ı|ııı|ıı
CISCO
The bridge to possible

Cisco CLI Analyzer

User Guide

October 2025

Contents

Overview of the Cisco CLI Analyzer

New Features for v3.7.3

The latest version of the Cisco CLI Analyzer updates functionality and addresses performance items:

- Security updates and fixes
- Fixed a bug where the close button for CHH pop-ups was non-functional
- Fixed a bug where the Bulk Credential Add feature would only affect the first device in the list
- Added device identification for Cisco Secure Firewall 3100 Series

For information on functionality of previous versions, please check the [Frequently Asked Questions](#).

About the Cisco CLI Analyzer

The Cisco CLI Analyzer is a smart SSH client designed to help troubleshoot and check the overall health of your supported devices. For a full list of tools included in the Cisco CLI Analyzer, see [Tool Descriptions](#).

Note: You must have a valid Cisco.com account to use the Cisco CLI Analyzer. If you do not have a valid Cisco.com account, [register](#) on Cisco.com and then [associate a service contract](#) to your profile.

System Requirements

Ensure that your system meets these minimum software and hardware requirements to run the Cisco CLI Analyzer.

Software

- Windows 10 x64 or Windows 11
- macOS version 13 (Ventura)

Hardware

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

Check the [version information](#) to ensure that you install the version of the application that works with your system hardware.

Versions of the Cisco CLI Analyzer

The Cisco CLI Analyzer offers several versions to best work with different processing hardware. Check below for information on installing or upgrading the application on your system, and refer to the [Frequently Asked Questions](#) for information on earlier versions.

Windows-Based Computers

If you are running Windows 10 or Windows 11, use the appropriate Windows installation files to download and install the latest version.

Mac Computers

The Cisco CLI Analyzer supports two different architectures – Intel-based (x64) and ARM-based (M-Series).

Intel-Based Macs

If you are running an Intel-based macOS, follow the standard upgrade process and ensure that you use **only** the Intel version of the macOS files to download and install the latest version.

ARM-Based Macs (e.g., M-Series)

If you are running an ARM-based macOS, download the ARM-based version of the macOS files and perform a fresh installation. This process will retain your individual settings.

Note: If you use the files that do not match your architecture, the installation will fail, and you'll need to reboot your macOS before performing a fresh installation with correct files for your version.

Download and Install the Cisco CLI Analyzer

Complete these steps to download and install the Cisco CLI Analyzer.

Note: Installing a new version of this application will replace any previous versions on your computer.

1. From the [Software Download area for the Cisco CLI Analyzer](#), click the link for your operating system.
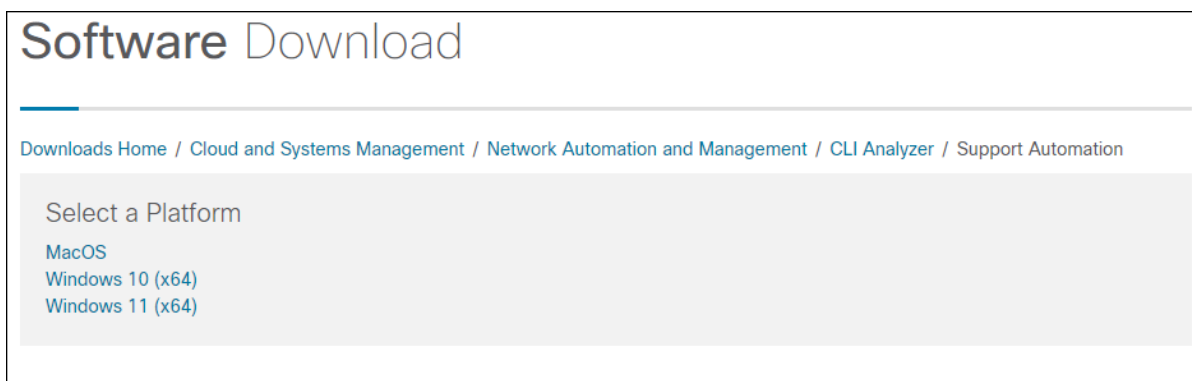
2. Click on the release number for the version you want to download. The latest release always contains the most current features and functionality.

3. Click the **Download** icon.

Software Download

Downloads Home / Cloud and Systems Management / Network Automation and Management / CLI Analyzer / Support Automation / Windows 11 (x64)- 3.7.0

Search...

Expand All | Collapse All

Latest Release

3.7.0

All Release

3

3.7.0

3.6.8

CLI Analyzer

Release 3.7.0
🔔 My Notifications

Related Links and Documentation
CLI Analyzer Overview
CLI Analyzer Help

File Information	Release Date	Size
Cisco CLI Analyzer SSH client software Cisco-CLI-Analyzer.3-7-0.x64.msi	10-May-2023	132.32 MB

4. Follow the instructions on the Strong Encryption Eligibility dialog, then click **Accept**.

5. Review the linked documents on the Cisco's End User Software License Agreement dialog, then click **Accept License Agreement**.

6. After the file downloads, double-click the executable to launch the setup wizard, then click **Next** to begin installation.
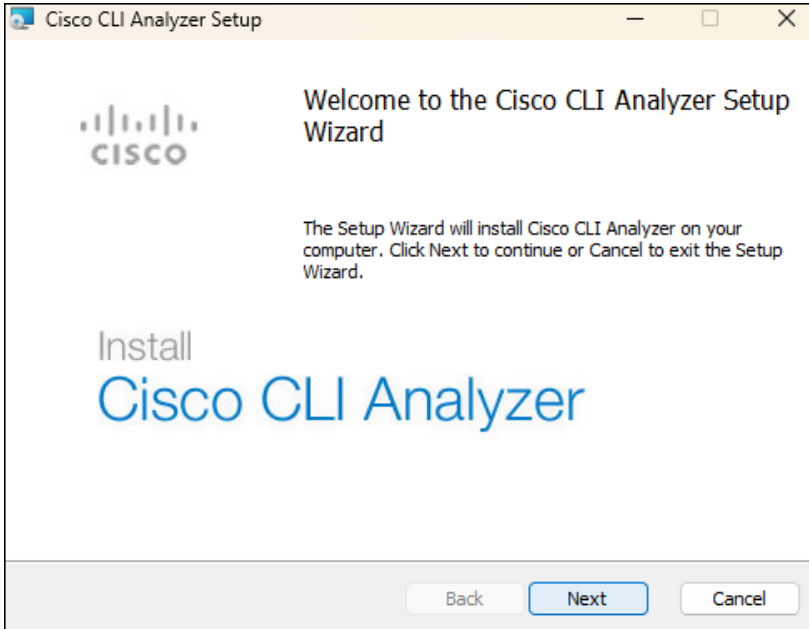
7. Configure the options to set the installation location, create a shortcut, or install for multiple user profiles. Click **Next**.
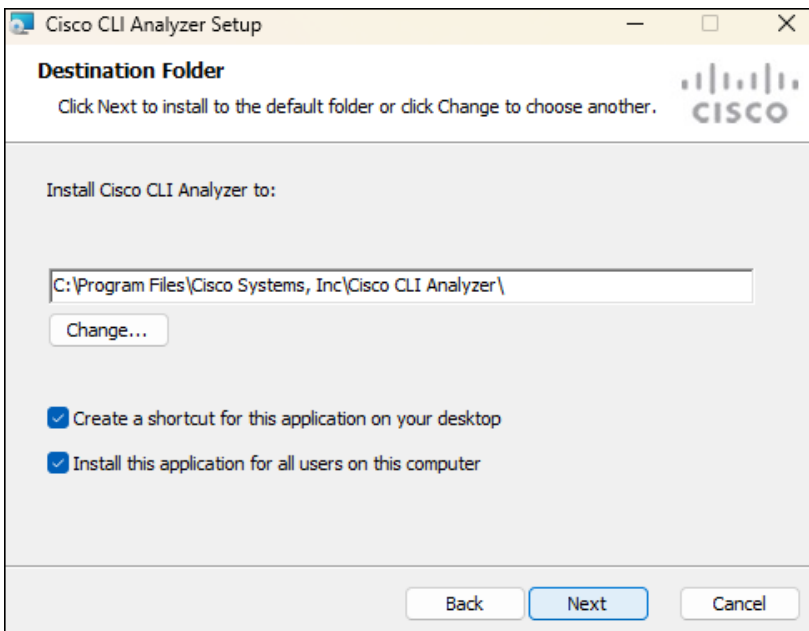
8. Click **Install** to set up the Cisco CLI Analyzer on your computer.
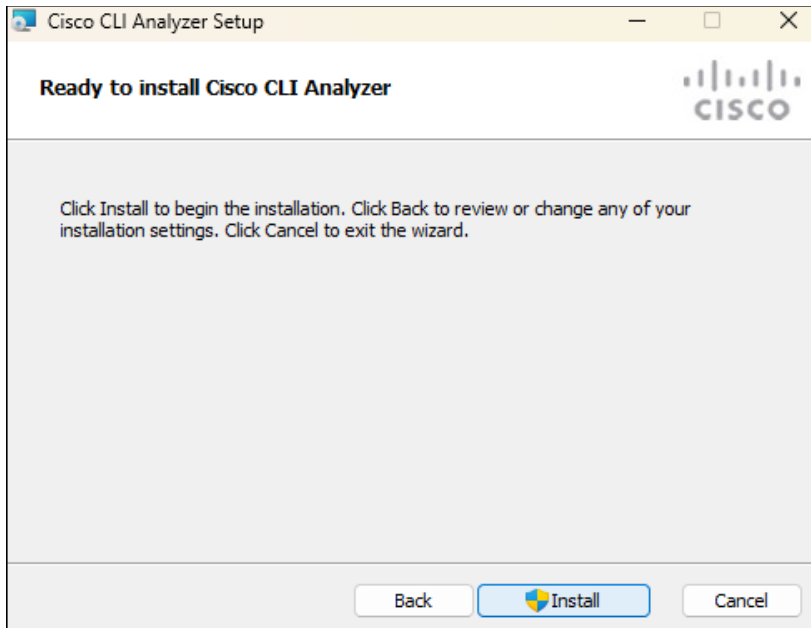
9. After installation is complete, click **Finish** to close the setup wizard.
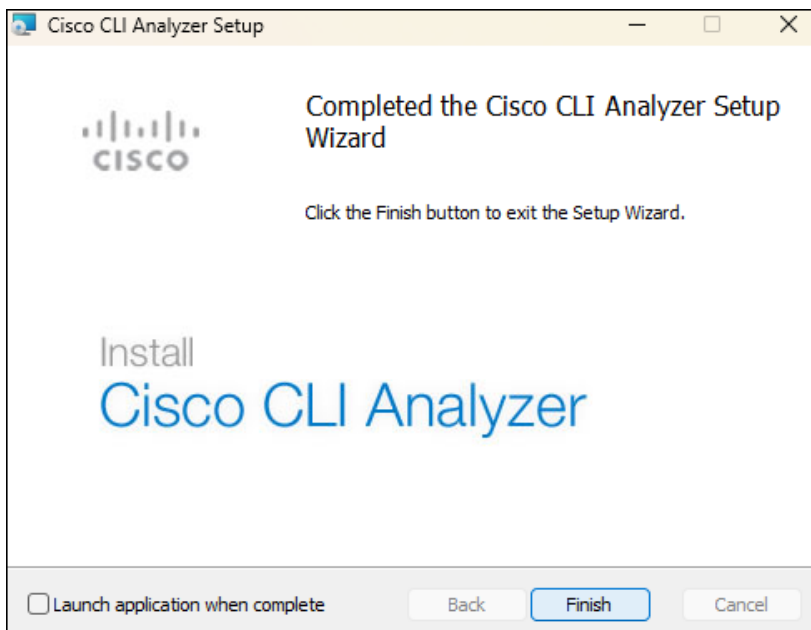
Note: If you need to repair the Cisco CLI Analyzer or want to remove the application, run the executable file again.
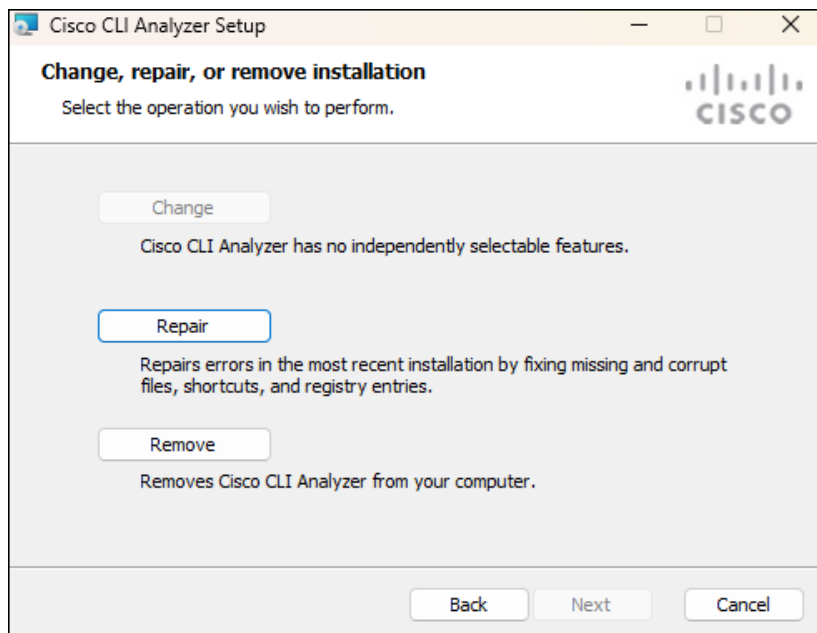
Supported Devices and Platforms

The Cisco CLI Analyzer identifies the device details and provides analysis tools for these devices and operating systems.

Note: Not every analysis tool is available on every platform.

- ACI-OS
- AP-COS
- APIC
- ASA
- DNAC
- Hyperflex

- IOS
- IOS-XE
- IOS-XR ISE
- NGFW
- NX-OS

- SMB
- StarOS
- UCS (B and C Series)
- VxWorks
- WLC

External Site Access Requirements

Some tools temporarily upload files to be processed to a file management system. Cisco CLI Analyzer versions 3.6.6 and later upload files to Amazon Web Services (AWS) S3.

Note: If your organization enforces access lists for external sites, you must permit access to **cxd-prd-files-bucket.s3-accelerate.amazonaws.com**.

Note: If your access list uses IP addresses, refer to the AWS documentation on AWS IP address ranges.

Tool Descriptions

If you have ideas for new tools or suggestions to enhance these tools, [send us feedback](#).

BGP Top Talkers

Supported platforms: IOS-XR

This tool helps determine which Border Gateway Protocol (BGP) peers have the highest rates of messages sent or received during a certain period of time.

Case Create

Supported platforms: ASA, IOS, IOS-XE, IOS-XR

This tool automates the collection of support case data for supported platforms. For devices on other platforms (FX-OS, NX-OS, UCS), you can [create a case](#) manually.

Configuration Difference

Supported platforms: ASA, IOS, IOS-XR

This tool compares the startup configuration and running configuration of the device and color-codes them to highlight differences. It also allows you to download each configuration as a text file.

Crashinfo Analyzer

Supported platforms: IOS, IOS-XE

This tool analyzes a crashinfo file that you upload and compares the contents of the file with known issues to determine the cause of the system reset.

Firewall Top Talkers

Supported platforms: ASA

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 to see how much traffic each connection passed in the time between the outputs. It also identifies new connections 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.

Health Diagnostics

Supported platforms: NX-OS

This tool detects and reports known issues such as system problems, configuration mistakes, and best practice violations, based on Cisco TAC knowledge.

IP Multicast Analysis

Supported platforms: IOS, IOS-XE

This tool provides an analysis of the global IPv4 multicast traffic that is flowing through the device, as well as control plane traffic.

