TREND MICRO™ Interscan Web Security Virtual Appliance

AMEA Partner case submission handbook

TREND MICRO™ AMEA Partner case submission handbook
Document Version 1.0
***Prepared by**: Aljohn Neil Cabansag*
***Edited by:** Wilson Salvador*

Table of contents

Introduction

This guide will help partners/customer to know the common issues on IWSVA and how to troubleshoot it. It contains step by step procedure, IWSVA command and useful tools.

Common Issues

User(s) are not able to access website(s).

This topic discuss the following issues/errors.

1. How to check if IWSVA is blocking a URL or website?. *see* *How to Search Logs*
2. Broken Pages (e.g some content of the website is not dispalying properly). *see* *How to use Network Developer Tools (Chrome)*
3. How to check if IWSVA can access the webiste via CLI. *see* *Accessing website via IWSVA CLI*
4. Network Related Issues. *see* *Common Network Troubleshooting Tips*
   - DNS Issues.
   - Connection Timeout.

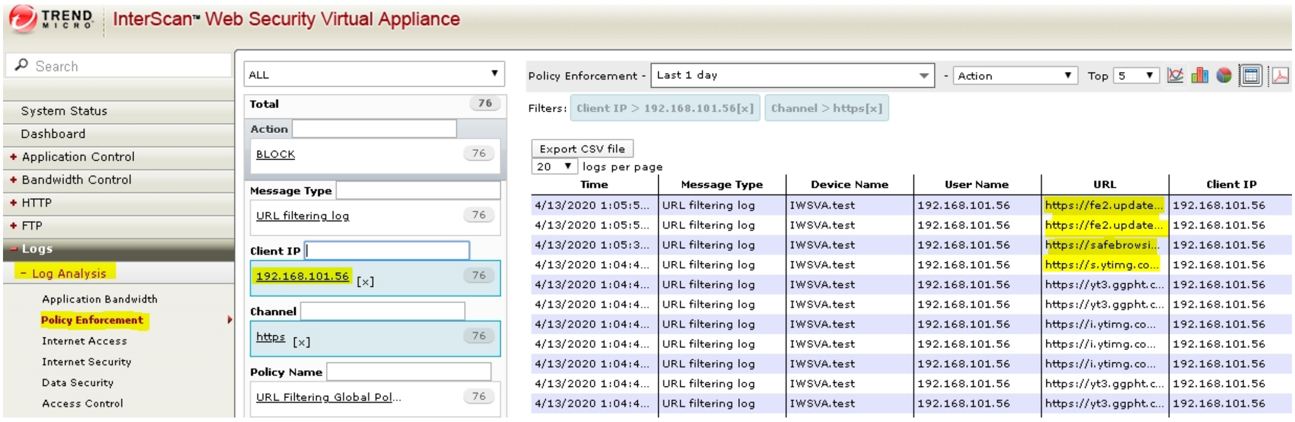
Troubleshooting Tips

How to check if IWSVA is blocking a URL or website?

Search for "Policy Enforcement" Logs

This procedure allows administrators to check if a URL or website is blocked by an IWSVA policy.

- Go to **Logs > Log Analysis > Policy Enforcement**.
- Enter Filter (e.g IP address or Username).



ALL

Total 76

Action: BLOCK 76

Message Type: URL filtering log 76

Client IP: 192.168.101.56 [x] 76

Channel: https [x] 76

Policy Name: URL Filtering Global Pol... 76

Policy Enforcement - Last 1 day - Action Top 5

Filters: Client IP > 192.168.101.56[x] Channel > https[x]

20 logs per page

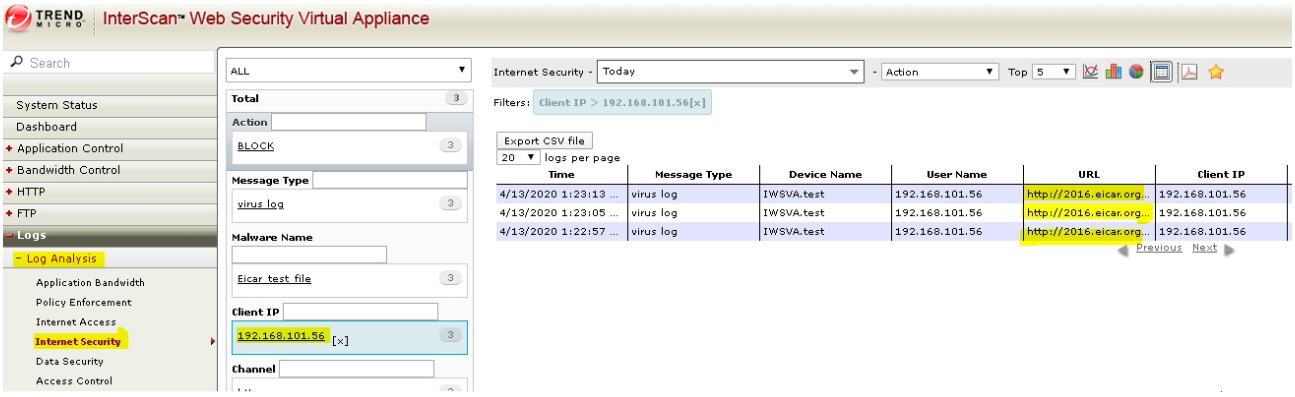
Time	Message Type	Device Name	User Name	URL	Client IP
4/13/2020 1:05:5...	URL filtering log	IWSVA.test	192.168.101.56	https://fe2.update...	192.168.101.56
4/13/2020 1:05:5...	URL filtering log	IWSVA.test	192.168.101.56	https://fe2.update...	192.168.101.56
4/13/2020 1:05:3...	URL filtering log	IWSVA.test	192.168.101.56	https://safebrowsi...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://s.ytimg.co...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://yt3.ggpht.c...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://yt3.ggpht.c...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://i.ytimg.co...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://i.ytimg.co...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://i.ytimg.co...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://yt3.ggpht.c...	192.168.101.56
4/13/2020 1:04:4...	URL filtering log	IWSVA.test	192.168.101.56	https://yt3.ggpht.c...	192.168.101.56

- If website is found add the website to white list.[How to White List]

Search for "Internet Security" Logs

This procedure allows administrators to check if a URL or website is blocked by IWSVA due to security reasons.

- Go to Logs > Log Analysis > Internet Access Logs.
- Enter Filter (e.g IP address or Username).



ALL

Total 3

Action: BLOCK 3

Message Type: virus log 3

Malware Name: Eicar test file 3

Client IP: 192.168.101.56 [x] 3

Channel

Internet Security - Today - Action Top 5

Filters: Client IP > 192.168.101.56[x]

20 logs per page

Time	Message Type	Device Name	User Name	URL	Client IP
4/13/2020 1:23:13 ...	virus log	IWSVA.test	192.168.101.56	http://2016.eicar.org...	192.168.101.56
4/13/2020 1:23:05 ...	virus log	IWSVA.test	192.168.101.56	http://2016.eicar.org...	192.168.101.56
4/13/2020 1:22:57 ...	virus log	IWSVA.test	192.168.101.56	http://2016.eicar.org...	192.168.101.56

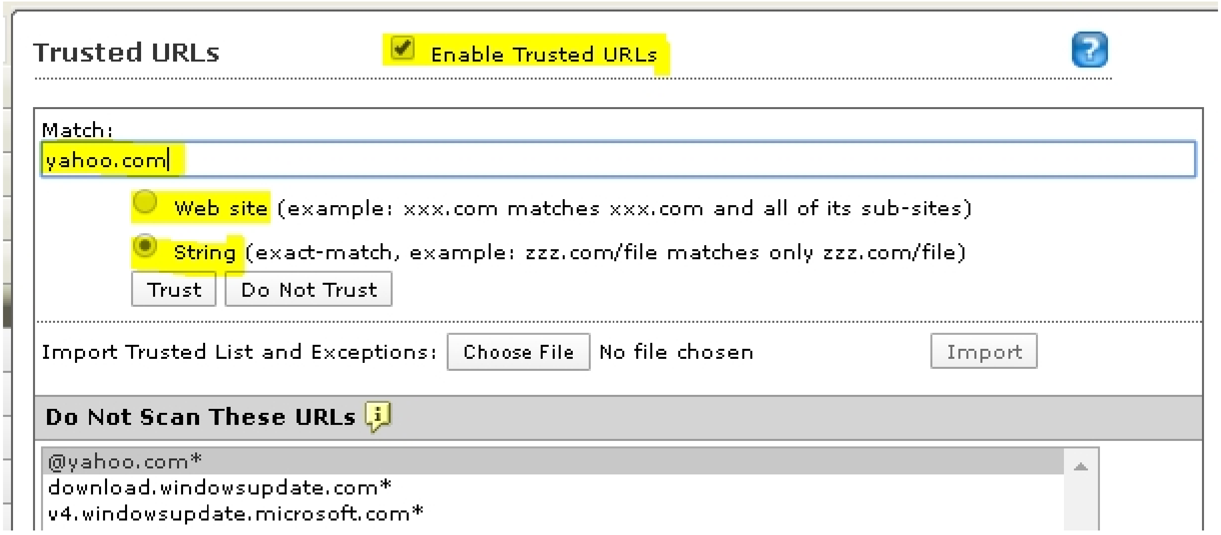
- If website is found add the website to white list.[How to White List]

How to white list a website or URL from IWSVA?

This procedure allows administrators to whitelist a website/URL and avoid being blocked by IWSVA.

