Cisco CLI Analyzer
User Guide

Version 2.0

March 16, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS(6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco CLI Analyzer User Guide

Table of Contents

New Features

These features are new in this version of Cisco CLI Analyzer:

- **System Diagnostics**—Diagnostic commands have been added for IOS, IOS-XE and IOS-XR. IOS-XR supports "Virtual TAC". Diagnostic commands are customized based on information received from your device.
- **Contextual Help & Highlighting**—Contextual Help and Highlighting (CHH) has been added for ASA, IOS, IOS-XE, IOS-XR and NX-OS commands.
- **Save Credentials**—You can save your CCO login information using a Master Password.
- **Device Detection and Update**—The Cisco CLI Analyzer detects supported software platforms (ASA, IOS, IOS-XE, IOS-XR and NX-OS) upon login. The application displays only tools and CHH that apply to your device, and also updates your local device session information to include serial number, software version, model, and device type.
- **Keyboard Shortcuts**—Press ALT+Q in order to open a quick-connect session. Press CTRL+TAB in order to cycle forward through your device and session tabs, or press CTRL+SHIFT+TAB in order to go back. Press CTRL+F in order to go directly to search highlighting and quickly search output in your CLI scrollback.
- **Contextual Menu**—Select any text within the CLI and right-click the selected text. New context menu options are available to **Search Cisco.com** for the selected text, and to **Request New CHH** for the selected text.
- **Console Selection Behavior**—On the Settings tab, you can choose to emulate the text selection behavior of PuTTY or SecureCRT as alternatives to the default behavior when you use the mouse to select text.

Get Started

About the Cisco CLI Analyzer

The Cisco CLI Analyzer is a smart SSH/Telnet client designed to help troubleshoot and check the overall health of your supported device. Features include:

- **ASA, IOS, IOS-XE, and IOS-XR System Diagnostics**—Utilizes Cisco TAC knowledge in order to analyze the ASA and detect known problems such as system problems, configuration mistakes, and best practice violations.
- **ASA Traceback Analyzer**—Attempts to match the root cause of a crash to a known bug if the ASA has experienced a system traceback. If a match is found, the ASA version or versions in which the bug is fixed are provided.
- **ASA Packet Tracer**—Allows administrators to send simulated packets through the ASA as a test. If the packet is dropped, the ASA configuration portion or feature that could have contributed to the packet drop is identified.
- **ASA Firewall Top Talkers**—Identifies the connections that pass traffic through your ASA that have the highest bit rates.
- **Contextual Help and Highlighting**—Provides information based on command outputs in an interactive way. Highlights enable real-time search capabilities in the console window.

Note: You must have a valid Cisco.com account in order to use the Cisco CLI Analyzer. If you do not have a valid Cisco.com account, you must register on the Cisco.com Registration page and associate a Service Contract to your Cisco.com profile.

System Requirements

The minimum software and hardware required in order to run the Cisco CLI Analyzer are as follows.

Software

- Windows 7 (32-bit or 64-bit)
- Mac OS X versions 10.8 (Mountain Lion) or later

Hardware

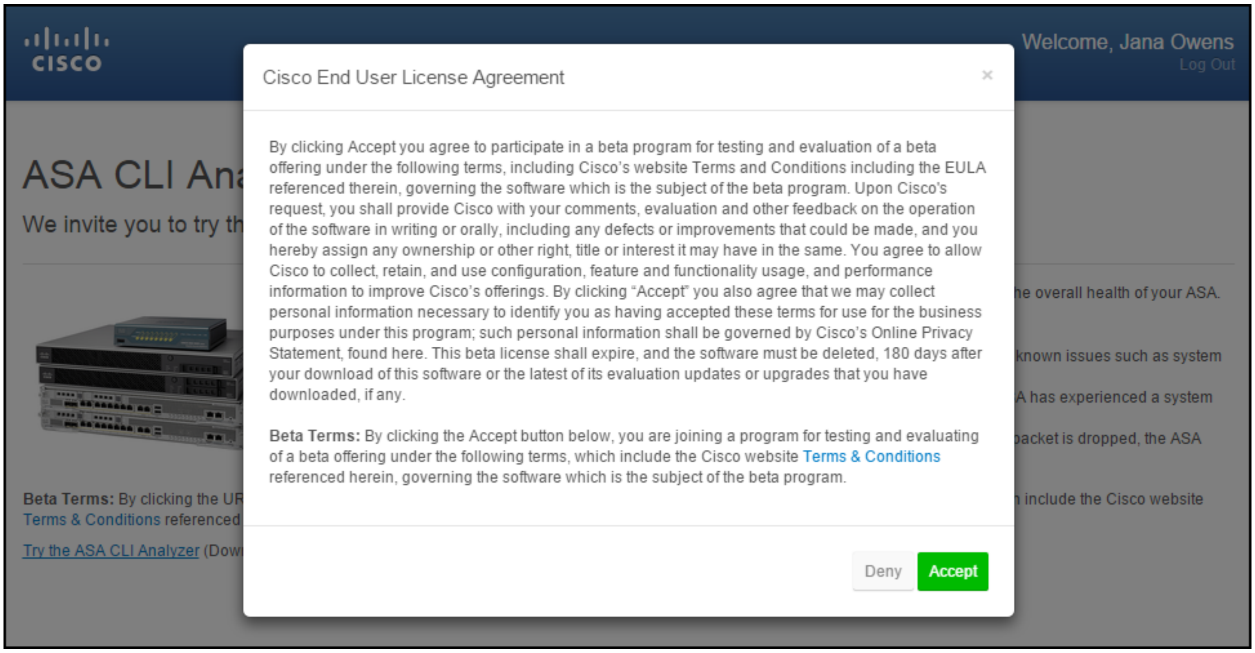
- 2 gigabytes (GB) of RAM
- 512 megabytes (MB) of available space on the hard disk

Download and Install the Cisco CLI Analyzer

Complete these steps in order to download and install the Cisco CLI Analyzer:

1. Open the Cisco Tools & Resources page in your browser and click **Cisco CLI Analyzer**.
2. On the Cisco CLI Analyzer web page, read the Beta Terms, and click **Try the Cisco CLI Analyzer**.

   The *Cisco End User License Agreement* page appears.



Cisco End User License Agreement

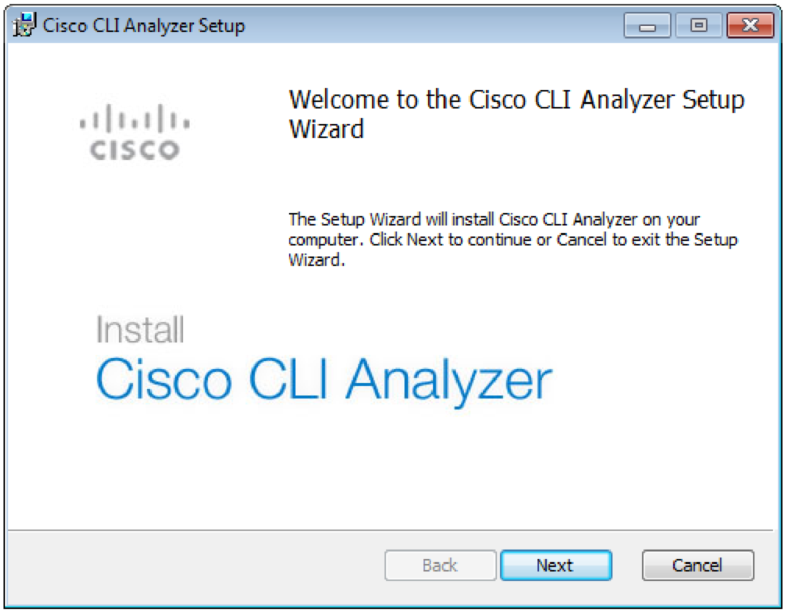
By clicking Accept you agree to participate in a beta program for testing and evaluation of a beta offering under the following terms, including Cisco's website Terms and Conditions including the EULA referenced therein, governing the software which is the subject of the beta program. Upon Cisco's request, you shall provide Cisco with your comments, evaluation and other feedback on the operation of the software in writing or orally, including any defects or improvements that could be made, and you hereby assign any ownership or other right, title or interest it may have in the same. You agree to allow Cisco to collect, retain, and use configuration, feature and functionality usage, and performance information to improve Cisco's offerings. By clicking "Accept" you also agree that we may collect personal information necessary to identify you as having accepted these terms for use for the business purposes under this program; such personal information shall be governed by Cisco's Online Privacy Statement, found here. This beta license shall expire, and the software must be deleted, 180 days after your download of this software or the latest of its evaluation updates or upgrades that you have downloaded, if any.

Beta Terms: By clicking the Accept button below, you are joining a program for testing and evaluating of a beta offering under the following terms, which include the Cisco website Terms & Conditions referenced herein, governing the software which is the subject of the beta program.

3. Click **Accept**.

   The *Cisco File Exchange* page appears.
4. On the *Cisco File Exchange* page, click the link that corresponds to your operating system.
5. After the file is downloaded, double-click the executable in order to begin installation.

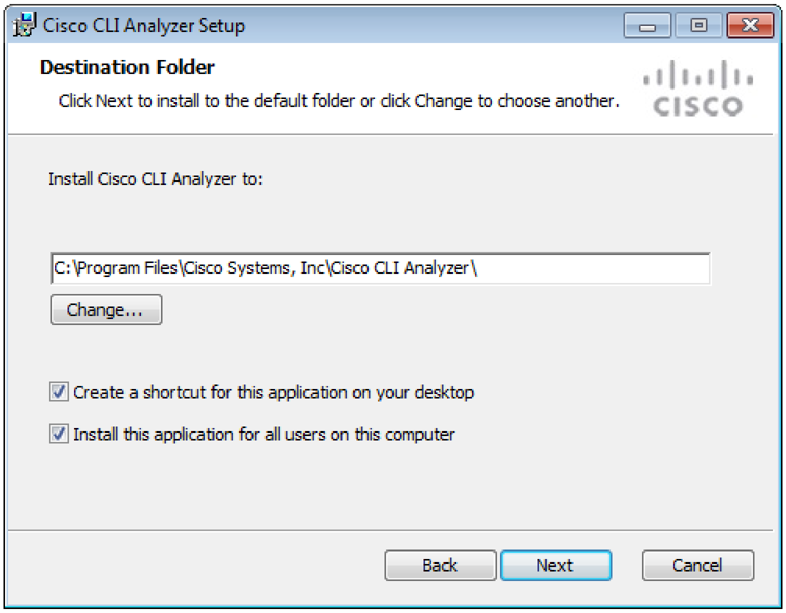
The *Cisco CLI Analyzer Setup Wizard* appears.



The Setup Wizard will install Cisco CLI Analyzer on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

6. Click **Next**.

The *Destination Folder* dialog window appears.



Click Next to install to the default folder or click Change to choose another.

Install Cisco CLI Analyzer to:

C:\Program Files\Cisco Systems, Inc\Cisco CLI Analyzer\

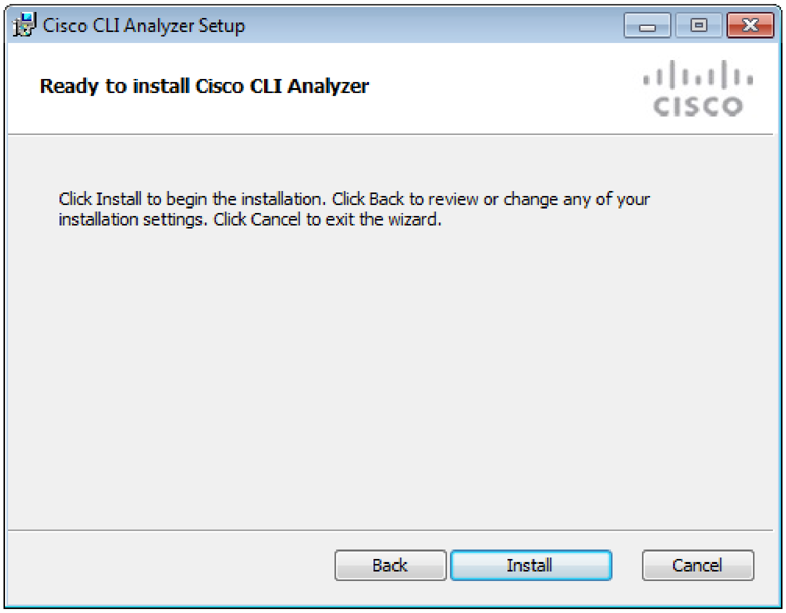
☑ Create a shortcut for this application on your desktop

☑ Install this application for all users on this computer

If you prefer to install to a location other than the default folder, click **Change** in order to enter a new destination folder.

7. If you would like to add a desktop shortcut, check the **Create a shortcut for this application on your desktop** check box.
8. Click **Next**.

The *Ready to install Cisco CLI Analyzer* dialog window appears.

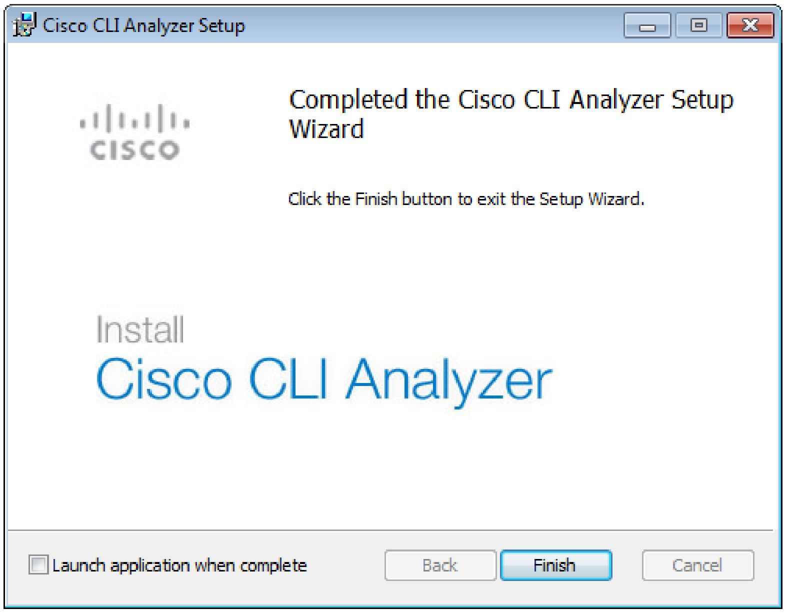


Ready to install Cisco CLI Analyzer

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

9. On the *Ready to install Cisco CLI Analyzer* dialog window, click **Install**.

   After installation is complete, the *Completed the Cisco CLI Analyzer Setup Wizard* dialog window appears.