IP Route Analysis

Supported platforms: IOS, IOS-XE, NX-OS

This tool provides four different reports based on the analysis of IPv4 or IPv6 routes. (The NX-OS platform supports only IPv4 routes.)

- Route instability: checks for routing changes within a 60 second interval
- Route summary with next hop
- Routing table subnet prefix distribution
- Summary of administrative distances for all protocols

Note: If the routing table has 100,000 routes or more, this tool will not work.

L2VPN Service Check

Supported platforms: IOS-XR

This tool allows you to select an L2VPN Bridge-Domain or Xconnect. The tool then runs several **show** commands to determine the status of the L2VPN service.

L2VPN Top Talkers

Supported platforms: IOS-XR

This tool helps determine which Layer 2 VPN point-to-point circuits and Bridge-Domains have the highest packet rates during a certain period of time.

LPTS Top Talkers

Supported platforms: IOS-XR

This tool helps determine the types of traffic that are handed off from hardware to software processing and their rates. Local Packet Transport Services (LPTS) is the router feature that decides which traffic (such as Telnet, SSH, and SNMP) must be handed off, and limits rates in order not to overload the software.

(See a demonstration video of IOS-XR tools.)

Packet Capture

Supported platforms: ASA, IOS, IOS-XE, NX-OS

This tool helps you set up and perform a packet capture and analyze the results. You can specify the kind of packets to capture based on the device platform, decode captured packets in the terminal, and view traffic analytics.

Packet Tracer

Supported platforms: ASA

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.

Show Run Diagnostics

Supported platforms: AireOS (on Wireless LAN Controller)

Show Tech Diagnostics

Supported platforms: AireOS (on Wireless LAN Controller)

System Diagnostics

Supported platforms: ASA, IOS, IOS-XE, IOS-XR

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

Note: This analysis sends the output of the **show tech-support** command to Cisco to be processed. IOS-XR analysis will vary in the use of **show** commands.

TAC Data Collection

Supported platforms: ASA, IOS, IOS-XE, IOS-XR, NX-OS, UCS, AireOS (on Wireless LAN Controller)

This tool automates the collection of diagnostic data needed to resolve support cases. A TAC engineer provides a TaskID code to you. When you enter the TaskID into the TAC Data Collection tool, the Cisco CLI Analyzer automatically performs the diagnostic commands and uploads the output to the support case.

(See a [demonstration video](#) of this tool.)

Traceback Analyzer

Supported platforms: ASA

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.

Unused Policy Detector

Supported platforms: ASA

This tool looks for unused configuration policies such as unused access-lists, object-groups, and objects. Some of these could also indicate misconfigurations. This tool collects the output of the commands **show run** and **show access-list | excl ^ |elem**. The output is uploaded to Cisco for analysis. Full tool functionality is available in ASA releases 9.x and above.

Upgrade Helper

Supported platforms: NX-OS

This tool provides supported upgrade paths for NX-OS 7K platforms.

Zone Based Firewall Visualizer

Supported platforms: IOS, IOS-XE

This tool creates a diagram that illustrates the complex and nested zone-based firewall policies on the router.

Get Started

After installing the Cisco CLI Analyzer, you can configure application settings and view and manage devices.

Open the Cisco CLI Analyzer

Click the **Cisco CLI Analyzer** icon on your computer's desktop to open the Cisco CLI Analyzer application.

As of version 3.7.2, the Cisco CLI Analyzer uses your system browser to log in to Cisco. When prompted, enter your Cisco.com username/email and password, then click the **Open Cisco CLI Analyzer** button to launch the application.

Note: To bypass the authentication confirmation in the future, check the **Always allow cway.cisco.com to open link...** check box. (See the Feature Guide in the application for more details.)

Note: If application settings prompt you for a master password, enter the password and click **OK**.

The Cisco CLI Analyzer interface appears, displaying the Devices window as the application home page.

View Your Devices

The Devices window displays information about each of your devices at a glance. Here you can see device information in list or tile format, initiate connections, and perform other functions. The tabs at the top of the sidebar allow you to switch between the Devices window and other application functions such as Settings and File Analysis.
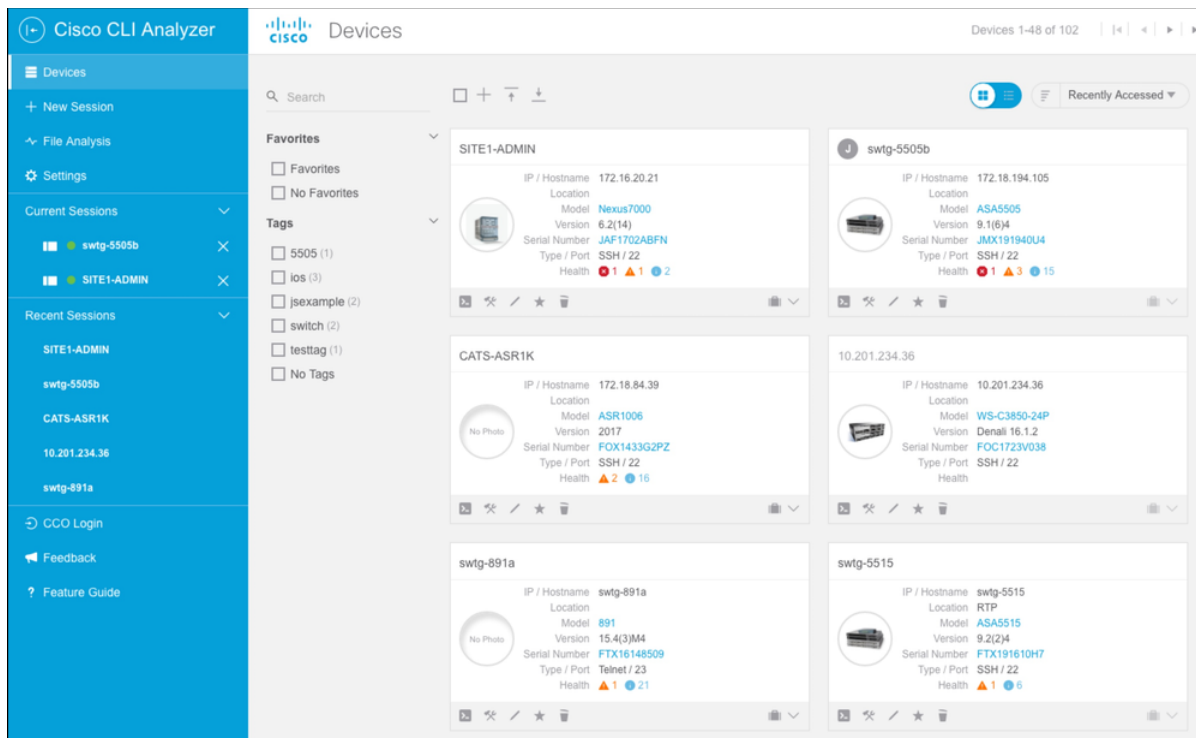
In Grid View, information appears on device cards along with an image of the device (when available). The toolbar at the bottom of the device card provides options to open a session, view tool results, open a support case, and perform other functions.

Device cards also display the health of each device, according to the most recent scan. Click the Health information to open the Tool Results window for additional details.

Note: Supported devices include ASA, IOS, IOS-XE, IOS-XR, NX-OS, and WLC. The health information is based on the System Diagnostics tool results, except for WLC devices, which use Show Tech Diagnostics tool results.
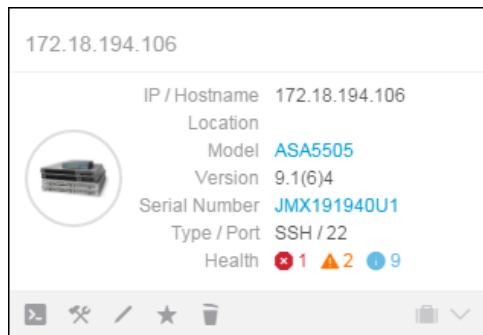
The Devices window features:

- **Current Sessions (in sidebar):** Click a device to switch to the console window for that device. A green circle appears beside devices with an active connection; a red circle appears beside disconnected devices. Click the X beside a device to close the current session and remove it from the list.

- **Recent Sessions (in sidebar):** Click a device to open the Session Login screen. Hover the pointer over a device to show the time and date of the last active session with that device. Click the X beside a device to remove the recent session from the list.

- **Toolbar:** The toolbar provides options that allow you to search and sort the device list, to perform bulk actions on selected devices, and to add, import, and export devices.

- **Filters:** Check filter check boxes to hide devices that do not match the filter criteria. Filters can be based on the devices that are marked as favorites or on tags added to devices. Click the **Filter** button 🎚 Filter above the device list to show or hide available filters.

  Check a check box in the list of filters to show only devices that match your selected filter. (For example, check the **No Favorites** check box to show only devices that are not marked as Favorites.)

- **Adjustable Sidebar:** Click the ◀ and ▶ buttons to collapse and expand the sidebar.

You can perform these actions on each device in your list:

- Click the **Connect** icon (▶_) to connect to that device.

- Click the **Tool Results** icon (🛠) to view the tool results for the device in the Tools Results window.

- Click the **Edit** icon (✏) to open the Edit Device window, where you can update device information.

- Click the **Toggle Favorite** icon (★) to mark the device as a Favorite. Click the button again to remove the device from Favorites.

- Click the **Delete Device** icon (🗑) to remove the device from your device list.

- Click the **Support Cases** icon (🗄) for devices with support coverage to open a support case or view/update existing cases.

- Click the hyperlinked serial number of a device to check the service contract status of that device. The Cisco Device Coverage Checker tool opens in a browser window. (See a [demonstration video](#) of this feature.)

- To select a device in Grid View, hover the mouse pointer over a device card and click the check mark (✓) in the upper right corner. To select a device in List View, click the check box (☐) next to the device. When the device is highlighted, the Bulk Actions button becomes available. To deselect a device, click anywhere on the device card to deselect it in Grid View, or uncheck the check box in List View.

- To highlight all the devices in the list, check the **Select All** check box (☐). The check box indicates that all devices are selected (☑) and the Bulk Actions button becomes available. Click any individual device card to deselect that device.

- With one or more devices selected, click the **Bulk Actions** button (③ Bulk Actions ∨) and then choose an option in the drop-down list to perform that action (Connect, Check Coverage, Apply Credential Profile, Refresh Coverage, Delete Devices, Add Tags, or Delete Tags).

- To sort devices into a specific order, click the sorting menu in the upper right (Device Name ▾) and choose a property from the drop-down list. In List View, click a column heading to sort by that property.

- Click the sorting icons to toggle between descending sort order (≣) and ascending sort order (☰).

- Check a check box in the list of filters to show only devices that match your selected filter. (For example, check the **No Favorites** check box to show only devices that are not marked as Favorites.)

- Enter a search term in the Search field and press **Enter** to search the device list.

Configure Application Settings

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

The settings appear on these five tabs.

- [General tab](#)
- [Connection tab](#)
- [Security tab](#)
- [Display tab](#)
- [Advanced tab](#)

Configure the General Tab

These settings affect multiple areas of functionality.
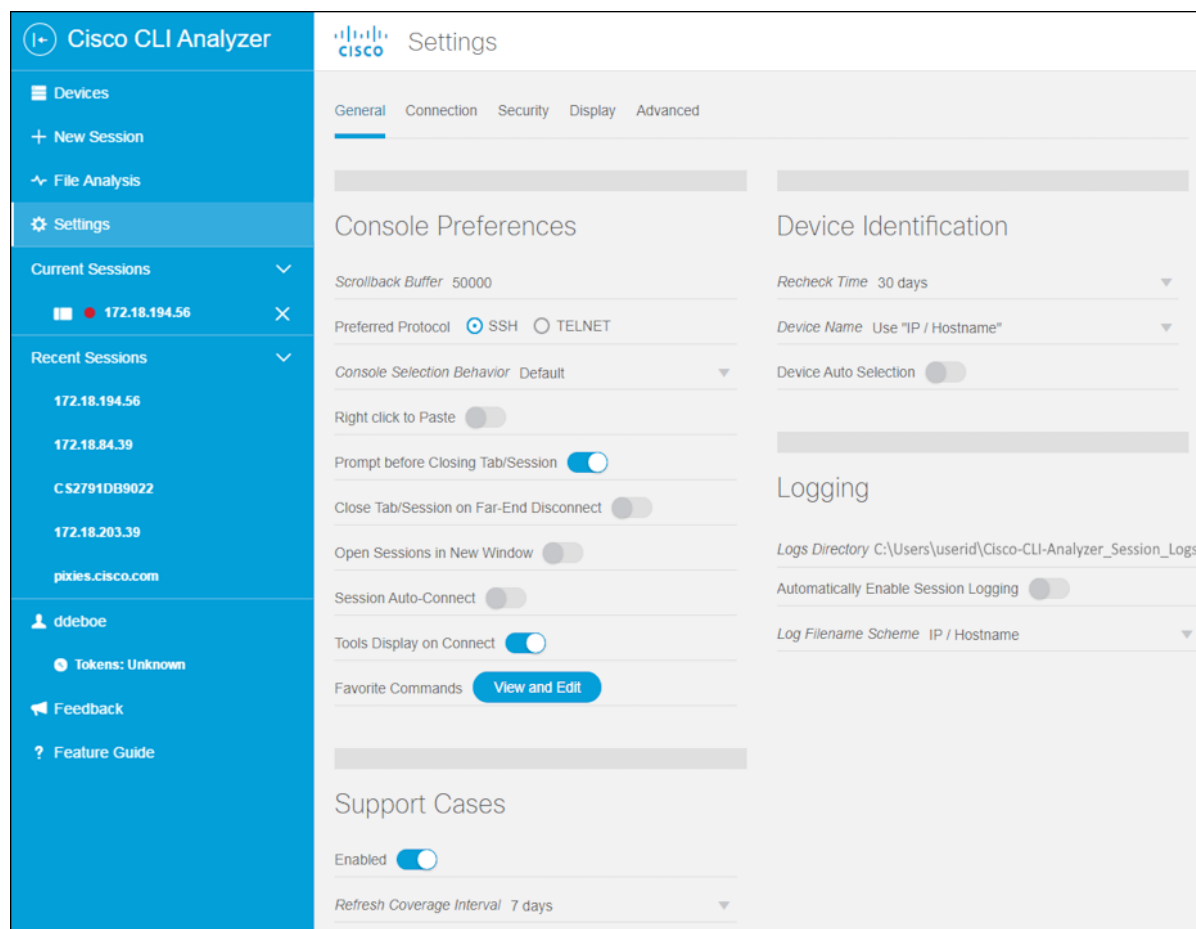
Console Preferences

- **Scrollback Buffer:** You can configure the number of command lines that are retained in memory. To configure the scrollback buffer, enter a number between 100 and 50,000.

- **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.

- **Console Selection Behavior:** Choose your preferred experience when you use the mouse 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.

- **Right click to Paste:** Click the toggle button to enable or disable the ability to paste clipboard content into the console window with the right mouse button. (When this feature is enabled, the context menu does not appear when you right-click inside the console window.)

- **Prompt Before Closing Tab/Session:** Click the toggle button to enable or disable the End Session dialog window. This window displays when you close the tab for a current session and prompts you to confirm whether you want to close the session.

- **Close Tab/Session on Far-End Disconnect:** Click the toggle button to enable or disable the option to close a device session tab automatically when the connection is terminated at the device end.

- **Open Sessions in New Window:** Click the toggle button to enable or disable the option to open new device sessions in a separate window by default. Regardless of the default setting, you can always manually detach console windows and reattach them to the main application window.

- **Session Auto-Connect:** Click the toggle button to enable or disable the option to skip the session login screen when user credentials are remembered. When the option is disabled, the login screen always appears when a new session is initiated.