Add URL or website under "Global Trusted URL's"

- Go to **HTTP > URL Access Control > Global Trusted URL's.**
- Make sure "Enable Trusted URL's" is checked.
- Add the URL (e.g yahoo.com) as "Web Site" Click Trust.
- Add the URL (e.g yahoo.com) as "String" Click Trust.
- **Click Save.**



Trusted URLs ☑ Enable Trusted URLs

Match: yahoo.com

○ Web site (example: xxx.com matches xxx.com and all of its sub-sites)

● String (exact-match, example: zzz.com/file matches only zzz.com/file)

Import Trusted List and Exceptions: No file chosen

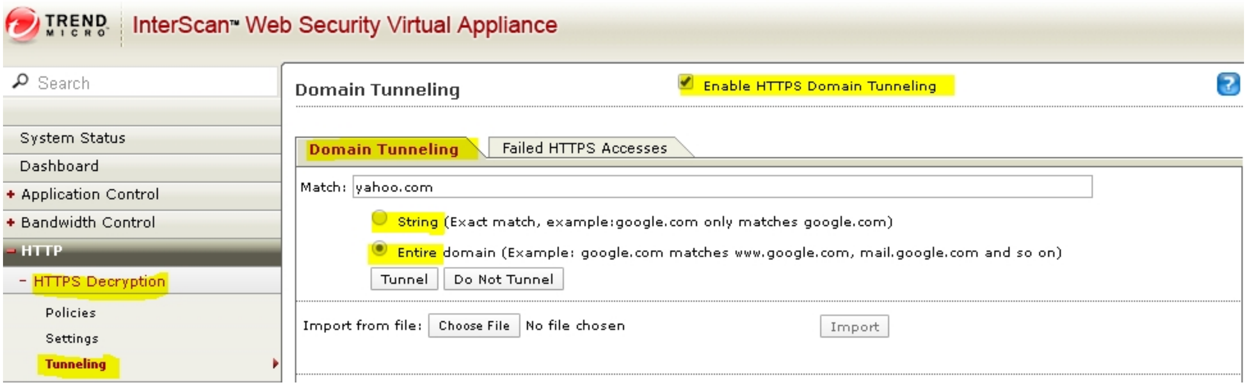
Do Not Scan These URLs

@yahoo.com*
download.windowsupdate.com*
v4.windowsupdate.microsoft.com*

Note: Please make sure to clear cache and cookies before testing again

Add HTTPs website under "Tunneled Domain"

- Go to HTTP > HTTPS Decryption > Tunnelling > Domain Tunneling.
- Make sure "Enable HTTPS Domain Tunneling" is checked.
- Add the URL (e.g yahoo.com) as "Web Site" Click Tunnel.
- Add the URL (e.g yahoo.com) as "Entire Domain" Click Tunnel.
- **Click Save.**



TREND MICRO InterScan™ Web Security Virtual Appliance

Domain Tunneling ☑ Enable HTTPS Domain Tunneling

Match: yahoo.com

○ String (Exact match, example:google.com only matches google.com)

● Entire domain (Example: google.com matches www.google.com, mail.google.com and so on)

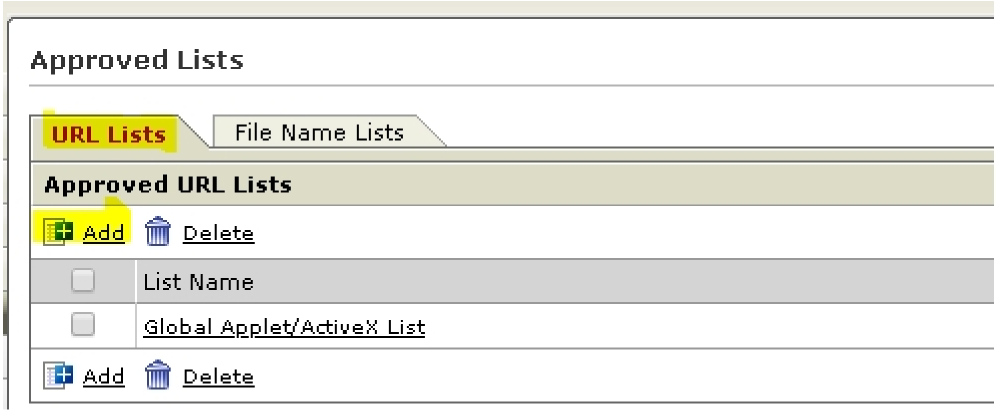
Import from file: No file chosen

Note: Please make sure to clear cache and cookies before testing again

Add URL or website under "Approved Lists"

For Policy Based Whitelist.

- Go to **HTTP** > **Configuration > Approved Lists** > Click **Add**.

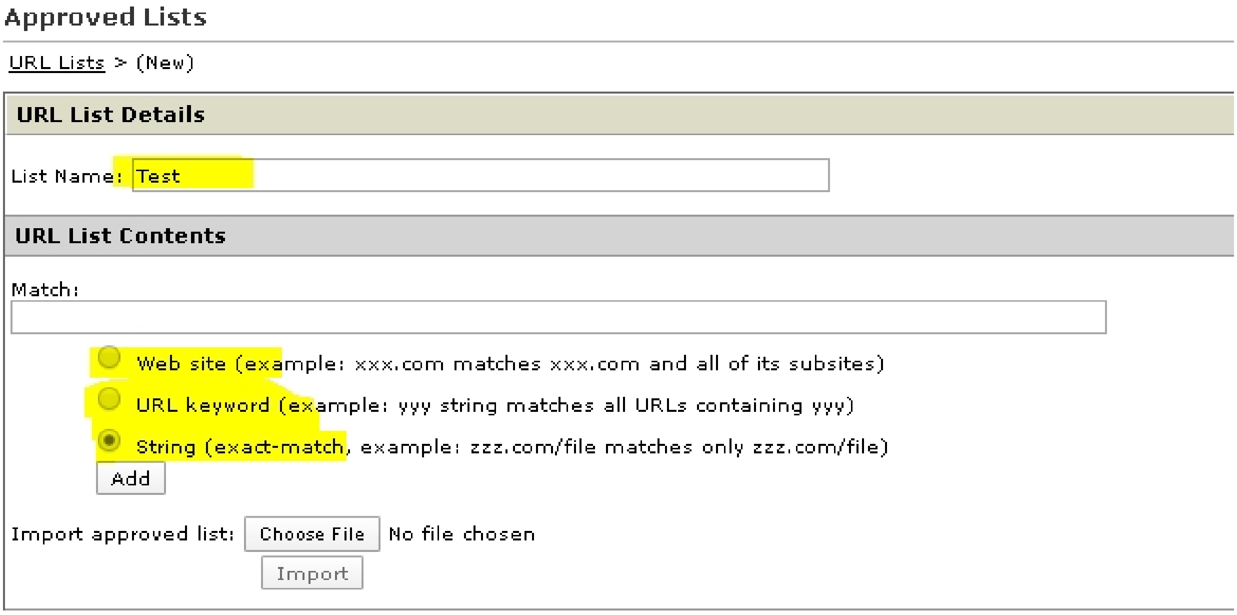


Approved Lists

Approved URL Lists

☐	List Name
☐	Global Applet/ActiveX List

- Enter the Name of the Lists.
  - Add the URL (e.g yahoo.com) as "Web Site" Click Add.
  - Add the URL (e.g yahoo.com) as "URL Keyword" Click Add.
  - Add the URL (e.g yahoo.com) as "String" Click Add.



Approved Lists

URL Lists > (New)

URL List Details

List Name: Test

URL List Contents

Match:

○ Web site (example: xxx.com matches xxx.com and all of its subsites)

○ URL keyword (example: yyy string matches all URLs containing yyy)

● String (exact-match, example: zzz.com/file matches only zzz.com/file)

Import approved list: Choose File No file chosen

- Click **Save**.
- Assign to a Policy. (eg. URL filtering Policies)

Note: Please make sure to clear cache and cookies before testing again

Error 4xx

You might need to use the Network Developer Tool to check the error code. How to use Network Developer Tools (Chrome)

1. 400 Bad Request.
The 400 status code, or *Bad Request* error, means the HTTP request that was sent to the server has invalid syntax.

Solution:

- The user's cookie that is associated with the site is corrupt. Clearing the browser's cache and cookies could solve this issue.
- Malformed request due to a faulty browser try another browser or update the browser.

2. 401 Unauthorized.
The 401 status code, or an *Unauthorized* error, means that the user trying to access the resource has not been authenticated or has not been authenticated correctly.

Solution:
Make sure that LDAP is sync and user is allow to use the proxy. LDAP Related Issues

3. 403 Forbidden

The 403 status code, or a *Forbidden* error, means that the user made a valid request but the server is refusing to serve the request, due to a lack of permission to access the requested resource.

Solution:
Most likely block by IWSVA, make sure website is whitelisted by policy.How to White List

4. 404 Not Found

The 404 status code, or a Not Found error, means that the user is able to communicate with the server but it is unable to locate the requested file or resource.

Solution:
Make sure you are accessing the correct URL string.

Resource: https://www.digitalocean.com/community/tutorials/how-to-troubleshoot-common-http-error-codes

Error 5xx

You might need to use the Network Developer Tool to check the error code. How to use Network Developer Tools (Chrome)

1. 502 Bad Gateway
The 502 status code, or Bad Gateway error, means that the server is a gateway or proxy server, and it is not receiving a valid response from the backend servers that should actually fulfill the request.

2. 503 Service Unavailable
The 503 status code, or Service Unavailable error, means that the server is overloaded or under maintenance. This error implies that the service should become available at some point.

3. 504 Gateway Timeout
The 504 status code, or Gateway Timeout error, means that the server is a gateway or proxy server, and it is not receiving a response from the backend servers within the allowed time period.