Completed the Cisco CLI Analyzer Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Launch application when complete

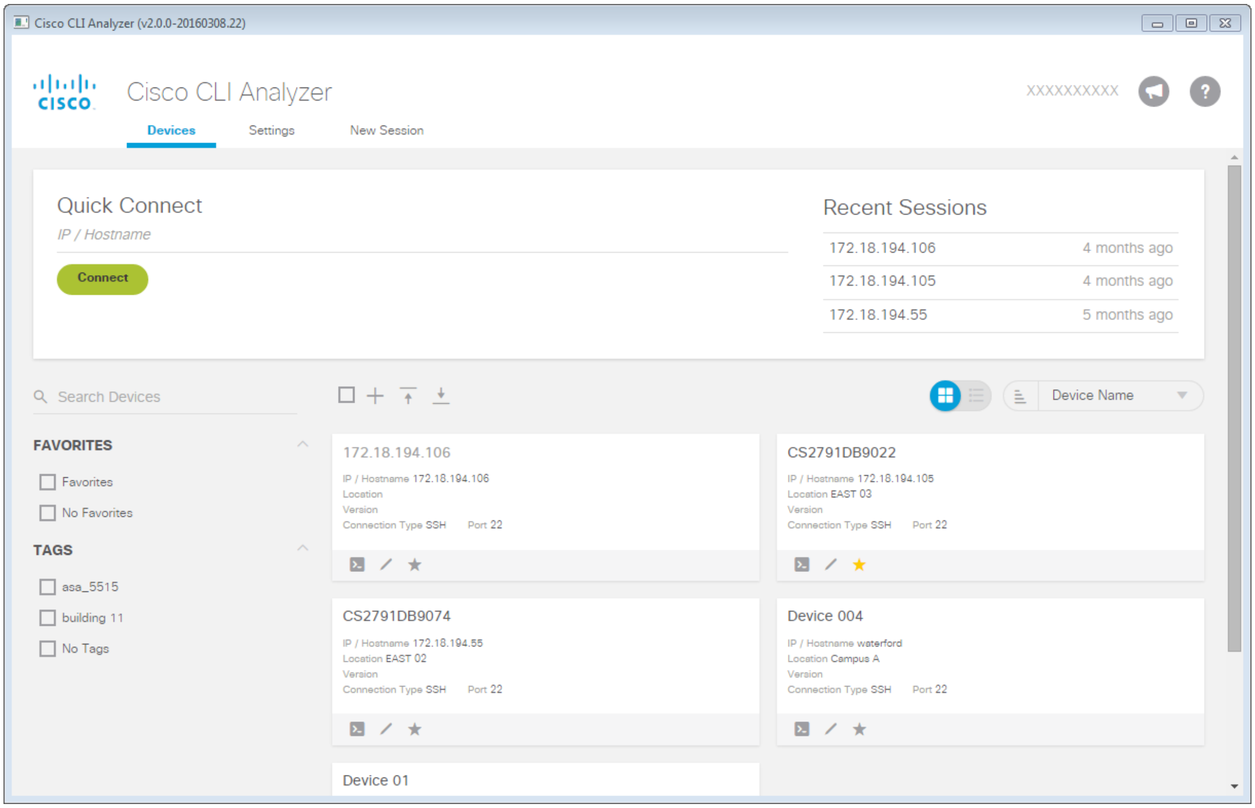
10. If you want to launch the application on exit, check the **Launch application when complete** check box.
11. Click **Finish** in order to exit the Cisco CLI Analyzer Setup Wizard.

Note: After installation is complete, you can run the Cisco CLI Analyzer executable again in order to repair or remove the application.

Access the Cisco CLI Analyzer

After the Cisco CLI Analyzer is installed, click the **Cisco CLI Analyzer** icon in order to open the Cisco CLI Analyzer interface.

The Cisco CLI Analyzer interface appears with the *Devices* tab selected.



172.18.194.106	4 months ago
172.18.194.105	4 months ago
172.18.194.55	5 months ago

172.18.194.106
IP / Hostname 172.18.194.106
Location
Version
Connection Type SSH Port 22

CS2791DB9022
IP / Hostname 172.18.194.105
Location EAST 03
Version
Connection Type SSH Port 22

CS2791DB9074
IP / Hostname 172.18.194.55
Location EAST 02
Version
Connection Type SSH Port 22

Device 004
IP / Hostname waterford
Location Campus A
Version
Connection Type SSH Port 22

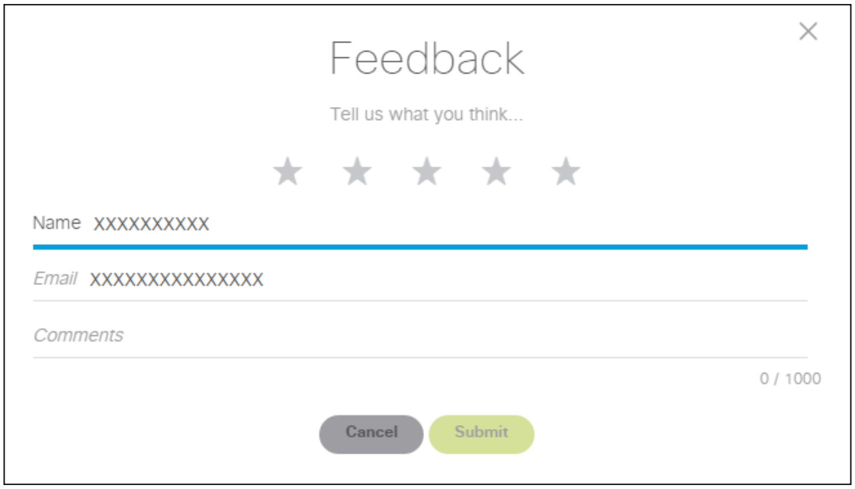
Device 01

After the Cisco CLI Analyzer opens, you can configure global console settings, add devices to your device list, or connect to a device. See these topics for more information:

- Global Console Settings
- Add a Device to the Device List
- Connect to a Device

Submit Comments and Questions

In order to submit comments and questions about the Cisco CLI Analyzer tool, click the Feedback icon (📢) in the top left corner of the window in order to open the *Feedback* form. Enter your name, email address, and comments in the fields provided. Optionally, select a star rating. When you are finished, click **Submit** in order to send your feedback.



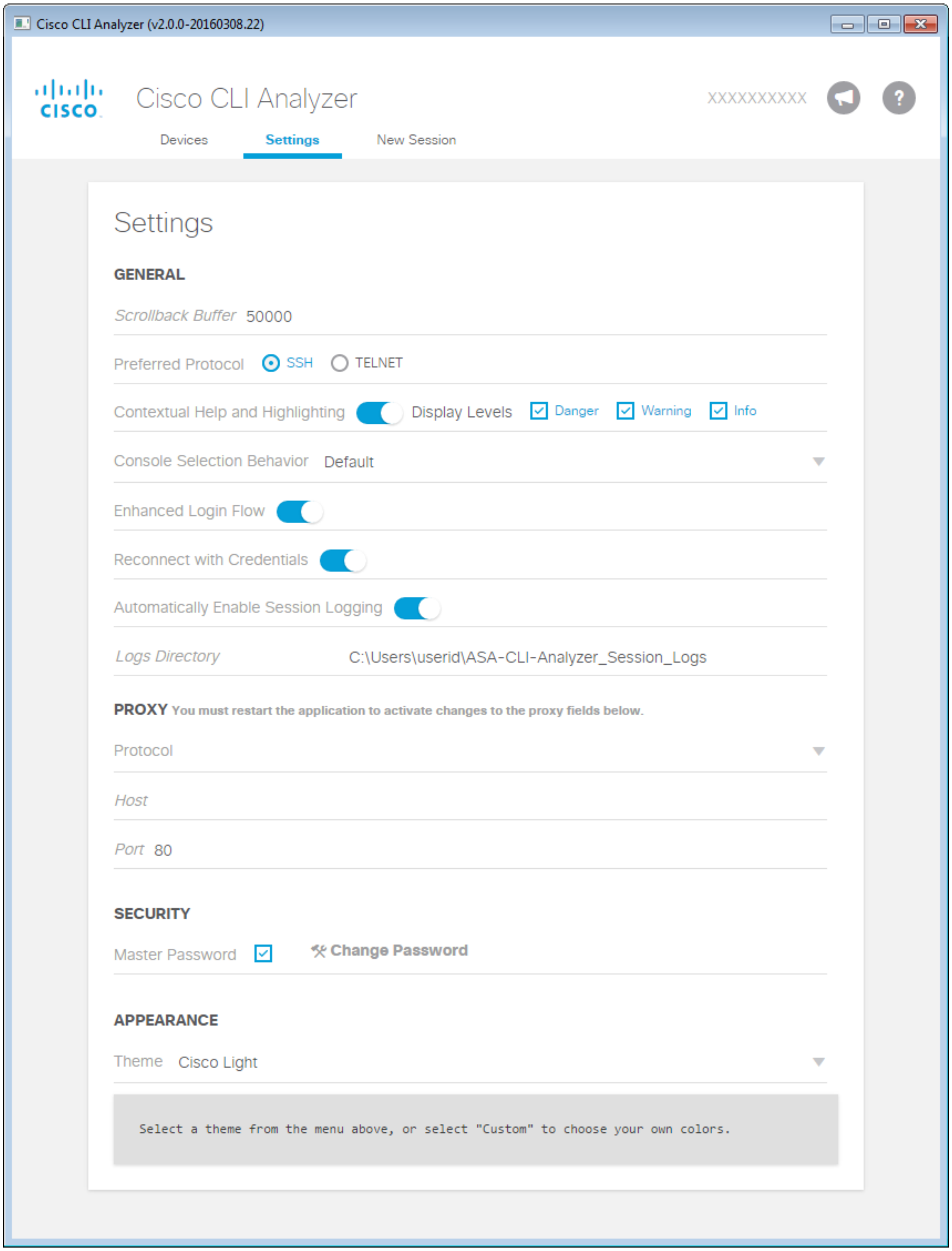
Name XXXXXXXXXX

Email XXXXXXXXXXXXXXX

Configure Application Settings

Global Console Settings

Click the Settings tab in order to access global console settings. These settings apply across all device sessions.



Settings

GENERAL

Scrollback Buffer 50000

Preferred Protocol ● SSH ○ TELNET

Contextual Help and Highlighting (on) Display Levels ☑ Danger ☑ Warning ☑ Info

Console Selection Behavior Default

Enhanced Login Flow (on)

Reconnect with Credentials (on)

Automatically Enable Session Logging (on)

Logs Directory C:\Users\userid\ASA-CLI-Analyzer_Session_Logs

PROXY You must restart the application to activate changes to the proxy fields below.

Protocol

Host

Port 80

SECURITY

Master Password ☑ Change Password

APPEARANCE

Theme Cisco Light

Select a theme from the menu above, or select "Custom" to choose your own colors.

Scrollback Buffer

In the Scrollback Buffer area of the Settings tab, you can configure the number of command lines retained in memory. In order to configure the scrollback buffer, enter a number between 100 and 50000 in the Scrollback Buffer field.

Preferred Protocol

Choose the protocol (SSH or Telnet) that you use most frequently. This protocol is selected by default when you create a new connection.

Contextual Help and Highlighting

Click the toggle button in order to enable or disable contextual help and highlighting. This feature is enabled by default. For more information, see Contextual Help and Highlighting.

By default, all notification types (Danger, Warning, and Info) are enabled. You can use the Display Levels check boxes in order to filter the notification types that you want to display. Clear the check boxes beside notification types that you want to filter out (disable).

Console Selection Behavior

Choose your preferred experience when you use the mouse in order to select text within the console window. In addition to the default text selection behavior, you can choose to emulate the behavior of PuTTY or SecureCRT.

Enhanced Login Flow

Click the toggle button in order to enable or disable a simplified version of the Session Login window. When enabled, you are not prompted to enter basic connectivity information about the device if the Cisco CLI Analyzer already has that information.

Reconnect with Credentials

Click the toggle button in order to enable or disable the ability to reconnect with the login credentials you previously entered. When enabled, login credentials are remembered for each session tab and persist until the session tab is closed.

Automatically Enable Session Capture

Click the toggle button in order to enable or disable automatic session logs. When enabled, activity is logged by default when you connect to a device, and a log file is saved automatically when you disconnect. You can still start and stop logging sessions manually from within the console. For more information, see Log Your Current Session.

Logs Directory

By default, log files are saved in these locations:

- **Windows:** C:\Users\<userid>\Cisco-CLI-Analyzer_Session_Logs
- **Mac OS X:** /Users/<userid>/Cisco-CLI-Analyzer_Session_Logs

In order to choose a different folder, click the path currently displayed. Browse to the desired folder, select it, and click **OK**.

Proxy

For details, see Proxy Settings.

Master Password

Check the check box in order to allow the Cisco CLI Analyzer to save a master password. Enabling a master password allows you to store credentials for individual devices so that you do not have to enter them every time. The application uses Secure Hash Algorithm 3 (SHA-3) in order to securely store the password as a hash value in the database.

If this feature is enabled, when you open the Cisco CLI Analyzer, the application prompts you to enter the master password. If you do not enter the master password, you must enter credentials for each individual device session.

In order to change the password, click **Change Password**. Enter the old master password and the new one.

Theme

In the Appearance area of the Settings tab, you can configure the text and background colors of the console window. In order to configure the console window, click the **Theme** field and select a predefined color theme, or select **Custom** in order to choose your own colors.

If you choose **Custom**, a set of Text and Background color buttons appears. Click a color button in order to display the color palette, from which you can choose a color. A preview of your current theme or color selection is displayed in the Preview window.

Note: Search terms use their own text and background colors. For information on how to search, see Search the Command Output.

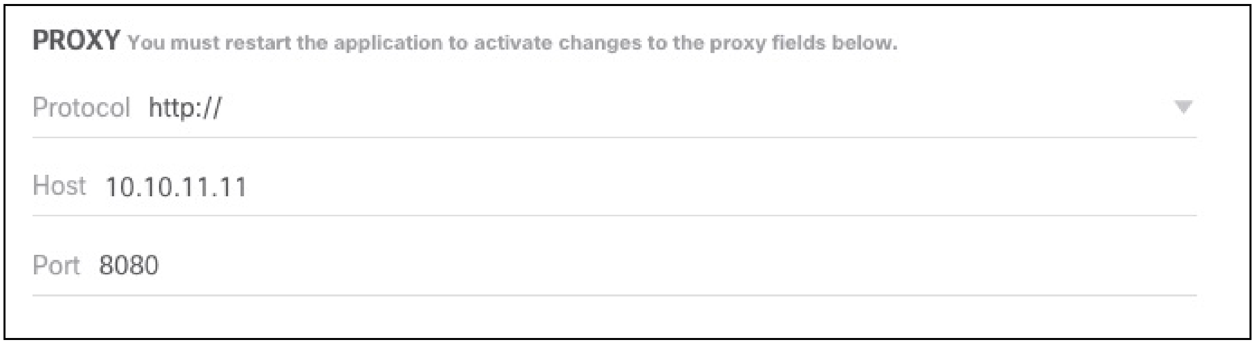
Proxy Settings

If you use a proxy server for outbound web connections, you must provide information about the proxy in order to utilize the TAC tools (such as the ASA and IOS System Diagnostics and the ASA Traceback Decoder tools) and auto updates.

On the **Settings** tab, complete the fields in the Proxy area:

- **Protocol:** Click inside the field and choose a protocol from the drop-down list. Supported protocols include HTTP, HTTPS, Socks, and Socks5.
- **Host:** Enter the IP address of the proxy server.
- **Port:** Enter the port number to use.

Note: You *must* restart the application in order for Proxy settings to take effect.



PROXY You must restart the application to activate changes to the proxy fields below.

Protocol http://

Host 10.10.11.11

Port 8080

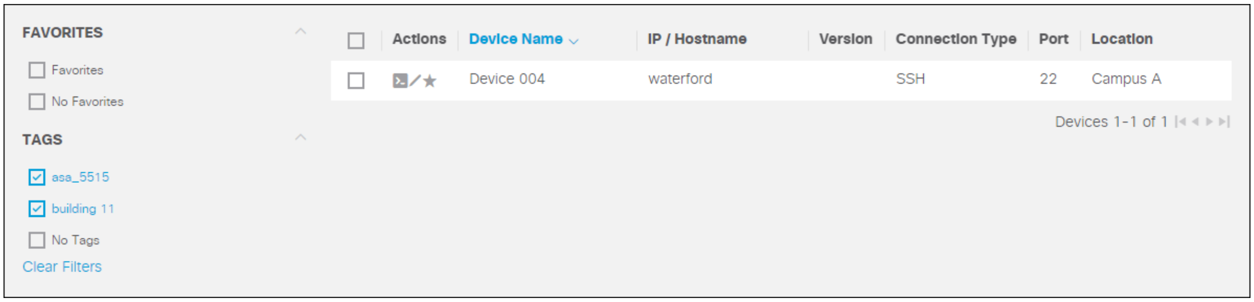
Manage Your Devices

Locate Devices

Use filters and searches in order to locate specific devices in the device list.

