure Threshold:** Default: 5 (4 – 50)

The number of unique non-resolving unknown DNS requests within the "Monitoring Window" resulting in DNS Protected Mode.

- A higher value will reduce the speed and accuracy of detection but will reduce potential false positives.

**Monitoring Window:** Default: 80 mins (30 mins – 14400 mins)

The length of the window in minutes in which DNS resolution activity is counted.

- A longer window will detect slower executing connection request activity but will increase potential false positives.

**Protected Mode Duration:** Default: 60 mins (40 mins – 120 mins)

The minimum time in minutes the DNS Protected Mode is active once triggered.

- A higher value will mitigate stealthier malware behavior.

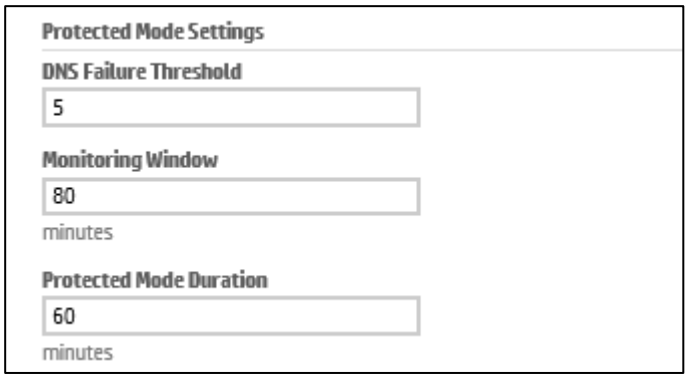



Figure 2: HP Connection Inspector Protected Mode Settings in the EWS

## Self-Healing (Remediation) Settings

**Number of Tines in Protected Mode:** Default: 3 (1 – 10)

Number of DNS Protected Mode events that occur before a system restart.

- A higher value will increase the time before a system restart.

**Cumulative Protected Mode Duration:** Default: 80 mins (60 mins – 140 mins)

Total duration of DNS Protected mode events in minutes since device startup before initiating a system restart. The Cumulative DNS Protected Mode setting determines when a system restart occurs.

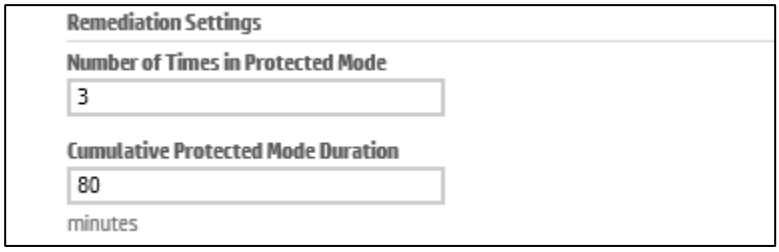



Figure 3: HP Connection Inspector Remediation Self-Healing Settings in the EWS

## White List Settings

The White List option allows adding DNS addresses that will never be blocked and are not counted towards detection statistics. If HP Connection Inspector generates false positives the DNS names or domains that cause the false positives can be added to the white list.


Figure 4: HP Connection Inspector White List Settings in the EWS

## Restore Default Settings

Restores the HP Connection Inspector to default values and resets Protected mode counters and monitoring statistics to the default values.


Figure 5: HP Connection Inspector Restore Settings in the EWS

# Protected Mode

## Entering Protected Mode

The device enters Protected mode when the following conditions are met:

- The number of unique, non-resolved, unknown DNS requests exceeds the DNS Failure Threshold setting.

## DNS Behavior in Protected Mode

DNS resolution is allowed for

- A user-defined whitelist of domains and associated domain suffixes
- Domains that have successfully resolved since system startup contained in the History List
- Destinations in the current domain and associated domain suffixes
- Trusted domains (when Cross Origin Resource Sharing is enabled)

When a device is in Protected Mode, DNS requests that are not in the History or Whitelist are not permitted.

# Self-Healing Mode

The device initiates a system restart when one of the following conditions is met:

- The number of DNS Protected Mode events exceeds the “Number of DNS Protected Mode Events” setting
- The total DNS Protected Mode duration exceeds the “Cumulative DNS Protected Mode Duration” setting
- When a system restart remediation event is initiated, the device will automatically reboot unless the Auto-recover feature is disabled, or a possible network anomaly occurs twice within 30 minutes, the device reboots and holds at the preboot menu to prevent a potential malware exploit from executing.

# Error and Status Messages

## Event log Messages

This message indicate that the product detected and recovered from a network anomaly self-healing event.

