.:|:.:|:.
cisco

Introduction and purpose:

This document provides details steps for deploying Splunk version 4.2 and 4.3 release, Configuring and Implementing Splunk software and uploading Splunk for Cisco Ironport WSA APP (SplunkforCiscoIronportWSA). In addition it contains command line (CLI) details for Splunk services and verification of connectivity/operation with screen capture/snapshot for visual review.

Components Used:

The information in this document is based on Windows 2008 R2 server and Splunk version 4.3 Build 115073.

Document Audience:

This documentation is primarily for Customer support engineers, Sales Engineers and customers who are engage in planning, deploying/implementing, and configuring Splunk in Windows or Unix/Linux environment.

System Requirements:

Splunk Advanced Web Reporting runs on Windows and Red Hat Linux. There is no support for virtualization for production instances of Splunk Advanced Web Reporting. Reference hardware can be commodity-grade with the minimum specifications below.

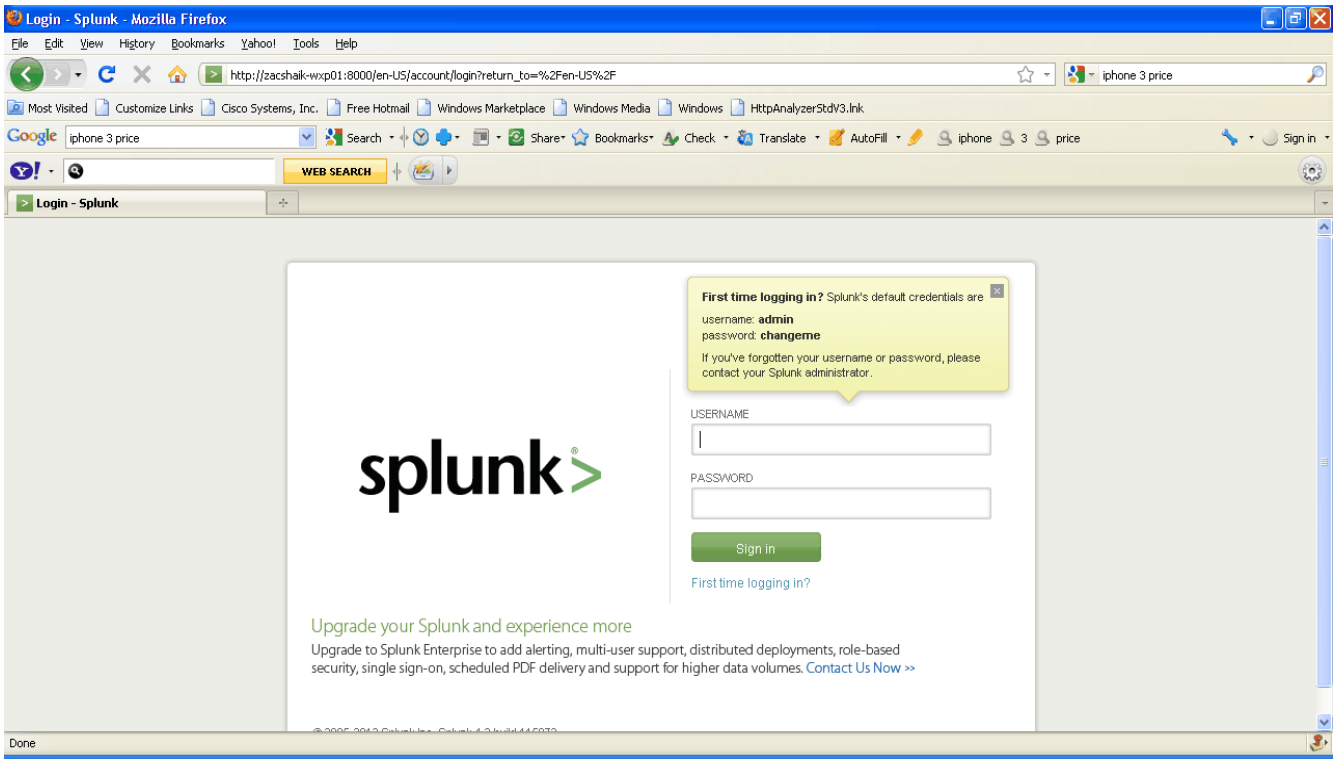
- Intel x86 64-bit chip architecture with 2 CPUs, 4 cores per CPU, and 2.5 to 3 GHz per core.
- 16 GB RAM
- (4) 300-GB SAS hard disks at 10,000 rpm each in RAID 10 (800 IOPS or better)
- (1) Gigabit Ethernet network interface card (NIC). A second NIC for a management network is recommended

Note: These hardware specifications are recommended for an organization with more than 25,000 users. Please talk to your account team to understand the hardware specifications you will need to run Splunk Advanced Web Reporting at your organization.

Step 1:
Download Splunk from www.splunk.com

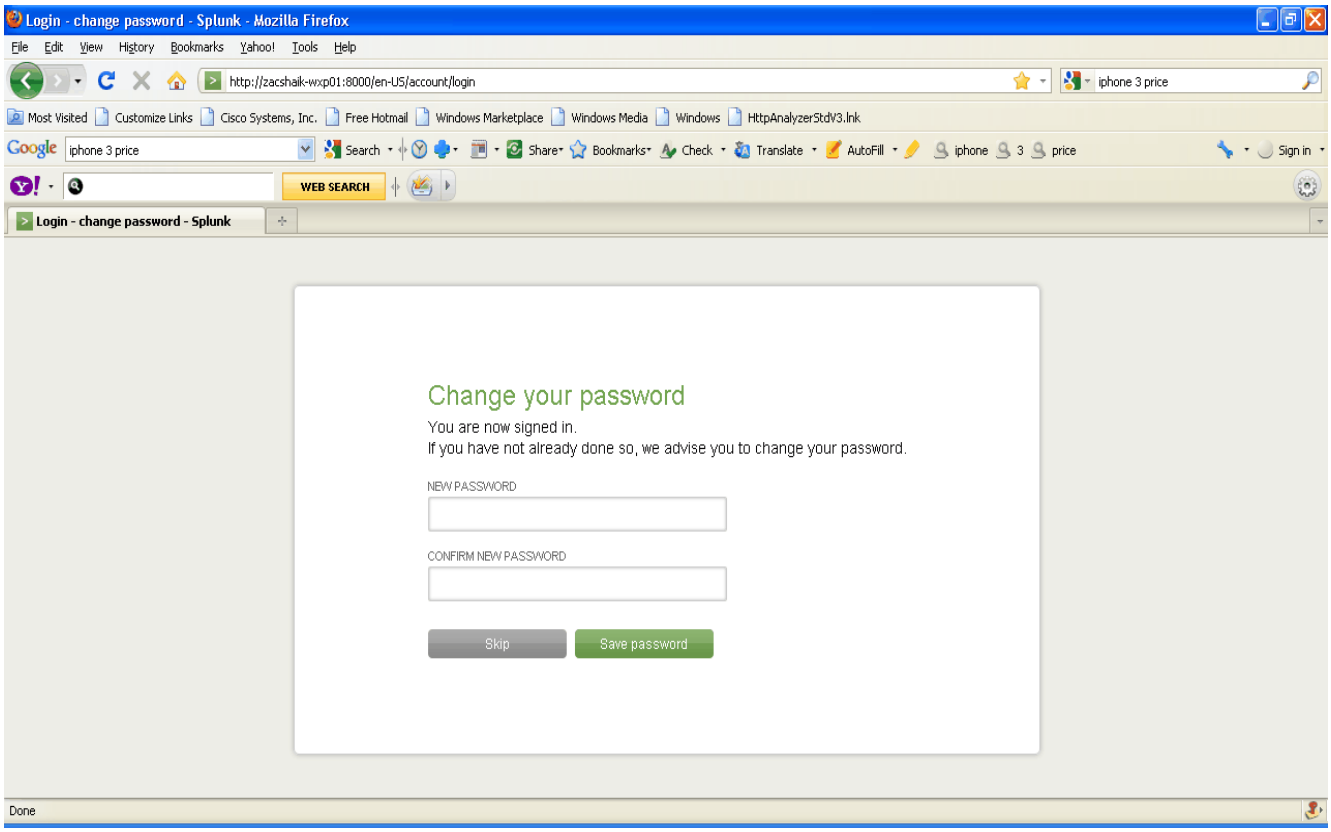
Step 2:
Install Splunk on the local host/server.

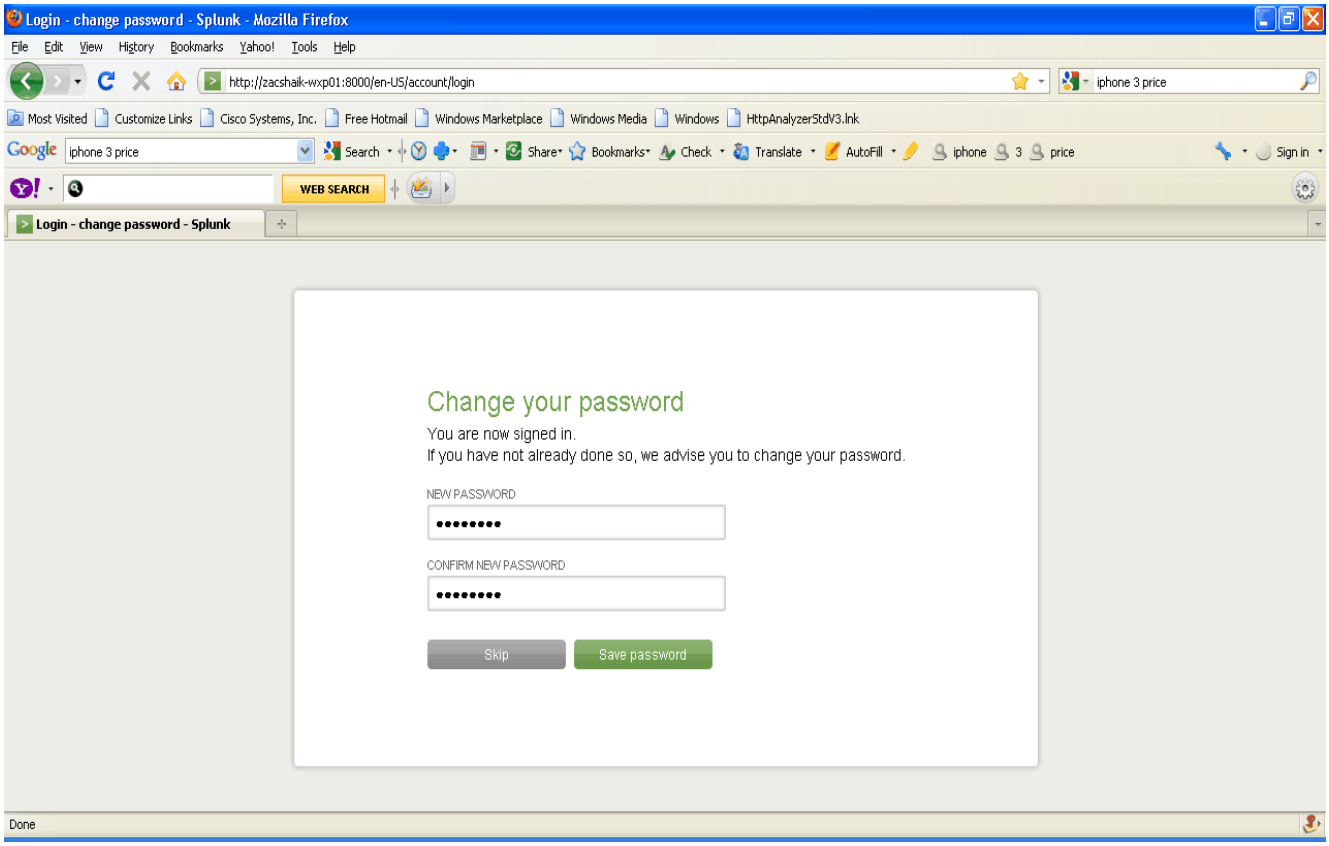
Step 3:
Once the installation is completed logon via Splunk GUI for the first time, and change admin password.