Note: Most Error 5xx can be troubleshoot by the following:

1. Check if IWSVA can connect to website.Accessing website via IWSVA CLI
2. Use common tool for network troubleshooting.Common Network Troubleshooting Tips
3. Do packet capture on IWSVA and client. Logs to Collect

Resource: https://www.digitalocean.com/community/tutorials/how-to-troubleshoot-common-http-error-codes

Certificate Issues

1. HTTPS Certificate Failure appears when accessing some sites. see KB1099448

2. A certificate warning appears in the web browser. see KB1121715

3. Creating Certificates for HTTPS decryption. see KB1060746

Note: openssl_client can help on checking for HTTPS issues. openssl

Logs and information to collect

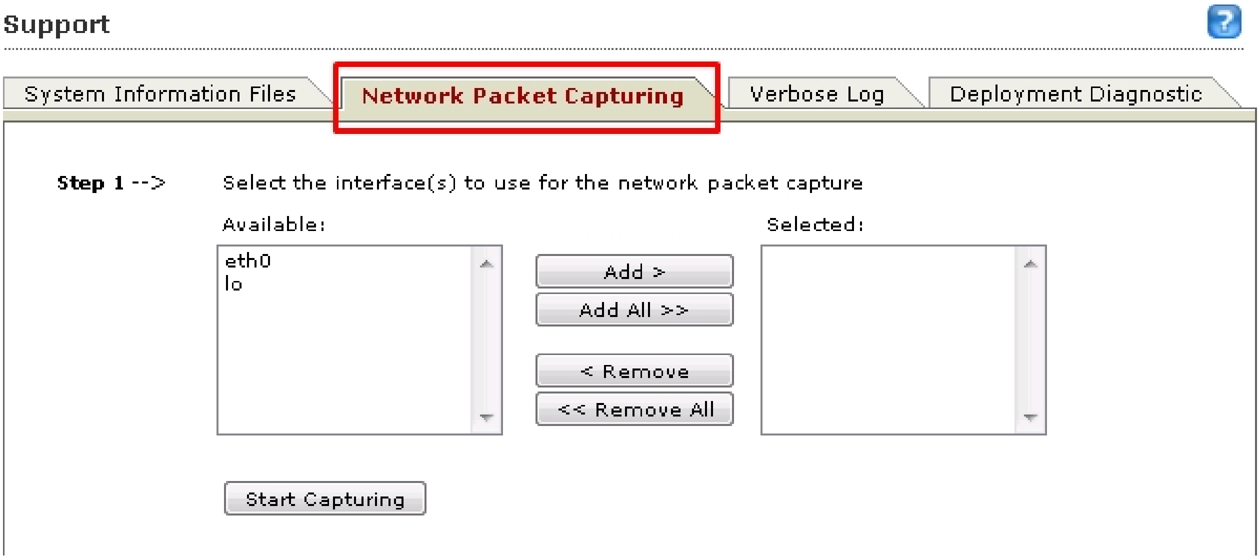
Important: Provide the result of the troubleshooting tips.

1. HTTP debug Logs.

- Go to > Support > Verbose Log, Enter and add the IP of the machine that accessing the URL.
- Start Verbose logging, REPLICATE the issue.
- Stop Verbose logging and DOWNLOAD HTTP log file

2. Packet Capture.

- On the IWSVA console, go to **Administration** > **Support** > **Network Packet Capturing** tab.
- Start Packet capture, REPLICATE the issue
- Stop Packet capture and DOWNLOAD pcap.



Step 1 --> Select the interface(s) to use for the network packet capture

Available:
eth0
lo

Selected:

3. IWSVA System Information Files

Useful Links

1. Collecting Debug logs in IWSVA
2. How to troubleshoot common http error codes?

LDAP Related Issues

This topic discuss the following issues/errors.

1. Cannot connect or sync ldap.LDAP Connectivity
2. User cannot authentication via IWSVA.Authentication Issues

Troubleshooting Tips

Testing LDAP Connectivity

To test whether your LDAP server is accessible from the IWSVA server, open a command prompt on the IWSVA server (or, from the command line in a UNIX environment) and type the following:

- Log on to IWSVA SSH as root

```
[root@iwsva ~]# telnet ldap_server_hostname/IP 389
```

Note: If you do not receive an error message, the port and DNS host name of the LDAP server are confirmed.

Check if IWSVA can resolve the LDAP server

- Log on to IWSVA SSH as root

```
[root@iwsva ~]# nslookup ldap_server_hostname
```

How to troubleshoot IWSVA authentication issues?

Note: The steps below will log out user that are currently using IWSVA so plan accordingly

1. Clear the cache and cookies of computer and re-login.

How to clear cache.

2. Force LDAP sync via IWSVA CLI.

- Log in to the IWSVA Command Line Interface (CLI) as "root".
- Navigate to the commonldap folder using this command:

  ```
  [root@iwsva ~] cd /etc/iscan/commonldap/
  ```

- Use the tool to force the synchronization:

  ```
  [root@iwsva ~] sh LdapSyncTool.sh
  ```

- To apply the change, restart the IWSS authentication daemon using the following command:

  [root@iwsva ~] /etc/iscan/S99ISAuthDaemon restart

3. Clear IP user cache.

- Log in to the IWSVA Command Line Interface (CLI) as "root".
- Stop the Authentication and the HTTP Daemon with the following commands:

  ```
  [root@iwsva ~] /usr/iwss/S99ISAuthDaemon stop
  [root@iwsva ~] /usr/iwss/S99ISproxy stop
  ```

- Clear the IP user cache with the following command:

  ```
  [root@iwsva ~]/usr/iwss/S99ISAuthDaemon clean
  ```

- Start the Authentication and the HTTP Daemon with the following commands:

  ```
  [root@iwsva ~]/usr/iwss/S99ISAuthDaemon start
  [root@iwsva ~] /usr/iwss/S99ISproxy start
  ```

Logs and information to collect

Important: Provide the result of the troubleshooting tips.

1. LDAP Verbose Logs

- Log in to the IWSVA Command Line Interface (CLI) as "root".
- Edit the /etc/iscan/commonldap/LdapSetting.ini

[root@iwsva ~] vi /etc/iscan/commonldap/LdapSetting.ini

- Search for the following parameter and set verbose to "yes".

  ```
  # set auth daemon to debug mode
  verbose=yes
  ```

- Restart the authentication service using the following command:
  # /etc/iscan/S99ISAuthDaemon restart

Note: Reverting the verbose, do the same step and set the verbose to "no".

2. IWSVA System Information Files

Useful Links

1. Clearing the ip user cache in IWSVA
2. IWSVA synchronizees with Active Directory only After 24 hours

IWSVA URL Logs Issue

This topic discuss issues related to "logs is not showing on the console" (e.g Internet Access Logs, etc).

Troubleshooting Tips

How to troubleshoot URL logs issues?

1. Check if the Logs Data Size adhere to IWSVA Sizing Guide.

2. Restart Common Logs Services.

   - Stop the CommonLog service using this command:

     [root@iwsva ~] cd /etc/iscan/commonldap/ stop

   - Start the CommonLog service

     [root@iwsva ~] cd /etc/iscan/commonldap/ start.

3. Refer to Useful KB link for other errors: Useful Links

Logs and information to collect

Important: Provide the result of the troubleshooting tips.

IWSVA System Information Files

Useful Links

1. "No data was found for selected parameters" message appears when displaying the internet access logs
2. "request has timed out" appears when viewing internet access log in IWSVA.
3. Internet access logs show only ip addressess in the domain section
4. Deleting logs generated with ip-user-cache on IWSVA

Performance Issues

This topic discuss the following issues/errors.

1. Slow Web Browsing
2. High CPU/Memory

Troubleshooting Tips

How to troubleshoot slow web browsing issue?

1. Try to browse the affected website(s) using another browser (e.g. Firefox, IE, or Chrome).
2. Try to browse the affected websites(s) from another PC.
3. Check the system resource usage (CPU, memory, disk space, swap, etc.).
    - Go to System Status

1. Check the DNS response time by doing nslookup on IWSVA. Common Network Troubleshooting Tips

2. On IWSVA command line, try to access the affected website(s) directly using wget and see if there's is a significant delay.Accessing website via IWSVA CLI

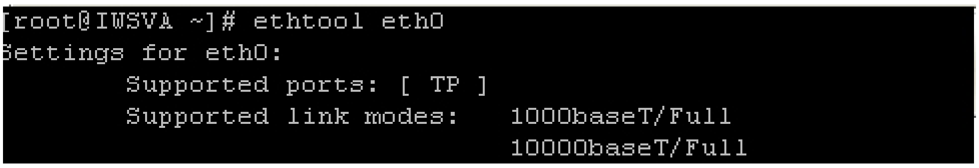
3. Check if IWSVA is configured to use proxy server to get updates and Web Reputation queries, and make sure that the proxy server is reachable and very responsive.
    - Go to Update > Connection Settings to check the proxy.
    - Check if proxy can be reached.Common Network Troubleshooting Tips

4. Run the Connectivity Test tool to check the connection speed:
    - Go to Administration > Support > Deployment Diagnostics

5. Try to clear the WRS/URL Cache.
    - Go to HTTP > Configuration > WRS/URL Cache

6. Try to isolate the issue by disabling each Feature one by one. (e.g Turn off Application Control , Bandwidth Control, HTTPS Decryption, etc) and check which service Feature cause the issue.

7. If the issue is affecting all websites, make sure that the duplex mode of the switch and IWSVA's network interface are the same. Duplex mode on IWSVA can be determined by executing "**ethtool eth0**".



```
[root@IWSVA ~]# ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:    1000baseT/Full
                                 10000baseT/Full
```

How to troubleshoot High CPU/memory issues?

1. Check if there Many Instances of URL is being blocked.
   - Check Policy Enforcement Logs for TOP URL that is being blocked. How to Search Logs
   - Add to whitelist and check if performance is improved.How to White List

2. Check if IWSVA can accomodate the request based on sizing guide. IWSVA Sizing Guide

3. Check if there might be a specific action that triggers the issue. (e.g. accessing specific URL, downloading file, etc.)

4. Check which process is using most of the resources by using "top" command. Using Top Command

5. Check the system resource usage (CPU, memory, disk space, swap, etc.) using “top” command. Using Top Command

6. Check the CPU Usage history on the System Dashboard to have an idea when the high cpu usage started.Checking IWSVA Performance History

7. Check the update log file what are the last components that were updated before the issue appeared. Command below will display last 30 instance of update logs

```
[root@iwsva ~]# cat -n 30 /etc/iscan/log/update.log.<date>.0001
```

Note: you can rollback update if needed.Updating/Rollback Pattern

8. Check the audit trail log file to find out the last configuration changes on IWSVA. Command below will display last 30 instance of update logs

```
[root@iwsva ~]# cat -n 30  /etc/iscan/log/audit.trail.log
```

Logs and information to collect

Important: Provide the result of the troubleshooting tips.

1. Answers to the following questions

- What's the hardware specs of the server experiencing the problem (CPUs, RAM, disk, etc.)?
- How many users are using their server at any given time?
- Which User Identification option is used (no identification, IP address, host name, or LDAP)?
- If they're on ICAP mode, which Caching device are they running in conjunction with appliance?
- How does HTTP flow in their network from the internet to the browser? Please send a diagram of their network.
- Is the issue consistently happening throughout the day or only during specific times in a day (i.e. peak hours)?
- Have they tried restarting the Proxy component of the appliance to see if it fixes the problem?