- **Tools Display on Connect:** Click the toggle button to show or hide analysis tools in a new session. If the tools panel is hidden when a session opens, click the **Tools** icon (⚙) to show the panel.

- **Favorite Commands:** Click the **View and Edit** button to open the Favorite Commands window. Use the tabs at the top of the window to configure commands for the chosen type of device. Click a command, then click the up and down arrow buttons to move the command within the list; this changes the number of its associated command key. (See a demonstration video of this feature.)
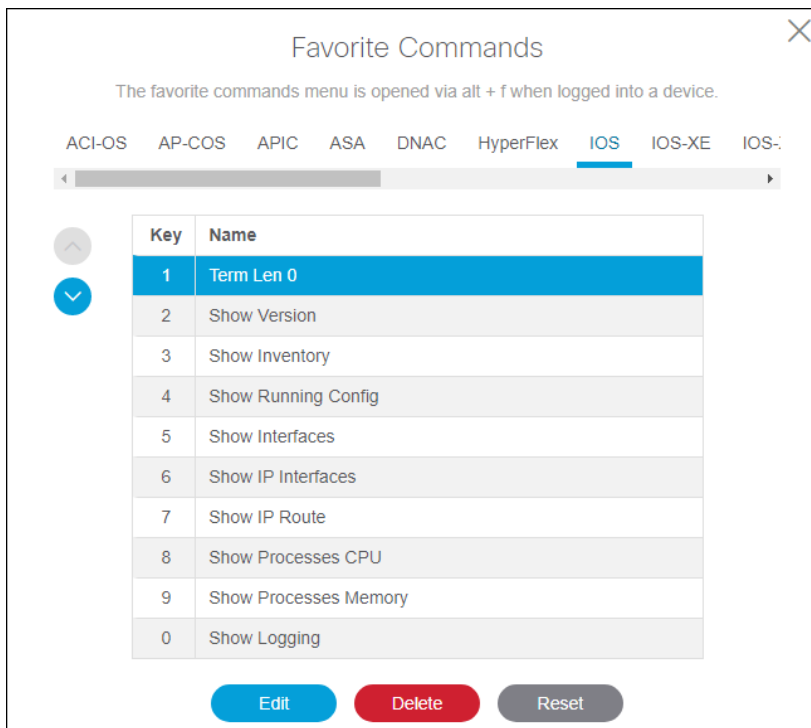
Select a command in the list and click **Edit** to modify the command and/or its name. You can enter commands on multiple lines.
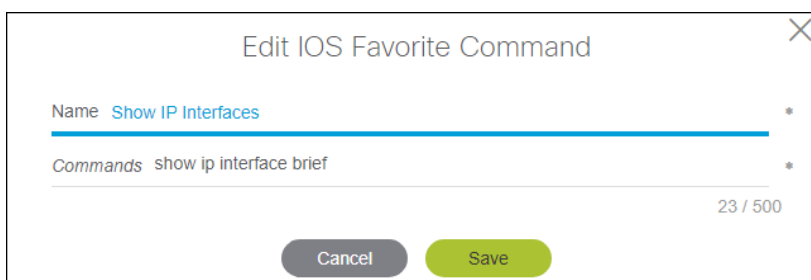
In a console session, click the **Favorites** icon (⭐)on the toolbar to select from a list of favorite commands. Alternatively, press **Alt+F** to display the list of commands.
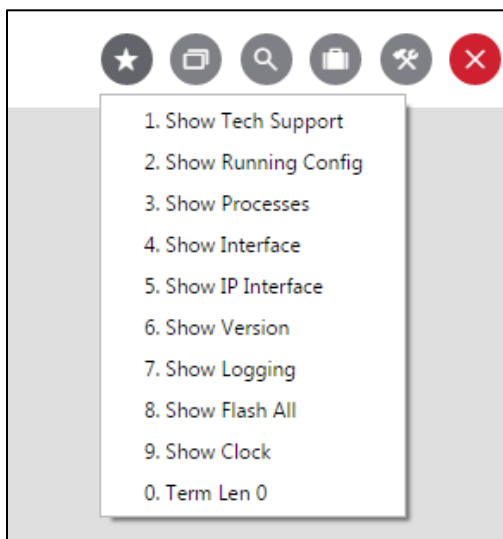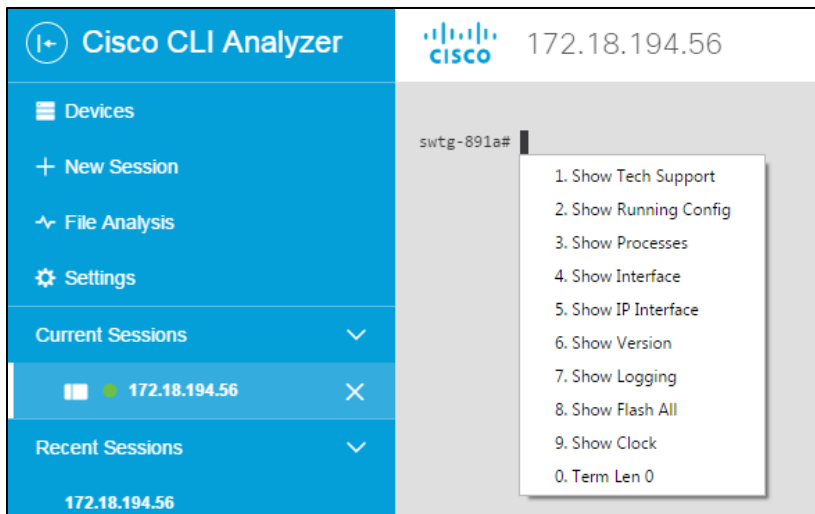
Support Cases

- **Enabled:** Click the toggle button to enable or disable the creation of support cases. This feature is enabled by default.

- **Refresh Coverage Interval:** Choose how frequently the Cisco CLI Analyzer should check support coverage on devices and update the information on the Devices list. You can also refresh coverage manually for selected devices with the **Bulk Actions** button.

Device Identification

- **Recheck Time:** Choose the number of days to wait between automatic executions of the **show version** (or appropriate) command. (Default = 30 days.) If you choose **Always Check**, the command runs automatically at the beginning of every device session.

- **Device Name:** Choose whether new devices that you add to the list are named by IP address or by the device name from the router.

Logging

- **Logs Directory:** By default, log files are saved in these locations:

  - **Windows:** C:\Users\<userid>\Cisco-CLI-Analyzer_Session_Logs

  - **macOS**: /Users/<userid>/Cisco-CLI-Analyzer_Session_Logs

  To choose a different folder, click the path that is currently displayed. Browse to the desired folder, select it, and click **OK**.

- **Automatically Enable Session Logging:** Click the toggle button 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.

- **Log Filename Scheme:** Choose whether to name log files by the device's IP address or by the device name from the router.

Configure the Connection Tab

These settings affect the initiation and sharing of device sessions.

Serial Connection Defaults

Note: TAC tools are not available in device sessions that use a serial connection.

- **Port Name:** Choose the COM port to use for serial connections or enter a port number manually. The drop-down list shows only active COM ports that are detected on the system.
- **Baud Rate:** Choose the baud rate to use for serial connections. If the console window does not display its contents correctly, you might need to adjust this value.
- **Data Bits:** Enter the number of data bits to use, or click the up and down arrows to adjust the number of bits.
- **Stop Bits:** Enter the number of stop bits to use, or click the up and down arrows to adjust the number of bits.
- **Parity:** Choose the parity type to use for serial connections.
- **Flow Control:** Choose the flow control type(s) to use for serial connections.

Session Sharing

- **Enabled:** Click the toggle button to enable shared device sessions.
- **Port:** Enter the port number to use for shared device sessions. (Session Sharing must be disabled to change the port number.) You must provide this port number to remote users who want to connect to a shared session.
- **Remote Logging Enabled:** When enabled, remote users have the option to log the device session.

Send KeepAlive String

- **SSH Enabled:** Click the toggle button to enable or disable KeepAlive strings in SSH sessions.
- **Telnet Enabled:** Click the toggle button to enable or disable KeepAlive strings in Telnet sessions.
- **String:** Type the character(s) to send in the KeepAlive string. By default, the string is a single space.
- **Interval (seconds):** Enter or select the number of seconds between each KeepAlive string.

Send SSH KeepAlive Packets

This option is useful when, in between the Cisco CLI Analyzer and the SSH server, there are NAT/routers that drop connections after a period of inactivity.

Note: This setting has no effect on the session timeout for far-end Cisco devices.

- **Enabled:** Click the toggle button to enable or disable KeepAlive packets in SSH sessions.
- **Interval (seconds):** Enter or select the number of seconds between each KeepAlive packet.

Ignore SSH-KeyScan Failures

Note: This override has no effect on devices with a Jump Server Profile.

- **Enabled:** Click the toggle button to ignore SSH-KeyScan failures for all devices. This option globally disables the prompt that is displayed when the Cisco CLI Analyzer application cannot retrieve the RSA Host Key for a device.

Configure the Security Tab

These settings affect the credentials that are used to connect to devices.
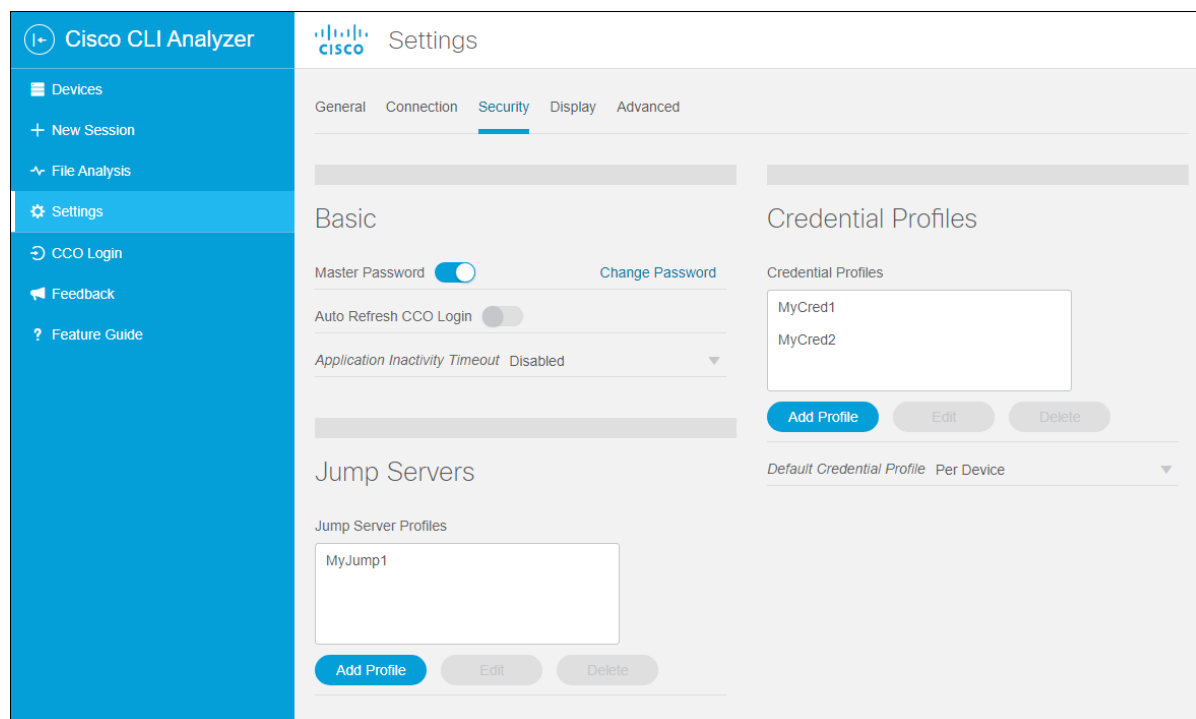
Basic

- **Master Password:** Click the toggle button to allow the Cisco CLI Analyzer to save a master password. The 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) 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.

  To change the password, click **Change Password**. Enter the old master password and the new one.

- **Auto Refresh CCO Login:** When this setting is enabled, the Cisco CLI Analyzer encrypts and stores CCO login information for 30 days. During that time, the application does not prompt you to enter your CCO login to access features that require it.

  Note: This feature requires that the Master Password is enabled.

- **Application Inactivity Timeout:** Choose the duration of inactivity before which the application will enter locked mode, or choose **Disabled** to disable the timeout feature. When the application is locked, you must enter the master password to unlock it. If you do not have the master password, you can close the application and reopen it, and then clear the master password.

  Note: This feature requires that the Master Password is enabled.

Jump Servers

Jump server profiles contain the credentials needed to connect to a jump server and the commands to run on the server after connection. You can create and edit profiles based on your devices and needs.

1. To create a profile, click the **Add Profile** button in the Jump Servers area.

2. Enter the jump server's name and IP address, the port number and connection type to use, and the username and password.

3. In the Commands area, enter the commands that you want to run.

    Note: Versions 3.5 and later support regex values in the expect string.

    *   Use **-r** to indicate that the value is a regular expression.

    *   Use **-i** to indicate case insensitivity.

4. Click the **Add Profile** button.
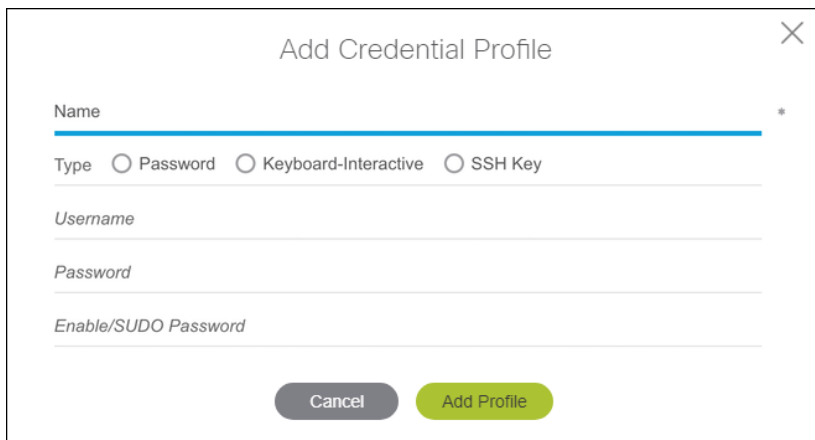
Note: For most devices and connections, the Keyboard Interactive feature should be off. Please check the Frequently Asked Questions for more information.

Credential Profiles

- **Credential Profiles:** Create and manage user profiles that you can use to initiate device sessions. To create a profile, click **Add Profile** in the Credential Profiles section, then enter a name for the profile and choose the type of credentials used to access the device.
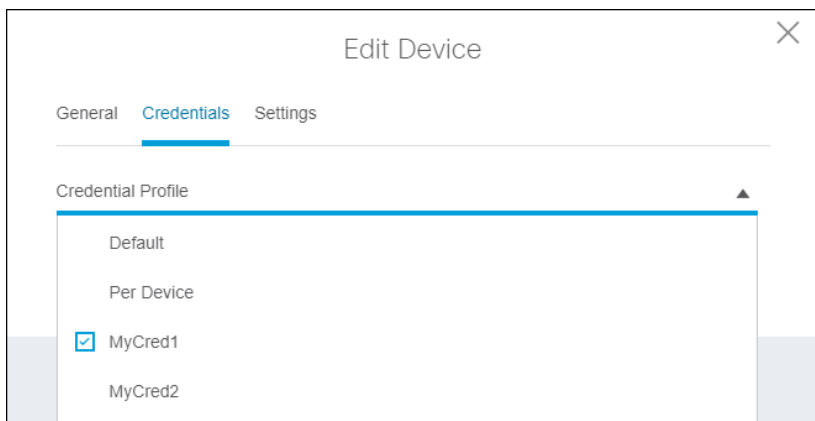
Note: For most devices and connections, the Keyboard Interactive feature should be off. Please check the [Frequently Asked Questions](#) for more information.