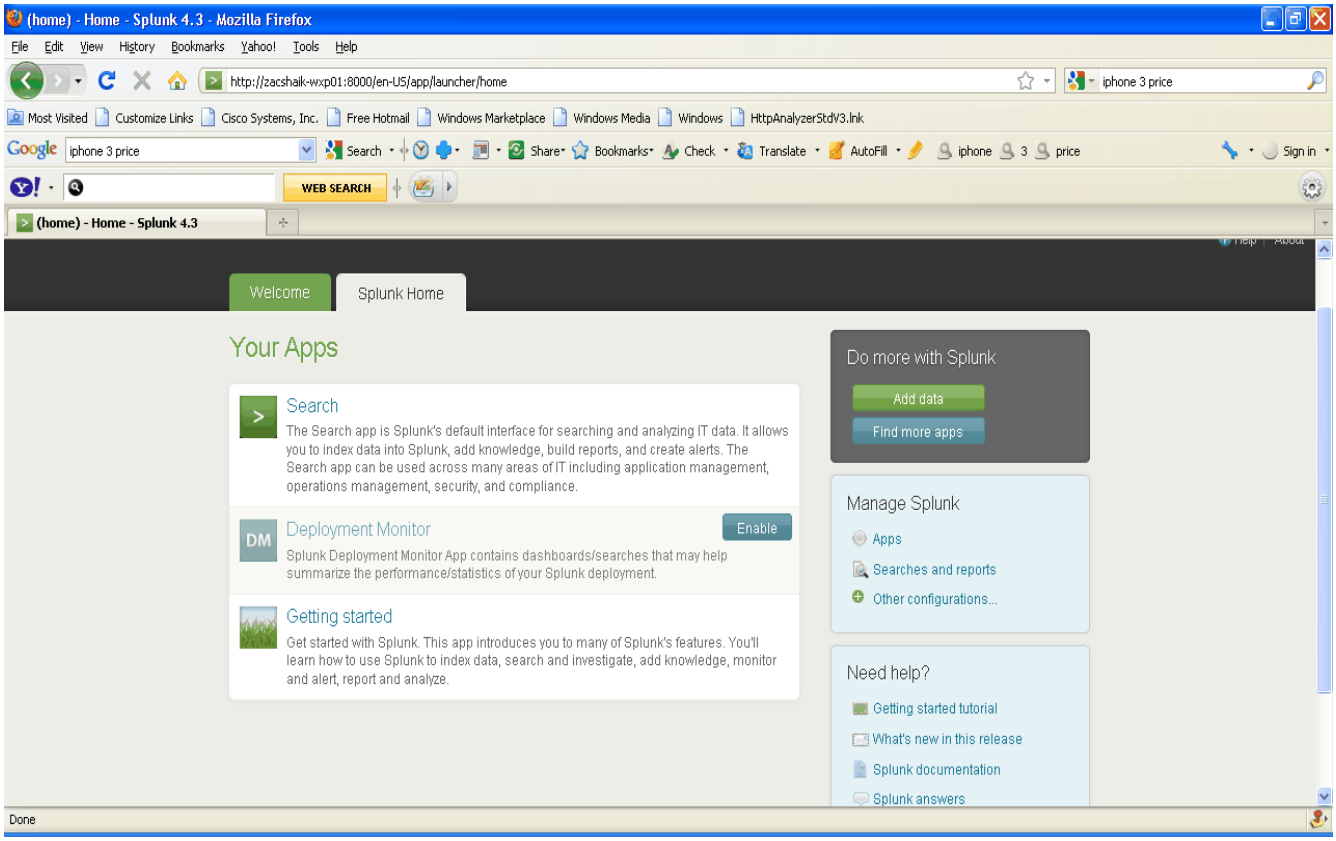
Step 4:

Enter username: admin password changeme, and enter desired password for admin account for subsequent logins.




Login - change password - Splunk - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://zacshaik-wxp01:8000/en-US/account/login
iphone 3 price
Most Visited Customize Links Cisco Systems, Inc. Free Hotmail Windows Marketplace Windows Media Windows HttpAnalyzerStdV3.lnk
Google iphone 3 price Search Share Bookmarks Check Translate AutoFill iphone 3 price Sign in
WEB SEARCH
Login - change password - Splunk
Change your password
You are now signed in.
If you have not already done so, we advise you to change your password.
NEW PASSWORD
CONFIRM NEW PASSWORD
Skip
Save password
Done

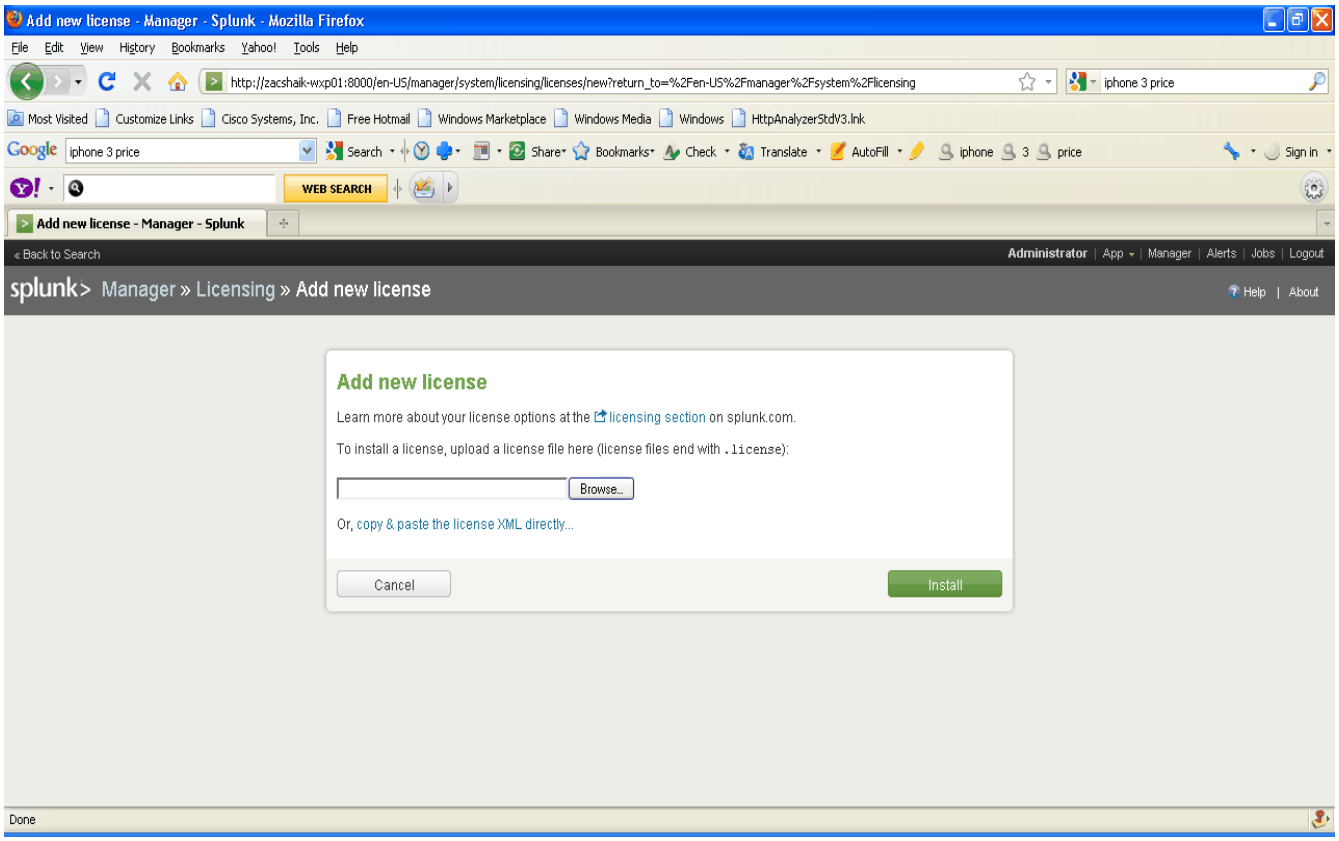
This will bring you to the Splunk Welcome/Home/default Screen.