2. Screenshot of TOP command. Using Top Command

3. IWSVA System Information Files

Web UI/Console Issues

This topic discuss the following issues/errors.

1. Common Error Message
2. Cannot connect to console

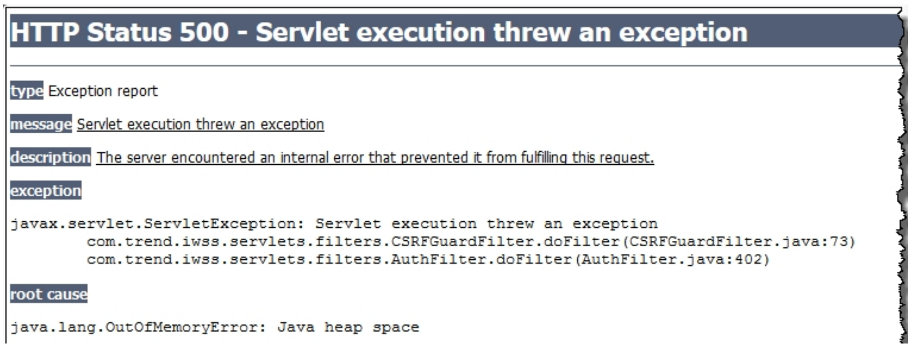
Troubleshooting Tips

Common Error Messages

1. Unable to export configuration file.

Error: **HTTP 500 status.**
Root Cause: "***java.lang.OutOfMemoryError: Java heap space***".

see KB 1114920



HTTP Status 500 - Servlet execution threw an exception

type Exception report

message Servlet execution threw an exception

description The server encountered an internal error that prevented it from fulfilling this request.

exception

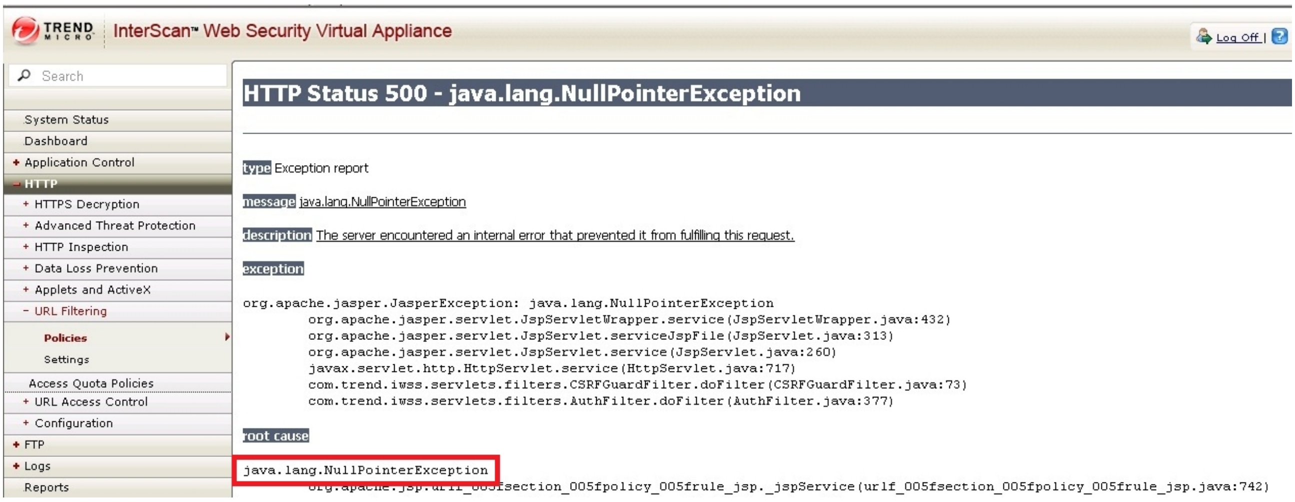
```
javax.servlet.ServletException: Servlet execution threw an exception
	com.trend.iwss.servlets.filters.CSRFGuardFilter.doFilter(CSRFGuardFilter.java:73)
	com.trend.iwss.servlets.filters.AuthFilter.doFilter(AuthFilter.java:402)
```

root cause

```
java.lang.OutOfMemoryError: Java heap space
```

2. You receive "**HTTP Status 500 - java.lang.NullPointerException**" error.

see KB 1105051



HTTP Status 500 - java.lang.NullPointerException

type Exception report

message java.lang.NullPointerException

description The server encountered an internal error that prevented it from fulfilling this request.

exception

```
org.apache.jasper.JasperException: java.lang.NullPointerException
	org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:432)
	org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
	org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
	com.trend.iwss.servlets.filters.CSRFGuardFilter.doFilter(CSRFGuardFilter.java:73)
	com.trend.iwss.servlets.filters.AuthFilter.doFilter(AuthFilter.java:377)
```

root cause

```
java.lang.NullPointerException
	org.apache.jsp.urlf_005fsection_005fpolicy_005frule_jsp._jspService(urlf_005fsection_005fpolicy_005frule_jsp.java:742)
```

How to troubleshoooot unable to connect to IWSVA Console?

1. Check the GUI port by doing telnet to the assigned GUI port (1812/8443) and check if the port is responding.

   ```
   [root@iwsva ~]# telnet localhost 1812
   Trying 127.0.0.1...
   Connected to localhost.
   Escape character is '^]'.

   [root@iwsva ~]# telnet localhost 8443
   Trying 127.0.0.1...
   Connected to localhost.
   Escape character is '^]'.
   ```

2. Try to restart the GUI service, and wait for about a minute before trying to access the GUI again.

   ```
   [root@iwsva ~]# /usr/iwss/S99IScanHttpd restart
   ```

3. Try to access the GUI using another PC (Same network of the IWSVA)
4. Check the connection to the Postgres database. Checking Database Connection
5. Check if there’s still enough disk space. Checking disk space information
6. Make sure that ownership of the IWSVA files are set to user and group "iscan". Checking File Ownership

Logs and information to collect

Important: Provide the result of the troubleshooting tips.

1. Answers to the following questions.

- What is the error message they're seeing when logging in the GUI? Get a screenshot.
- Which protocol are they using to access the GUI (HTTP or HTTPS)?
- Is the appliance reachable via TELNET from the workstation they're trying to open the GUI on? For example, "telnet <appliances_ip> 1812". "telnet <appliances_ip> 8443".

2. IWSVA System Information Files

3. Web UI Logs (Use WinSCP to copy)

```
/var/iwss/tomcat/logs/*
```

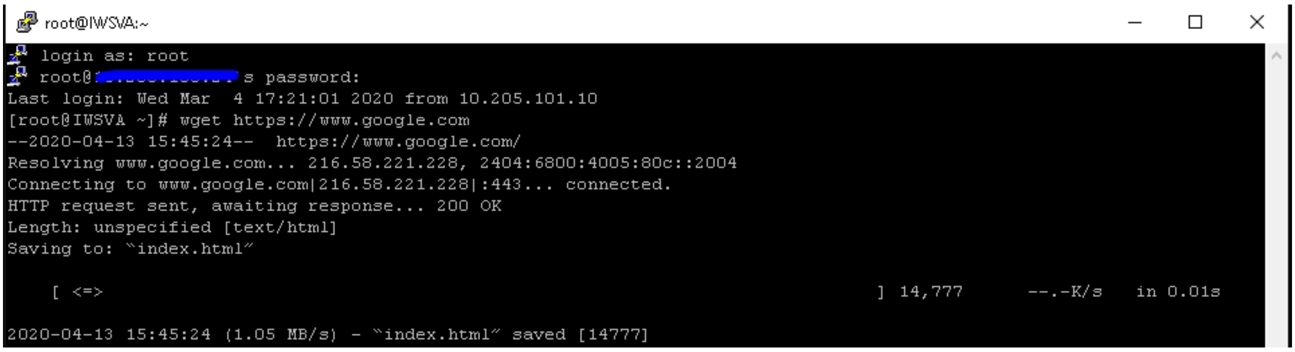
Index

How to check if IWSVA can connect to a website using CLI?

- Log in to IWSVA SSH as root.
- Type the command.

[root@iwsva ~] wget <URL>

example : *[root@iwsva ~] wget https://www.google.com*



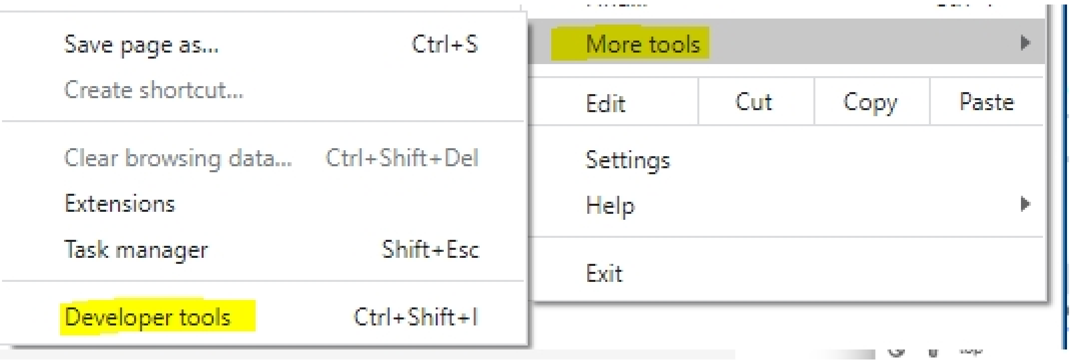
```
login as: root
root@[redacted]'s password:
Last login: Wed Mar  4 17:21:01 2020 from 10.205.101.10
[root@IWSVA ~]# wget https://www.google.com
--2020-04-13 15:45:24--  https://www.google.com/
Resolving www.google.com... 216.58.221.228, 2404:6800:4005:80c::2004
Connecting to www.google.com|216.58.221.228|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `index.html'

    [ <=>                                                                      ] 14,777      --.-K/s   in 0.01s

2020-04-13 15:45:24 (1.05 MB/s) - `index.html' saved [14777]
```

Note: The response MUST show connected any error like "Unable to resolve" or "Timeout" means its a network issue.Refer to Common Network Troubleshooting Tips

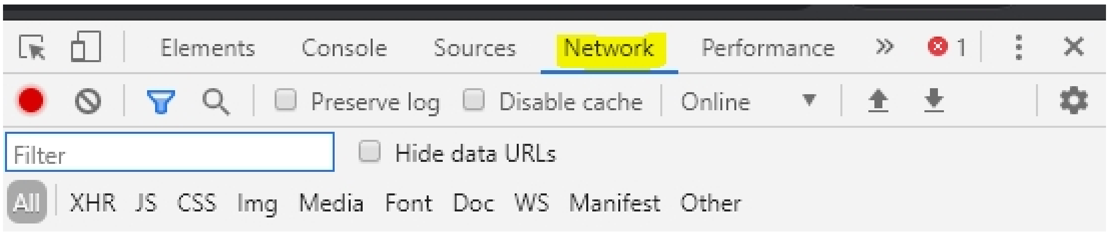
How to use Network Developer Tools (Chrome)?