Filters

Filters are based on tags and favorites. Check the filter boxes on the left side of the device list in order to display only devices with the selected tags or the selected favorite status (either favorites or non-favorites).



FAVORITES

□ Favorites
□ No Favorites

TAGS

☑ asa_5515
☑ building 11
□ No Tags

Clear Filters

□	Actions	Device Name	IP / Hostname	Version	Connection Type	Port	Location
□	★	Device 004	waterford		SSH	22	Campus A

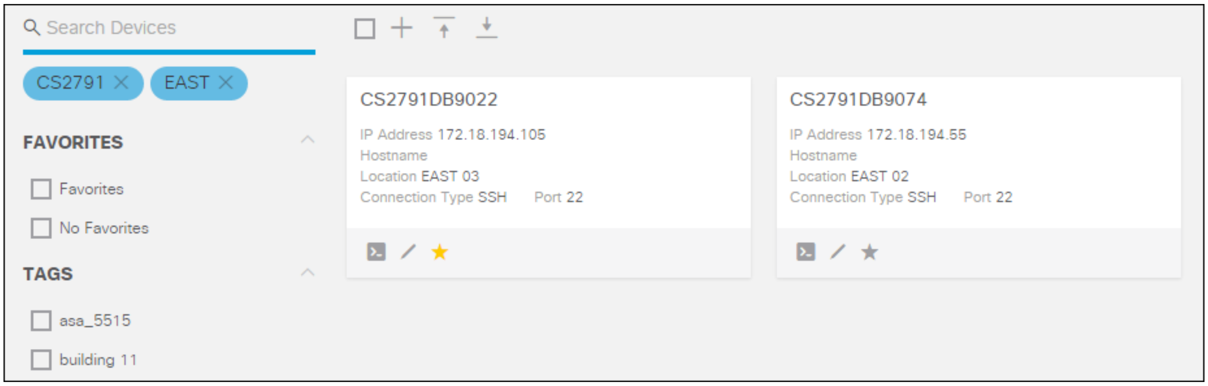
Devices 1-1 of 1

In order to remove all active filters, click **Clear Filters** below the filter check boxes. The device list displays all devices.

Searches

Enter a keyword in the **Search** box and press **Enter** in order to filter the device list to show devices whose properties include the keyword.

The keyword is displayed in a bubble below the **Search** box and remains an active filter that can be combined with other filter selections. In order to remove the keyword as an active filter, click the X on the keyword bubble.



Search Devices

CS2791 ✕ EAST ✕

FAVORITES

□ Favorites
□ No Favorites

TAGS

□ asa_5515
□ building 11

CS2791DB9022
IP Address 172.18.194.105
Hostname
Location EAST 03
Connection Type SSH Port 22

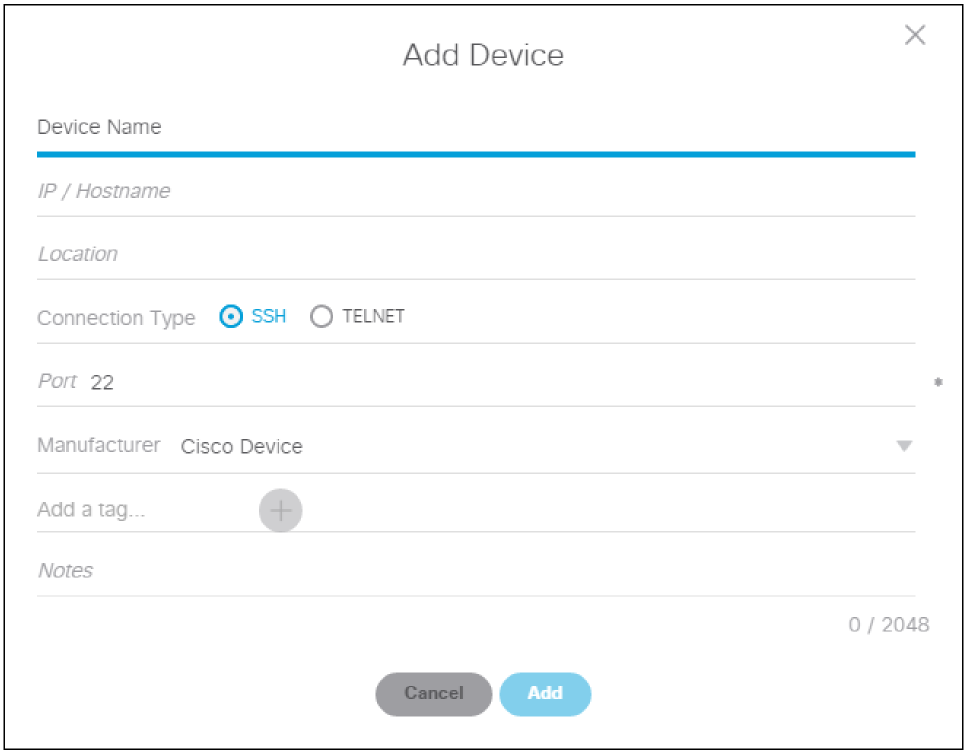
CS2791DB9074
IP Address 172.18.194.55
Hostname
Location EAST 02
Connection Type SSH Port 22

Add a Device to the Device List

Complete these steps in order to add a device to the Devices list:

1. In the Cisco CLI Analyzer, click the **Devices** tab, and click the **Add Device** button (+) on the Device List toolbar, located below the Quick Connect box.

   The *Add Device* dialog window appears.



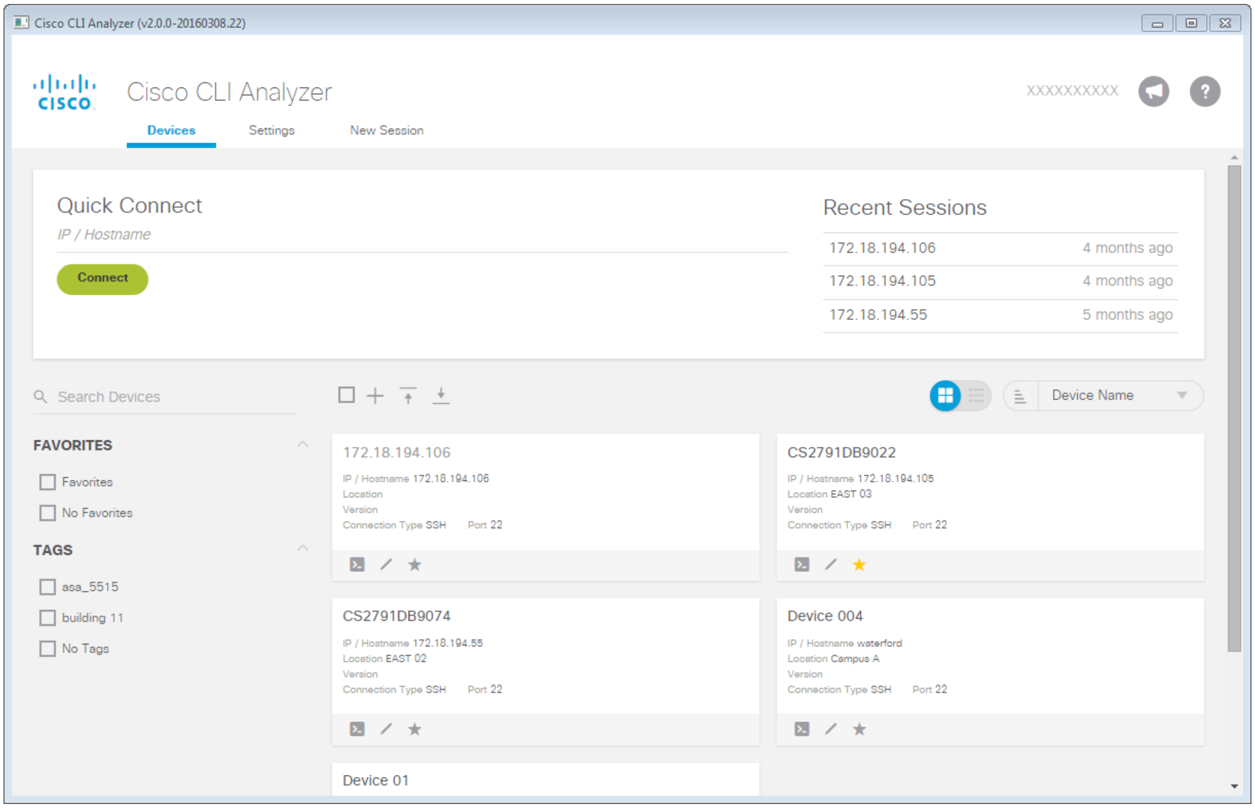
Connection Type ● SSH ○ TELNET

Port 22

Manufacturer Cisco Device

2. Enter a name for the device in the **Device Name** field.
3. Enter the IP address or host name in the **IP/Hostname** field.
4. Enter the physical location of the device in the **Location** field.
5. Click the radio button for the protocol (**SSH** or **Telnet**) you want to use.
6. If you use a non-standard port number, enter it in the **Port** field.
7. Choose **Cisco Device** or **Non-Cisco Device** in the **Manufacturer** field.
8. Assign one or more Tags to describe your device. Click **Add a tag...** and type a tag, then click the + button.
9. Click **Add**.

The device is added to the Devices list.



Recent Sessions

172.18.194.106	4 months ago
172.18.194.105	4 months ago
172.18.194.55	5 months ago

FAVORITES

□ Favorites
□ No Favorites

TAGS

□ asa_5515
□ building 11
□ No Tags

172.18.194.106
IP / Hostname 172.18.194.106
Location
Version
Connection Type SSH Port 22

CS2791DB9022
IP / Hostname 172.18.194.105
Location EAST 03
Version
Connection Type SSH Port 22

CS2791DB9074
IP / Hostname 172.18.194.55
Location EAST 02
Version
Connection Type SSH Port 22

Device 004
IP / Hostname waterford
Location Campus A
Version
Connection Type SSH Port 22

Device 01

After the device is added to the Devices list, you can perform these actions:

- Click the **Connect** button (>_) below a device in order to connect to that device.
- Click the **Edit** button (✎) below a device in order to open the Edit Device window, where you can update device information.
- Click the **Favorites** button (★) below a device in order to mark the device as a Favorite. The button icon changes to an orange star (★). Click the button again in order to remove the device from Favorites.

After additional devices are added to the Devices list, you can use these actions in order to navigate the list.

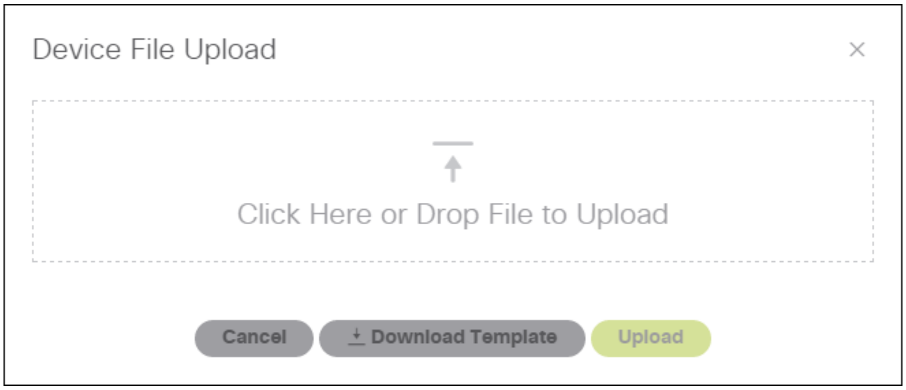
- Hover the pointer over a device and click the **Select** button (✓) in order to select the device. The device is highlighted and the **Bulk Actions** button becomes available. In order to deselect the device, click anywhere on the device.
- Click the **Select All** button (□) in order to select all devices in the list. The button icon changes (☑) in order to show that all devices are selected. The **Bulk Actions** button becomes available.
- With one or more devices selected, click the **Bulk Actions** button (Bulk Actions (3) ⌄) and then click an option in the drop-down list in order to perform that action (Connect, Delete, Add Tags, or Delete Tags).
- Click the **Sort By** button (Activity Date ⌄) and choose Device Name, Location, or Activity Date from the drop-down list in order to sort the list of devices by the selected property.
- Click the **Sort** button (≡) in order to change the sort order of the list from descending to ascending. The button icon changes in order to show an ascending sort order (≡).
- Check a check box in the list of filters in order to show only devices that match your selected filter. (For example, select the **No Favorites** check box in order to show only devices that are not marked as Favorites.)
- Enter a search term in the **Search Devices** field and press **Enter** in order to search the device list.

Import Devices from a CSV File

You can import devices to the Device List from a CSV file. Complete these steps in order to import a CSV file.

1. On the Devices tab of the Cisco CLI Analyzer, click the **Upload** button (⤒) on the Device List toolbar (located below the Quick Connect area). On the drop-down menu, choose **Import from CSV**.

   The *Device File Upload* dialog window appears.



2. Complete one of these steps:
   - Click **Click or drop file to upload**. In the Open dialog, navigate to the CSV file you want to import, choose it, and click **Open**.
   - Drag the CSV file from a separate window onto the text “Click or drop file to upload.” Be sure that the icon below the pointer indicates that the file will be moved before you release the mouse button to drop the file.
3. Click **Upload**.

The devices imported from the CSV file appear in the Device List.

Import Devices from PuTTY

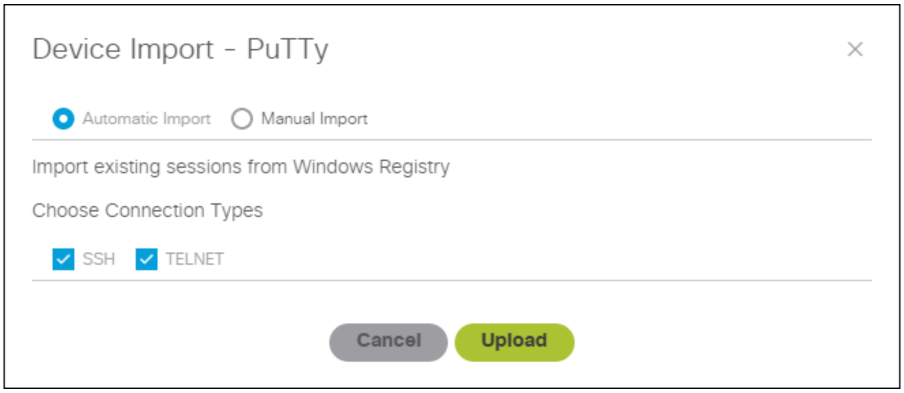
You can import devices to the Device List from a PuTTY export file. There are two options: to import automatically with settings from the Windows Registry, or to import manually with a configuration file that you create.

Use the steps for the automatic or manual import process as needed.

Automatic Import

1. On the Devices tab of the Cisco CLI Analyzer, click the Upload button (⭱) on the Device List toolbar (located below the Quick Connect area). On the drop-down menu, choose **Import from PuTTY**.

   The *Device Import - PuTTY* dialog window appears.