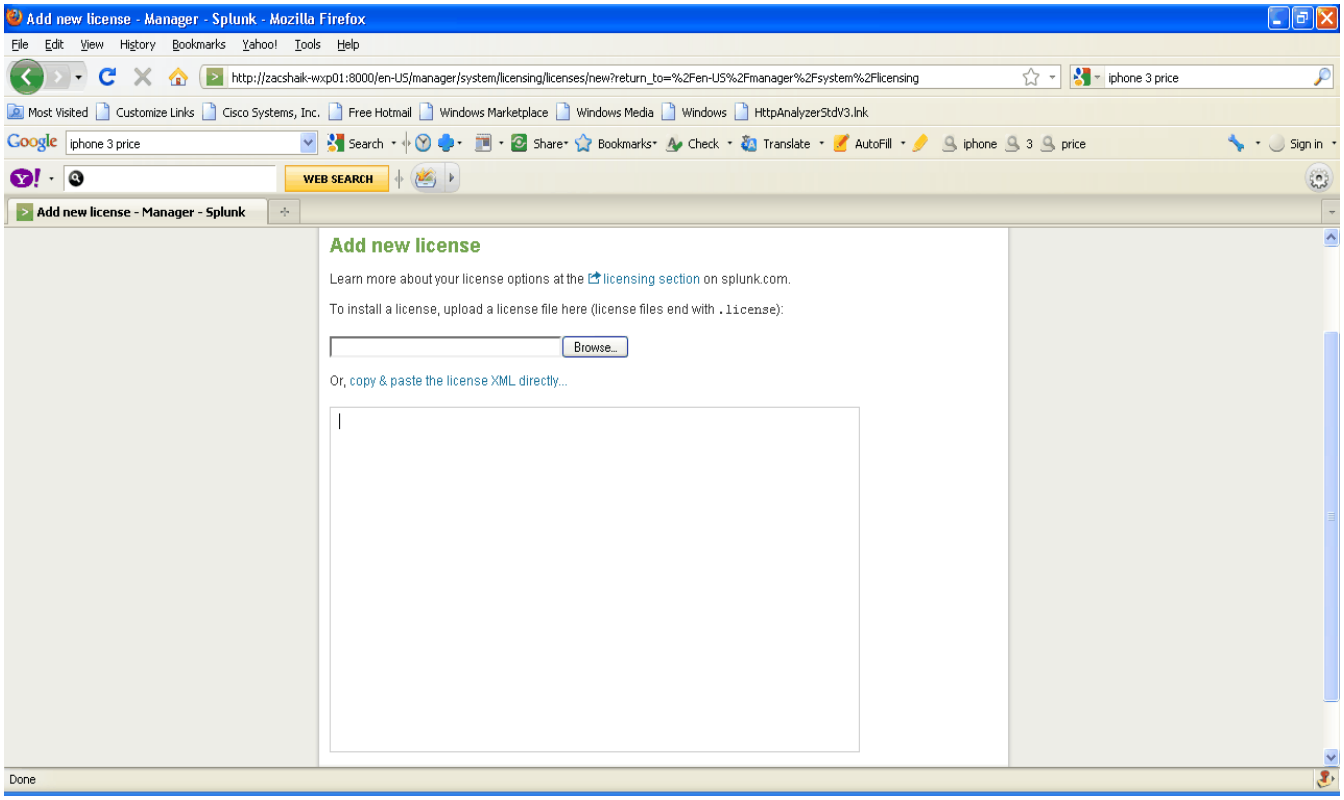


Step 5

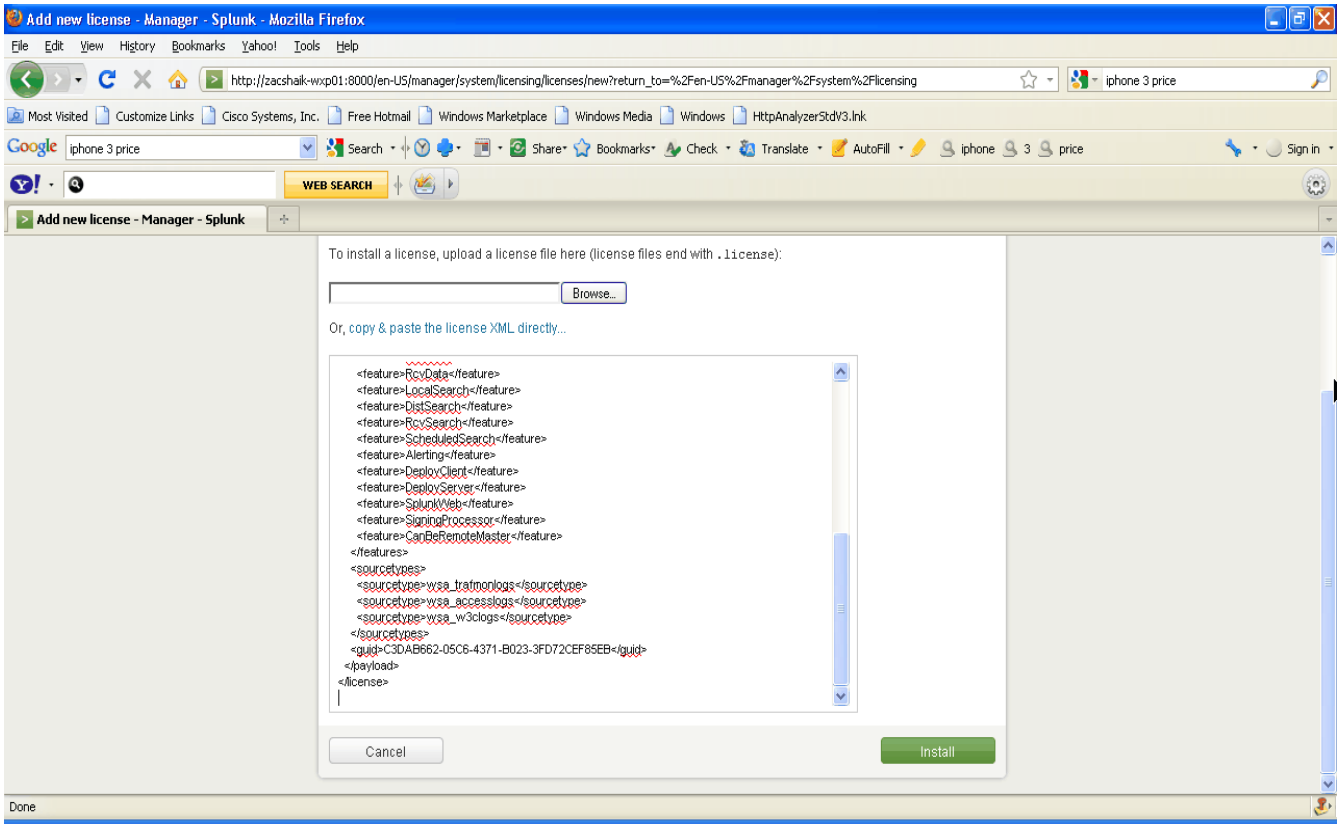
Add Splunk permanent License via Splunk GUI: (default license is for 30 days 500 MB indexing per day)

Manager » Licensing » Add new license > copy & paste the license XML directly...

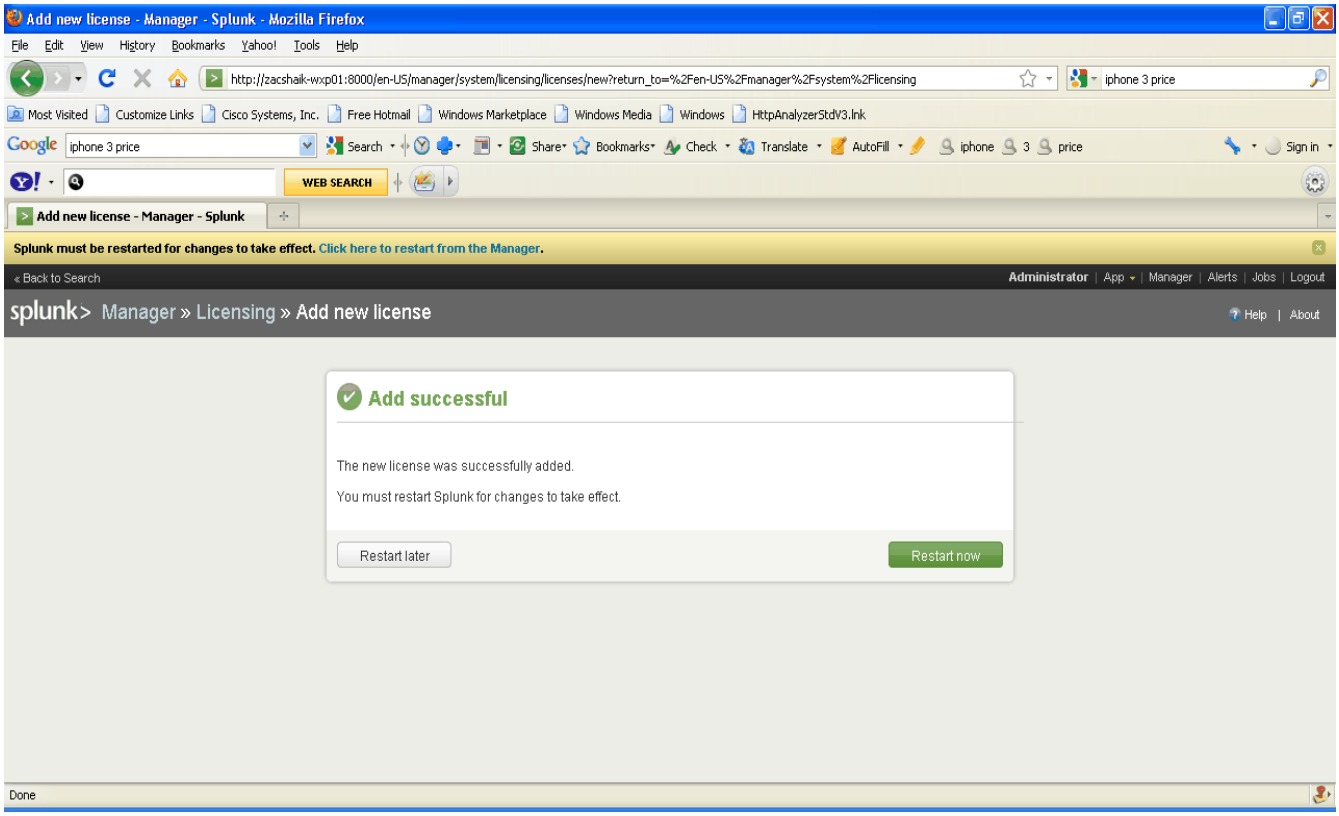




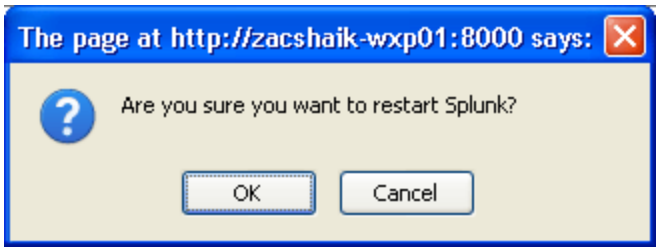
Copy and paste license file and click on install

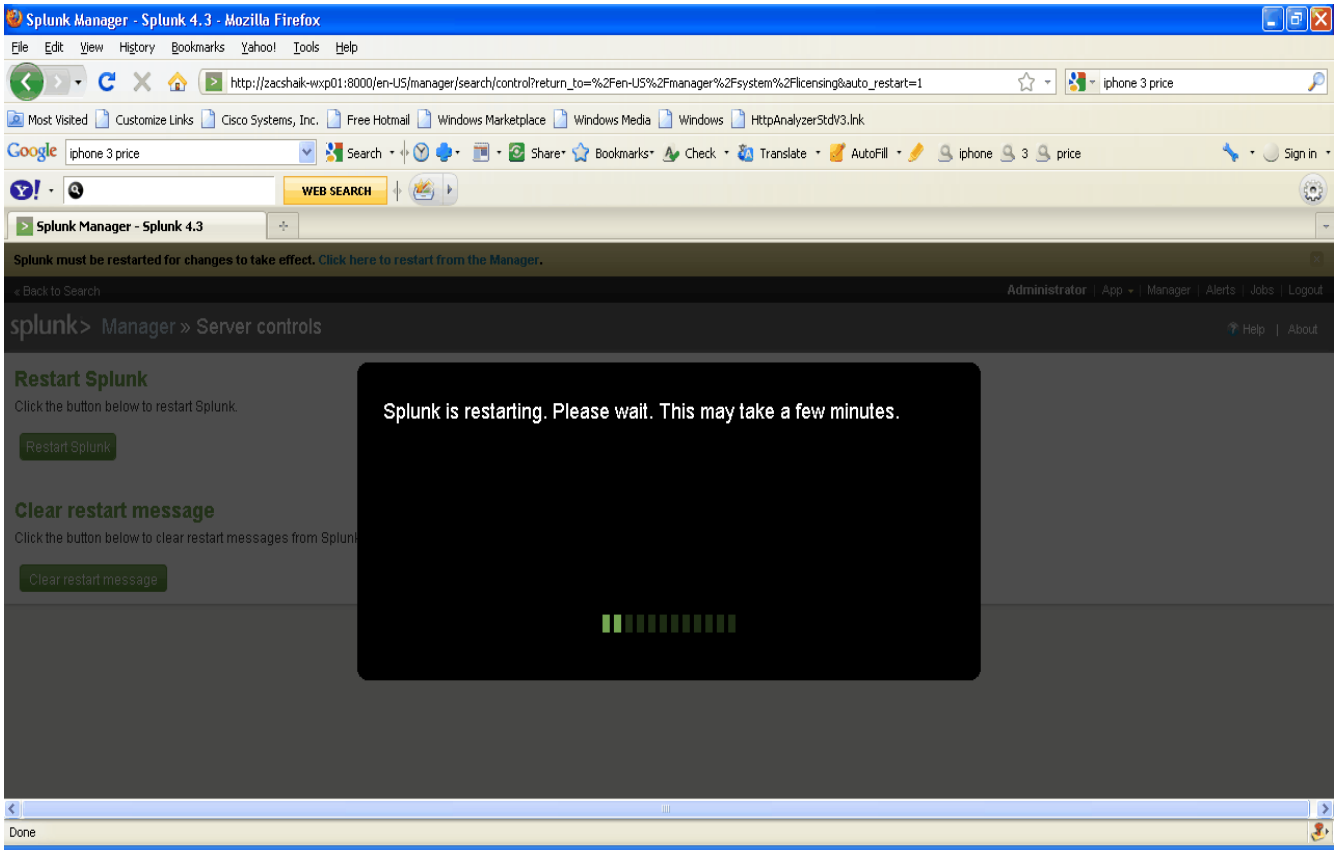


Following Screen appears:

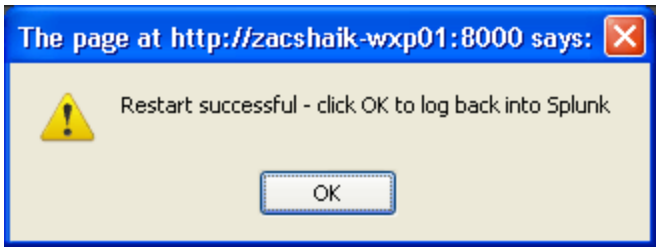


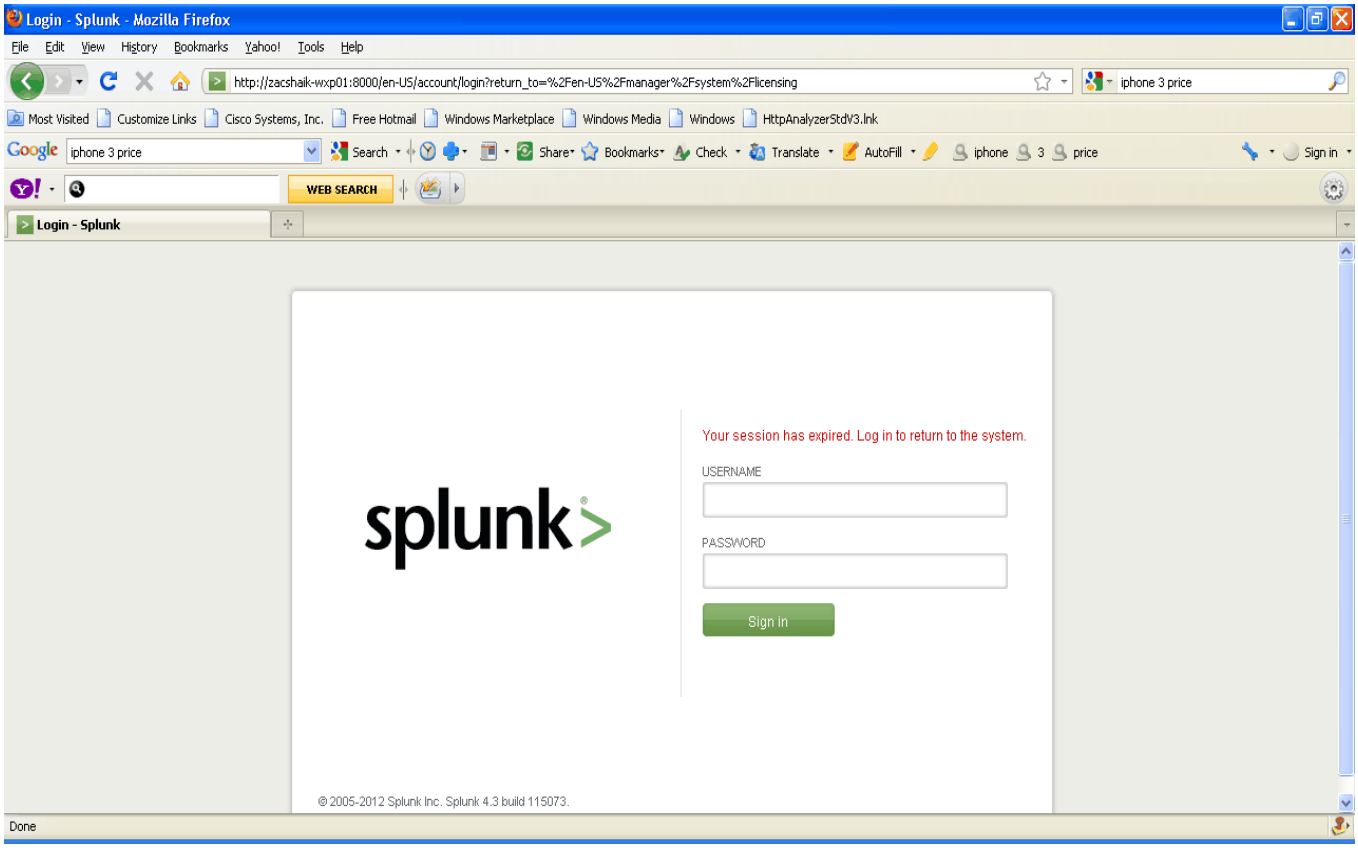
Click on “restart now”, follow the screen:



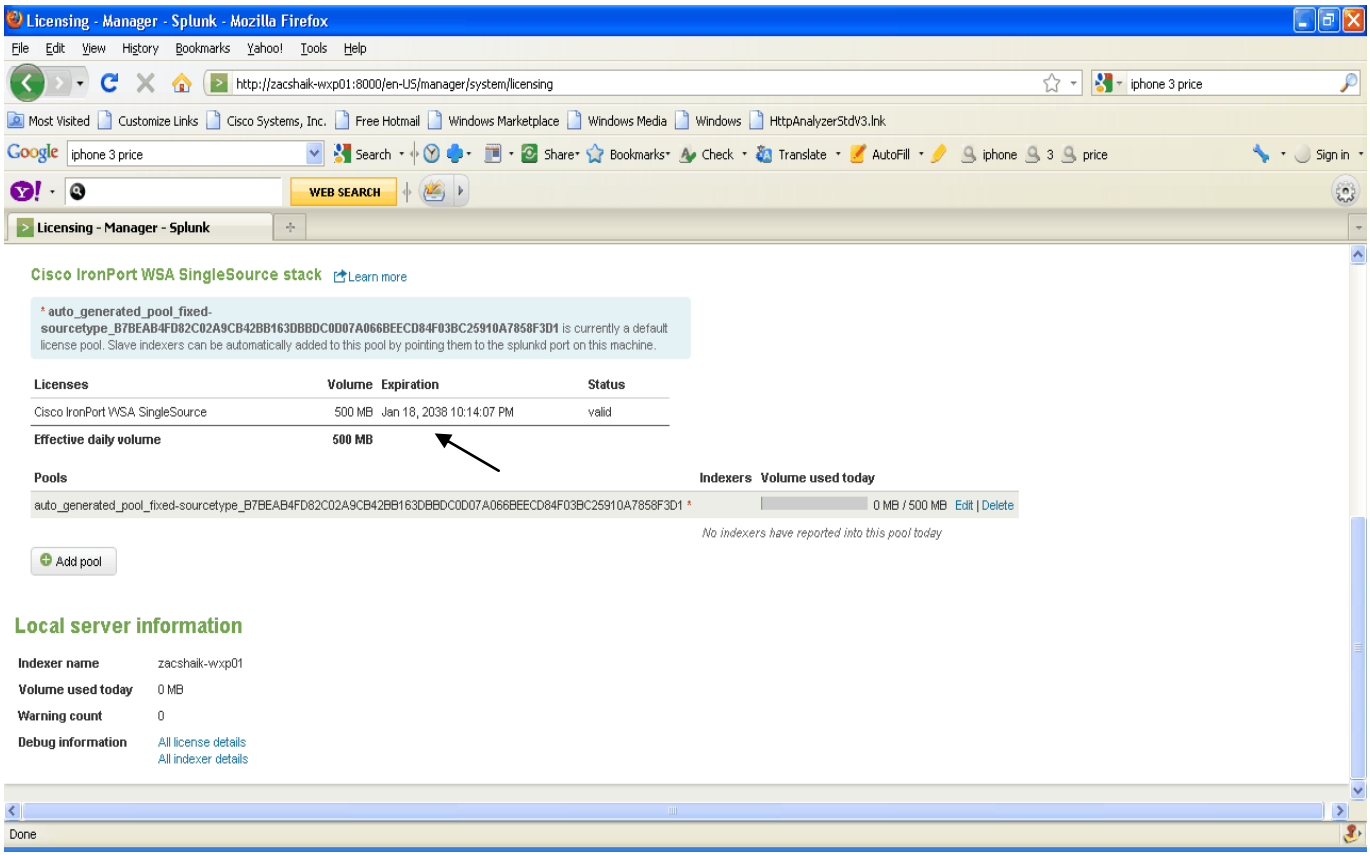


Once the Splunk is up, log back in and verify the License status (indexing volume per day, expiration etc...)




Login - Splunk - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://zacshaik-wxp01:8000/en-US/account/login?return_to=%2Fen-US%2Fmanager%2Fsystem%2Flicensing
iphone 3 price
Most Visited Customize Links Cisco Systems, Inc. Free Hotmail Windows Marketplace Windows Media Windows HttpAnalyzerStdV3.lnk
Google iphone 3 price Search Share Bookmarks Check Translate AutoFill iphone 3 price Sign in
WEB SEARCH
Login - Splunk
splunk>
Your session has expired. Log in to return to the system.
USERNAME
PASSWORD
Sign in
© 2005-2012 Splunk Inc. Splunk 4.3 build 115073.
Done

Manager » Licensing verify the expiration date (screen below show 500 MB per day expiration Jan 18, 2038)



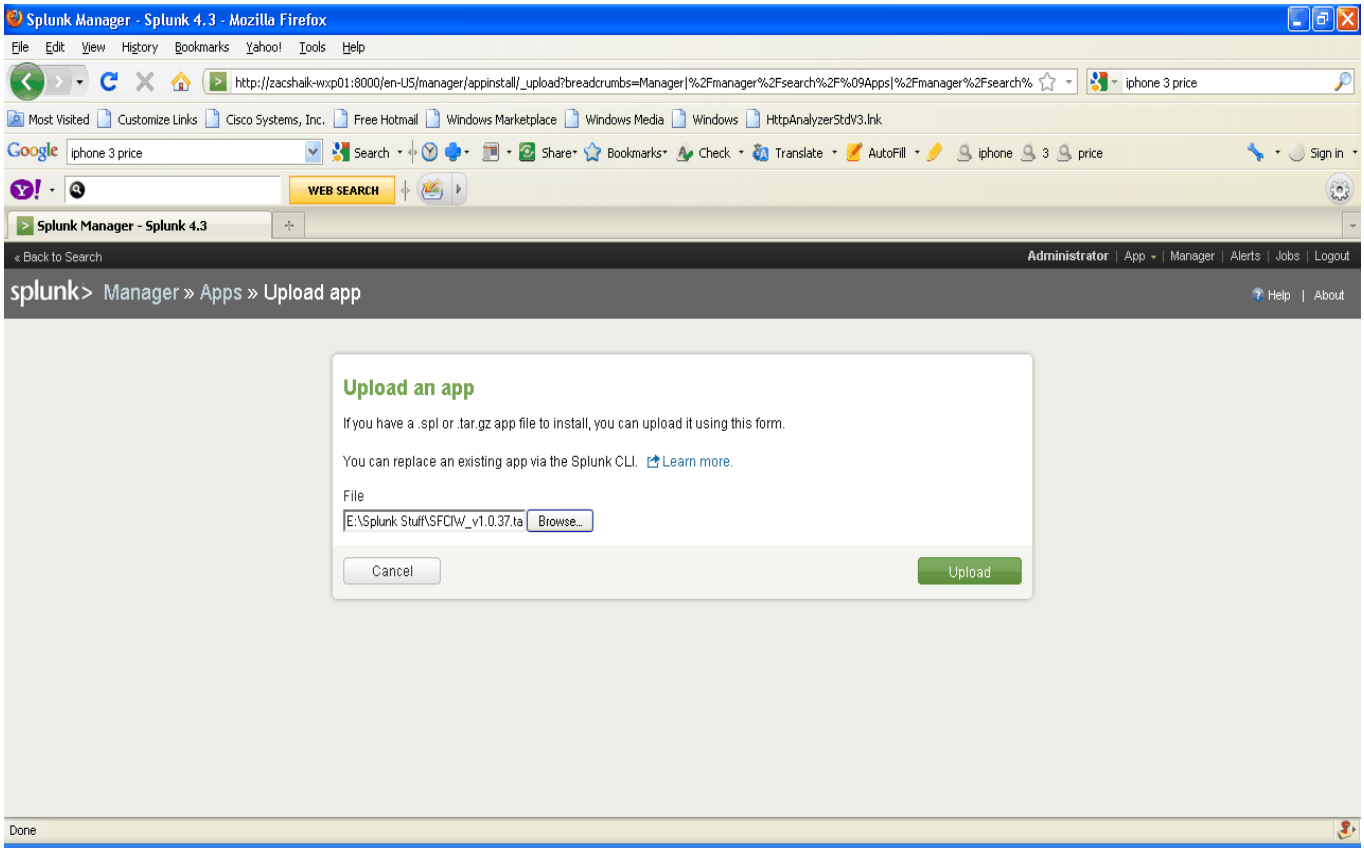
Step 6:

Upload "SplunkforCiscoIronportWSA" APP (APP file is available on Cisco Portal file name "SFCIW_v1.0.37.tar (link below)):