Website spawns several URLS when it is access and the sometimes block page of IWSVA will not show since it is not the main website. Network Developer Tools helps you to find the URL and add it to white-list. **This is useful for page not displaying correctly and broken pages.**

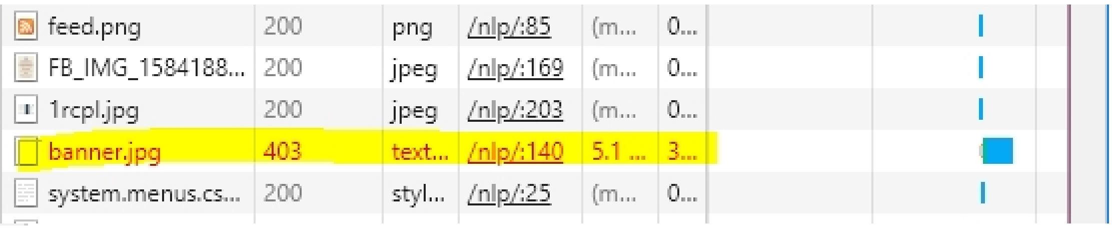
- When using chrom press **Ctrl +Shift +i**



- Click Network Tab and Access the Website.

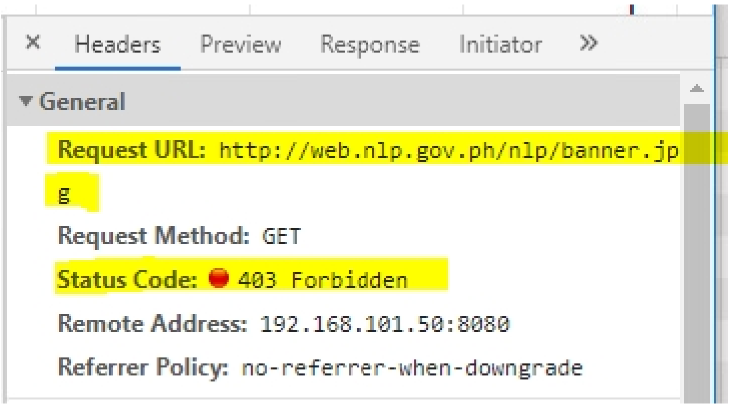


- Look for any Error code 4xx (403 , 402 etc).



feed.png	200	png	/nlp/:85	(m...	0...
FB_IMG_1584188...	200	jpeg	/nlp/:169	(m...	0...
1rcpl.jpg	200	jpeg	/nlp/:203	(m...	0...
banner.jpg	403	text...	/nlp/:140	5.1 ...	3...
system.menus.cs...	200	styl...	/nlp/:25	(m...	0...

- Double Click the URL to view the Request URL. in the example above click **banner.jpg**



Request URL: http://web.nlp.gov.ph/nlp/banner.jpg

Request Method: GET

Status Code: ● 403 Forbidden

Remote Address: 192.168.101.50:8080

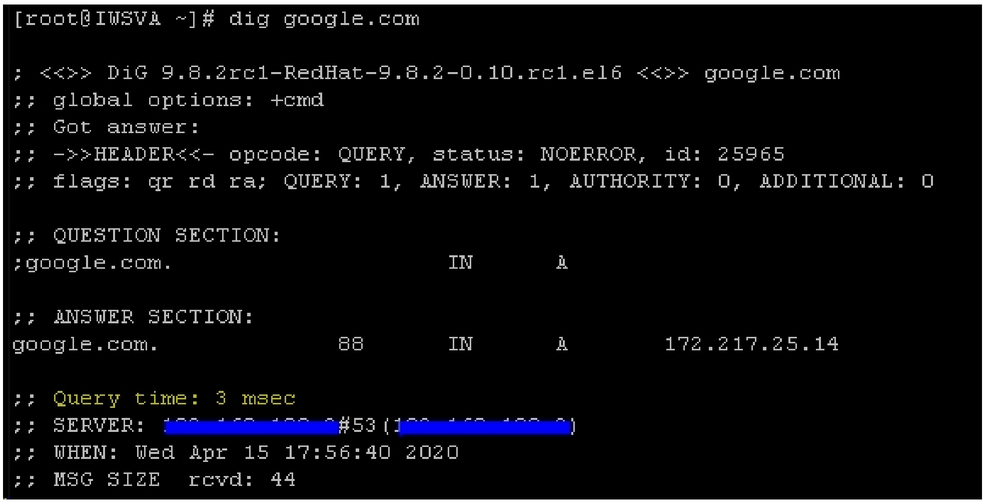
Referrer Policy: no-referrer-when-downgrade

- Once URL is found add it to white list.How to White List

Common Network Troubleshooting Tools and Tips.

dig - command to check if IWSVA can resolve the website and the DNS resolution time. ***(ideal response time is 100msec if not try to change DNS server)***

[root@iwsva ~]# dig google.com



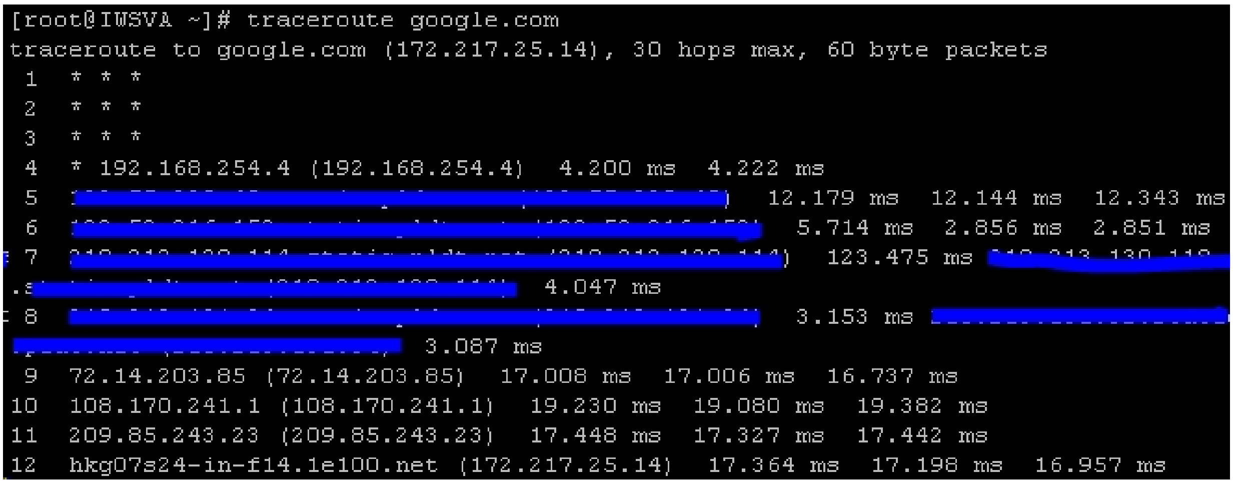
```
[root@IWSVA ~]# dig google.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25965
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             88      IN      A       172.217.25.14

;; Query time: 3 msec
;; SERVER: [redacted]#53([redacted])
;; WHEN: Wed Apr 15 17:56:40 2020
;; MSG SIZE  rcvd: 44
```

traceroute - command useful for isolating which hop is having an issue

The Traceroute tool will show you each hop sequentially, and total hops required. For each hop, it will display the hop #, roundtrip times, best time (ms), IP address, TTL, and country.

[root@iwsva ~]# traceroute google.com

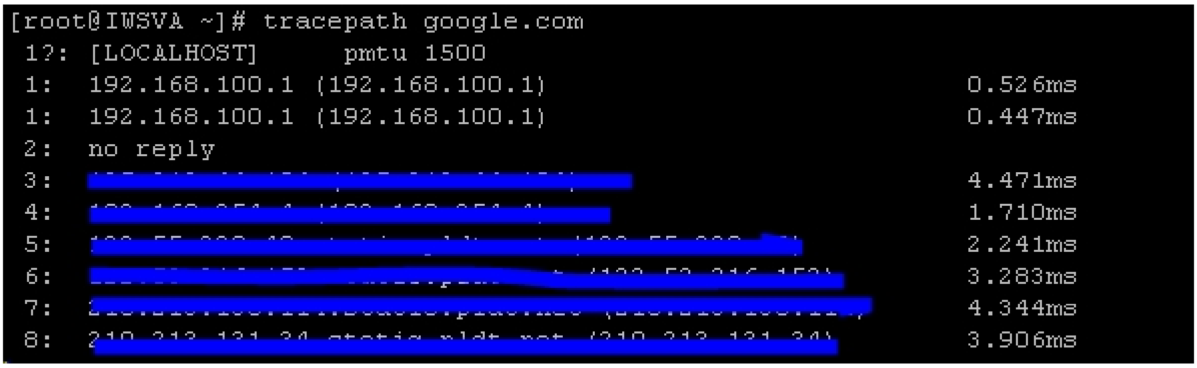
Note: If the route don't came back check which is the last IP where it stopped that may be the cause of the issue.



```
[root@IWSVA ~]# traceroute google.com
traceroute to google.com (172.217.25.14), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * 192.168.254.4 (192.168.254.4)  4.200 ms  4.222 ms
 5  [redacted])  12.179 ms  12.144 ms  12.343 ms
 6  [redacted])  5.714 ms  2.856 ms  2.851 ms
 7  [redacted])  123.475 ms [redacted]
[redacted]  4.047 ms
 8  [redacted]  3.153 ms [redacted]
[redacted]  3.087 ms
 9  72.14.203.85 (72.14.203.85)  17.008 ms  17.006 ms  16.737 ms
10  108.170.241.1 (108.170.241.1)  19.230 ms  19.080 ms  19.382 ms
11  209.85.243.23 (209.85.243.23)  17.448 ms  17.327 ms  17.442 ms
12  hkg07s24-in-f14.1e100.net (172.217.25.14)  17.364 ms  17.198 ms  16.957 ms
```

tracepath - It traces path to *destination* discovering MTU along this path. It uses UDP port *port* or some random port. It is similar to **traceroute**, only does not not require superuser privileges. Useful as well to check which host is not reachable.