To apply a credential profile to a device, edit the device and choose the credential profile that the device accepts.

Note: You can also use the Bulk Actions feature to assign credential profiles to multiple devices. In the Devices window, select the devices, click the **Bulk Actions** button, and choose **Apply Credential Profile**.

- **Default Credential Profile:** You can set a credential profile to use as the default profile for sessions. To set a default profile, click the **Default Credential Profile** drop-down listing and choose the appropriate profile. If you choose Per Device, there is no default profile, and devices configured to accept the default profile will accept only their own individual credentials instead.

Configure the Display Tab

These settings affect the appearance of text, background colors, and highlights.
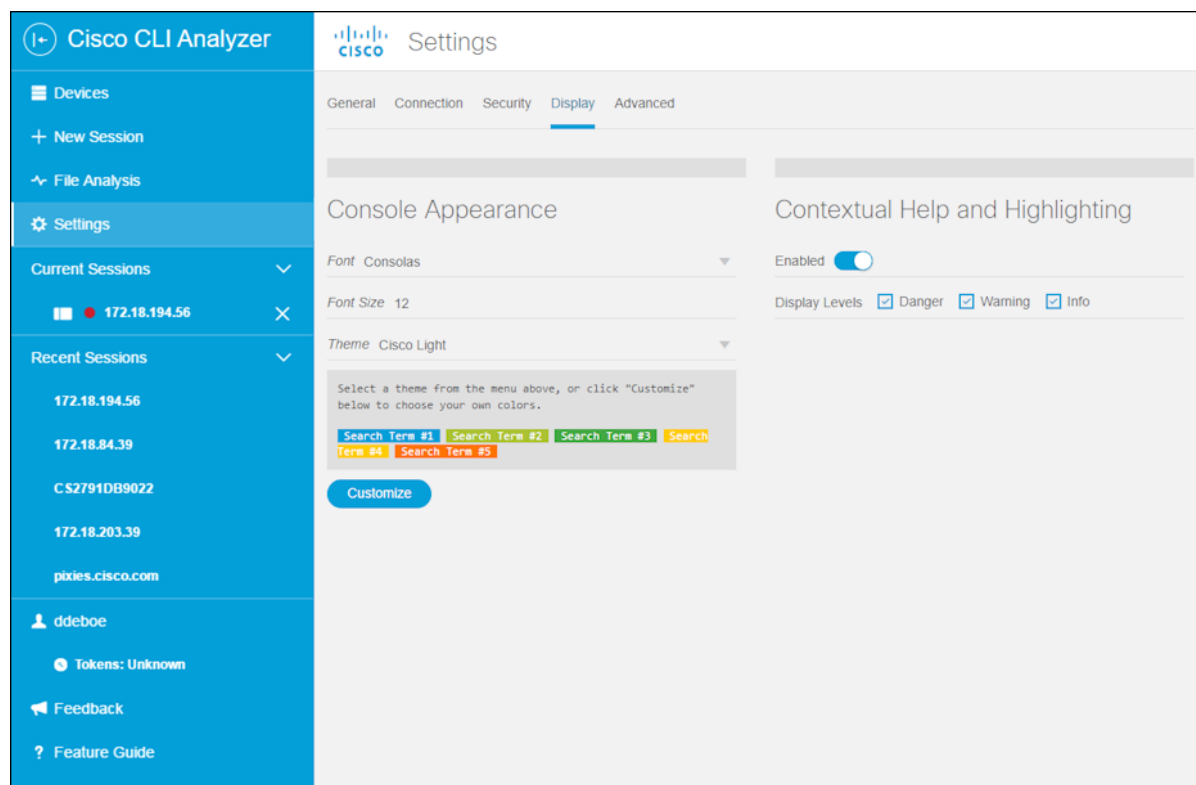
Console Appearance

- **Font:** Choose the font type that you prefer from the drop-down list.

- **Font Size:** Click inside the field and enter a font size between 8 and 20, or click the up and down arrows to change the font size.

- **Theme:** Choose a predefined color theme, or click **Customize** to choose your own colors.

  If you choose **Customize**, a set of Text and Background color buttons appears. Click a color button 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.

  (See demonstration videos showing how to select a theme and create a custom theme.)

- **Note:** Search terms use their own text and background colors. For more information, see how to search command output.

Contextual Help and Highlighting

- **Enabled:** Click the toggle button to enable or disable contextual help and highlights. This feature is enabled by default. For more information, see how to use contextual help and highlights.

- **Display Levels:** Check the check boxes for the notification types (Danger, Warning, and Info) that you want to display. Uncheck the check boxes for the notification types that you want to disable.

Configure the Advanced Tab

These settings apply to proxy servers and special key sequences.
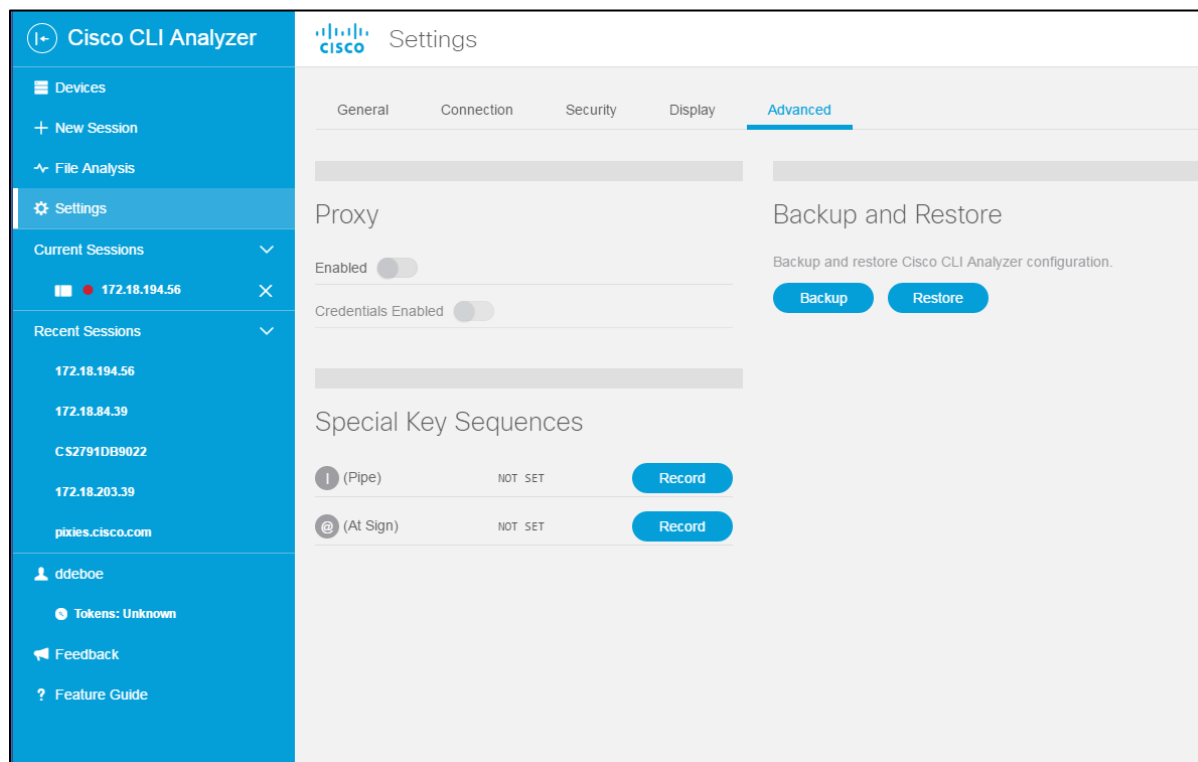
Proxy

- **Enabled:** Click the toggle button to enable the use of a proxy server for outbound web connections.

  Complete these fields in the Enable Proxy Settings dialog, then click the **Enable Settings** button.

  - **Protocol:** Click inside the field and choose a protocol from the drop-down list. The 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 before Proxy settings become active.

- **Credentials Enabled:** Click the toggle button, enter the username and password for the proxy server, then click the **Enable Credentials** button.

  See a [demonstration video](#) of this feature.

Special Key Sequences

You can specify key combinations to insert special characters in the terminal window: the "pipe" (|) character and the "at" (@) character.

To set a key sequence, click the **Record** button, press the desired sequence of keys, and then click **Set**. To delete a recorded key sequence, click the **X** beside the sequence.

Backup and Restore

You can create a backup copy of the settings, devices, and tool results as a compressed file (in .tgz format). You can also restore a backup created on this Cisco CLI Analyzer installation or another one. When you restore the backed-up information, it overwrites the existing configuration.

Click the **Backup** button to save a backup copy. When prompted to confirm the backup, click the **Backup** button. Navigate to the folder where you want to save the file, type a name for the file, and click the **Save** button.

Click the **Restore** button to restore the information contained in a backup file. Either drag the backup file onto the indicated area or click the area and browse to select the file. Click **Restore**. The Cisco CLI Analyzer will restart automatically after the configuration is restored.

Manage Your Devices

Locate Devices

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

Use Filters

Filters are based on tags and favorites. Check the filter boxes on the left side of the device list to display only devices with the selected tags or the selected favorite status (either favorites or non-favorites). To remove all the active filters, click the **Clear All Filters** button below the filter check boxes.

Note: If filter boxes do not appear in the Devices window, click the **Filter** button (**Filter**) to show the Filters area.
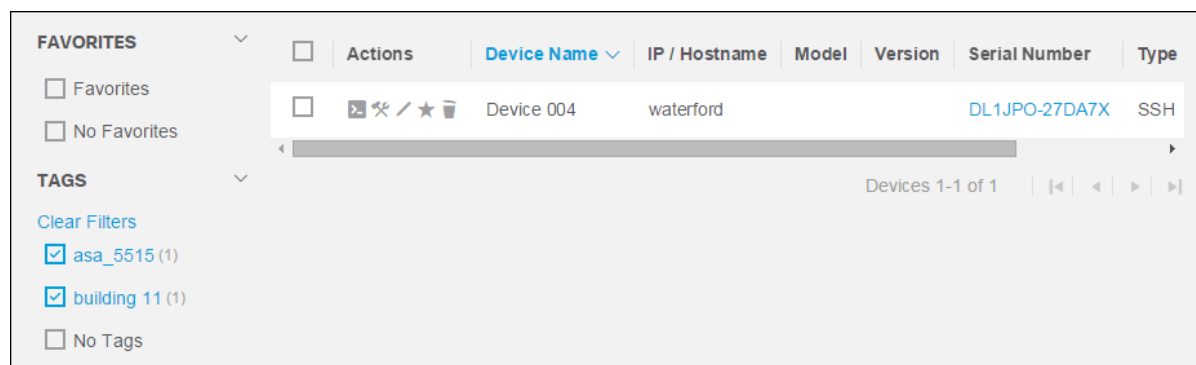
Use Search

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

The keyword is displayed below the Search box and remains an active filter that can be combined with other filter selections. To remove the keyword as an active filter, click the **X** next to the keyword.

Q Search Devices	□ + ⊤ ⊥	
CS2791 ✕ EAST ✕	**CS2791DB9022**	**CS2791DB9074**
FAVORITES ∧	IP Address 172.18.194.105	IP Address 172.18.194.55
☐ Favorites	Hostname	Hostname
☐ No Favorites	Location EAST 03	Location EAST 02
	Connection Type SSH Port 22	Connection Type SSH Port 22
TAGS ∧	⊵ ╱ ★	⊵ ╱ ★
☐ asa_5515		
☐ building 11		
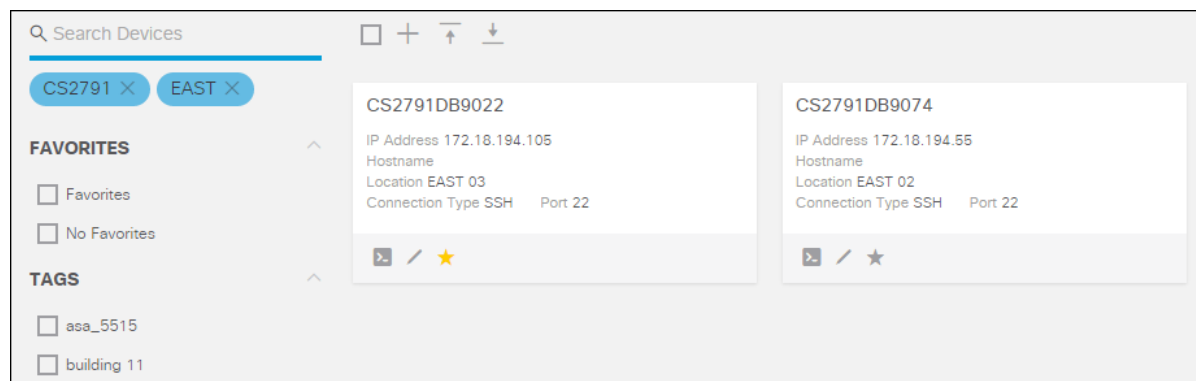
Sort Devices

In List View, click a column header to sort the list by that property. Click the column header again to switch between ascending and descending order.
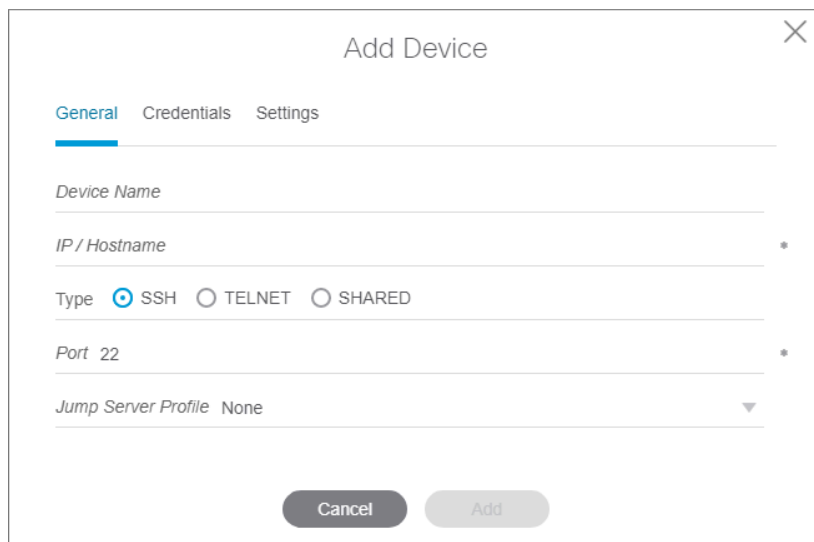
In List View or Grid View, click the sorting menu in the upper right (Device Name ▾) and choose a property from the drop-down list.

Click the sorting icons to toggle between descending sort order (⩲) and ascending sort order (⩵).

Add a Device to the Device List

Complete these steps to add a device to your device list.

1. In the Devices window, click the **Add Device** icon (＋) on the toolbar.

	Add Device	✕
General Credentials Settings		
Device Name		
IP / Hostname		∗
Type ⦿ SSH ○ TELNET ○ SHARED		
Port 22		∗
Jump Server Profile None		▾
Cancel	Add	

2. On the General tab, 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. Click the radio button for the protocol that you want to use (SSH, TELNET, or SHARED).

5. If you use a nonstandard port number, enter it in the Port field.

6. If you would like to connect to this device through a jump server, select the appropriate profile in the Jump Server Profile field.