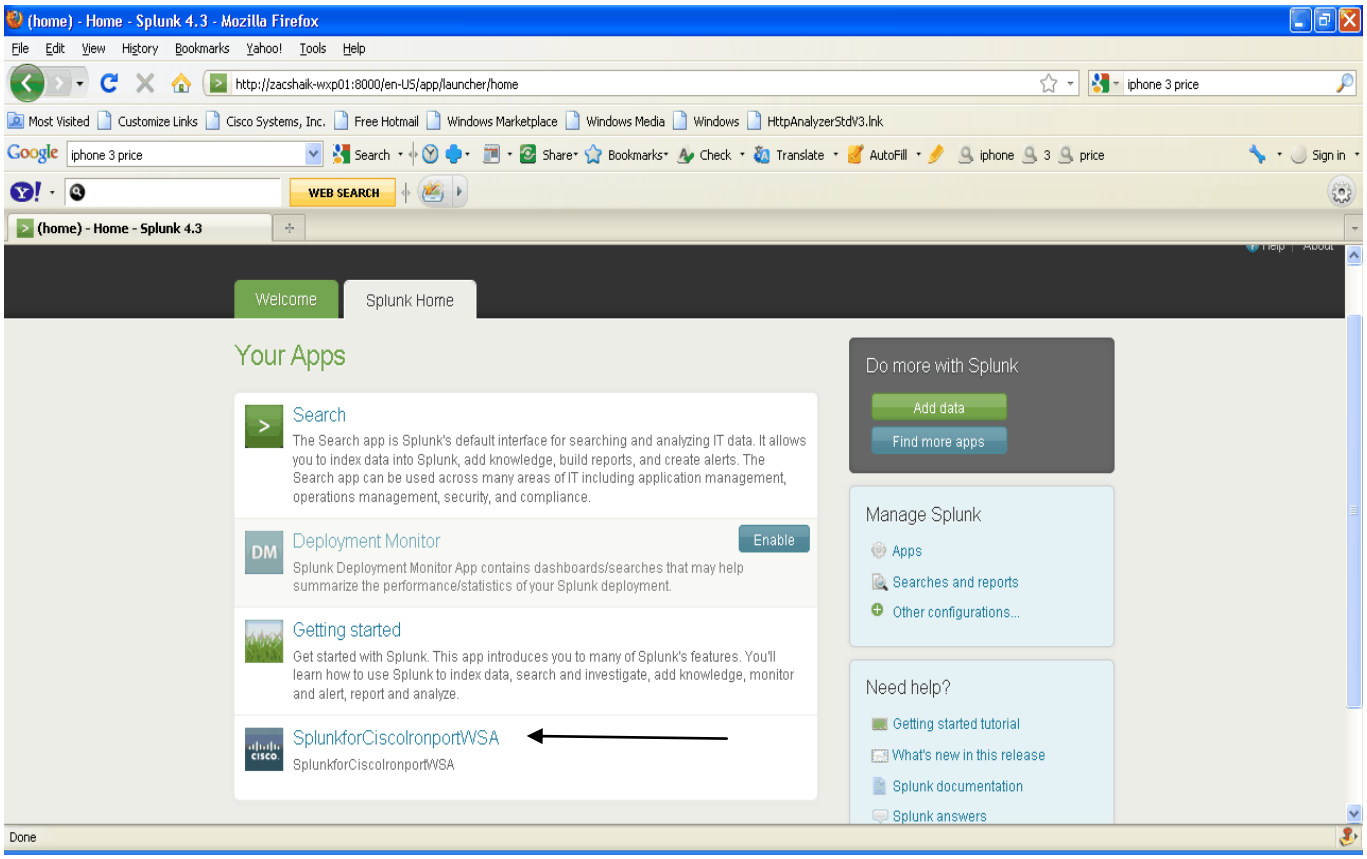
http://www.cisco.com/cisco/software/release.html?mdfid=282803425&flowid=4951&softwareid=283998384&release=Splunk%20Reporting%20SW&relind=AVAILABLE&rellifecycle=&reltype=all

From Splunk GUI:

Splunk > Manager » Apps » Upload app


Splunk Manager - Splunk 4.3 - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://zacshaik-wxp01:8000/en-US/manager/appinstall/_upload?breadcrumbs=Manager|%2Fmanager%2Fsearch%2F%09Apps|%2Fmanager%2Fsearch%
iphone 3 price
Most Visited Customize Links Cisco Systems, Inc. Free Hotmail Windows Marketplace Windows Media Windows HttpAnalyzerStdV3.lnk
Google iphone 3 price Search Share Bookmarks Check Translate AutoFill iphone 3 price Sign in
WEB SEARCH
Splunk Manager - Splunk 4.3
« Back to Search
Administrator | App | Manager | Alerts | Jobs | Logout
splunk> Manager » Apps » Upload app
Help | About
Upload an app
If you have a .spl or .tar.gz app file to install, you can upload it using this form.
You can replace an existing app via the Splunk CLI. Learn more.
File
E:\Splunk Stuff\SFCIW_v1.0.37.ta
Browse...
Cancel
Upload
Done

Once the app loaded review the Splunk home screen shows “SplunkforCiscoIronportWSA” (see below)



Step 7:

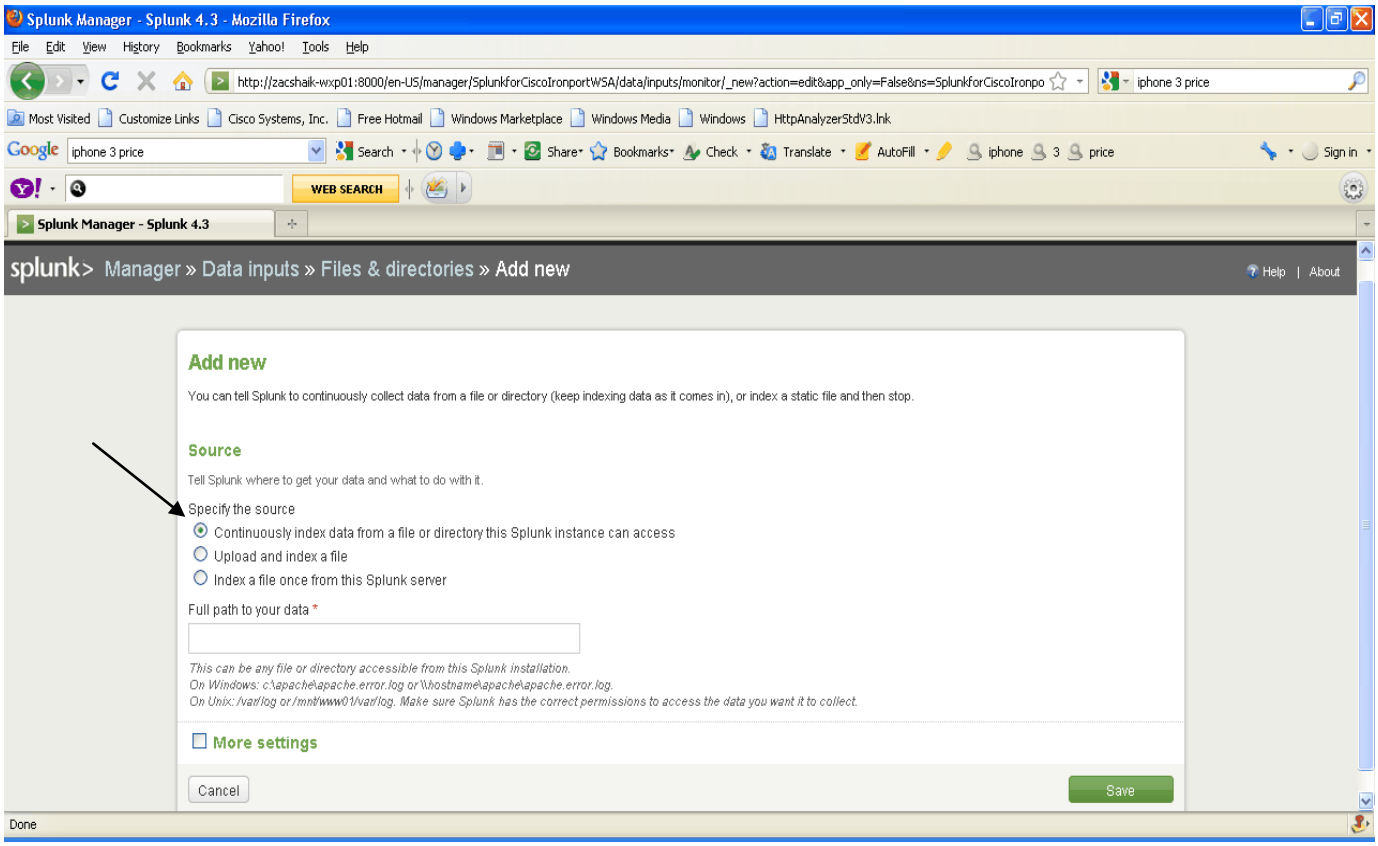
Add data source from Splunk GUI: (in following example WSA pushing the access logs to Splunk server via ftp to “C:\splunklogs\wsaaccesslogs\wsaone-accesslogs”

Please note: Each WSA will required to have it’s own logs directory for optimal results and for successful search within the Splunk

From Splunk GUI:

Manager » Data inputs » Files & directories » Data preview > Skip preview (manually configure your input) > Continue

That will bring you the Screen as follows:

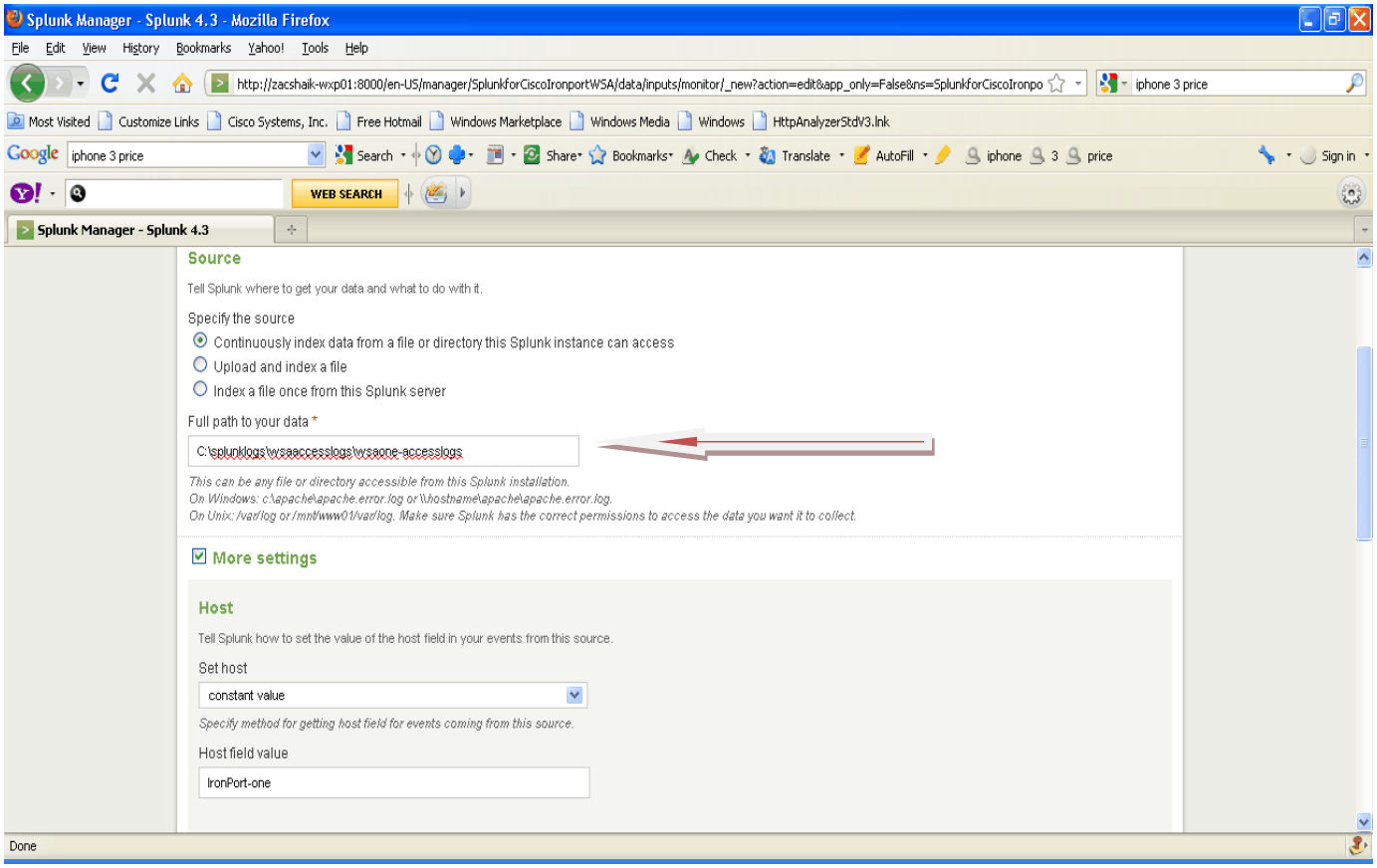


MUST check “Continuously index data from a file or directory this Splunk instance can access”, provide path and check “More setting”