[root@iwsva ~]# traceroute google.com



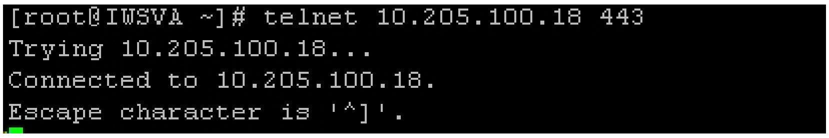
```
[root@IWSVA ~]# tracepath google.com
 1?: [LOCALHOST]      pmtu 1500
 1:  192.168.100.1 (192.168.100.1)                            0.526ms
 1:  192.168.100.1 (192.168.100.1)                            0.447ms
 2:  no reply
 3:  [redacted]                                               4.471ms
 4:  [redacted]                                               1.710ms
 5:  [redacted]                                               2.241ms
 6:  [redacted]                                               3.283ms
 7:  [redacted]                                               4.344ms
 8:  [redacted]                                               3.906ms
```

Note: you can add port like 443 and 80 to check if the website is reachable using the destination port.

example:
traceroute google.com/443
traceroute google.com/80

telnet - command to check if a destination port is open.

[root@iwsva ~]# telnet <IP> <port>

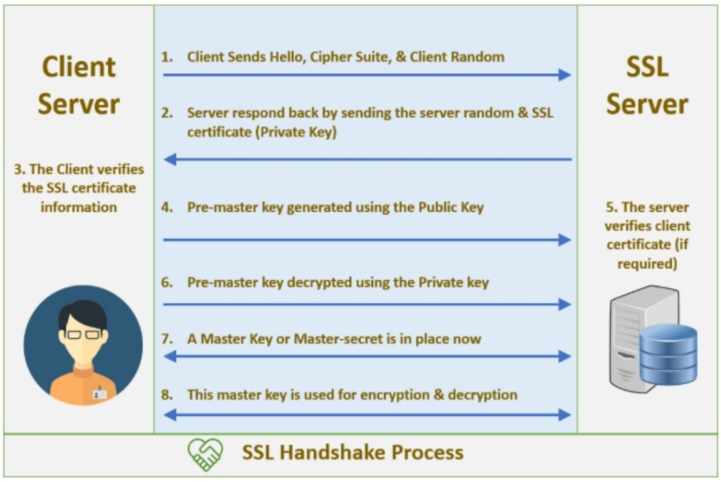


```
[root@IWSVA ~]# telnet 10.205.100.18 443
Trying 10.205.100.18...
Connected to 10.205.100.18.
Escape character is '^]'.
```

openssl s_client - command to check if the destination server SSL handshake is succesful. Useful for website using HTTPS. You can use this to inspect server certificates, cipher used and etc.

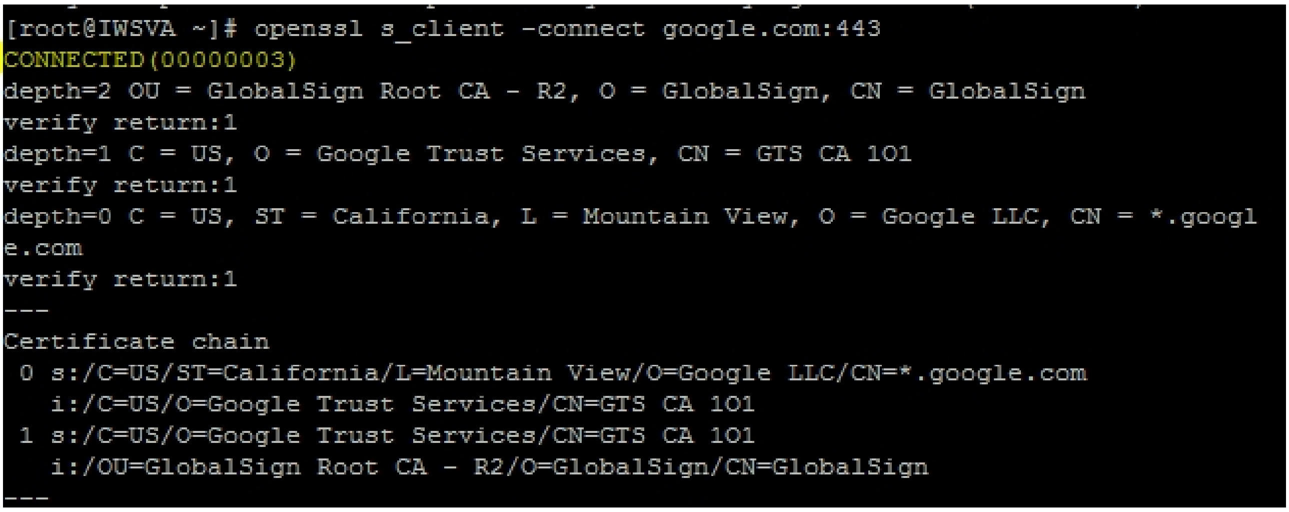
What is SSL handshake?

Source: https://cheapsslsecurity.com/blog/what-is-ssl-tls-handshake-understand-the-process-in-just-3-minutes/


Client Server
3. The Client verifies the SSL certificate information
1. Client Sends Hello, Cipher Suite, & Client Random
2. Server respond back by sending the server random & SSL certificate (Private Key)
4. Pre-master key generated using the Public Key
6. Pre-master key decrypted using the Private key
7. A Master Key or Master-secret is in place now
8. This master key is used for encryption & decryption
SSL Server
5. The server verifies client certificate (if required)
SSL Handshake Process

Command: *[root@iwsva ~]# openssl s_client -connect <hostname>:<port>*

e.g.   [root@iwsva ~]# openssl s_client -connect google.com



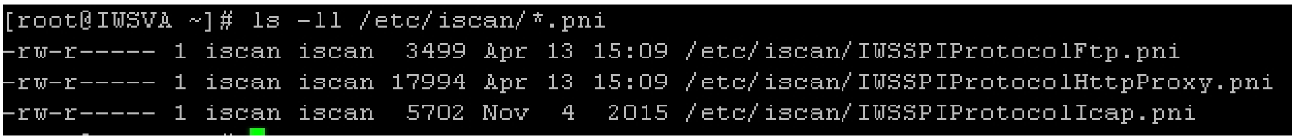
```
[root@IWSVA ~]# openssl s_client -connect google.com:443
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = *.googl
e.com
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google LLC/CN=*.google.com
   i:/C=US/O=Google Trust Services/CN=GTS CA 1O1
 1 s:/C=US/O=Google Trust Services/CN=GTS CA 1O1
   i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
---
```

Resource: https://support.pingidentity.com/s/article/OpenSSL-s-client-Commands

Checking IWSVA File Ownership and Permission

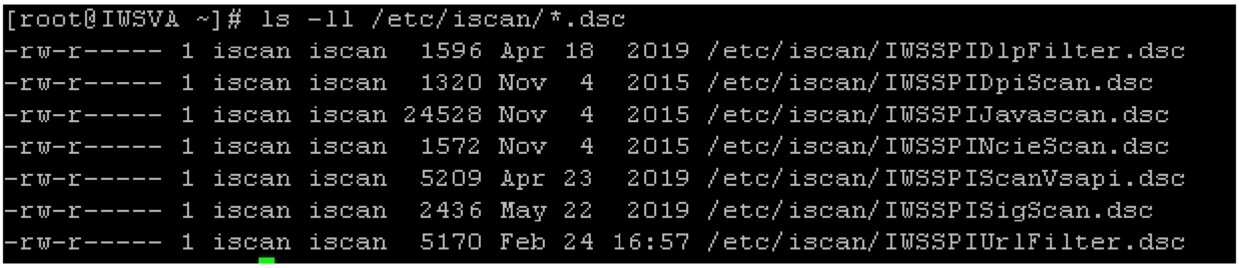
Make sure that the IWSVA file are own by IWSVA **(screenshot below for reference)**

[root@iwsva ~]# ls -ll /etc/iscan/.pni*



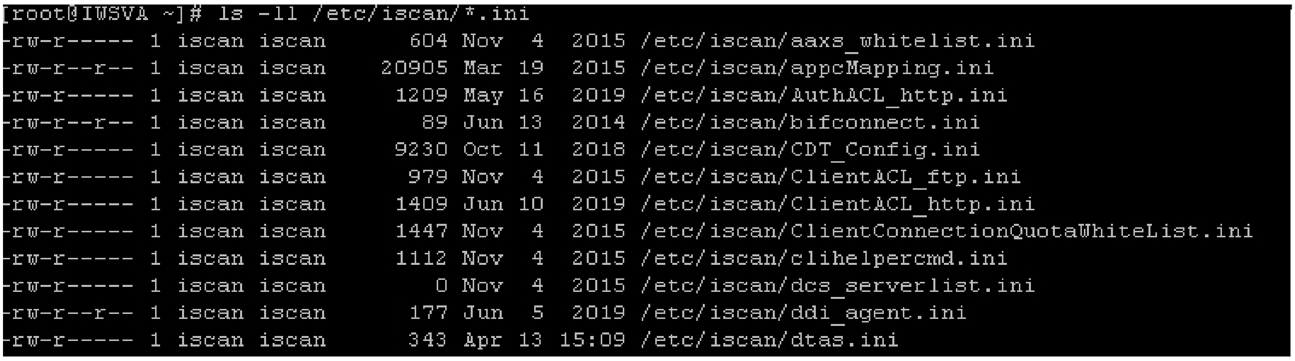
```
[root@IWSVA ~]# ls -ll /etc/iscan/*.pni
-rw-r----- 1 iscan iscan  3499 Apr 13 15:09 /etc/iscan/IWSSPIProtocolFtp.pni
-rw-r----- 1 iscan iscan 17994 Apr 13 15:09 /etc/iscan/IWSSPIProtocolHttpProxy.pni
-rw-r----- 1 iscan iscan  5702 Nov  4  2015 /etc/iscan/IWSSPIProtocolIcap.pni
```