Device Import - PuTTy

● Automatic Import ○ Manual Import

Import existing sessions from Windows Registry

Choose Connection Types

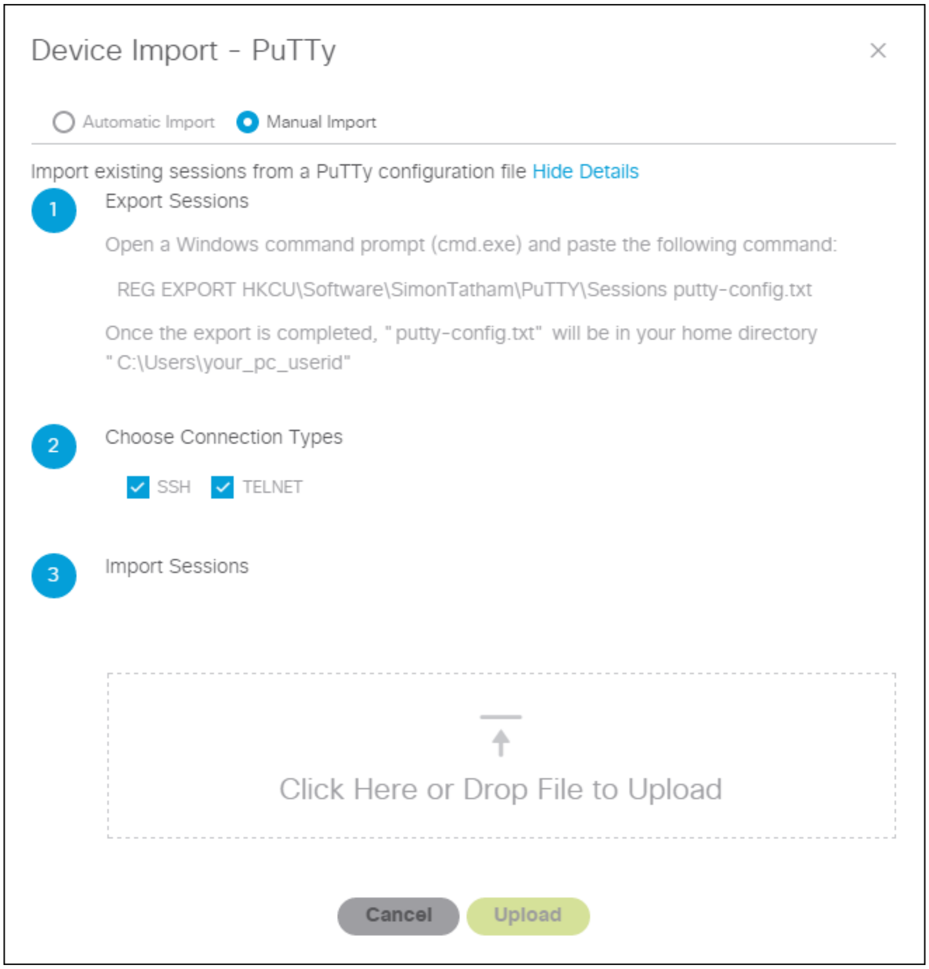
☑ SSH ☑ TELNET

2. Choose the connection type(s) to import: **SSH** and/or **Telnet**. Both check boxes are checked by default.
3. Click **Upload** and wait for the upload process to complete. Any errors during the upload are displayed in the bottom right corner of the application.

Manual Import

1. On the Devices tab of the Cisco CLI Analyzer, click the Upload button (⭱) on the Device List toolbar (located below the Quick Connect area). On the drop-down menu, choose **Import from PuTTY**.

   The *Device Import - PuTTY* dialog window appears.
2. Select **Manual Import** at the top of the window.
3. Click **View Details** in order to expand the window and show step-by-step instructions.



Device Import - PuTTy

○ Automatic Import ● Manual Import

Import existing sessions from a PuTTy configuration file Hide Details

1 Export Sessions

Open a Windows command prompt (cmd.exe) and paste the following command:

```
REG EXPORT HKCU\Software\SimonTatham\PuTTY\Sessions putty-config.txt
```

Once the export is completed, " putty-config.txt" will be in your home directory " C:\Users\your_pc_userid"

2 Choose Connection Types

☑ SSH ☑ TELNET

3 Import Sessions

Click Here or Drop File to Upload

4. Open a command shell window. At the command prompt, type (or copy and paste) this text:

   REG EXPORT HKCU\Software\SimonTatham\PuTTY\Sessions putty-config.txt

5. Press **Enter**. The file `putty-config.txt` is created in your home user directory:

   C:\Users\<your_user_name>

6. In the *Device Import - PuTTY* dialog window, choose the connection type(s) to import: **SSH** and/or **Telnet**. Both check boxes are checked by default.

7. Upload the PuTTY export file, `putty-config.txt`, by one of these methods:

   - Open the folder that contains the file in Windows Explorer. Drag the file from Windows Explorer onto the text “Click here or drag & drop the file to upload” in the Import Devices dialog window.
   - Click **Click here or drag & drop the file to upload** in the Import Devices dialog window. Browse to the folder that contains the PuTTY export file, choose the file, and click **Open**.

8. Click **Upload** and wait for the upload process to complete. Any errors during the upload are displayed in the bottom right corner of the application.

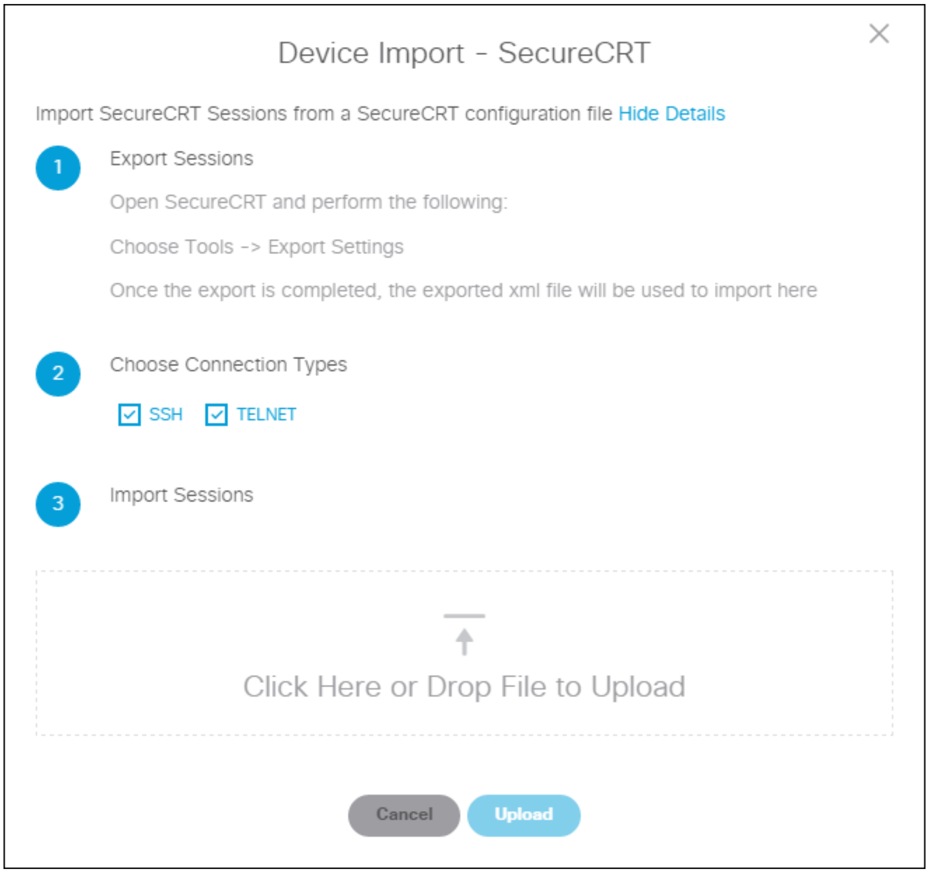
Import Devices from SecureCRT

You can import devices to the Device List from a SecureCRT export file. Complete these steps in order to create and import the file.

1. On the Devices tab of the Cisco CLI Analyzer, click the Upload button (⭱) on the Device List toolbar (located below the Quick Connect area). On the drop-down menu, choose **Import from SecureCRT**.

   The *Device Import - SecureCRT* dialog window appears.

2. Click **View Details** in order to expand the window and show step-by-step instructions.



Device Import - SecureCRT

Import SecureCRT Sessions from a SecureCRT configuration file Hide Details

1 Export Sessions

Open SecureCRT and perform the following:

Choose Tools -> Export Settings

Once the export is completed, the exported xml file will be used to import here

2 Choose Connection Types

☑ SSH ☑ TELNET

3 Import Sessions

Click Here or Drop File to Upload

3. Open SecureCRT. On the **Tools** menu, choose **Export Settings**. Complete the export process and note the location of the export file.

4. In the *Device Import - SecureCRT* dialog window, choose the connection type(s) to import: **SSH** and/or **Telnet**. Both check boxes are checked by default.

5. Upload the SecureCRT export file by one of these methods:

   - Open the folder that contains the file in Windows Explorer. Drag the file from Windows Explorer onto the text “Click here or drag & drop the file to upload” in the Import Devices dialog window.
   - Click **Click here or drag & drop the file to upload** in the Import Devices dialog window. Browse to the folder that contains the SecureCRT export file, choose the file, and click **Open**.

6. Click **Upload** and wait for the upload process to complete. Any errors during the upload are displayed in the bottom right corner of the application.

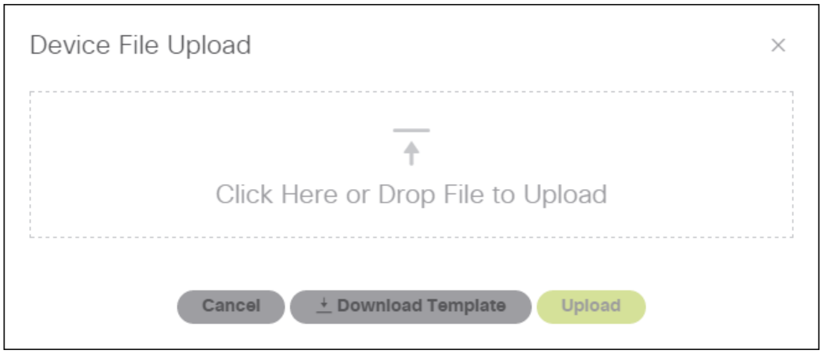
Create a CSV File of Devices

You can create a CSV file with device information that can be imported to the Cisco CLI Analyzer on any workstation.

Complete these steps in order to create a CSV file:

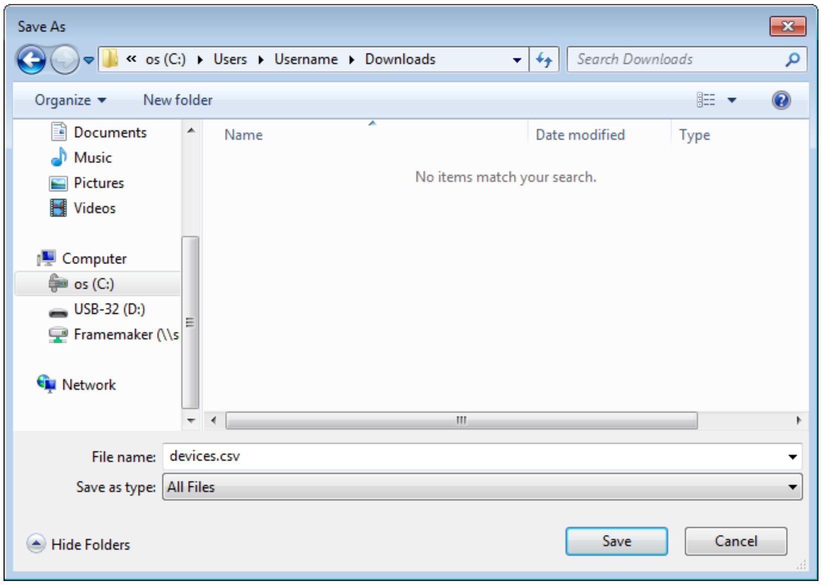
1. On the Devices tab of the Cisco CLI Analyzer, click the Upload button (↑) on the Device List toolbar (located below the Quick Connect area).

   The *Device File Upload* dialog window appears.



2. Click **Download Template**.

   The *Save As* dialog window appears.

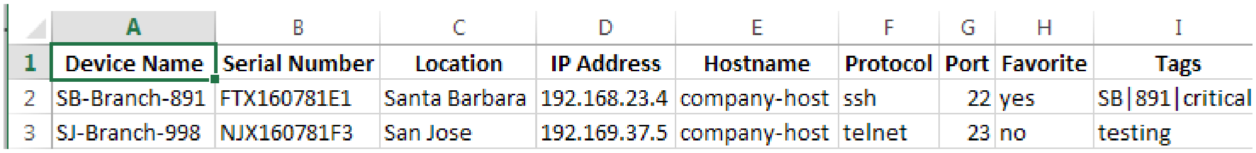


File name: devices.csv

Save as type: All Files

3. Navigate to the location where you want to save the CSV template and click **Save**.
4. Open the CSV file in your preferred application.
5. Enter the information for each device on a separate row. This information is required:
   - IP Address OR Hostname (DNS)
   - Protocol

   Other device information is optional and can be added from within the Cisco CLI Analyzer.



	A	B	C	D	E	F	G	H	I
1	Device Name	Serial Number	Location	IP Address	Hostname	Protocol	Port	Favorite	Tags
2	SB-Branch-891	FTX160781E1	Santa Barbara	192.168.23.4	company-host	ssh	22	yes	SB|891|critical
3	SJ-Branch-998	NJX160781F3	San Jose	192.169.37.5	company-host	telnet	23	no	testing

6. When you are finished, click **Save**.

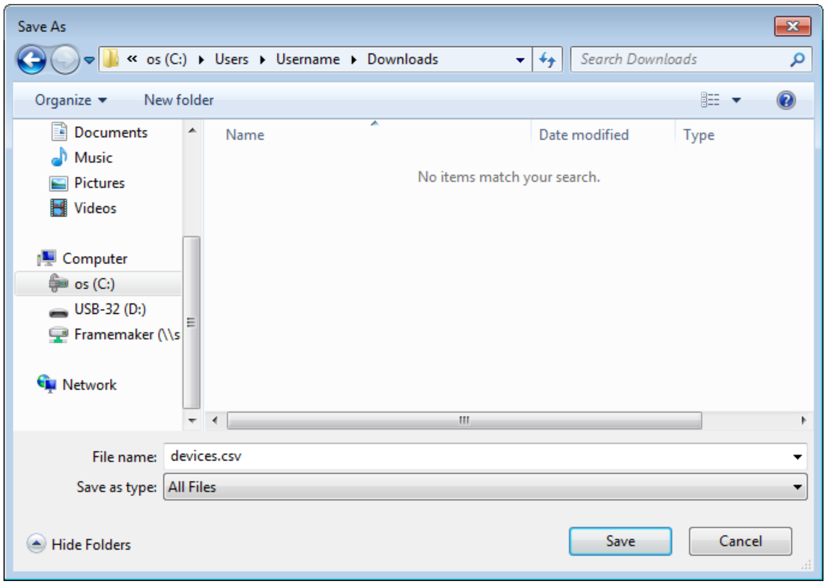
Export Devices

You can export information about the devices in your Device List to a CSV file. This allows you to import the information on another workstation.

Complete these steps in order to export device information to a CSV file:

1. On the Devices tab of the Cisco CLI Analyzer, click the **Export** button (⬆) on the Device List toolbar (located below the Quick Connect area).

   The *Save As* dialog window appears.