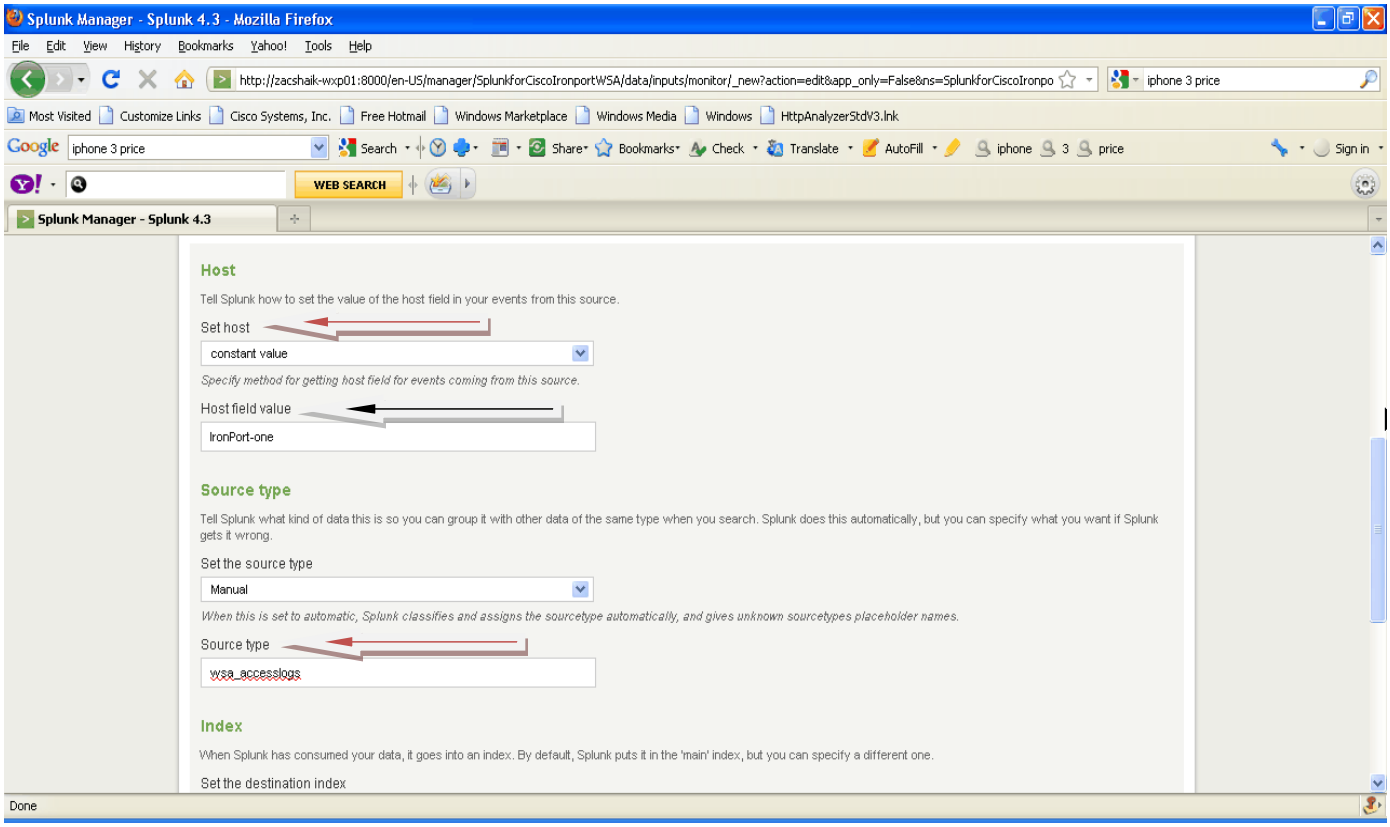
Configure following values under “More setting”:

Host field value (this is WSA hostname e.g. if this is first WSA access logs path then enter the WSA actual hostname)

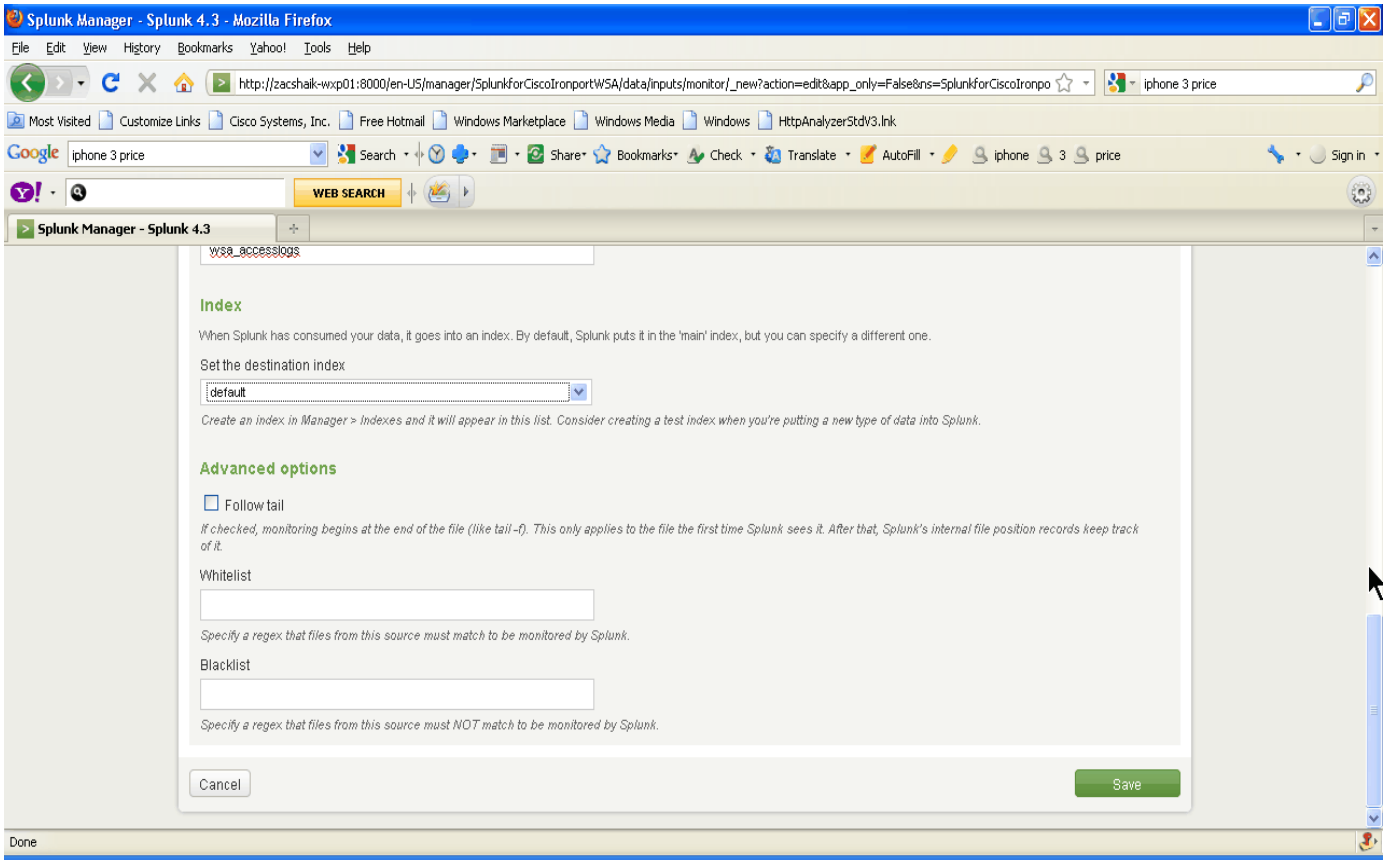
Set the source type (choose “Manual” from the drop down), and under “Source type” enter wsa_accesslogs (for access logs and wsa_trafmonlogs for L4TM logs)



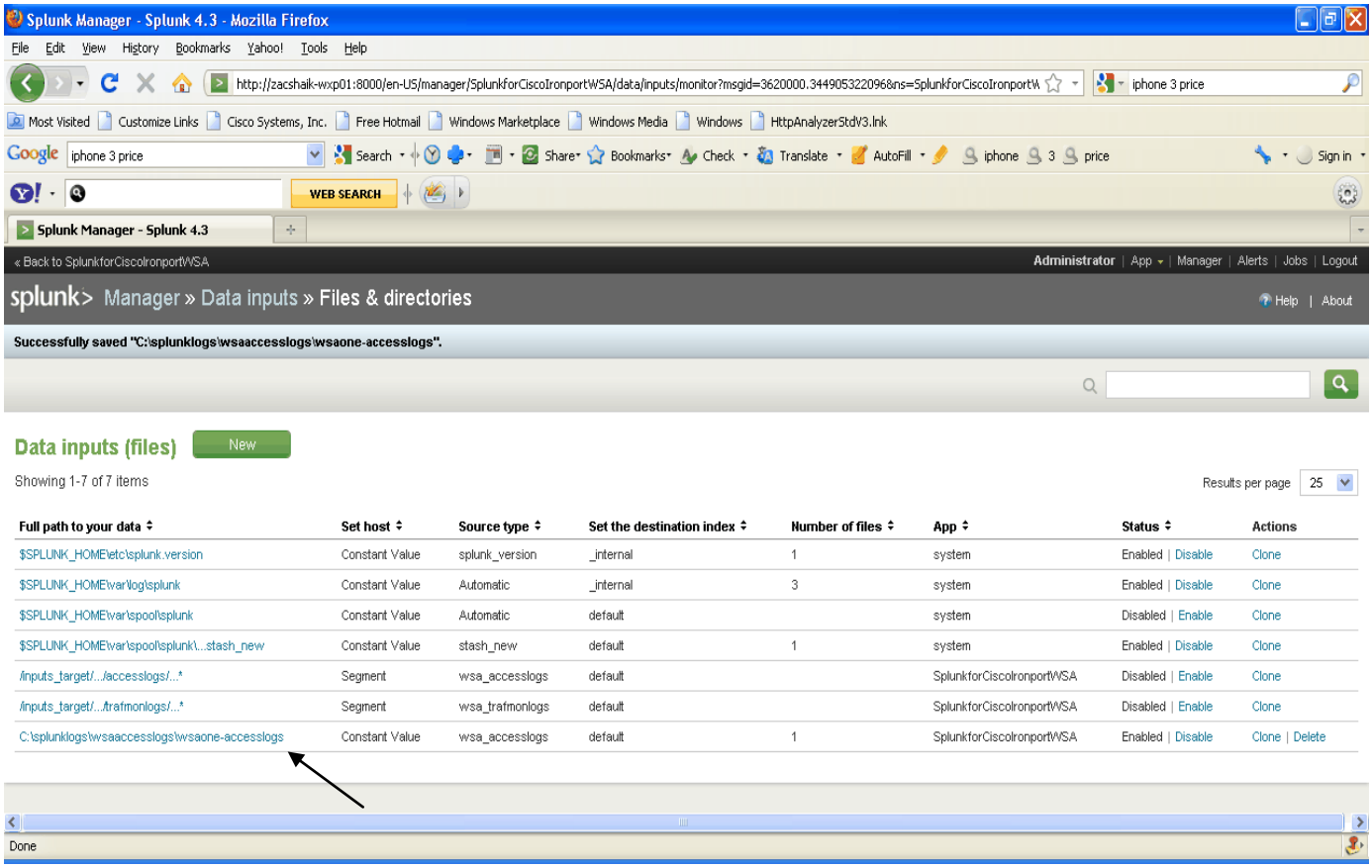
IMPORTANT: PLEASE NOTE ONCE SPLUNK READ AND INDEX WSA "ACCESSLOGS" OR "TRAFMONLOGS" IT WILL DELETE THESE LOGS (DEFAULT BEHAVIOR), IF THE INTENTION IS TO "RETAIN" THESE LOGS FOR AUDIT OR ANY OTHER REASONS. WE NEED TO STAGE/SAVED THESE LOGS ON AN FTP SERVER NOT ON LOCAL DRIVE/PATH WHERE SPLUNK IS INSTALLED.