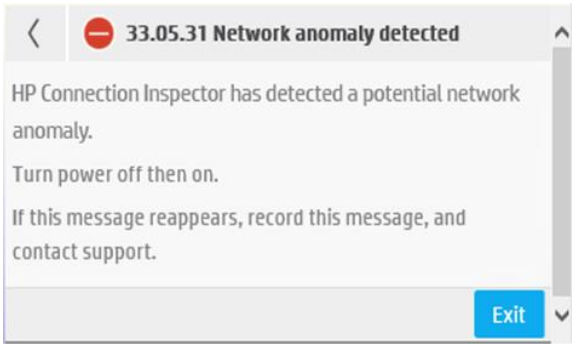
| Event log error code and message | Cause | Recommended action |
|---|---|---|
| 33.05.31 Network Anomaly Detected | The printer detected and recovered from a corrupted potential network anomaly.<br>The number of protected mode events has exceeded the Number of Times in Protected Mode setting.<br>The total time in protected mode has exceeded the Cumulative Protected Mode Duration setting | Review the syslog messages for the domain request triggering a system reset. Determine if this domain should be added to the whitelist. |

**Note:** If the Auto-recover feature is disabled, or a possible network anomaly occurs twice within 30 minutes, the device reboots and holds at the preboot menu to prevent a potential malware exploit from executing.

| Event | Firmware | Description or Personality |
|---|---|---|
| 33.05.31 | 2405110_019361 | Potential Network Anomaly detected |

## Control Panel Messages

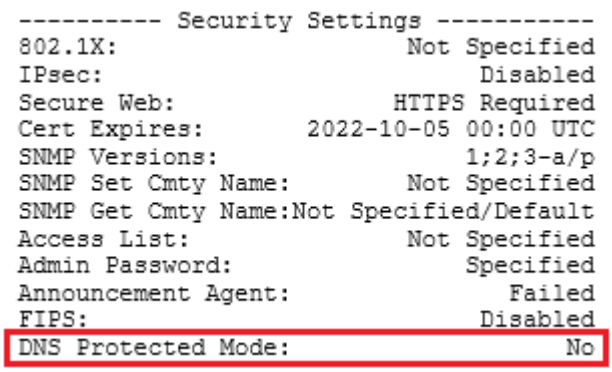
A security alert message is shown on the control panel before a system reset self-recovery event.



## Jetdirect configuration page status

The Jetdirect Configuration page shows the Protected Mode status for HP Connection Inspector

- Yes – Device in protected mode
- No – Device not in protected mode
- N/A – HP Connection Inspector disabled




## Syslog Messages

Syslog messages are sent from the device for the following settings changes and events.

### HP Connection Inspector configuration changes

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector enabled; time="<timestamp>" user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | HP Connector Inspector feature was enabled. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector disabled; time="<timestamp>" user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | HP Connector Inspector feature was disabled. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Protected Mode settings modified; time="*<timestamp>*" item=dns_failure_threshold value=*<value>* old_value=*<old value>* user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | The DNS failure threshold setting for the HP Connection Inspector feature was modified. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Protected Mode settings modified; time="*<timestamp>*" item=monitoring_window value=*<value>* old_value=*<old value>* user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | The monitoring window setting for the HP Connection Inspector feature was modified. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Protected Mode settings modified; time="*<timestamp>*" item=protected_mode_duration value=*<value>* old_value=*<old value>* user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | The protected mode duration setting for the HP Connection Inspector feature was modified. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Protected Mode settings modified; time="*<timestamp>*" item=number_of_times_in_protected_mode value=*<value>* old_value=*<old value>* user="*<user>*" source_IP="*<client computer IP address>*" outcome=success |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | The number of times in protected mode setting for the HP Connection Inspector feature was modified. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Protected Mode settings modified; time="*<timestamp>*" item=cumulative_protected_mode_duration value=*<value>* old_value=*<old value>* user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | The cumulative protected mode duration setting for the HP Connection Inspector feature was modified. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Advanced settings modified; time="*<timestamp>*" action=whitelist-exception_list_entry_added value="*<entry>*" user="*<user>*" source_IP="*<client computer address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | An entry was added to the whitelist / exception list for the HP Connection Inspector feature. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector Advanced settings modified; time="*<timestamp>*" action=whitelist-exception_list_entry_deleted value="*<entry>*" user="*<user>*" source_IP="*<client computer IP address>*" outcome=success interface=*<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | An entry was deleted from the whitelist / exception list for the HP Connection Inspector feature. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector settings modified; time="*<timestamp>*" action=factory_defaults_restored user="*<user>*" source_IP="*<client computer IP address*" outcome=success interface= *<interface>* |
| **Interface(s):** | EWS |
| **Syslog severity:** | Informational |
| **Explanation:** | HP Connection Inspector feature settings were restored to factory defaults. |

## HP Connection Inspector Protection events

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector event; time="*<timestamp>*" event= protected_mode_entered outcome=success |
| **Interface(s):** | N/A |
| **Syslog severity:** | Warning |
| **Explanation:** | HP Connection Inspector feature has entered protected mode. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector event; time="*<timestamp>*" event= protected_mode_exited outcome=success |
| **Interface(s):** | N/A |
| **Syslog severity:** | Warning |
| **Explanation:** | HP Connection Inspector feature has exited protected mode. |

| | |
|---|---|
| **Message:** | *<device type>*: HP Connection Inspector event; time="*<timestamp>*" event= dns_query value="*<host name>*" outcome=failure |
| **Interface(s):** | N/A |
| **Syslog severity:** | Warning |
| **Explanation:** | HP Connection Inspector feature has detected dns query failure for a hostname. |



Version 2.0 October 2018
Public