   Note: This field is visible only if you have added at least one jump server profile to the Cisco CLI Analyzer. See the Security tab of the Settings window for more information.
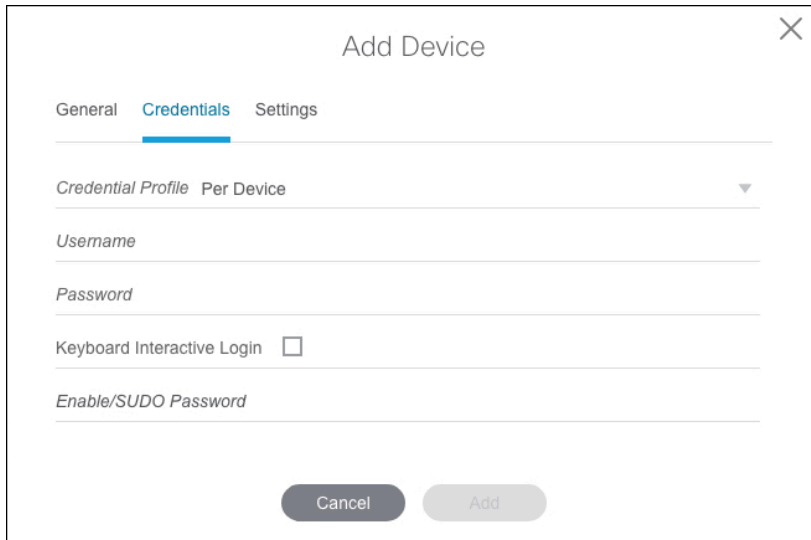
7. Click the **Credentials** tab and select a credential profile to connect to this device.

   a. If you want to specify the credentials individually for this device, choose **Per Device** and fill in the information in steps 8–10.

   b. If you want to use the default profile specified on the Security tab, choose **Default** and skip to step 11.

   c. If you want to use one of the credential profiles you set up on the Security tab, choose the desired profile and skip to step 11.

   Note: This field is visible only if you have added at least one credential profile to the Cisco CLI Analyzer. See the Security tab of the Settings window for more information.
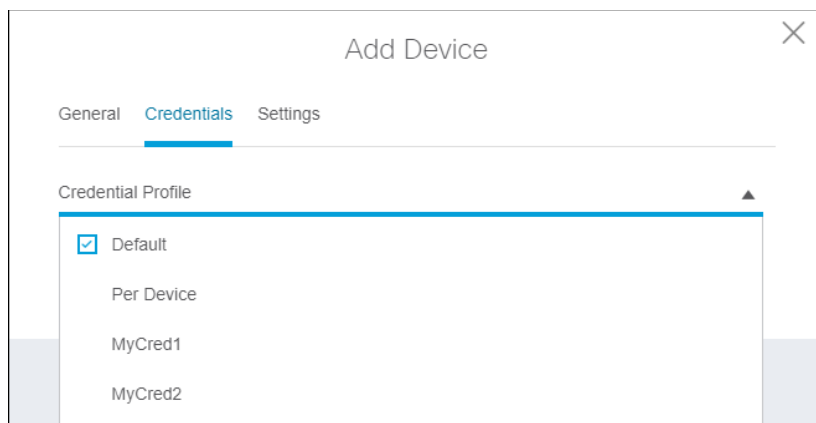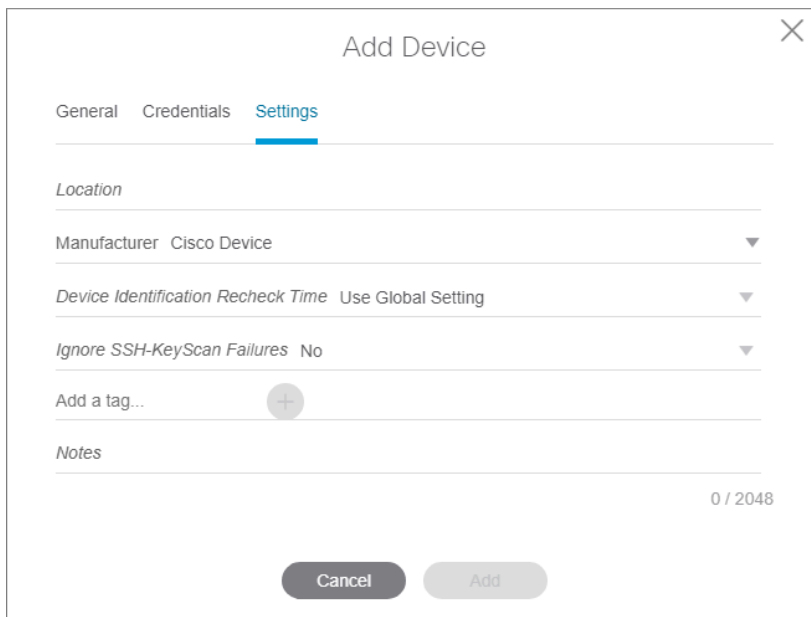
8. Enter the username and password to use when connecting to the device.

9. If your device has an Enable or SUDO password, enter it in the Enable/SUDO Password field.

   Note: For most devices and connections, the Keyboard Interactive feature should be off. Please check the Frequently Asked Questions for more information.

Add Device

General   Credentials   Settings

Credential Profile   Per Device ▾

Username

Password

Keyboard Interactive Login ☐

Enable/SUDO Password

Cancel   Add

10. Click the **Settings** tab.

Add Device

General   Credentials   Settings

Location

Manufacturer   Cisco Device ▾

Device Identification Recheck Time   Use Global Setting ▾

Ignore SSH-KeyScan Failures   No ▾

Add a tag...   +

Notes

0 / 2048

Cancel   Add

11. In the Location field, enter the physical location of the device.

12. In the Manufacturer field, choose **Cisco Device** or **Non-Cisco Device**.

13. In the Device Identification Recheck Time field, choose how frequently the **show version** command should run upon connection to the device. You can choose to use the global setting defined on the General tab of the Settings window, or you can choose an individual value for this device.

14. In the Ignore SSH–KeyScan Failures field, choose whether Cisco CLI Analyzer should display a prompt if it cannot retrieve the RSA Host Key when connecting to a device via SSH.

    Note: This field is disabled if the global Ignore SSH–KeyScan Failures option is enabled on the [Connection tab](#) of the Settings window or if a jump server profile is added to the device.

15. To assign tags to your device, click the **Add a tag...** line, type the desired tag, then press **Enter** or click the **Add** icon (+).

16. If desired, enter additional information about the device in the Notes field.

17. Click the **Add** button to add the new device to your device list.

Import Devices from a CSV File

You can import devices to your device list from a CSV file.

Note: Imported devices are configured to accept the default credential profile that is selected on the Security tab of the Settings window. If the default credential profile setting is Per Device, the imported devices will accept only their own credentials.

Complete the steps below to create a CSV file of devices and to upload the file to your device list.

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.

1. In the Devices window of the Cisco CLI Analyzer, click the **Import Devices** icon (↑) on the Device List toolbar. From the drop-down menu, choose **Import from CSV**.
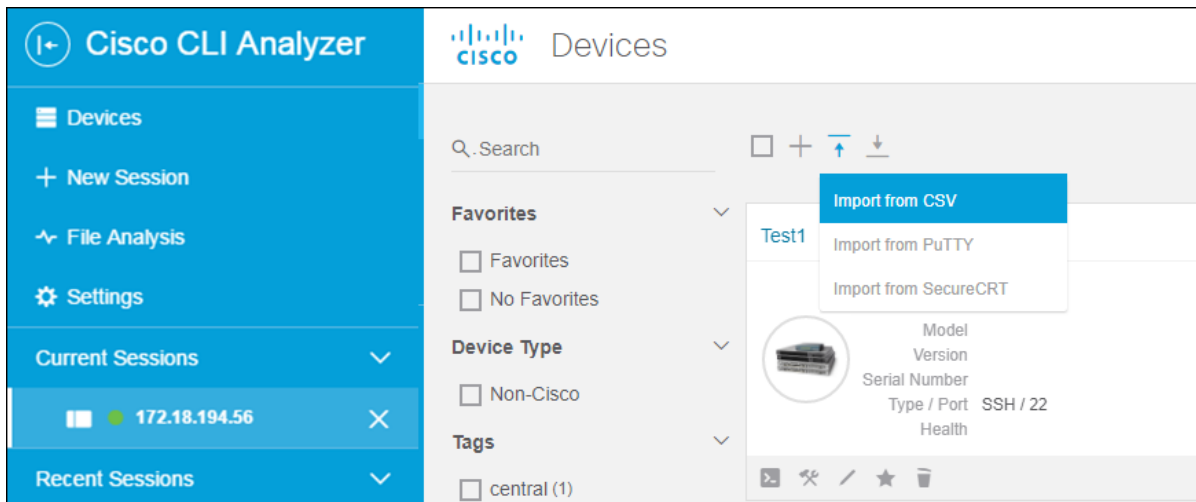
2. Click the **Download Template** button to download a CSV template that shows recommended information and includes example data.

3. Open the CSV file in your preferred application, such as Microsoft Excel.

4. Enter information for each device on a separate row.

   o IP address **or** hostname (DNS) is required.

   o Protocol is required.

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

	A	B	C	D	E	F	G	H	I	J
1	Device Name	Detected Device Name	Serial Number	Location	IP Address / Hostname	Protocol	Port	Favorite	Tags	Manufacturer
2	SB-Branch-891		FTX160781E1	Santa Barbara	company-host	ssh	22	yes	SB|891|critical	Cisco
3	SJ-Branch-998		NJX160781F3	San Jose	192.169.37.5	telnet	23	no	testing	Cisco
4	SJ-Branch-997		NJX160781F2	San Jose	192.169.37.4	ssh	22	no	testing	Non-Cisco
5		SJ-Branch-996	NJX160781F1	San Jose	192.169.37.3	ssh	22	no	testing	Cisco

5. Save the completed template as a CSV file.

Upload a CSV File of Devices

1. In the Device File Upload dialog, complete one of these steps.

   o Click the **Click Here or Drop File to Upload** area. In the Open dialog, navigate to the CSV file you want to import, select it, and click **Open**.

   o Drag the CSV file from a separate window onto the drop area. 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.
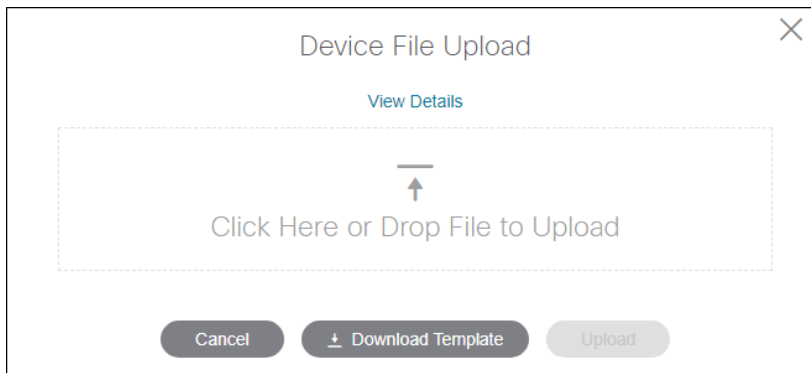
2. Click **Upload** to import the devices from the CSV file into your device list.

Import Devices from PuTTY

You can import devices to your 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.

Note: Imported devices are configured to accept the default credential profile that is selected on the Security tab of the Settings window. If the default credential profile setting is Per Device, the imported devices will accept only their own credentials.

In the Devices window of the Cisco CLI Analyzer, click the **Import Devices** icon (↑) and choose **Import from PuTTY** from the drop-down menu. Complete the steps for the automatic or manual import process.

Use Automatic Import

1. Click the **Automatic Import** radio button.

2. Check the check box(es) for the connection type(s) to import: SSH and/or Telnet.

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.
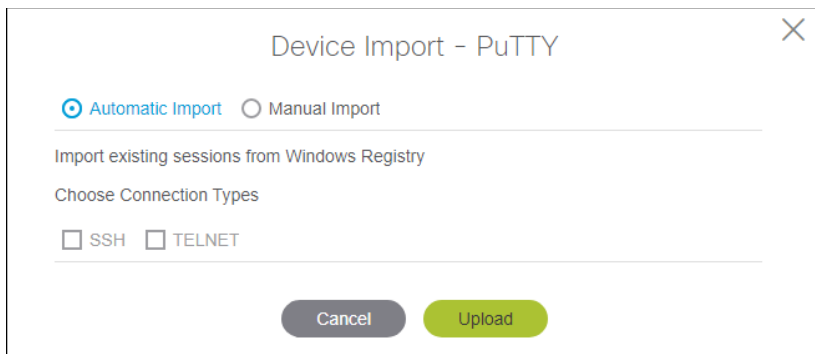
Use Manual Import

1. Select the **Manual Import** radio button.

2. Click **View Details** to expand the window and show step-by-step instructions.
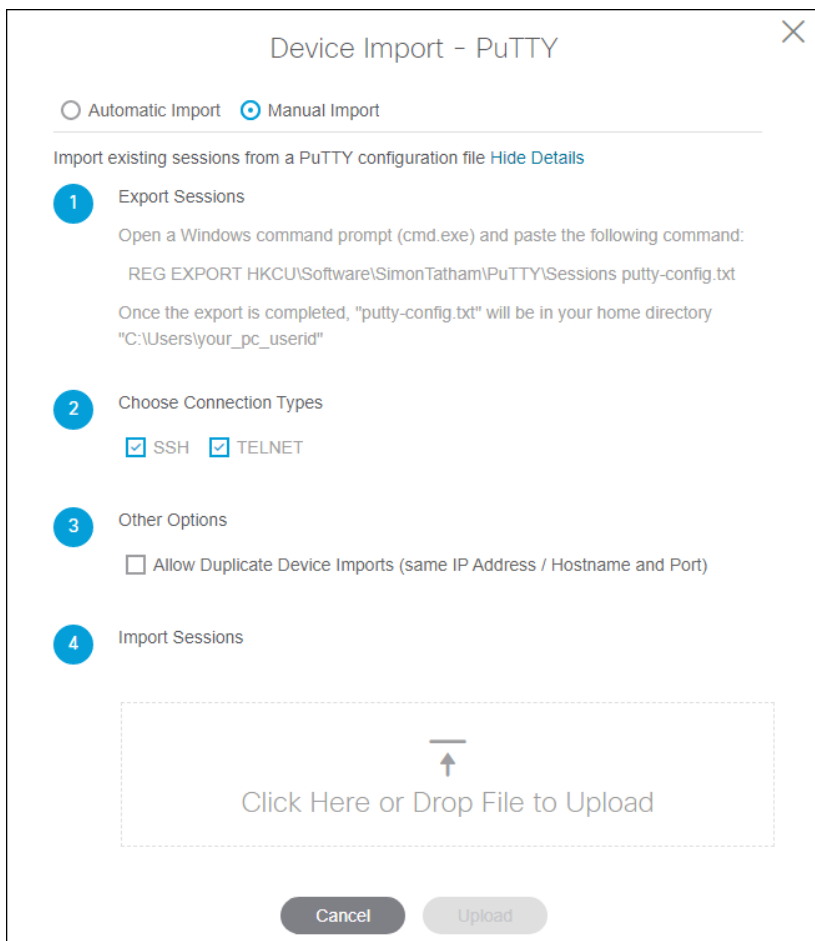
3. Open a command shell window. At the command prompt, type (or copy and paste) this text:

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

4. Press **Enter** to create the putty-config.txt file in your home user directory (such as C:\Users*<your_user_name>*).

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

6. Upload the PuTTY export file by one of these methods:

    o   In Windows Explorer, open the folder that contains the PuTTY export file. Drag the file from Windows Explorer onto the drop area in the Device Import dialog.

    o   Click the **Click here or drag & drop the file to upload** area in the Device Import dialog. Browse to the folder that contains the PuTTY export file, choose the file, and click **Open**.

7. 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.