Clicks save on the bottom of the page, and repeat this step for each WSA access logs and L4TM logs,


Splunk Manager - Splunk 4.3 - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://zacshaik-wxp01:8000/en-US/manager/SplunkforCiscoIronportWSA/data/inputs/monitor/_new?action=edit&app_only=False&ns=SplunkforCiscoIronpo
iphone 3 price
Most Visited Customize Links Cisco Systems, Inc. Free Hotmail Windows Marketplace Windows Media Windows HttpAnalyzerStdV3.lnk
Google iphone 3 price Search Share Bookmarks Check Translate AutoFill iphone 3 price Sign in
WEB SEARCH
Splunk Manager - Splunk 4.3
wsa_accesslogs
Index
When Splunk has consumed your data, it goes into an index. By default, Splunk puts it in the 'main' index, but you can specify a different one.
Set the destination index
default
Create an index in Manager > Indexes and it will appear in this list. Consider creating a test index when you're putting a new type of data into Splunk.
Advanced options
Follow tail
If checked, monitoring begins at the end of the file (like tail -f). This only applies to the file the first time Splunk sees it. After that, Splunk's internal file position records keep track of it.
Whitelist
Specify a regex that files from this source must match to be monitored by Splunk.
Blacklist
Specify a regex that files from this source must NOT match to be monitored by Splunk.
Cancel
Save
Done

We *should * see Data input similar to following screen:

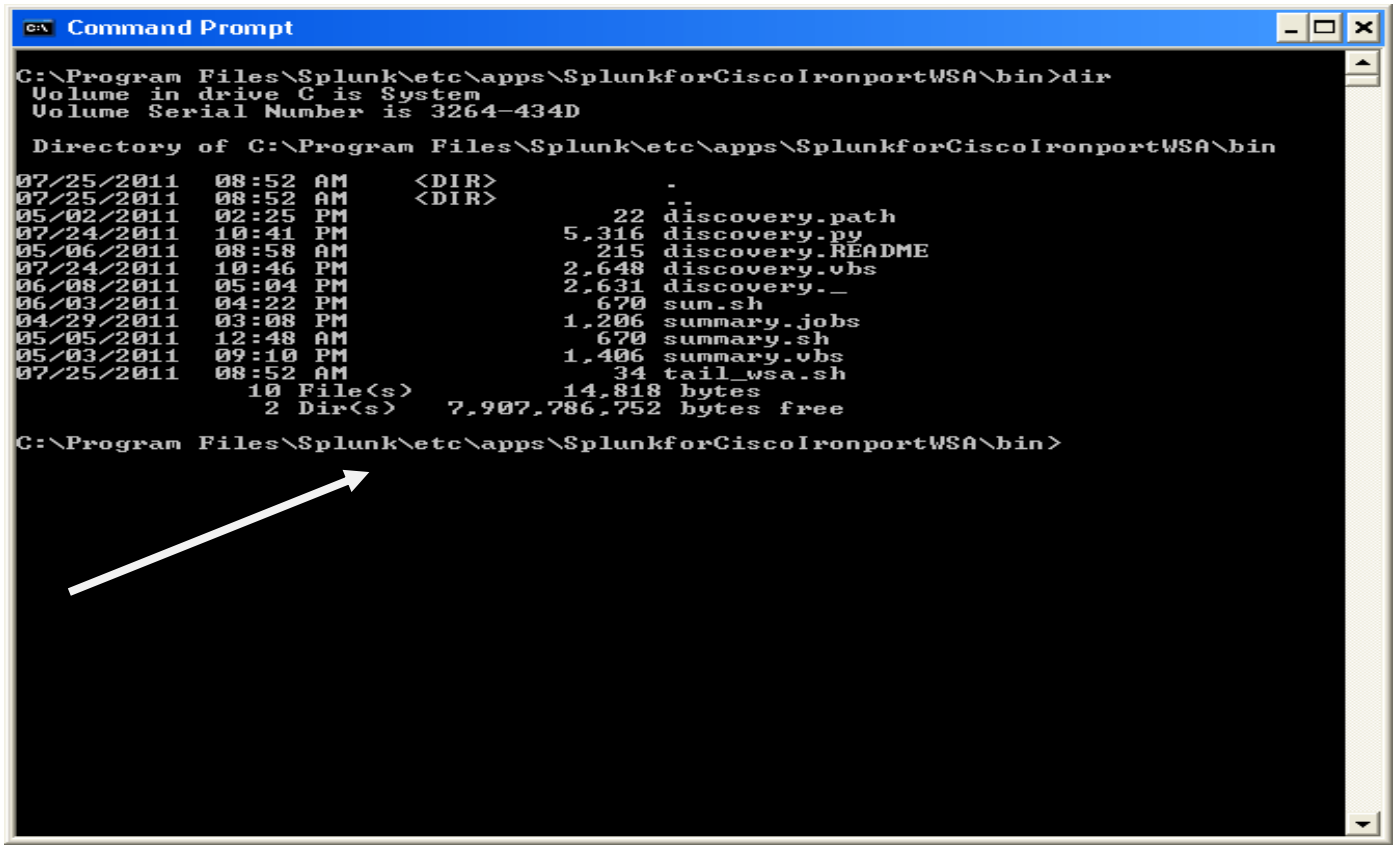


Step 8: Add WSA historical access logs and L4TM logs in to Splunk, Two steps process:

8.1 Copy logs in to Appropriate WSA access logs or L4TM logs directory

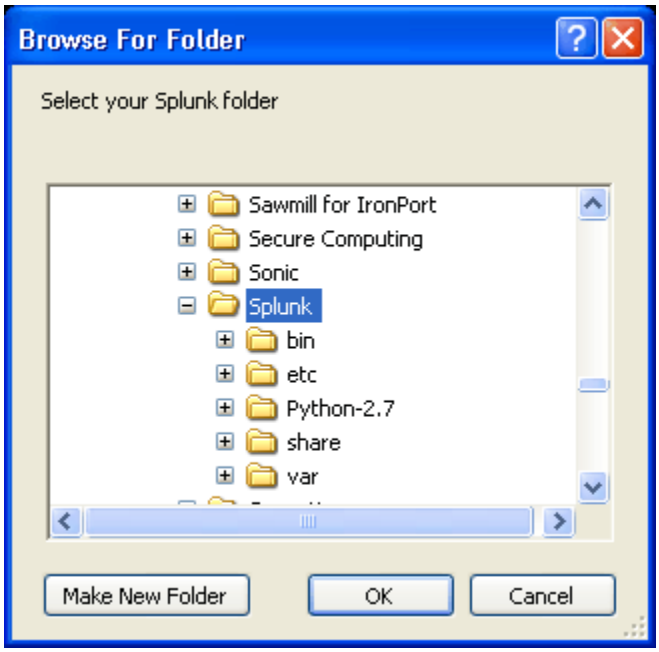
8.2 Run summary.vbs/sh from Splunk CLI

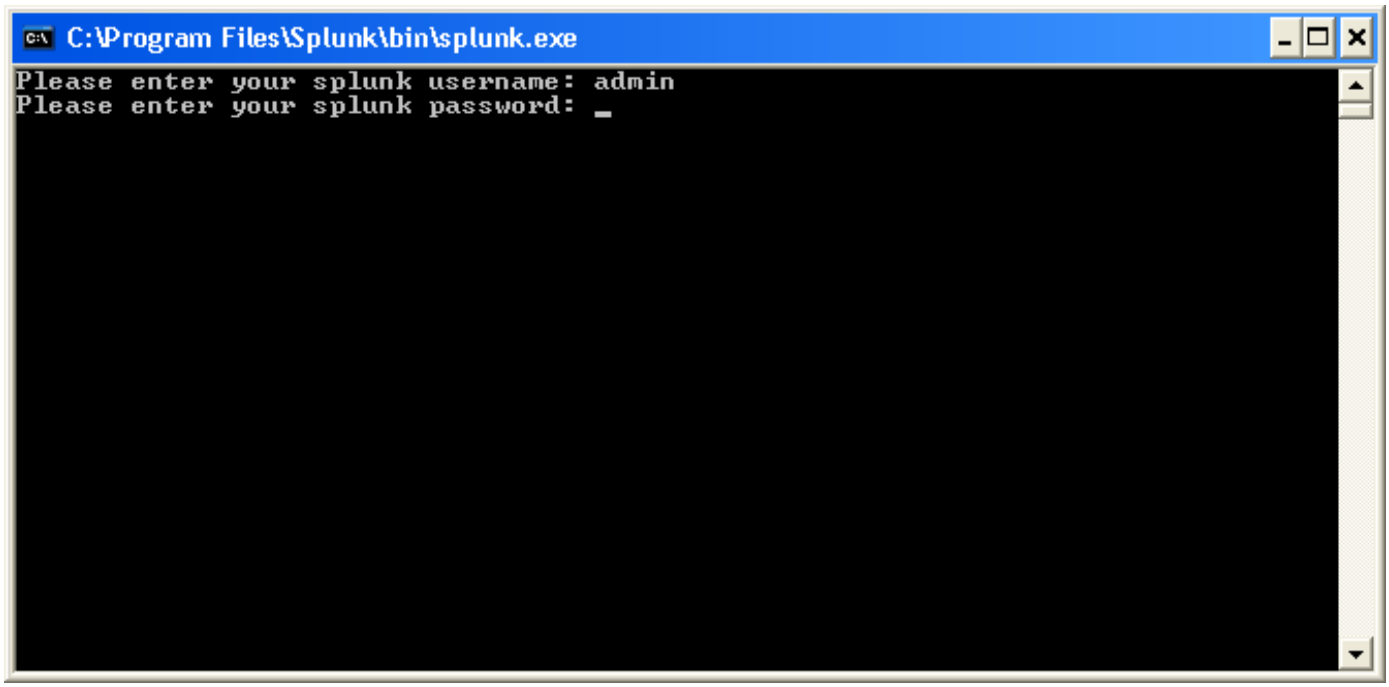
Once the logs are moved to appropriate logs directory, Execute step 2 from Splunk CLI,



Run **summary.vbs/sh from (see above screen shot)**
C:\"Program Files\Splunk\etc\apps\SplunkforCiscoIronportWSA\bin>"