File name: devices.csv

Save as type: All Files

2. Navigate to a location on your computer, optionally change the file name of the CSV file, and click **Save**.

Connect to a Device

Complete these steps in order to connect to a device:

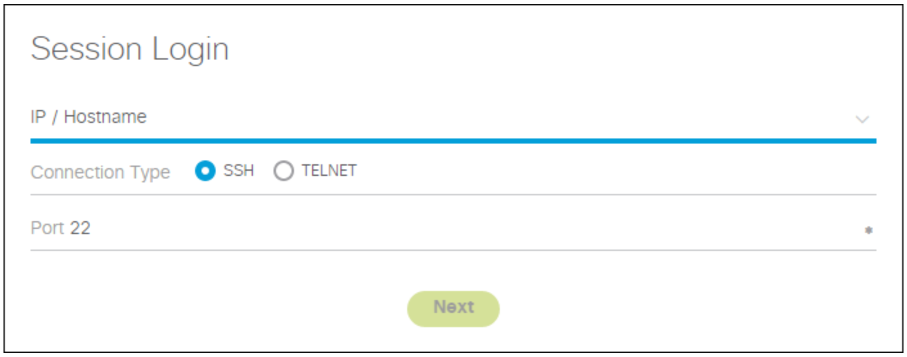
1. On the **Devices** tab, complete one of these actions in order to start a new session:
   - In the **Quick Connect** field, enter the hostname or IP address of the device in the field provided, and press Enter or click **Connect**.
   - Click a device in the Recent Sessions list.
   - Click **New Session**.
   - Click the >_ button on the device entry in the Devices list.

   A new session tab appears, and the *Session Login* screen opens.

Note: The contents of the Session Login screen depend on whether the **Enhanced Login Flow** option is enabled in the Settings window. The rest of this procedure describes the steps to take if the option is enabled. The steps are similar if the option is disabled, but the screen layout is different.

---

2. If you are prompted for basic connectivity information for the device, enter the requested information and click **Next**. Otherwise, skip this step and continue to step 3.
   - Enter the IP address or hostname of the device in the **IP/Hostname** field. You can also click the arrow beside the field and choose a device to which you have connected in a recent session.
   - Select the option button for the connection type (**SSH** or **Telnet**) that you want to use.
   - Enter the appropriate port number in the **Port** field.



Session Login

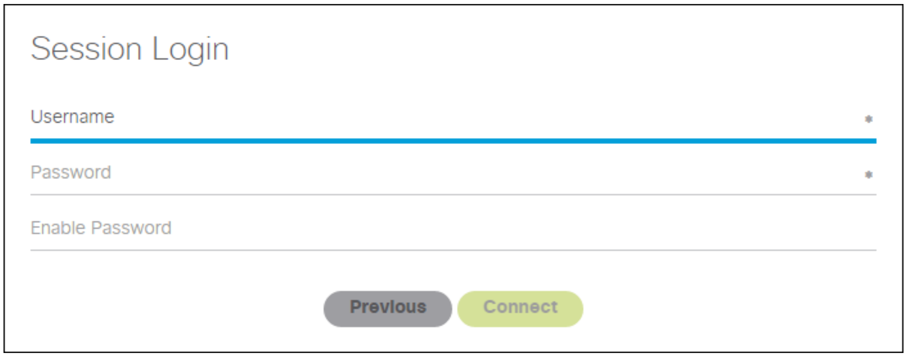
IP / Hostname

Connection Type ● SSH ○ TELNET

Port 22

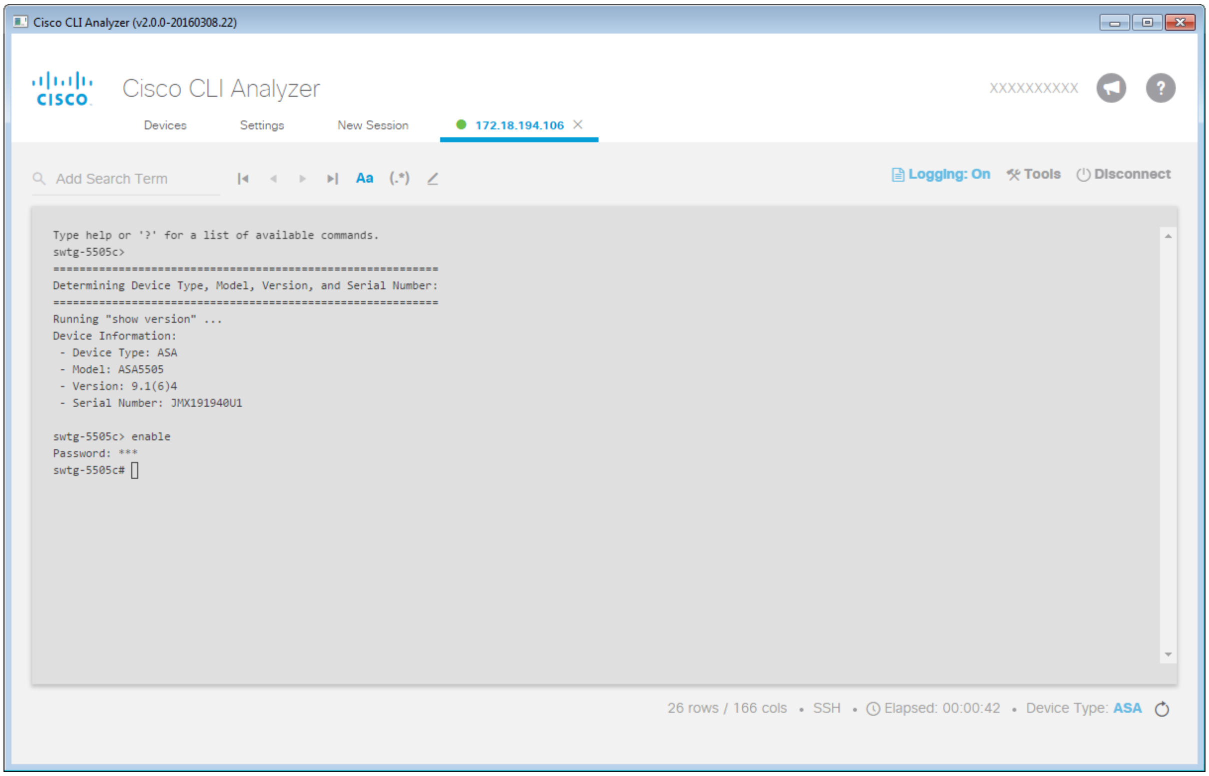
   The Cisco CLI Analyzer checks for a connection to the device. If the device is found, the screen changes in order to accept login information.

3. In the fields provided, enter the user name and password that are required to access the device.
4. Optionally, enter the password for Enable access in the **Enable Password** field. If you leave the field empty, you will be required to enter the enable command and the password manually at the command prompt before you run scripts that require Enable access.



5. Click **Connect**.

   A session window opens and the session tab icon displays green in order to indicate an active session.



```
Type help or '?' for a list of available commands.
swtg-5505c>
===========================================================
Determining Device Type, Model, Version, and Serial Number:
===========================================================
Running "show version" ...
Device Information:
 - Device Type: ASA
 - Model: ASA5505
 - Version: 9.1(6)4
 - Serial Number: JMX191940U1

swtg-5505c> enable
Password: ***
swtg-5505c# 
```

26 rows / 166 cols • SSH • Elapsed: 00:00:42 • Device Type: ASA

Note: The status bar at the bottom of the window displays row and column count, as well as connection protocol, start time, and elapsed time.

Once you are connected, you can perform these actions:

- Log your current session
- Run CLI commands
- Run Cisco CLI Analyzer scripts
- Search the command output

Note: Click **Disconnect** in order to disconnect from the device. If your session times out and you are automatically disconnected, click **Reconnect**.

Features

Log Your Current Session

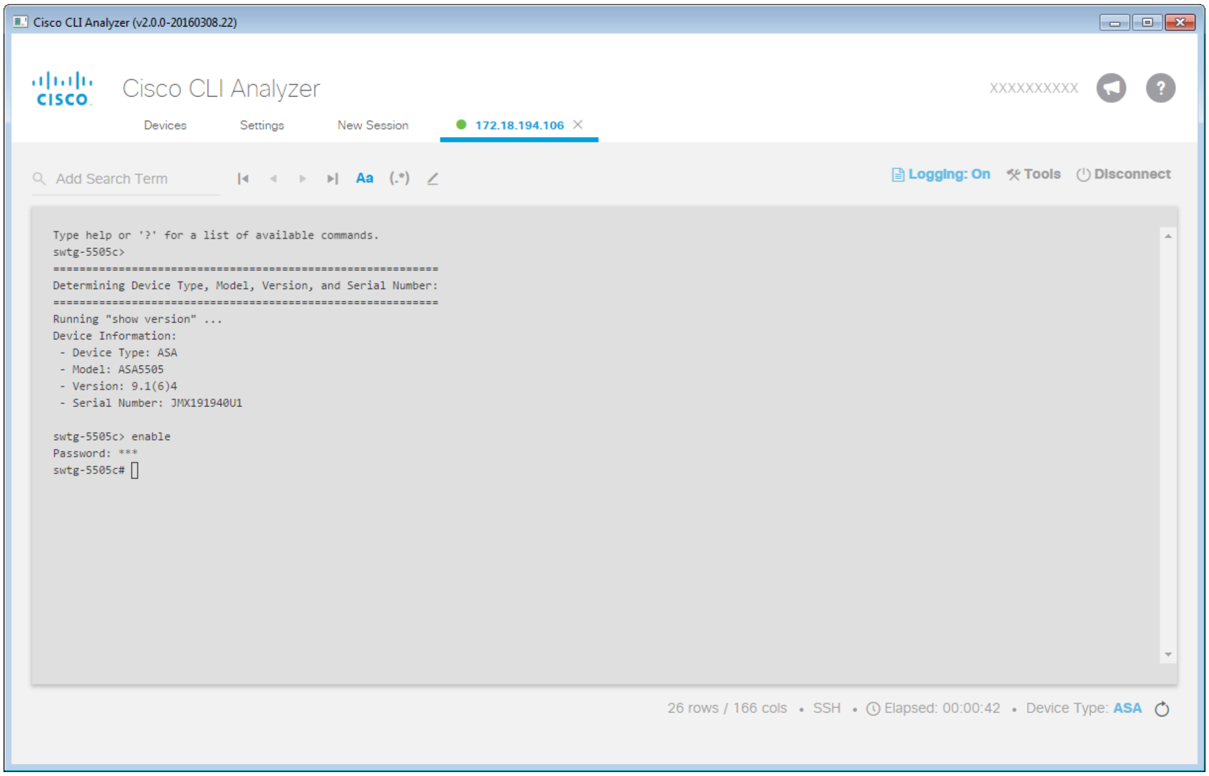
The Cisco CLI Analyzer allows you to capture your current console session and save the output to your local computer.

Note: An option on the Settings tab lets you log session activity automatically when you connect to a device, and save the log file automatically when you disconnect. For more information, see Automatically Enable Session Capture.

Complete these steps in order to log your current session:

1. Connect to a device as described in Connect to a Device.
2. If the **Logging** button label shows that Logging is off, click the button in order to turn on the feature.

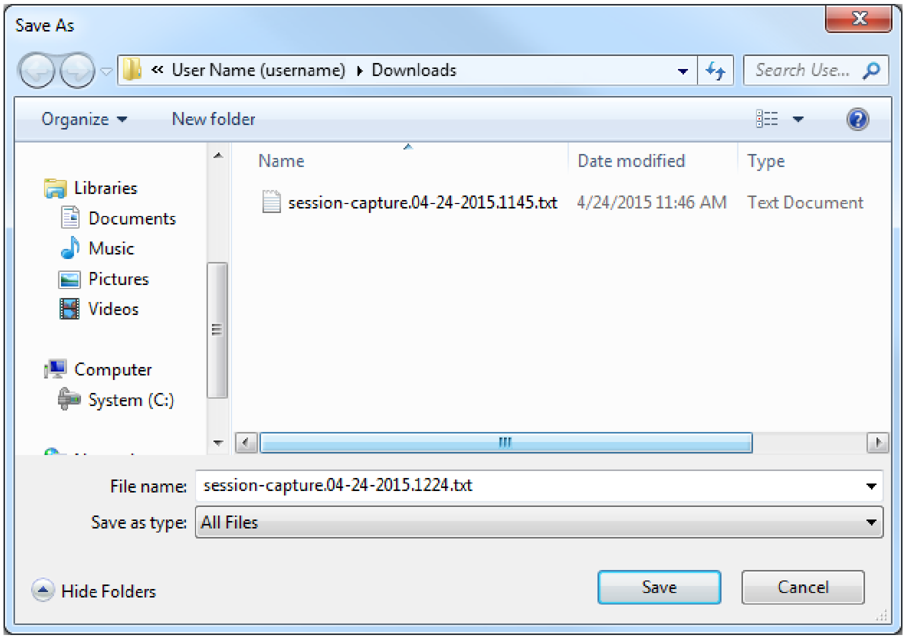
   The session log starts and the Logging button displays Logging: On.



```
Type help or '?' for a list of available commands.
swtg-5505c>
===========================================================
Determining Device Type, Model, Version, and Serial Number:
===========================================================
Running "show version" ...
Device Information:
 - Device Type: ASA
 - Model: ASA5505
 - Version: 9.1(6)4
 - Serial Number: JMX191940U1

swtg-5505c> enable
Password: ***
swtg-5505c#
```

3. When you complete the session, click **Logging: On**.

   The *Save As* dialog window appears.



Name	Date modified	Type
session-capture.04-24-2015.1145.txt	4/24/2015 11:46 AM	Text Document

File name: session-capture.04-24-2015.1224.txt

Save as type: All Files

By default, log files are saved in these locations:

- **Windows:** C:\Users\<userid>\Cisco-CLI-Analyzer_Session_Logs
- **Mac OS X:** /Users/<userid>/Cisco-CLI-Analyzer_Session_Logs

4. Navigate to a location on your computer, and click **Save**.

Add Tags to Devices

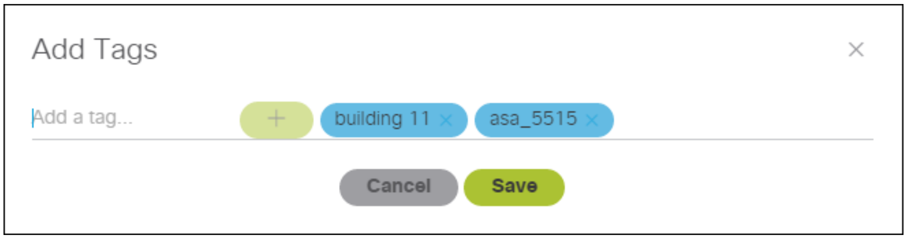
Assign tags (text references) to your devices in order to locate them easily without the need to navigate hierarchical trees. Apply tags to groups of devices in order to organize and quickly filter the Devices tab.

Tags can include these character types:

- Lowercase letters (uppercase letters are automatically converted to lowercase)
- Numbers
- Spaces
- Hyphens (-)and underscores (_)

In order to add device tags:

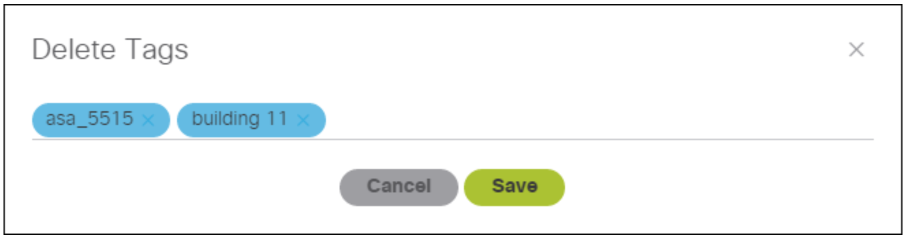
1. On the Devices tab, click the **Select** button (✓) on each device you want to tag.
2. Click the **Bulk Actions** button (Bulk Actions (3)⌄). On the drop-down menu, click **Add Tags**.
3. In the *Add Tags* window, click **Add a tag...** and type the tag that you want to add to the selected devices. Click the + button. Repeat this step for each tag that you want to add.