Note: Imported devices are configured to accept the default credential profile that is selected on the Security tab of the Settings window. If the default credential profile setting is Per Device, the imported devices will accept only their own credentials.

1. In the Devices window of the Cisco CLI Analyzer, click the **Import Devices** icon (↑) and choose **Import from SecureCRT** from the drop-down menu. Complete the steps for the automatic or manual import process.

2. Click **View Details** to expand the window and show step-by-step instructions.
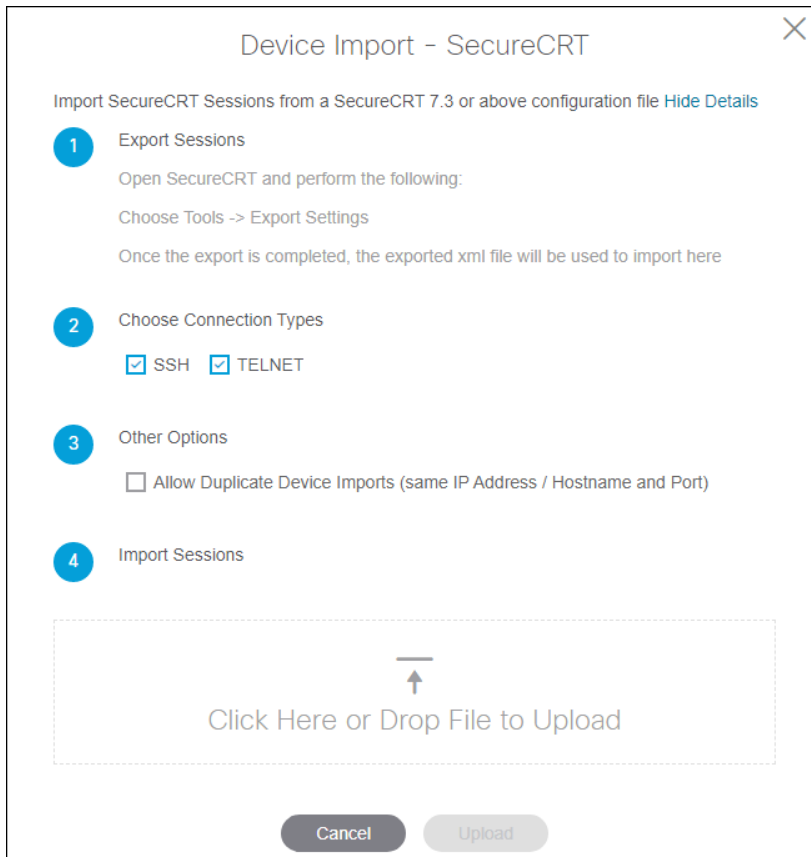
3. Open SecureCRT. On the Tools menu, choose **Export Settings**. Complete the export process and note the location of the export file.

4. In the Device Import - SecureCRT dialog, 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 the following methods.

   o   In Windows Explorer, open the folder that contains the SecureCRT export file. Drag the file from Windows Explorer onto the drop area in the Device Import dialog.

   o   Click the **Click here or drag & drop the file to upload** area in the Device Import dialog. 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.

Export Devices

You can export information about the devices in your device list to a CSV file. This allows you to transfer the information to another workstation.
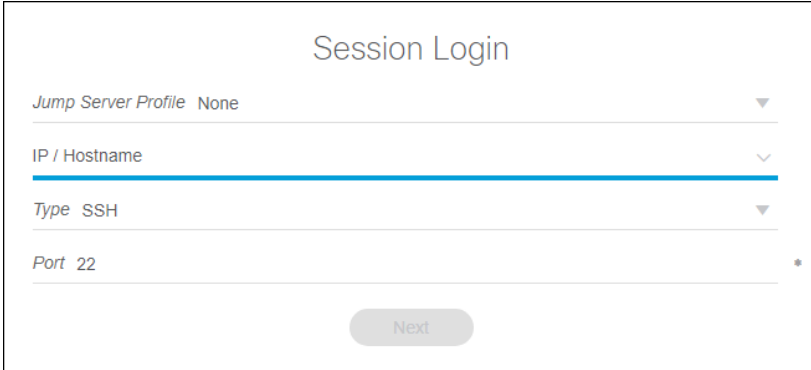
In the Devices window, click the **Export Devices** icon (⤓) to save the CSV file to your computer.

Connect to a Device (SSH or Telnet)

Complete these steps to use the SSH or Telnet connection type to connect to a device.

1. In the Devices window, complete one of these actions to start a new session.

    o Click **New Session** in the left panel.

    o Click a device in the Recent Sessions list.

    o Click the **Connect** icon (▸_) on the device card of a chosen device.

2. If you are prompted for basic connectivity information for the device, enter the requested information in the Session Login dialog and click **Next**. Otherwise, skip to step 3.

    o If you want to use a jump server, choose the desired profile from the **Jump Server Profile** drop-down list.

      Note: This field is visible only if you have added at least one jump server profile to the Cisco CLI Analyzer. See the Security tab of the Settings window for more information.

    o 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 from a recent session.

    o Choose the connection type (SSH or TELNET) that you want to use.

    o Enter the appropriate port number in the Port field.

Session Login	
Jump Server Profile None	▾
IP / Hostname	⌄
Type SSH	▾
Port 22	•
Next	
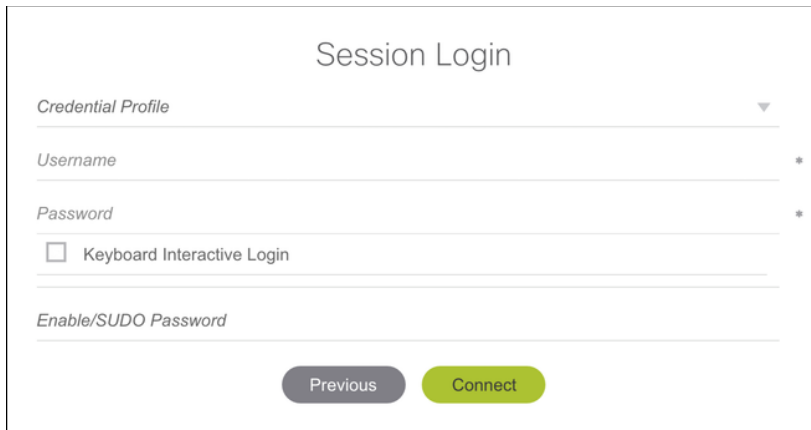
The Cisco CLI Analyzer checks for a connection to the device. If the device is found, the screen changes to accept login information.

3. From the Credential Profile drop-down menu, choose the desired profile to connect to the device.

    o To specify the device credentials individually, choose **Per Device** and fill in the information.

    o To use the default profile specified on the Security tab, choose **Default** and skip to step 7.

    o To use one of the credential profiles you set up on the Security tab, choose the desired profile and skip to step 7.

Note: This field is visible only if you have added at least one credential profile to the Cisco CLI Analyzer. See the [Security tab](#) of the Settings window for more information.

4. In the Username field, enter the username to use when connecting to the device.

5. In the Password field, enter the password to use when connecting to the device.

6. If your device has an enable or SUDO password, enter it in the Enable/SUDO Password field. If you leave this 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.

Note: For most devices and connections, the Keyboard Interactive feature should be off. Please check the [Frequently Asked Questions](#) for more information.

7. Click the **Connect** button to view the session window. The list of Current Sessions shows the newly established connection, with a green indicator confirming that the session is active.

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.

By default, the **show version** (or appropriate) command runs automatically at every session. You can change how frequently this command runs on the General tab of the Settings window. You can also edit the frequency on individual devices.

After you are connected, you can perform the following actions.

- [Log your current session](#)

- [Work with shared device sessions](#)

- [Create a backup copy of the running configuration](#)

- [Run CLI commands](#)

- [Run Cisco CLI Analyzer scripts](#)

- [Search the command output](#)

Note: Click **Disconnect** to disconnect from the device. If your session times out and you are automatically disconnected, click **Reconnect**. You can also double-click the session in the Current Sessions list in the Devices window to reconnect.

Initiate an SSH Session from the Command Line

When you open the Cisco CLI Analyzer from the command line, you can add arguments to initiate an SSH device session immediately when the application opens.

Note: Ensure that no other instances of the Cisco CLI Analyzer are open before you proceed.

Use the command appropriate to your operating system.

- **Windows**: C:\Program Files\Cisco Systems, Inc\Cisco CLI Analyzer\nw.exe "--ssh *<username>@<deviceIP>*"

- **macOS**: open "/Applications/Cisco CLI Analyzer.app" --args "--ssh *<username>@<deviceIP>*"

Note: The <username> value is the account to use to log in to the device, and the <deviceIP> value is the IP address of the device.

Connect to a Device (Serial)

You can connect a PC to a COM port on the device. (Bluetooth wireless serial adapters are not supported.)
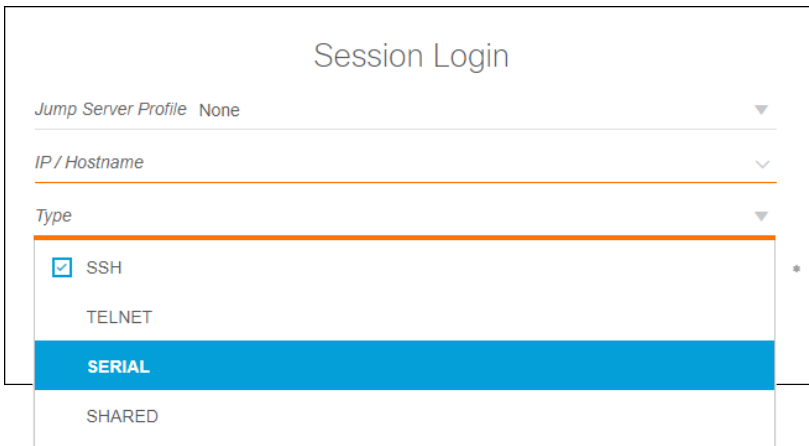
Serial connections differ from SSH/Telnet connections in several ways.

- Serial connections do not create entries in the Devices list for the connected devices.

- Serial connections do not support device identification, system diagnostic tools, or hardware flow control.

Complete these steps to connect to a device using a serial connection type.

1. In the Devices window, complete one of these actions to open the Session Login dialog.

   o Click **New Session** in the left panel.

   o Click a device in the Recent Sessions list.

2. In the Type field, choose **SERIAL** from the drop-down list.

Session Login

Jump Server Profile	None ▼
IP / Hostname	⌄
Type	▼

☑ SSH

TELNET

SERIAL

SHARED

3. Choose the COM port to use for the connection, then enter information in the remaining fields.

Session Login

Type	SERIAL ▼
Port Name	COM3 ▼
Baud Rate	9600 ▼
Data Bits	8
Stop Bits	1
Parity	NONE ▼
Flow Control	☐ XON/XOFF ☐ RTS/CTS

Connect

4. Click the **Connect** button to launch the session.

5. Enter your user credentials at the command prompt.

   Note: These credentials are not stored; you must enter them every time you open a serial device connection.

Send Break

While the serial connection is active, you can enter a "send break" command by either of the following methods.

- Press **Ctrl+Shift+S.**

- Right-click inside the console window and choose **Send BREAK** from the context menu.

Note: This functionality requires a USB/serial adapter and a Cisco device that both support Send Break. You must also trigger a Send Break at the correct time during the reboot of a Cisco device.

View a Device Session in a Separate Window

See a demonstration video of this feature.

On the General tab of the Settings window, you can enable the option to open every device session in a separate window by default.

You can also manually detach an existing session from the main window or reattach a session to the main application window.

To change a window from attached to detached or vice versa, click the icon on the right end of the session status bar.

- Window is currently detached

- Window is currently attached

On the sidebar, the list of current sessions displays an icon that indicates whether the session is attached to the main application window or in a separate window.
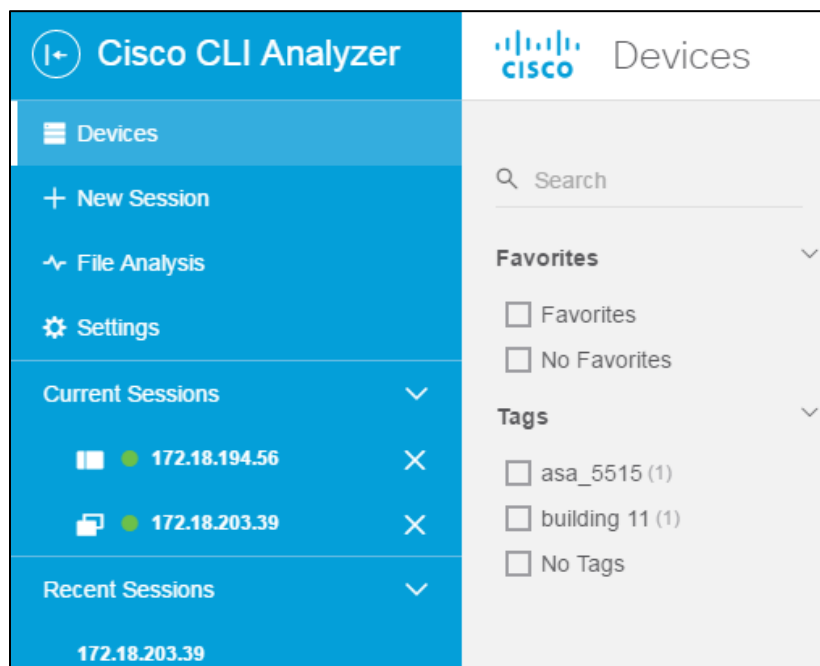
Work With Shared Device Sessions

You can use shared device sessions to train users and help troubleshoot problems when peer-to-peer connections are available.

The session initiator retains control of the session and can grant read/write permissions to one remote user at a time. Other remote users are limited to read-only access.

Note: Shared sessions are only supported on internal networks. Shared session connections via the Internet or through NATs and firewalls are not yet supported.

Note: Shared sessions use AES-256 encryption.

See a [demonstration video](#) of this feature.

Create and Manage a Shared Session

Complete these steps to use the SSH or Telnet connection type to connect to a device.

Note: Ensure that session sharing is enabled on the [Advanced tab](#) of the Settings window.

1. Connect to a device normally. Choose the **SSH** or **TELNET** connection type.

2. In the session window, click the **Share** icon (⬜) to show the Shared Session toolbar.

3. Click **Share Session**.

4. Provide information from the toolbar to remote users who want to join.

   o   IP address of the PC on which you have initiated the shared session

   o   Port number

   o   Session key
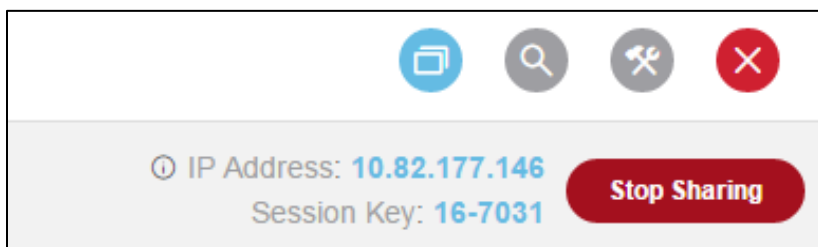
5. When a remote user joins the session, a confirmation dialog prompts you to authorize the connection. Click the **Authorize** button.
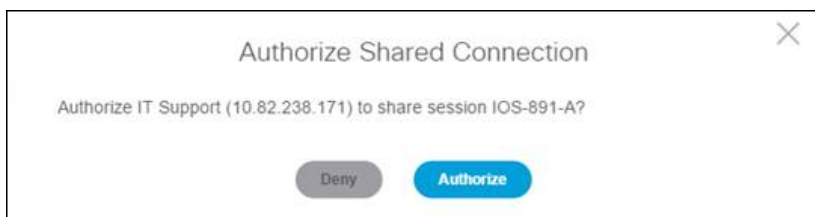
6. The remote user's name appears in a button on the toolbar. Click the button to access session options for the remote user.