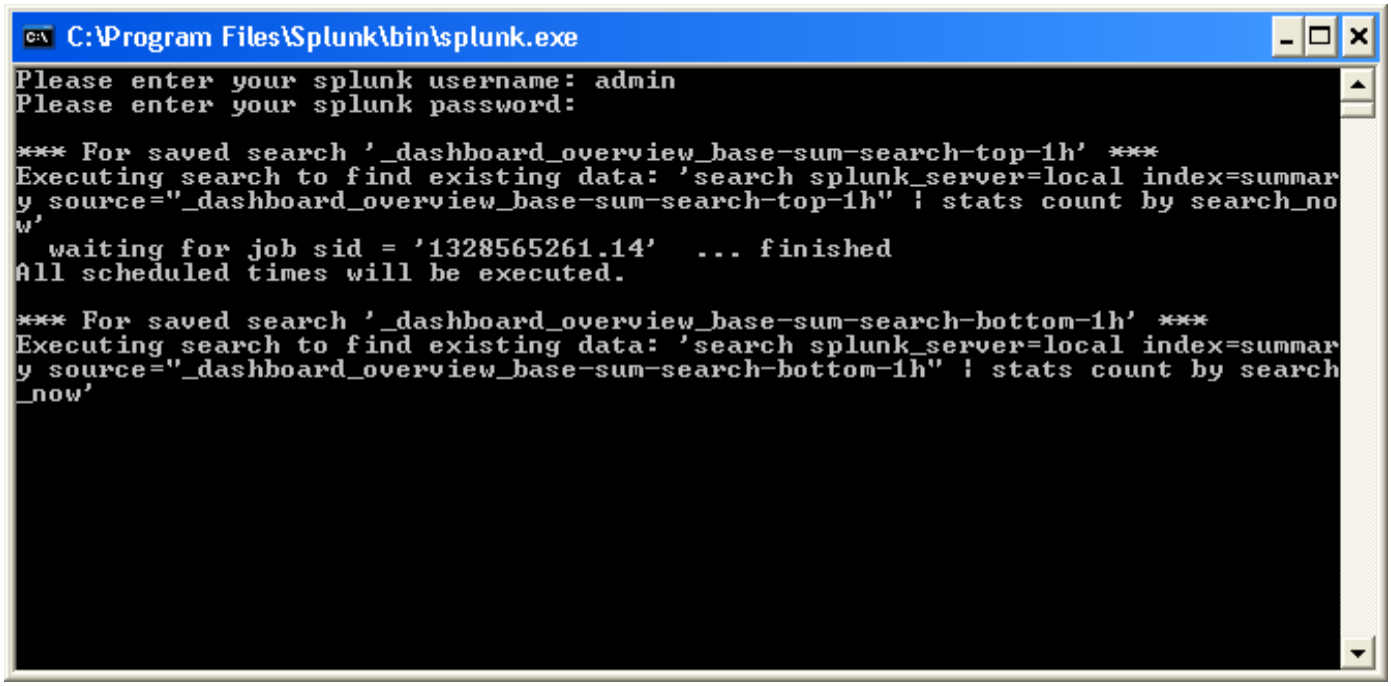
When prompt point to "Splunk" directory under c:\ Program Files\Splunk and enter Splunk admin credentials

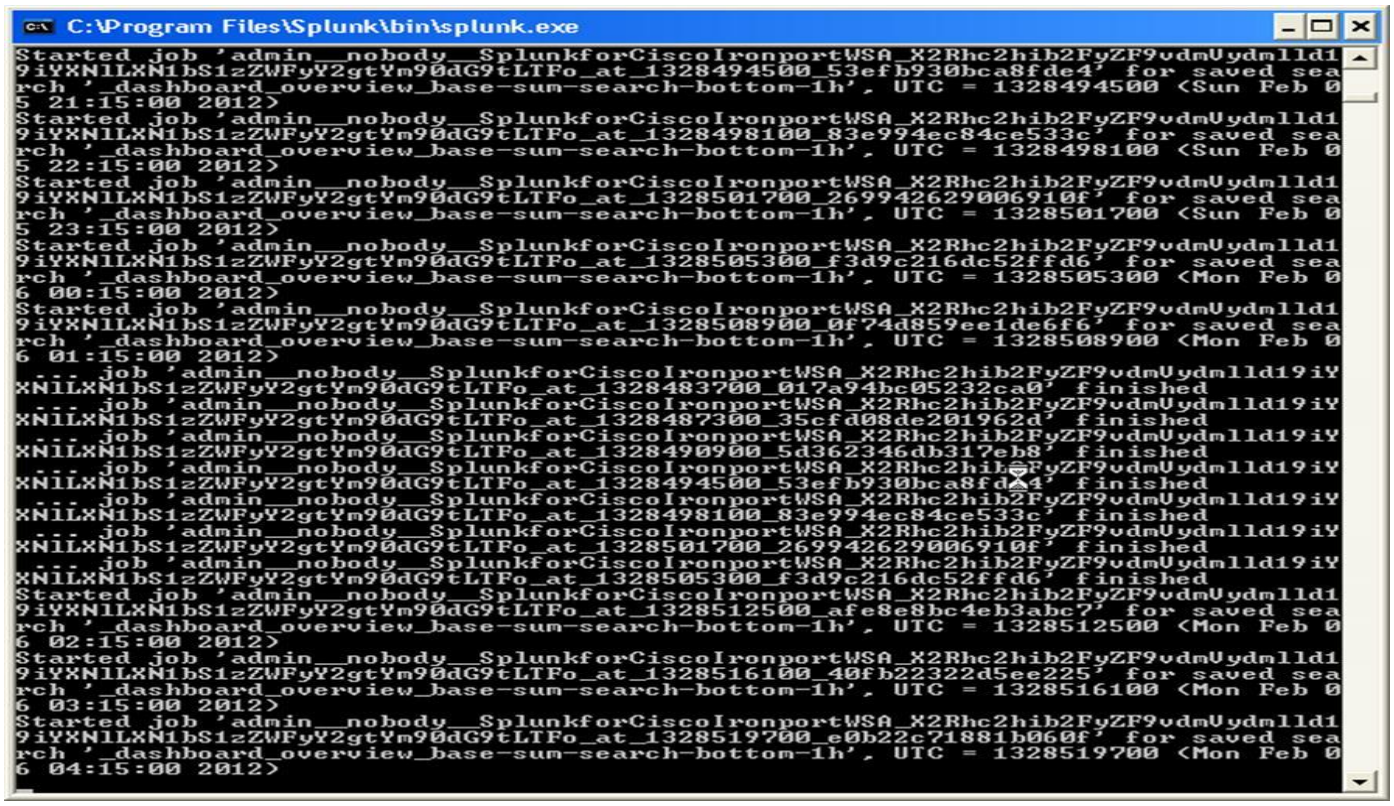

Browse For Folder
Select your Splunk folder
Sawmill for IronPort
Secure Computing
Sonic
Splunk
bin
etc
Python-2.7
share
var
Make New Folder
OK
Cancel


C:\Program Files\Splunk\bin\splunk.exe
Please enter your splunk username: admin
Please enter your splunk password:

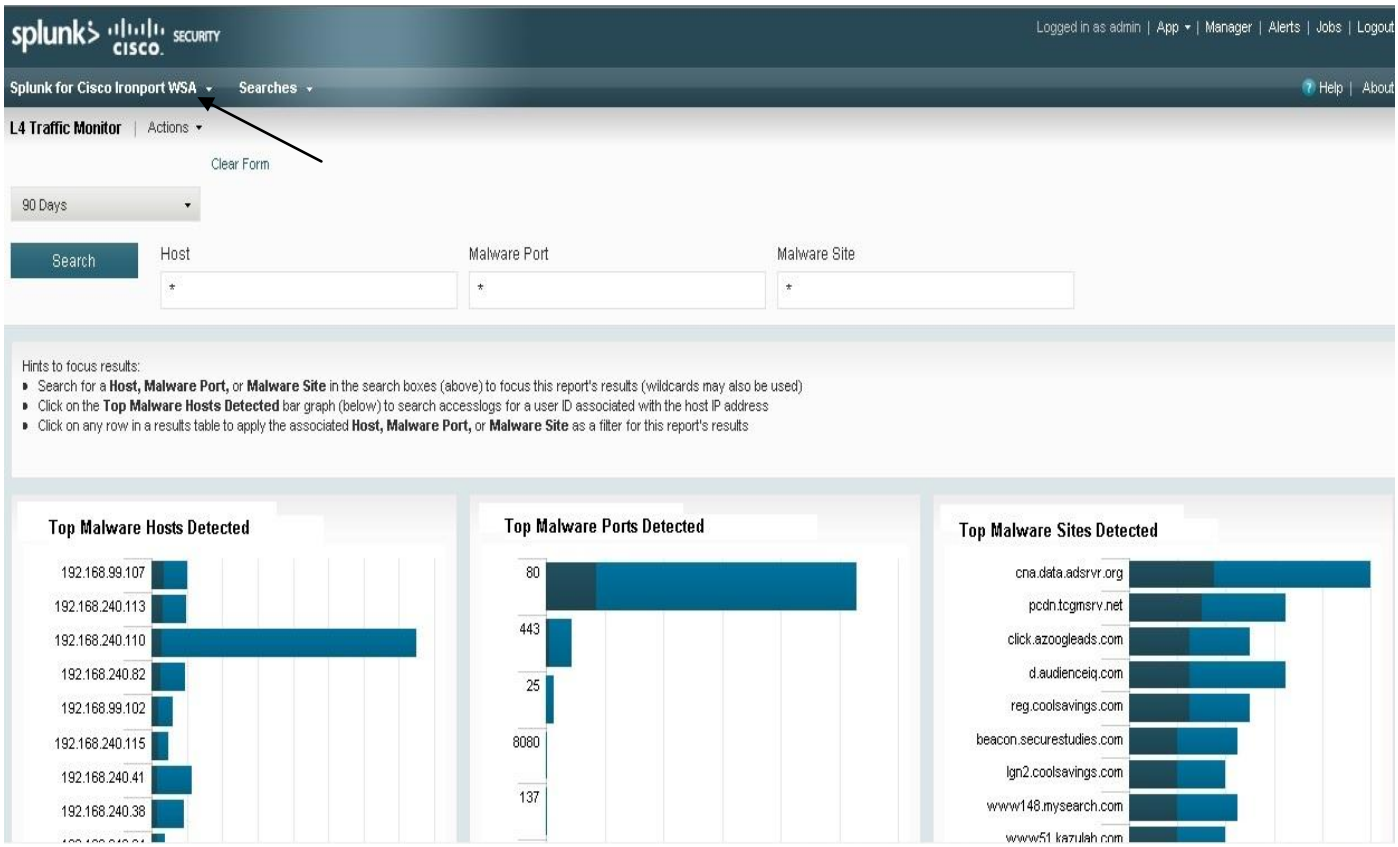
Screen Similar to below will appear and let it run in the background, once this process is completed. ALL historical logs will be imported in to Splunk database:

Please note it *may* take a while, and all depends how much historical logs data have to be process by Splunk,





Once the Summary run completed we should start seeing current and historical data (see below):


splunk> cisco. SECURITY
Logged in as admin | App | Manager | Alerts | Jobs | Logout
Splunk for Cisco Ironport WSA
Searches
Help | About
L4 Traffic Monitor | Actions
Clear Form
90 Days
Search
Host
Malware Port
Malware Site
*
*
*
Hints to focus results:
Search for a Host, Malware Port, or Malware Site in the search boxes (above) to focus this report's results (wildcards may also be used)
Click on the Top Malware Hosts Detected bar graph (below) to search accesslogs for a user ID associated with the host IP address
Click on any row in a results table to apply the associated Host, Malware Port, or Malware Site as a filter for this report's results
Top Malware Hosts Detected
192.168.99.107
192.168.240.113
192.168.240.110
192.168.240.82
192.168.99.102
192.168.240.115
192.168.240.41
192.168.240.38
Top Malware Ports Detected
80
443
25
8080
137
Top Malware Sites Detected
cna.data.adsrvr.org
pcdn.tcgmsrv.net
click.azoogleads.com
d.audienceiq.com
reg.coolsavings.com
beacon.securestudies.com
lgn2.coolsavings.com
www148.mysearch.com

Other Resources:
http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge > Splunk knowledge base (KB)
http://answers.splunk.com > Splunk Blog, FAQ, Wiki Documentations, Splunk Community, post questions etc.
http://splunk-base.splunk.com/answers/ > Find an Answer for common Splunk issues
http://splunk-base.splunk.com/ask/ > Post a questions to Splunk
http://www.splunk.com/support/list/forum > Splunk Forums
http://docs.splunk.com/Documentation/Splunk > Splunk version specific documentations
http://wiki.splunk.com/Community:TroubleshootingIndexedDataVolume > Troubleshooting Indexed Data Volume
http://www.cisco.com/cisco/software/type.html?mdfid=282803424&flowid=4950

Splunk Video KB FAQ here:
http://www.splunk.com/videos
http://www.splunk.com/base/documentation
www.splunk.com > Current Splunk versions