4. Click **Save**.

In order to remove device tags:

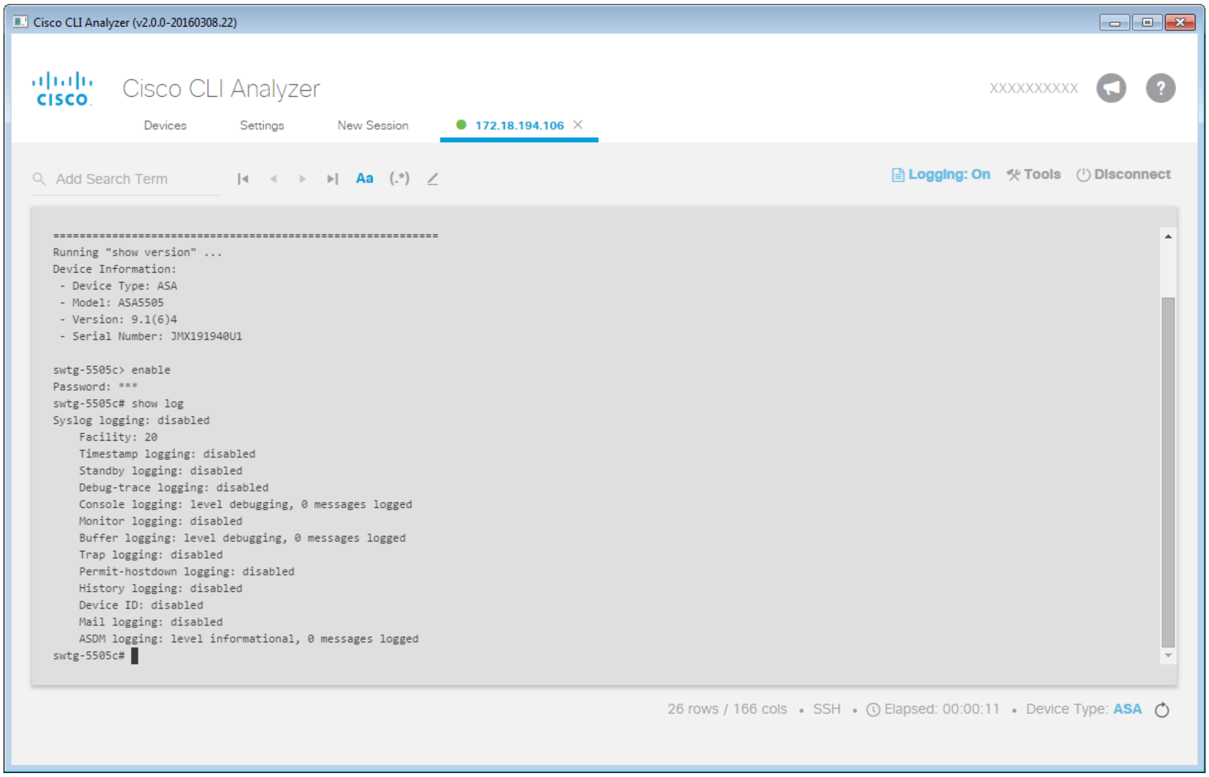
1. On the Devices tab, click the **Select** button (✓) on each device from which you want to remove tags.
2. Click the **Bulk Actions** button (Bulk Actions (3)⌄). On the drop-down menu, choose **Delete Tags**.
3. In the *Delete Tags* window, click the X on each tag that you want to delete.



4. Click **Save**.

Run CLI Commands

In order to run CLI commands, connect to a device as described in Connect to a Device, enter a command at the command prompt, and press Enter.



```
==========================================================
Running "show version" ...
Device Information:
 - Device Type: ASA
 - Model: ASA5505
 - Version: 9.1(6)4
 - Serial Number: JMX191940U1

swtg-5505c> enable
Password: ***
swtg-5505c# show log
Syslog logging: disabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: level debugging, 0 messages logged
    Monitor logging: disabled
    Buffer logging: level debugging, 0 messages logged
    Trap logging: disabled
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level informational, 0 messages logged
swtg-5505c#
```

Run Cisco CLI Analyzer Scripts

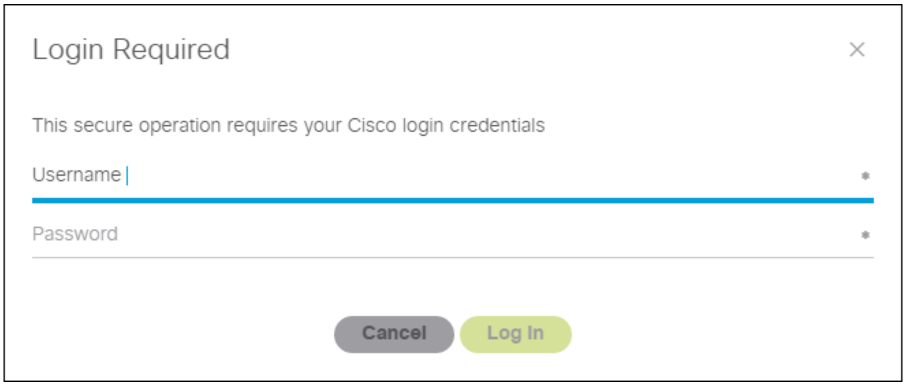
Run Cisco CLI Analyzer Scripts

The Cisco CLI Analyzer allows you to run scripts that help identify, troubleshoot, and resolve problems that you might experience in support of your ASA, IOS, IOS-XE, or IOS-XR device. These scripts appear in the Tools panel of a device session window.

CCO Login

Many script operations require you to log in with your Cisco account. You can log in when prompted to do so, or click **Login** in the top right corner of the Cisco CLI Analyzer window and enter your user credentials at any time.

Note: Your profile must be associated with an active Customer or Partner contract in order to use these tools.



Login Required

This secure operation requires your Cisco login credentials

Username *

Password *

Tool Descriptions

In order to submit ideas for new tools or suggestions to enhance these tools, send us feedback as described in Submit Comments and Questions.

System Diagnostics for ASA, IOS, IOS-XE, and IOS-XR

This tool utilizes Cisco TAC knowledge in order to analyze a Cisco supported device and detect known problems such as system problems, configuration mistakes, and best practice violations.

Note: This analysis requires the output of the **show tech-support** command and is sent to Cisco in order to be processed. **IOS-XR** analysis will vary in the use of “show” commands.

ASA Firewall Top Talkers

This tool helps determine which connections that pass traffic through an ASA might have the highest bit rate during a certain period of time.

The tool compares two separate outputs of **show conn** or **show conn all**, taken a few seconds apart. It calculates the difference in the “bytes” value in order to see how much traffic each connection passed during the time between the first and second outputs. It also identifies new connections (those found in the second output but not the first).

The tool then displays a list of the connections of interest, sorted by amount of traffic. You can export the results in JSON or CSV format.

ASA Traceback Analyzer

This tool attempts to match the root cause of a crash to a known bug if the ASA has experienced a system traceback. If a match is found, the ASA version or versions in which the bug is fixed are provided.

Note: This analysis requires the output of the **show crashinfo** command and is sent to Cisco to be processed. All ASA software versions are supported.

ASA Packet Tracer

This tool allows administrators to send simulated packets through the ASA as a test. If the packet is dropped, the ASA configuration portion or feature that could have contributed to the packet drop is identified.

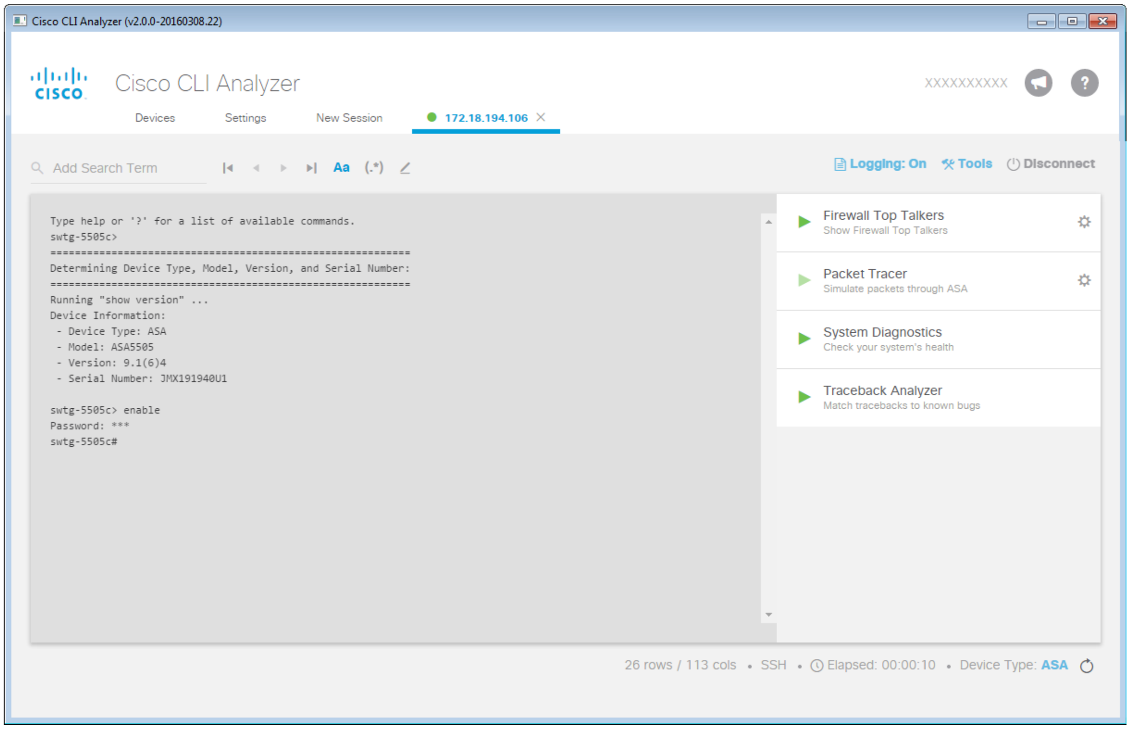
Note: ASA version 7.2 (the first version to include the command) and later are supported.

Run Scripts

Complete these steps in order to run a Cisco CLI Analyzer script:

1. Connect to a device as described in Connect to a Device, and click **Tools**.

   The *Tools* panel appears.



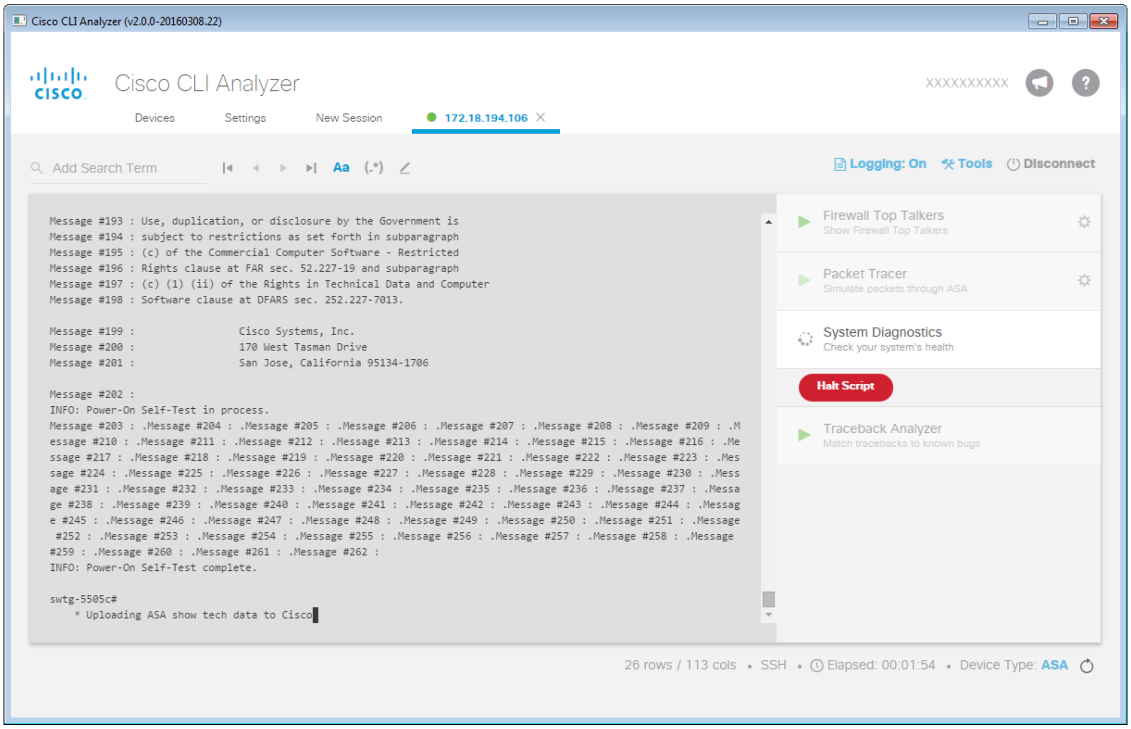
Cisco CLI Analyzer (v2.0.0-20160308.22)
Cisco CLI Analyzer
XXXXXXXXXX
Devices
Settings
New Session
172.18.194.106
Add Search Term
Aa
(.*)
Logging: On
Tools
Disconnect
Firewall Top Talkers
Show Firewall Top Talkers
Packet Tracer
Simulate packets through ASA
System Diagnostics
Check your system's health
Traceback Analyzer
Match tracebacks to known bugs
26 rows / 113 cols • SSH • Elapsed: 00:00:10 • Device Type: ASA

```
Type help or '?' for a list of available commands.
swtg-5505c>
===========================================================
Determining Device Type, Model, Version, and Serial Number:
===========================================================
Running "show version" ...
Device Information:
 - Device Type: ASA
 - Model: ASA5505
 - Version: 9.1(6)4
 - Serial Number: JMX191940U1

swtg-5505c> enable
Password: ***
swtg-5505c#
```

2. Click the Run button (▶) for the script that you want to run.

Note: In order to run the ASA Packet Tracer, you must configure additional settings. In order to configure the additional settings, click the **Configure** button located in the ASA Packet Tracer panel, and enter the configuration settings.

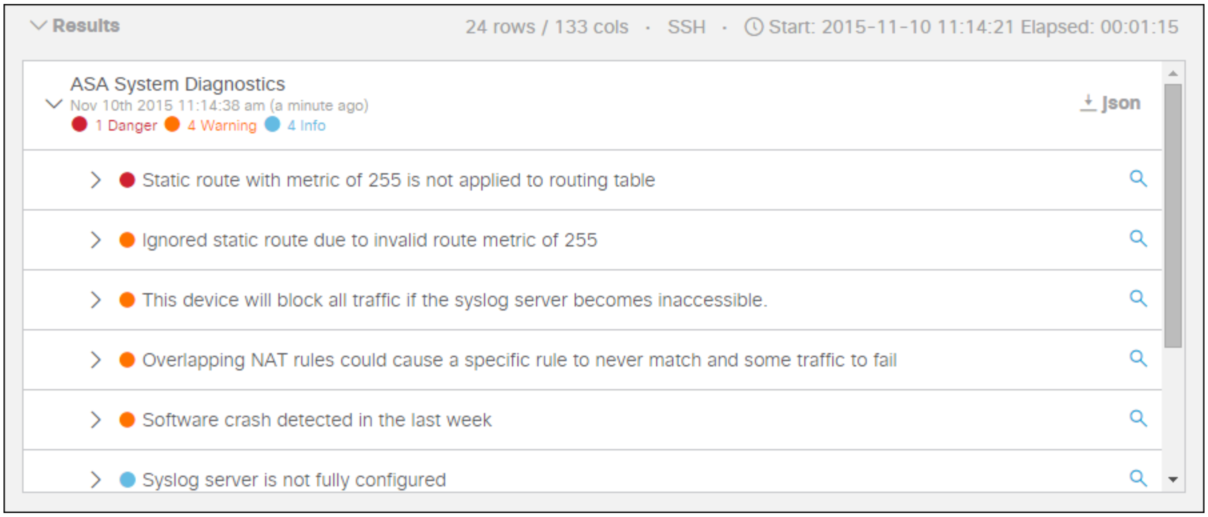
The script begins to run and the **Halt Script** button appears.