[root@iwsva ~]# ls -ll /etc/iscan/.dsc*



```
[root@IWSVA ~]# ls -ll /etc/iscan/*.dsc
-rw-r----- 1 iscan iscan  1596 Apr 18  2019 /etc/iscan/IWSSPIDlpFilter.dsc
-rw-r----- 1 iscan iscan  1320 Nov  4  2015 /etc/iscan/IWSSPIDpiScan.dsc
-rw-r----- 1 iscan iscan 24528 Nov  4  2015 /etc/iscan/IWSSPIJavascan.dsc
-rw-r----- 1 iscan iscan  1572 Nov  4  2015 /etc/iscan/IWSSPINcieScan.dsc
-rw-r----- 1 iscan iscan  5209 Apr 23  2019 /etc/iscan/IWSSPIScanVsapi.dsc
-rw-r----- 1 iscan iscan  2436 May 22  2019 /etc/iscan/IWSSPISigScan.dsc
-rw-r----- 1 iscan iscan  5170 Feb 24 16:57 /etc/iscan/IWSSPIUrlFilter.dsc
```

[root@iwsva ~]# ls -ll /etc/iscan/.ini*
***note**: all INI files under /etc/iscan*



```
[root@IWSVA ~]# ls -ll /etc/iscan/*.ini
-rw-r----- 1 iscan iscan      604 Nov  4  2015 /etc/iscan/aaxs_whitelist.ini
-rw-r--r-- 1 iscan iscan    20905 Mar 19  2015 /etc/iscan/appcMapping.ini
-rw-r----- 1 iscan iscan     1209 May 16  2019 /etc/iscan/AuthACL_http.ini
-rw-r--r-- 1 iscan iscan       89 Jun 13  2014 /etc/iscan/bifconnect.ini
-rw-r----- 1 iscan iscan     9230 Oct 11  2018 /etc/iscan/CDT_Config.ini
-rw-r----- 1 iscan iscan      979 Nov  4  2015 /etc/iscan/ClientACL_ftp.ini
-rw-r----- 1 iscan iscan     1409 Jun 10  2019 /etc/iscan/ClientACL_http.ini
-rw-r----- 1 iscan iscan     1447 Nov  4  2015 /etc/iscan/ClientConnectionQuotaWhiteList.ini
-rw-r----- 1 iscan iscan     1112 Nov  4  2015 /etc/iscan/clihelpercmd.ini
-rw-r----- 1 iscan iscan        0 Nov  4  2015 /etc/iscan/dcs_serverlist.ini
-rw-r--r-- 1 iscan iscan      177 Jun  5  2019 /etc/iscan/ddi_agent.ini
-rw-r----- 1 iscan iscan      343 Apr 13 15:09 /etc/iscan/dtas.ini
```

If any file ownership/permission is incorrect , make changes to correct. Changing File Ownership and Permission (Linux)

Checking Database Connection

- Login to the IWSVA shell as root.
- Find out the host address of the database server using the command in the following example:

[root@iwsva ~]# grep Servername /etc/iscan/odbc.ini Servername = localhost Servername = localhost

- After determining the host address, connect to the database using the command in the following example.

[root@iwsva51 ~]# /etc/iscan/PostgreSQL/bin/psql –h localhost -U sa -d iwss

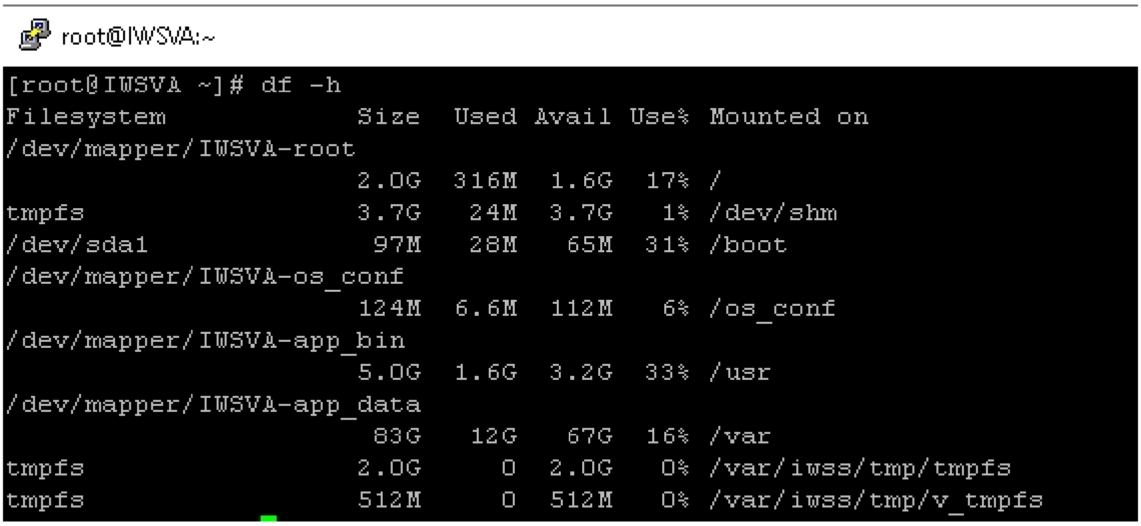
Welcome to psql 7.4.16, the PostgreSQL interactive terminal.
Type: \copyright for distribution terms \h for help with SQL commands \? for help on internal slash commands \g or terminate with semicolon to execute query

\q to quit iwss=#

Checking Disk Space Information

- Login to the IWSVA shell as root.
- Type the command "df -h"

[root@iwsva ~]df -h



root@IWSVA:~

```
[root@IWSVA ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/IWSVA-root
                      2.0G  316M  1.6G  17% /
tmpfs                 3.7G   24M  3.7G   1% /dev/shm
/dev/sda1              97M   28M   65M  31% /boot
/dev/mapper/IWSVA-os_conf
                      124M  6.6M  112M   6% /os_conf
/dev/mapper/IWSVA-app_bin
                      5.0G  1.6G  3.2G  33% /usr
/dev/mapper/IWSVA-app_data
                       83G   12G   67G  16% /var
tmpfs                 2.0G     0  2.0G   0% /var/iwss/tmp/tmpfs
tmpfs                 512M     0  512M   0% /var/iwss/tmp/v_tmpfs
```

Changing File Ownership and Permission (Linux)

Note: IWSVA files should be own by iscan:iscan

- File ownership

[root@iwsva ~]# chown iscan:iscan <file name>

- File permission

[root@iwsva ~]# chmod <permission> <file name>

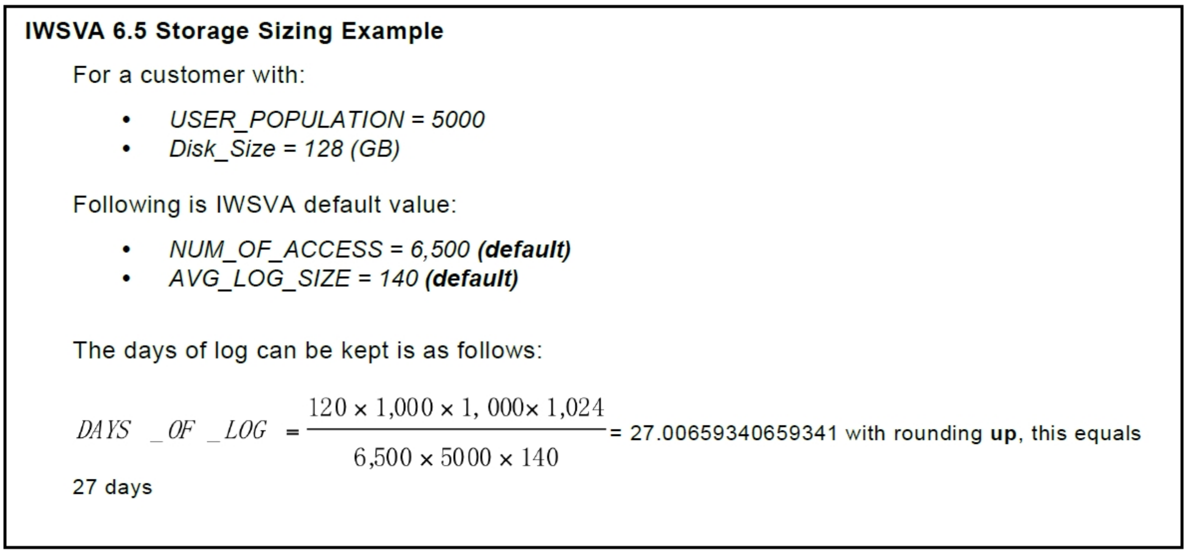
chmod preference: https://www.linode.com/docs/tools-reference/tools/modify-file-permissions-with-chmod/

Note: If unsure with the changes, check with support.