While the shared session is active, you can perform these actions.

- **Give write permissions to a remote user:** Click the user's button and choose **Give Write Permissions**. If another user already has this permission level, it is transferred to the new user.

- **Revoke write permissions:** This option only appears for a remote user with write permission. Click the user's button and choose **Revoke Write Permissions**.

- **Disconnect a remote user:** Click the user's button and choose **Disconnect User**.

- **Stop sharing the session:** Click the **Stop Sharing** button on the toolbar. If you subsequently share the same session again, a new session key is generated that you must provide to remote users.

- **Work in other device sessions:** You can leave the shared session open and switch to a different session. A remote user with write permissions can continue to work in the shared session. The Current Sessions list displays **[Shared]** beside each active shared session.
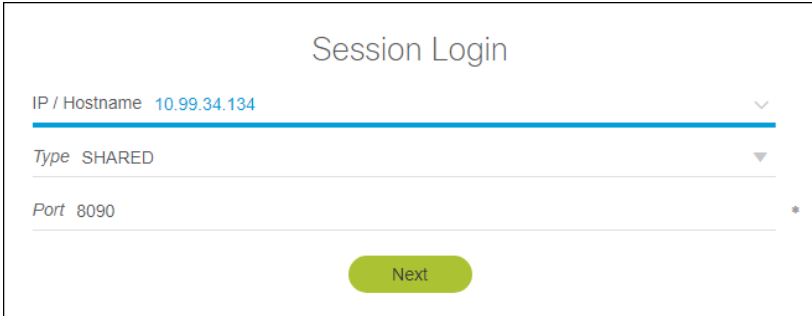
Join a Shared Session

To join a shared session, you must have this information (provided by the session initiator):

- IP address of the device

- Port number

- Session key
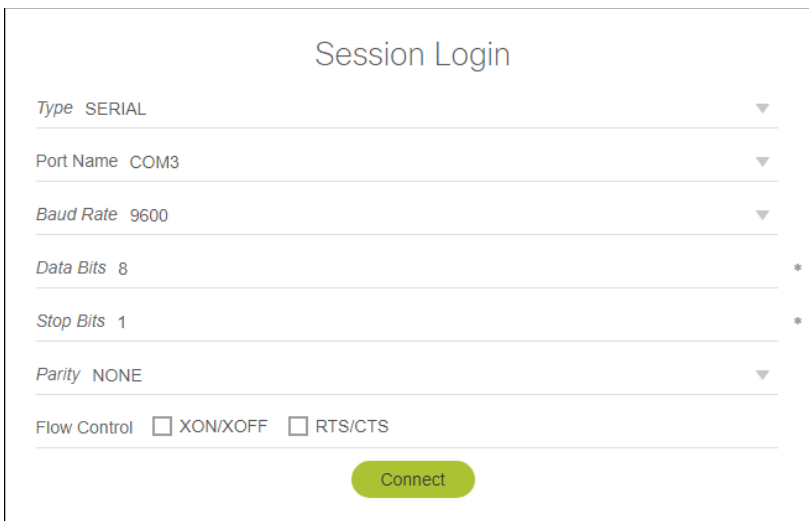
Complete these steps to create a shared device session.

1. In the Devices window, complete one of these actions to start a new session.

    o Click **New Session** in the left panel.

    o Click a device in the Recent Sessions list.

    o Click the **Connect** icon ( ) on the device card of a chosen device.

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.

    o 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.

    o From the Type drop-down menu, choose **SHARED**.

    o Enter the port number that the session initiator provided.

3. Click the **Next** button.

4. Enter a name by which to identify yourself in the shared session.

5. Enter the session key that the session initiator provided.

6. Click the **Connect** button.

After the session initiator authorizes your connection, the session window opens.

If the session initiator gives you write permissions, you can run commands and use analysis tools in the shared session. Results for the analysis tools that you run appear only on your client; the session initiator does not see them.

Work with Duplicate Devices

The Cisco CLI Analyzer lets you add devices that reside on different networks but use the same IP address or hostname and the same port.

Add a Device on a Different Network

When you add a new device to the Cisco CLI Analyzer, if the IP address or hostname and the port are identical to a device that is already in the database, the Duplicate Device window opens and displays information about the existing device.

If the existing device is the same as the one you are adding, click **Cancel** to avoid creating a duplicate entry. If it is a different device with the same IP address and port but on a different network, click **Add**.

Import Devices on a Different Network

When you import devices from a file, check the **Allow Duplicate Device Imports** check box to create a new entry for a device that has the same IP address or hostname and port as an existing device.

Before using this option, ensure that the imported devices are on different networks and are not duplicates.

Start Device Session

The Cisco CLI Analyzer assumes that you will use the New Session feature to connect to a device that is not in the database. When you click **New Session** and enter the IP/hostname and port of a device that is in the database, the Pick Session Device window opens and displays information about the existing device.

Click **Use Device** to create a session with the existing device. Alternatively, click **New Device** to create a new entry for a device with an identical IP address or hostname and port on a separate network.

Use Application Features

Use Keyboard Shortcuts

The table below shows the keyboard shortcuts that are supported on the Windows and OS X platforms. If no operating system is specified, the shortcut works on all supported platforms. Some functions have a shortcut that works on all platforms as well as additional shortcuts for specific operating systems.

Function	Shortcut
Start new session	Alt+Q
Copy selected item to clipboard	• Windows: Ctrl+C • OS X: Cmd+C
Search console	• Windows: Ctrl+F • OS X: Cmd+F
Select all text	• Windows: Ctrl+A • OS X: Cmd+A
Copy and paste	Ctrl+B
Open Favorite Commands list in console	Alt+F
Switch to previous tab	Ctrl+Shift+Tab
Switch to next tab	Ctrl+Tab
Paste clipboard contents	• Windows: Ctrl+V • OS X: Cmd+V
Scroll down one page	Page Down
Scroll up one page	Page Up
Toggle full screen	• All platforms: Shift+F • Windows: F11 • OS X: Cmd+F

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 [General tab](#) of the Settings window 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 how to [automatically enable session logging](#).

Complete these steps to log your current session.

1. Connect to a device as described in [Connect to a Device](#).

2. If the Logging toggle button is in the left (off) position, click the button to activate the feature and start the session log.
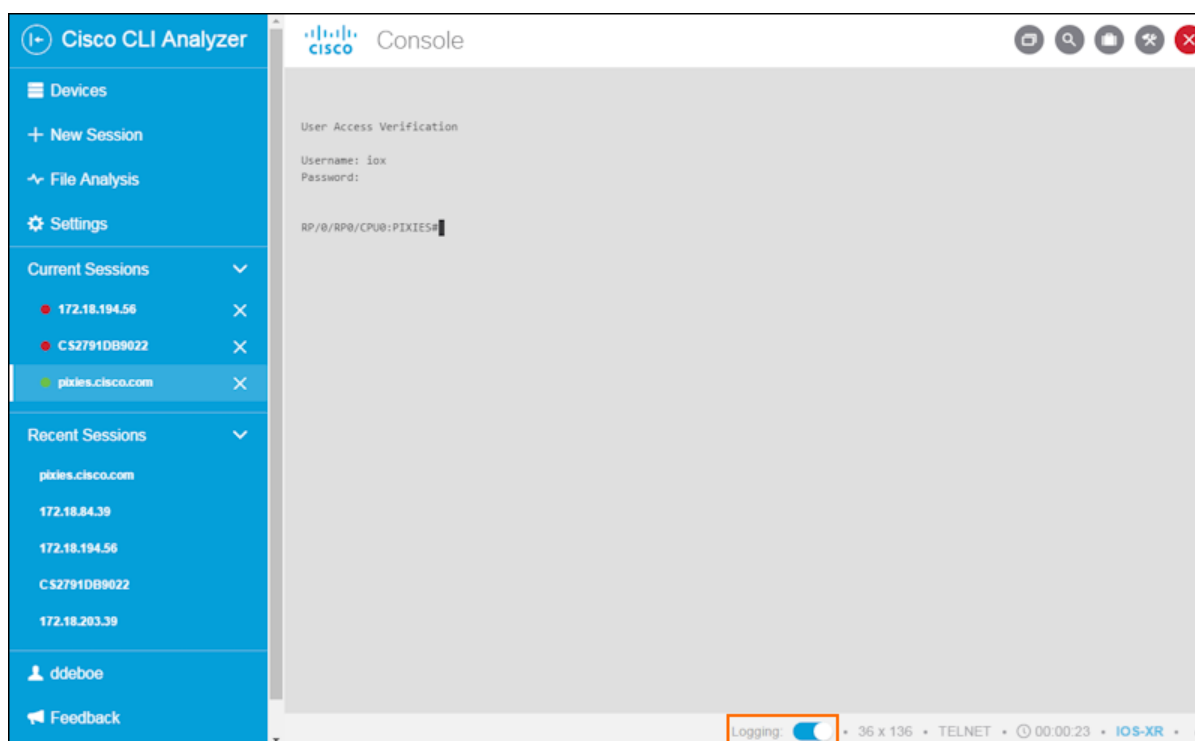
3. When you complete the session, click the **Logging** toggle button to save the log.

4. In the Save As dialog window, navigate to a location on your computer and click the **Save** button. By default, the Cisco CLI Analyzer saves log files to these locations.

   o **Windows:** C:\Users\<userid>\Cisco-CLI-Analyzer_Session_Logs

   o **macOS:** /Users/<userid>/Cisco-CLI-Analyzer_Session_Logs

Work With Tags for Your Devices

(See a [demonstration video](#) of this feature.)

Tags can help you organize devices and filter your device list quickly. Assign tags to your devices to locate them easily without needing to navigate hierarchical trees.

Tags can include these types of characters:

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

Complete these steps to add tags to a group of devices.

1. In the Devices window, click the check mark (✓) or check box (☐) the devices you want to tag.

2. Click the **Bulk Actions** button (③ Bulk Actions ∨), then choose **Add Tags** from the drop-down menu.

3. In the Add Tags dialog, click **Add a tag...** and type the desired tag. Press **Enter** or click the **Add** icon (+). Repeat this step for each tag that you want to add.
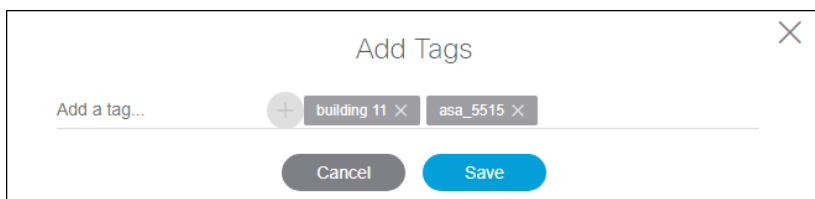
4. Click the **Save** button to add the tags to the selected devices.

Complete these steps to remove device tags from a group of devices.

1. In the Devices window, click the check mark (✓) or check box (☐) the devices you want to tag.

2. Click the **Bulk Actions** button (③ Bulk Actions ∨), then choose **Delete Tags** from the drop-down menu.

3. In the Delete Tags dialog, click the **X** on any tags that you want to keep.
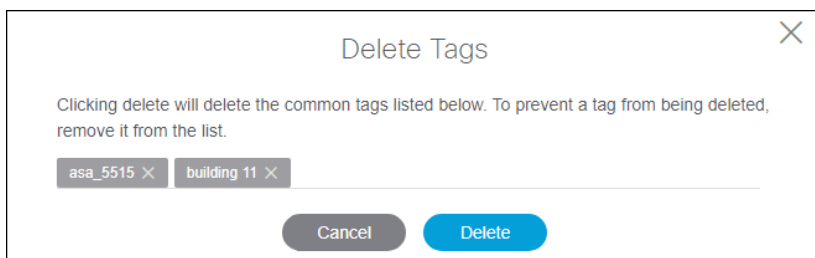
5. Click the **Delete** button to delete all the tags shown.

To add or delete tags for a single device, click the **Edit** icon (✎) for the device and click the **Settings** tab. Add or delete tags, then click the **Save** button.
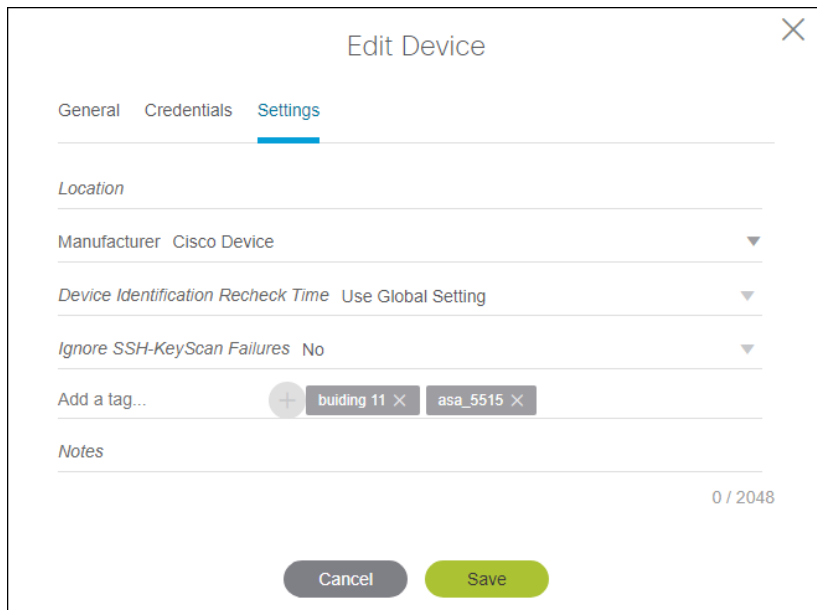
Run CLI Commands

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**.
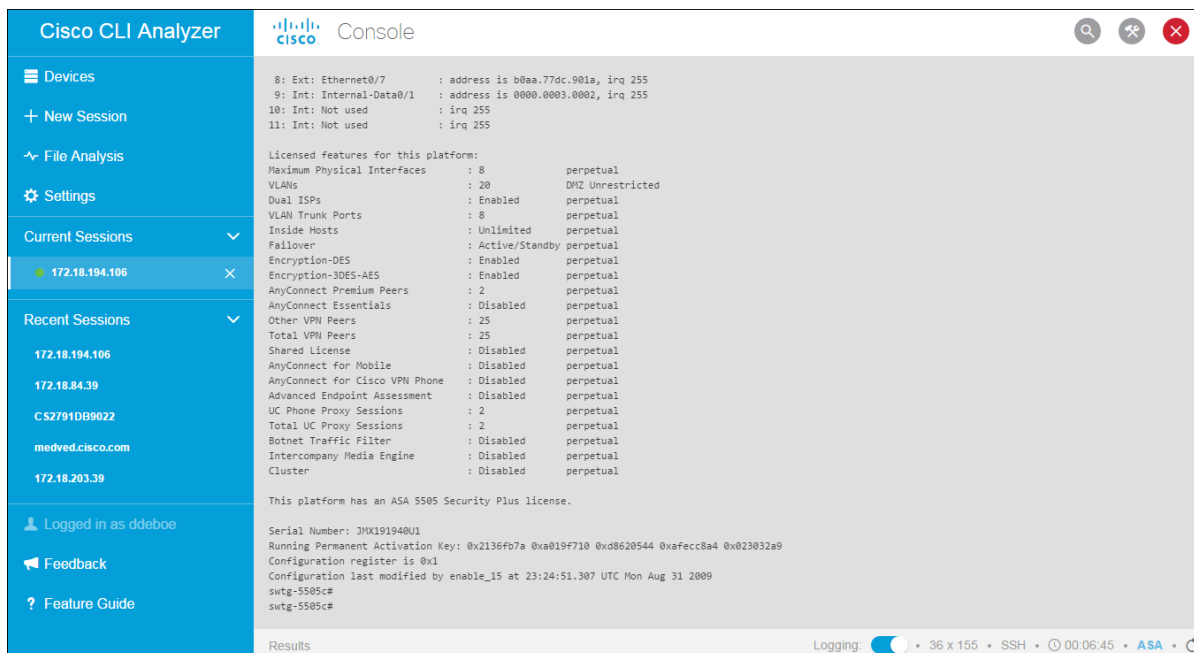
Run Cisco CLI Analyzer Scripts

The Cisco CLI Analyzer allows you to run scripts to 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's session window.