Cisco CLI Analyzer (v2.0.0-20160308.22)
Cisco CLI Analyzer
XXXXXXXXXX
Devices
Settings
New Session
172.18.194.106
Add Search Term
Aa
(.*)
Logging: On
Tools
Disconnect
Firewall Top Talkers
Show Firewall Top Talkers
Packet Tracer
Simulate packets through ASA
System Diagnostics
Check your system's health
Halt Script
Traceback Analyzer
Match tracebacks to known bugs
26 rows / 113 cols • SSH • Elapsed: 00:01:54 • Device Type: ASA

```
Message #193 : Use, duplication, or disclosure by the Government is
Message #194 : subject to restrictions as set forth in subparagraph
Message #195 : (c) of the Commercial Computer Software - Restricted
Message #196 : Rights clause at FAR sec. 52.227-19 and subparagraph
Message #197 : (c) (1) (ii) of the Rights in Technical Data and Computer
Message #198 : Software clause at DFARS sec. 252.227-7013.

Message #199 :                 Cisco Systems, Inc.
Message #200 :                 170 West Tasman Drive
Message #201 :                 San Jose, California 95134-1706

Message #202 :
INFO: Power-On Self-Test in process.
Message #203 : .Message #204 : .Message #205 : .Message #206 : .Message #207 : .Message #208 : .Message #209 : .M
essage #210 : .Message #211 : .Message #212 : .Message #213 : .Message #214 : .Message #215 : .Message #216 : .Me
ssage #217 : .Message #218 : .Message #219 : .Message #220 : .Message #221 : .Message #222 : .Message #223 : .Mes
sage #224 : .Message #225 : .Message #226 : .Message #227 : .Message #228 : .Message #229 : .Message #230 : .Mess
age #231 : .Message #232 : .Message #233 : .Message #234 : .Message #235 : .Message #236 : .Message #237 : .Messa
ge #238 : .Message #239 : .Message #240 : .Message #241 : .Message #242 : .Message #243 : .Message #244 : .Messag
e #245 : .Message #246 : .Message #247 : .Message #248 : .Message #249 : .Message #250 : .Message #251 : .Message
 #252 : .Message #253 : .Message #254 : .Message #255 : .Message #256 : .Message #257 : .Message #258 : .Message
#259 : .Message #260 : .Message #261 : .Message #262 :
INFO: Power-On Self-Test complete.

swtg-5505c#
    * Uploading ASA show tech data to Cisco
```

Note: If *Enable* access is required, you will be prompted to input credentials before the script runs.

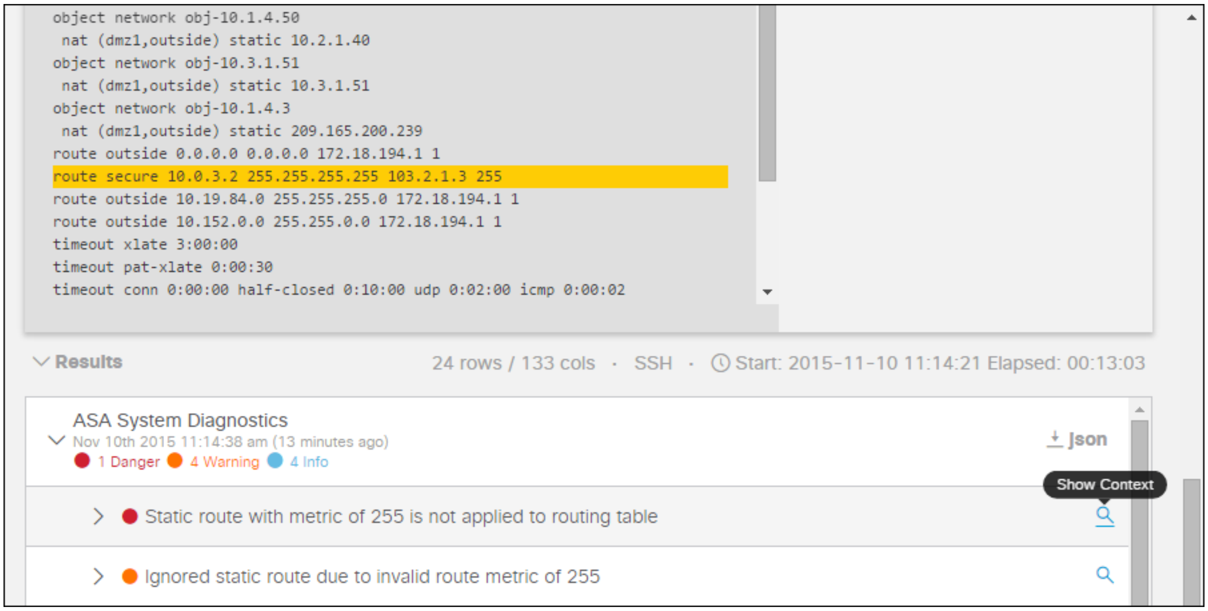
3. Wait for the script to complete, or click **Halt Script** to stop the script.
4. After the script completes, the session is listed in the Results area at the bottom of the page.


Results 24 rows / 133 cols · SSH · Start: 2015-11-10 11:14:21 Elapsed: 00:01:15

ASA System Diagnostics
Nov 10th 2015 11:14:38 am (a minute ago)
● 1 Danger ● 4 Warning ● 4 Info

- ● Static route with metric of 255 is not applied to routing table
- ● Ignored static route due to invalid route metric of 255
- ● This device will block all traffic if the syslog server becomes inaccessible.
- ● Overlapping NAT rules could cause a specific rule to never match and some traffic to fail
- ● Software crash detected in the last week
- ● Syslog server is not fully configured

5. Click an item in the Results list to expand and view additional details.
6. Click the 🔍 icon beside an item in the Results list in order to scroll to and highlight the associated text in the session window. **Notes:** This feature applies ONLY to System Diagnostic tools. If you are connected to an IOS-XR device, the text highlighting feature is not available and the 🔍 icon is not present.



```
object network obj-10.1.4.50
 nat (dmz1,outside) static 10.2.1.40
object network obj-10.3.1.51
 nat (dmz1,outside) static 10.3.1.51
object network obj-10.1.4.3
 nat (dmz1,outside) static 209.165.200.239
route outside 0.0.0.0 0.0.0.0 172.18.194.1 1
route secure 10.0.3.2 255.255.255.255 103.2.1.3 255
route outside 10.19.84.0 255.255.255.0 172.18.194.1 1
route outside 10.152.0.0 255.255.0.0 172.18.194.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 0:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

Results 24 rows / 133 cols · SSH · Start: 2015-11-10 11:14:21 Elapsed: 00:13:03

ASA System Diagnostics
Nov 10th 2015 11:14:38 am (13 minutes ago)
● 1 Danger ● 4 Warning ● 4 Info

● Static route with metric of 255 is not applied to routing table

● Ignored static route due to invalid route metric of 255

7. Click **json** in the top right corner of the Results area in order to export the results to a .json file.

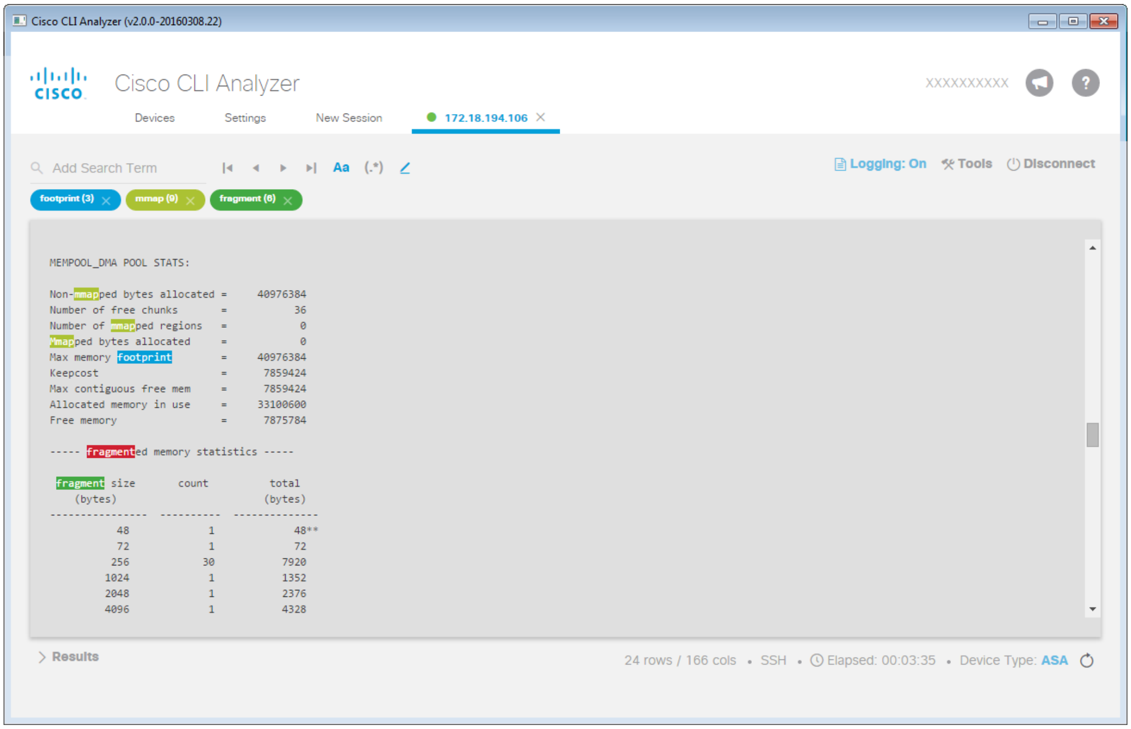
Search the Command Output

The Cisco CLI Analyzer includes a highlight feature that enables real-time search capabilities in the console window in order to search command output.

Complete these steps in order to search the command output:

1. Point to the **Highlight** button (✎) and check the tooltip in order to ensure that search result highlights are enabled. If highlights are disabled, click the button in order to enable highlights.
2. Enter a search term in the field provided, and press **Enter** or **Tab**. You can repeat this step in order to enter up to five (5) search terms.

   The specified search term or terms appear beside the search field along with the number of results for each term. Search results appear highlighted in the command window.



```
MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =     40976384
Number of free chunks       =           36
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =     40976384
Keepcost                    =      7859424
Max contiguous free mem     =      7859424
Allocated memory in use     =     33100600
Free memory                 =      7875784

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           48           1             48**
           72           1             72
          256          30           7920
         1024           1           1352
         2048           1           2376
         4096           1           4328
```

24 rows / 166 cols • SSH • Elapsed: 00:03:35 • Device Type: ASA

Note: Results appear highlighted in accordance with the colors assigned to each search term in the Highlighting area on the Settings tab. The search term that is currently selected is highlighted in red. For information on how to assign custom colors to your search terms, see Theme.

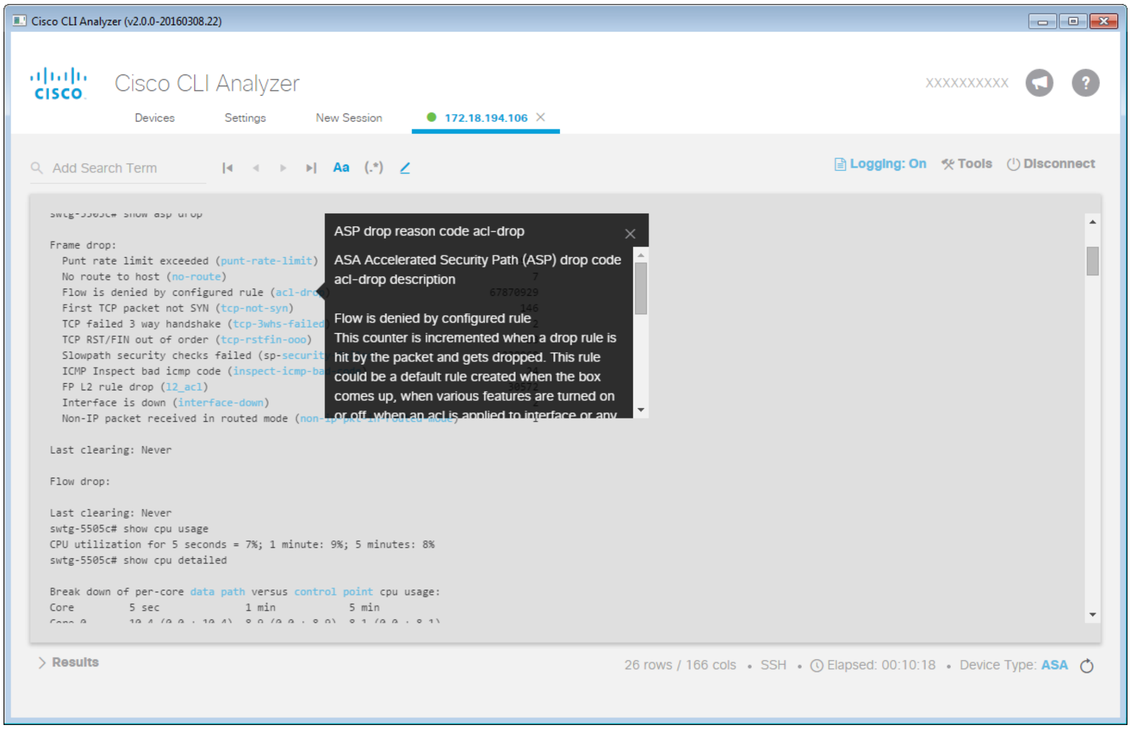
3. In order to navigate the search results, use these buttons:
   - Previous (◀)—Go to the previous match for the term.
   - Next (▶)—Go to the next occurrence for the matched term.
   - First (|◀)—Go to the first occurrence of the matched term within the output.
   - Last (▶|)—Go to the last occurrence of the matched term within the output.
4. In order to restrict search results to case sensitive matches, click the **Case Sensitive** button (**Aa**).
5. In order to enable or disable regular expressions, click the **RegEx** button ((.*)).

Note: RegEx is used in order to create wildcards or substitutions in your searches. For information on which expressions are supported, see Which expressions and characters are supported in the RegEx search feature?

6. In order to remove a search term, click the X for the search term in the search field.

Contextual Help and Highlighting

The Cisco CLI Analyzer provides a Contextual Help and Highlighting feature for certain commands. This feature highlights certain text in the CLI output and provides additional information about that text. In order to view contextual help, click the link that corresponds to the text for which you want to view additional information.