IWSVA Sizing Guide

http://files.trendmicro.com/documentation/guides/iwsva/IWSVA_65_External_Sizing_20Guide_v3.pdf

Sample Computation For Log Retention



IWSVA 6.5 Storage Sizing Example

For a customer with:

- *USER_POPULATION = 5000*
- *Disk_Size = 128 (GB)*

Following is IWSVA default value:

- *NUM_OF_ACCESS = 6,500* ***(default)***
- *AVG_LOG_SIZE = 140* ***(default)***

The days of log can be kept is as follows:

$$DAYS\_OF\_LOG = \frac{120 \times 1{,}000 \times 1,\ 000 \times 1{,}024}{6{,}500 \times 5000 \times 140}$$ = 27.00659340659341 with rounding **up**, this equals 27 days

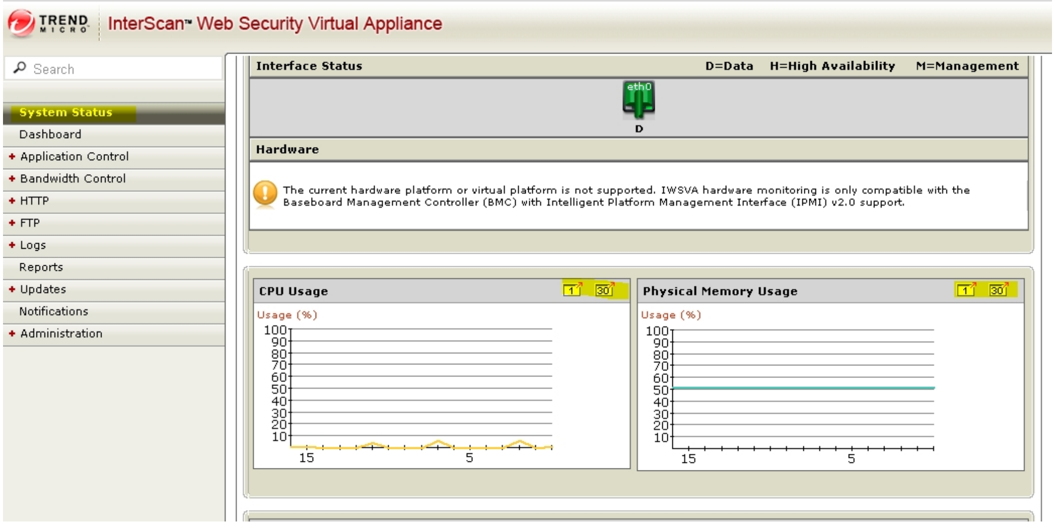
Using Top Command

Top command which is one of the most frequently used commands in our daily system administrative jobs. top command displays processor activity of your Linux box and also displays tasks managed by kernel in real-time.

https://www.tecmint.com/12-top-command-examples-in-linux/

Checking IWSVA Performance History

On the Summary then scroll donw to CPU and Memory Usage, there are small icons with numbers 1 and 30 which represents one day as well as 30 days performance history.



The current hardware platform or virtual platform is not supported. IWSVA hardware monitoring is only compatible with the Baseboard Management Controller (BMC) with Intelligent Platform Management Interface (IPMI) v2.0 support.

Installing Patch/Hotfix

Note: For latest IWSVA Patch you can check with Trend Micro Download Center.

1. Create a backup file. (For Best Practice)

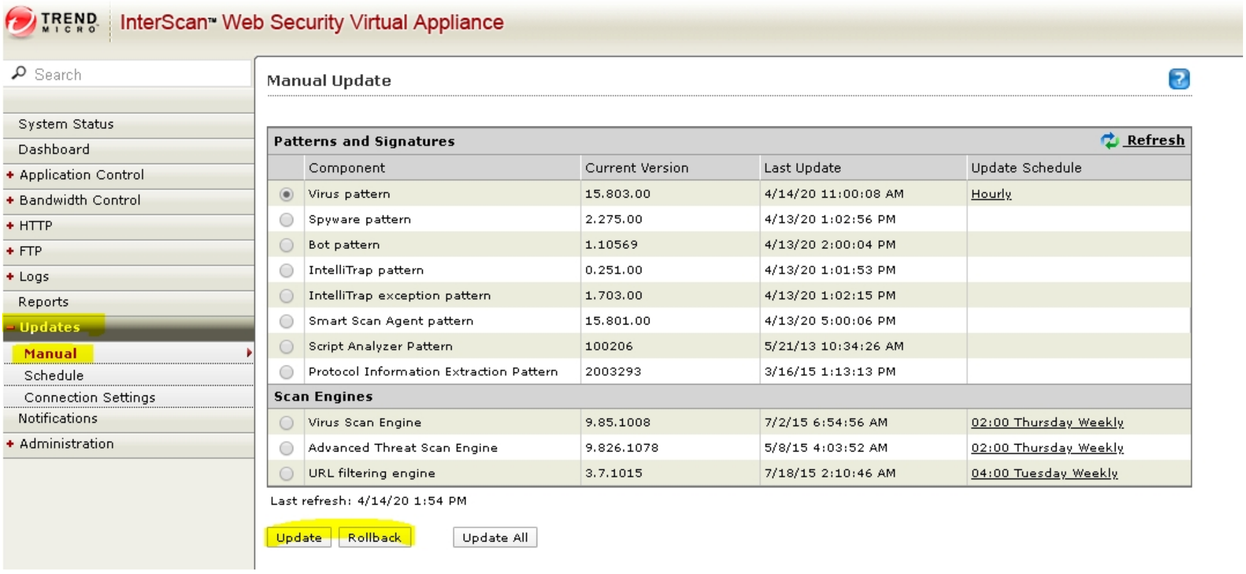
- Access the IWSVA web console.
- Select Administration > Configuration Backup/Restore.
- Click Export.

2. Installing the patch

- Log on to the IWSVA admin console GUI.
- Go to the "Administration > System Updates" page.
- Click "Browse".
- Browse your local hard disk for the patch file and click "Open".
- Click "Upload". Your browser uploads the patch file to IWSVA and IWSVA validates if the file is a legitimate patch.
- Click "Install".

Updating/Rollback Pattern

1. Go to Updates > Manual
2. Click Update or Rollback



Manual Update

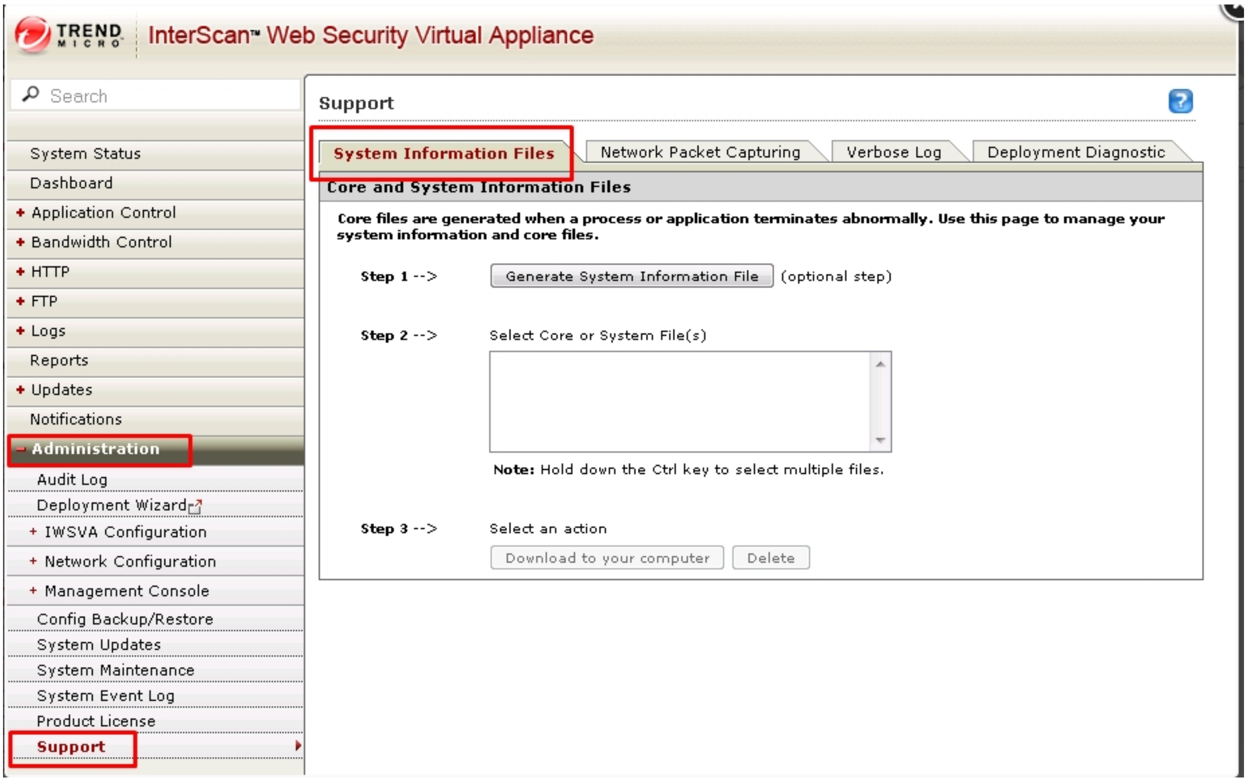
Patterns and Signatures — Refresh

	Component	Current Version	Last Update	Update Schedule
●	Virus pattern	15.803.00	4/14/20 11:00:08 AM	Hourly
○	Spyware pattern	2.275.00	4/13/20 1:02:56 PM	
○	Bot pattern	1.10569	4/13/20 2:00:04 PM	
○	IntelliTrap pattern	0.251.00	4/13/20 1:01:53 PM	
○	IntelliTrap exception pattern	1.703.00	4/13/20 1:02:15 PM	
○	Smart Scan Agent pattern	15.801.00	4/13/20 5:00:06 PM	
○	Script Analyzer Pattern	100206	5/21/13 10:34:26 AM	
○	Protocol Information Extraction Pattern	2003293	3/16/15 1:13:13 PM	
Scan Engines				
○	Virus Scan Engine	9.85.1008	7/2/15 6:54:56 AM	02:00 Thursday Weekly
○	Advanced Threat Scan Engine	9.826.1078	5/8/15 4:03:52 AM	02:00 Thursday Weekly
○	URL filtering engine	3.7.1015	7/18/15 2:10:46 AM	04:00 Tuesday Weekly

Last refresh: 4/14/20 1:54 PM

IWSVA System Information Files

- On the IWSVA console, go to **Administration** > **Support** > **System Information Files** tab.
- Click Generate System Information File and Download when finished.



Core and System Information Files

Core files are generated when a process or application terminates abnormally. Use this page to manage your system information and core files.

Step 1 --> Generate System Information File (optional step)

Step 2 --> Select Core or System File(s)

Note: Hold down the Ctrl key to select multiple files.

Step 3 --> Select an action

IWSVA Official Documents

Administration Guide:
https://docs.trendmicro.com/all/ent/iwsva/v6.5_sp2/en-us/iwsva_6.5_sp2_ag.pdf

Installation Guide:
https://docs.trendmicro.com/all/ent/iwsva/v6.5_sp2/en-us/iwsva_6.5_sp2_ig.pdf

Online Help:
https://docs.trendmicro.com/all/ent/iwsva/v6.5_sp2/en-us/iwsva_6.5_sp2_online_help/iwsva_help.htm

Feedback

For comments and suggestions you can answer a quick survey below.

- Comments and Suggestions