```
swtg-5505c# show asp drop

Frame drop:
  Punt rate limit exceeded (punt-rate-limit)
  No route to host (no-route)                                         7
  Flow is denied by configured rule (acl-drop)                 67870929
  First TCP packet not SYN (tcp-not-syn)                            146
  TCP failed 3 way handshake (tcp-3whs-failed)                        2
  TCP RST/FIN out of order (tcp-rstfin-ooo)
  Slowpath security checks failed (sp-securit
  ICMP Inspect bad icmp code (inspect-icmp-ba                        24
  FP L2 rule drop (l2_acl)                                        30572
  Interface is down (interface-down)                                  2
  Non-IP packet received in routed mode (non-                         1

Last clearing: Never

Flow drop:

Last clearing: Never
swtg-5505c# show cpu usage
CPU utilization for 5 seconds = 7%; 1 minute: 9%; 5 minutes: 8%
swtg-5505c# show cpu detailed

Break down of per-core data path versus control point cpu usage:
Core         5 sec              1 min              5 min
Core 0       10.4 (0.0 : 10.4)  8.0 (0.0 : 8.0)   8.1 (0.0 : 8.1)
```

ASP drop reason code acl-drop

ASA Accelerated Security Path (ASP) drop code acl-drop description

Flow is denied by configured rule
This counter is incremented when a drop rule is hit by the packet and gets dropped. This rule could be a default rule created when the box comes up, when various features are turned on or off, when an acl is applied to interface or any

Contextual Help and Highlighting is supported for these commands:

ASA Commands		
packet-tracer	show crypto ipsec sa	show nat
show access-list	show crypto isakmp sa	show nat detail
show asp drop	show crypto isakmp stats	show process
show blocks	show failover	show process cpu-hog
show capture	show failover history	show process cpu-usage
show conn	show interface	show running-config
show console-output	show kernel cgroup-controller detail	show scansafe statistics
show counters	show logging	show tech-support
show cpu detailed	show memory	show version
show cpu usage	show memory detail	write memory
show crypto ikev2 stats		write standby

IOS Commands

- show aaa servers
- show access-session
- show ap capwap summary
- show ap config general
- show ap dot11 24ghz coverage
- show ap dot11 24ghz network
- show ap dot11 24ghz summary
- show ap dot11 24ghz txpower
- show ap dot11 5ghz coverage
- show ap dot11 5ghz network
- show ap dot11 5ghz summary
- show ap dot11 5ghz txpower
- show ap groups
- show ap join stats summary
- show ap mac-address H.H.H join stats detailed
- show ap summary
- show atm pvc
- show authentication sessions
- show bgp
- show bgp () X:X:X:X::X
- show bgp (*) (vrf-vrf-name)?
- show bgp a.b.c.d
- show bgp internal
- show bgp neighbors
- show bgp summary
- show buffers
- show call active voice brief
- show call-manager-fallback
- show ccm-manager
- show ccm-manager music-on-hold
- show cellular
- show cellular [intf_num]
- show cellular profile
- show cem circuit
- show clock (detail)
- show controllers e1
- show controllers pos
- show controllers t1
- show controllers t3
- show controllers vdsl
- show crypto (gdoi|gkm) gm acl
- show crypto call admission statistics
- show crypto eli
- show crypto gdoi
- show crypto gdoi gm
- show crypto gdoi ks
- show crypto gdoi ks coop
- show crypto gdoi ks policy
- show crypto ikev2 sa
- show crypto ikev2 stats
- show crypto ipsec sa
- show crypto isakmp sa
- show crypto key mypubkey (rsa|ec|all)
- show crypto session
- show dial-peer voice summary
- show dot1x
- show dspfarm all
- show eigrp address-family ipv4 events
- show eigrp address-family ipv4 topology
- show eigrp address-family ipv6 events
- show eigrp address-family ipv6 topology
- show environment
- show fabric
- show interfaces
- show interfaces <int> counters
- show interfaces counters error
- show interfaces switching
- show ip bgp
- show ip bgp ?
- show ip bgp a.b.c.d
- show ip bgp internal
- show ip bgp neighbors
- show ip bgp summary show ip cef
- show ip device tracking
- show ip eigrp accounting
- show ip eigrp events
- show ip eigrp interfaces
- show ip eigrp neighbors
- show ip eigrp topology
- show ip interface
- show ip ospf database
- show ip ospf neighbors
- show ipv6 ospf statistic
- show ip ospf statistics
- show ip ospf statistics detail
- show ip route summary
- show ip traffic
- show ip wccp
- show ip(v6) eigrp traffic
- show ip(v6) ospf neighbor detail
- show ip(v6) protocols
- show ip(v6) route
- show ipv6 eigrp events
- show ipv6 eigrp interfaces
- show ipv6 eigrp neighbors
- show ipv6 eigrp topology
- show ipv6 interface
- show ipv6 ospf statistic detail
- show isdn service
- show isdn status
- show logging
- show mab
- show mac address-table
- show mac-address-table
- show macsec
- show memory
- show memory statistics
- show mgcp
- show netdr captured-packets
- show ospfv3 neighbor
- show ospfv3 neighbor detail
- show ospfv3 statistic
- show ospfv3 statistic detail
- show otv isis rib redistribution mac
- show platform
- show platform cpu packet buffered
- show platform hardware qfp active feature firewall drop
- show platform hardware qfp active feature ipsec datapath drops
- show platform hardware qfp active statistics drop
- show platform health
- show platform punt client
- show policy-firewall config
- show policy-firewall session
- show policy-map type inspect zone-pair sessions
- show ppp multilink
- show processes cpu
- show processes memory
- show redundancy states
- show run interface cellular
- show running-config
- show sccp connections
- show sip-ua calls
- show sip-ua status
- show spanning-tree
- show stcapp device summary
- show switch
- show switch stack-ports summary
- show tech-support
- show tech-support
- show tech-support wireless
- show telephony-service
- show version
- show voice call status
- show voice dsp group all
- show voice port summary
- show voice register global
- show voip rtp connections
- show vpdn tunnel
- show wireless client mac-address H.H.H detail
- show wireless client summary
- show wireless country configured
- show wireless detail
- show wireless mobility summary
- show wireless multicast
- show wireless summary
- show wireless wps summary
- show zone-pair security

IOS-XR Commands

admin show install
admin show version
show bgp all all summary
show bgp ipv4 unicast summary
show bgp ipv4 unicast summary
show bgp ipv6 unicast summary
show bgp summary
show bgp vpnv4 unicast summary
show bgp vpnv6 unicast summary
show controllers FortyGigE
show controllers GigabitEthernet
show controllers SONET
show controllers TenGigE
show controllers fabric fia stats
show controllers hundredGigE
show controllers np counters
show controllers pse statistics
show install
show interfaces
show logging
show platform
show processes
show processes blocked
show redundancy
show snmp
show snmp
show snmp request drop summary
show version

NX-OS Commands

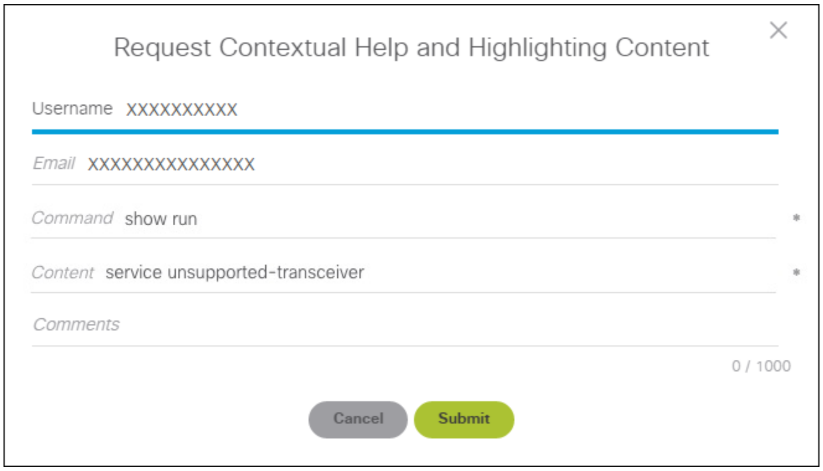
show accounting log
show copp status
show diagnostic content module
show diagnostic content module all
show diagnostic result module
show diagnostic result module all
show environment
show errdisable detect
show errdisable recovery
show fabricpath isis adjacency
show fabricpath isis route
show fcoe
show fex
show hardware internal forwarding rate-limiter usage
show hardware internal interface indiscard-stats front-port
show hardware ip verify
show hardware profile forwarding-mode
show hardware rate-limiter
show hsrp
show hsrp brief
show interface
show interface counters errors
show interface counters storm-control
show interface ethernet
show interface fc
show interface fex-fabric
show interface status err-disabled
show interface trunk
show interface vfc
show ip igmp groups
show ip igmp route
show ip traffic
show license usage
show logging log
show logging logfile
show module
show monitor
show monitor session
show otv
show otv isis adjacency
show otv site
show platform fwm info asic-errors
show platform fwm info pif
show platform software fcoe_mgr event-history errors
show policy-map interface
show policy-map interface control-plane
show policy-map interface type queuing
show port-channel database
show port-channel summary
show processes cpu
show processes log
show redundancy status
show spanning-tree
show spanning-tree detail
show switching-mode
show system internal forwarding ipv4 route summary
show system internal l2fm l2dbg macdb
show system internal l2fm l2dbg portdb
show system redundancy status
show system reset-reason
show user-account
show vdc
show version
show version
show vpc
show vrrp
show vtp status

Context Menu Options

The Cisco CLI Analyzer provides right-click menu options appropriate to the console text you highlight.

These options are available when you highlight and right-click any text in the console:

- **Copy**—Copies the selected text to the clipboard.
- **Paste**—Pastes text copied to the clipboard at the command prompt.
- **Copy & Paste**—Copies the selected text and pastes it at the command prompt as a single action.
- **Add Search Term**—Adds the selected text as a search term and highlights it.
- **Search Cisco.com**—Searches the Cisco.com web site for information about the highlighted text.
- **Request CHH Content**—Opens the *Request Contextual Help and Highlighting Content* dialog window, which you can use in order to submit a request for additional CHH content.



Request Contextual Help and Highlighting Content

Username XXXXXXXXXX

Email XXXXXXXXXXXXXXX

Command show run *

Content service unsupported-transceiver *

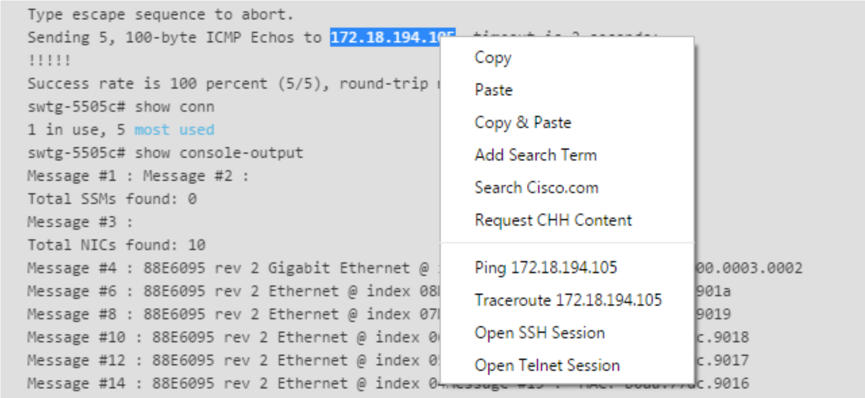
Comments

0 / 1000

These additional options are available when you highlight and right-click an IP address:

- **Ping**—Runs the ping command on the selected IP address.
- **Traceroute**—Runs the traceroute command on the selected IP address.
- **Open SSH Session**—Creates a new connection to the selected IP address with the SSH protocol.
- **Open Telnet Session**—Creates a new connection to the selected IP address with the Telnet protocol.

Note: You can double-click a term or IP address in the console to select it quickly, so you do not have to drag the cursor across the text you want to highlight.



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.194.10
!!!!!
Success rate is 100 percent (5/5), round-trip
swtg-5505c# show conn
1 in use, 5 most used
swtg-5505c# show console-output
Message #1 : Message #2 :
Total SSMs found: 0
Message #3 :
Total NICs found: 10
Message #4 : 88E6095 rev 2 Gigabit Ethernet @                    00.0003.0002
Message #6 : 88E6095 rev 2 Ethernet @ index 08                   901a
Message #8 : 88E6095 rev 2 Ethernet @ index 07                   9019
Message #10 : 88E6095 rev 2 Ethernet @ index 0                   c.9018
Message #12 : 88E6095 rev 2 Ethernet @ index 0                   c.9017
Message #14 : 88E6095 rev 2 Ethernet @ index 0                   c.9016
```

Frequently Asked Questions

Why do I need to log in with my Cisco.com account for some features?

You must have a valid Cisco.com account in order to use the Cisco CLI Analyzer. If you do not have a valid Cisco.com account, you must register on the Cisco.com Registration page and associate a Service Contract to your Cisco.com profile.

Why am I still unable to access the Cisco CLI Analyzer after I have entered my CCO account information?

Ensure your user name and password are correct and that you have an active support contract associated with your Cisco.com account. If you have verified these items and you are still unable to access the Cisco CLI Analyzer, use the Feedback form as described in Submit Comments and Questions.

How do I request features or provide product feedback?

In order to request additional features or provide product feedback, use the Feedback form as described in Submit Comments and Questions.

Why does ASA Traceback Decoder state that the crash.txt file cannot be found?

If your ASA appears to have crashed and rebooted, ASA Traceback Decoder might state that the crash.txt file cannot be found.

By default, an ASA saves crash information to the flash memory unless crashinfo save disable is added to the ASA config file. When this command is added to the config file, the file cannot be saved. In order to resolve this issue, ensure that the command is not enabled.

Note: In order to set the default behavior, add `no crashinfo save disable`. If a crash file is present, it will be stored in the local flash as “crash.txt.”

Which operating systems are supported in the Cisco CLI Analyzer?

For information on which operating systems are supported in the Cisco CLI Analyzer, see System Requirements.

What terminal emulation is supported in the Cisco CLI Analyzer?

The Cisco CLI Analyzer supports terminal emulator VT100.

What protocols are supported in the Cisco CLI Analyzer?

The Cisco CLI Analyzer supports Telnet and SSH version 2.

Which expressions and characters are supported in the RegEx search feature?

The Cisco CLI Analyzer RegEx search feature supports Javascript RegExp brackets, metacharacters, and quantifiers.

Brackets	**Description**
[abc]	Find any character that is specified between the brackets
[^abc]	Find any character that is NOT specified between the brackets
[0-9]	Find any digit within the range specified between the brackets
[^0-9]	Find any digit NOT within the range specified between the brackets
(x|y)	Find the specified characters

Metacharacter	**Description**
.	Find a single character (except newline or line terminator)
\w	Find a word character
\W	Find a non-word character
\d	Find a digit
\D	Find a non-digit character
\s	Find a whitespace character
\S	Find a non-whitespace character
\b	Find a match at the beginning/end of a word
\B	Find a match not at the beginning/end of a word
\0	Find a NUL character
\n	Find a new line character
\f	Find a form feed character
\r	Find a carriage return character
\t	Find a tab character
\v	Find a vertical tab character
\xxx	Find the character specified by an octal number xxx
\xdd	Find the character specified by a hexadecimal number dd
\uxxxx	Find the Unicode character specified by a hexadecimal number xxxx

Quantifier	**Description**
n+	Matches any string that contains at least one n
n*	Matches any string that contains zero or more occurrences of n
n?	Matches any string that contains zero or one occurrences of n
n{X}	Matches any string that contains a sequence of X n's
n{X,Y}	Matches any string that contains a sequence of X to Y n's
n{X,}	Matches any string that contains a sequence of at least X n's
n$	Matches any string with n at the end of it
^n	Matches any string with n at the beginning of it
?=n	Matches any string that is followed by a specific string n
!=n	Matches any string that is not followed by a specific string n