Complete these steps to run a Cisco CLI Analyzer script.

1. Connect to a device as described in <u>Connect to a Device</u>. If the Tools panel is hidden, click the Tools icon (⚒) to display the panel.
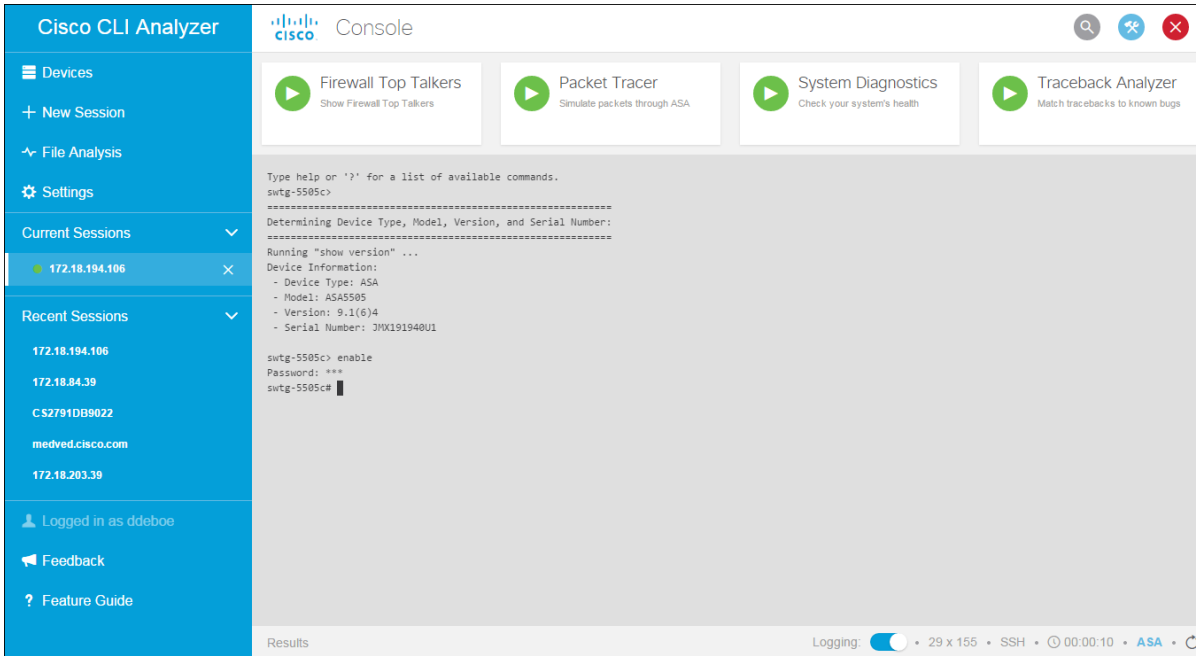
2. Click the **Run** icon (▶) for the script that you want to run.

3. If prompted, enter additional settings for the tool.

   Note: If Enable access is required, the Cisco CLI Analyzer will prompt you for credentials before the script runs.

4. Wait for the script to complete or click the **Halt** icon (⏹) to stop the script.
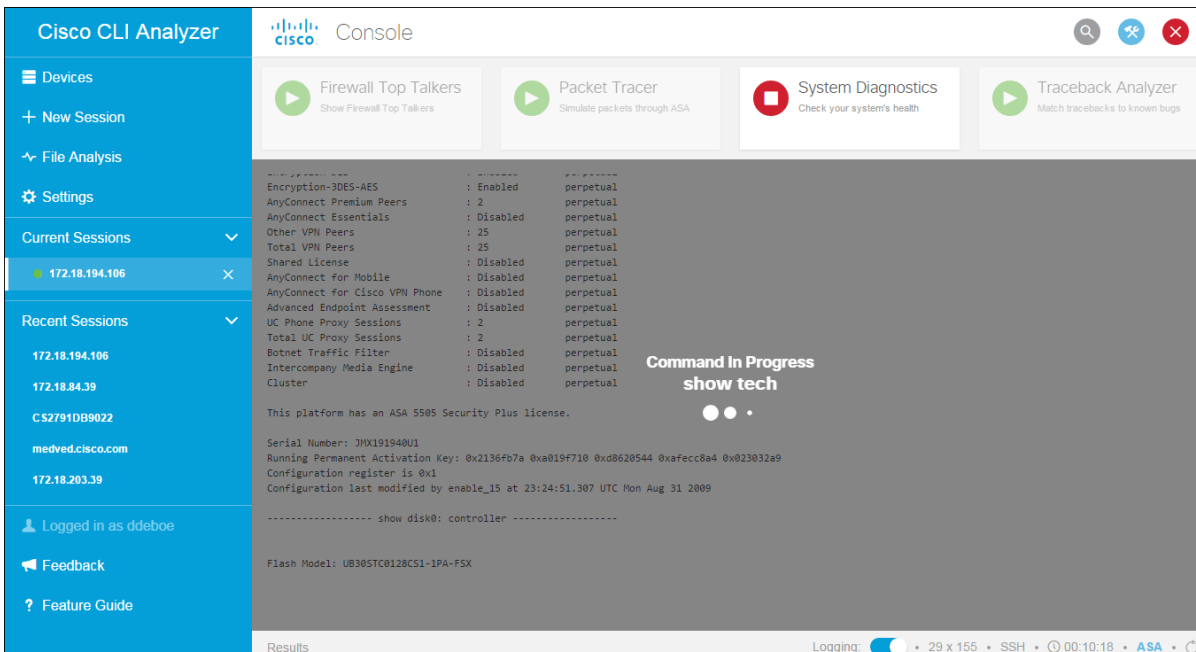
5. When the script completes, the Tool Results window opens with information from the session.

 Note: If the Tool Results window does not open, click **Results** in the bottom left corner of the session window.

6. Click an item in the Tool Results window to view additional details. The Tool Results window displays the most recent 25 results per device and retains this information even if you close the window or the Cisco CLI Analyzer application. (See a demonstration video of this feature.)
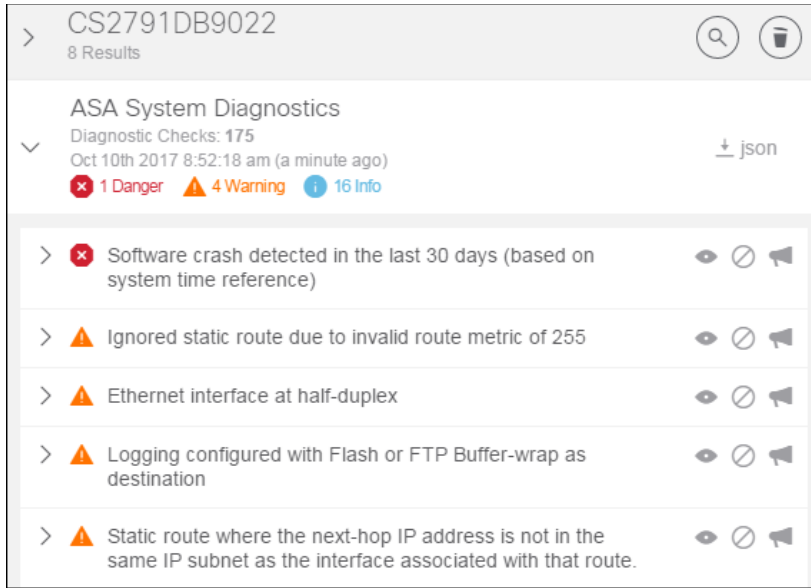
7. Click the **View** icon (👁) beside an item in the Results list to highlight and display the associated text in the session window.

 Note: 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 View icon is not present.
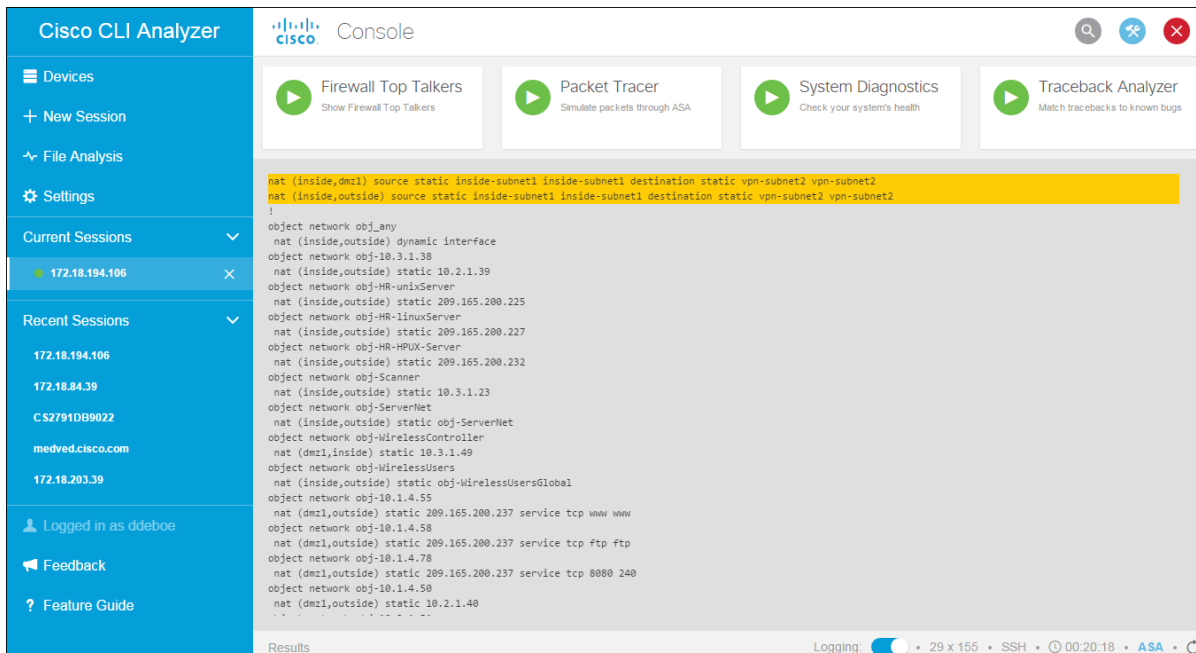
8. Click **json** in the top right corner of the Results area to export the results to a .json file.

Search the Tool Results Window

A large amount of information can appear in the Tool Results window. Use the search feature to help locate information that is of interest.

1. Click the **Search** icon (🔍) to open the Search bar at the top of the Tool Results window.

2. Type a search term in the box and press **Enter**. Sections of the Tool Results window that contain the search term expand automatically and highlight the term. The search term appears in a box on the Search bar, along with the number of times the term occurs. Up to five search terms can be active at the same time. To remove a search term, click the **X** beside it on the Search bar.

3. Use the arrow buttons beside the search box to jump to the first, previous, next, or last occurrence of the search term in the Tool Results window.
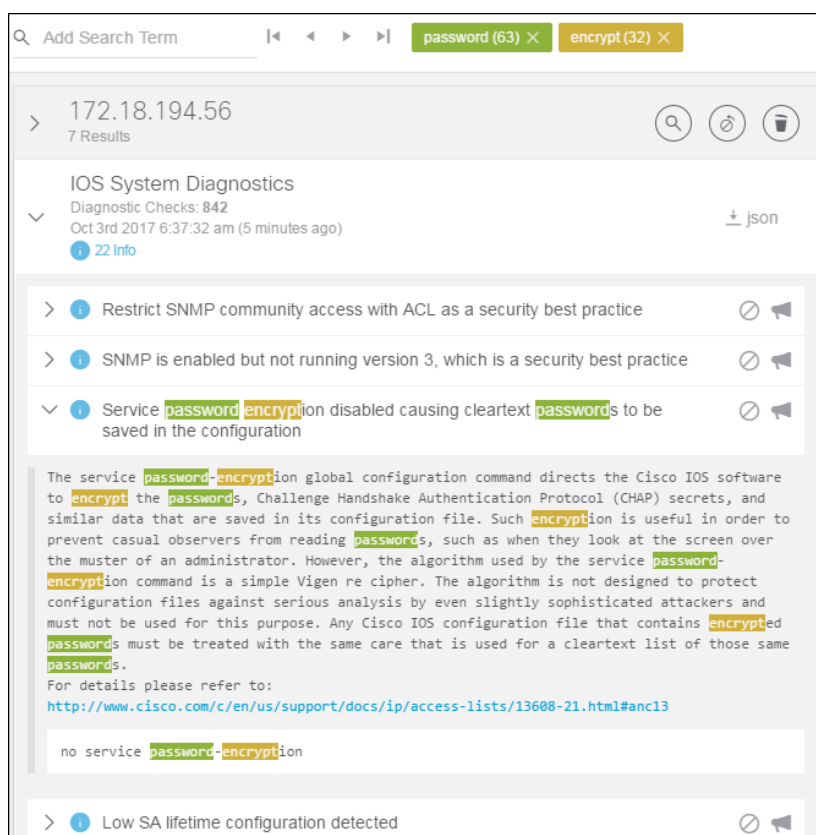
Filter Diagnostic Events

Some events that appear in the Tool Results window might be acceptable for your environment. You can filter the list to hide events that are not relevant to your network.

The following tools support event filtering.

- ASA System Diagnostics

- IOS System Diagnostics

- IOS-XE System Diagnostics

- IOS-XR System Diagnostics

- NX-OS System Diagnostics

- WLC Show Run Diagnostics

- WLC Show Tech Diagnostics

To hide an event in the Tool Results window, click the **Hide** icon (⊘) beside that event.
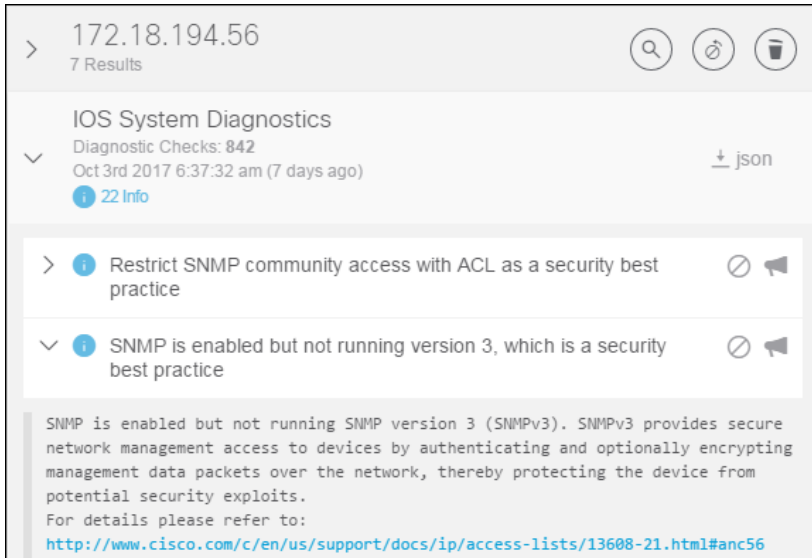
To stop hiding an event, click the **Unhide** icon (⊚) at the top of the window to see a list of hidden events.
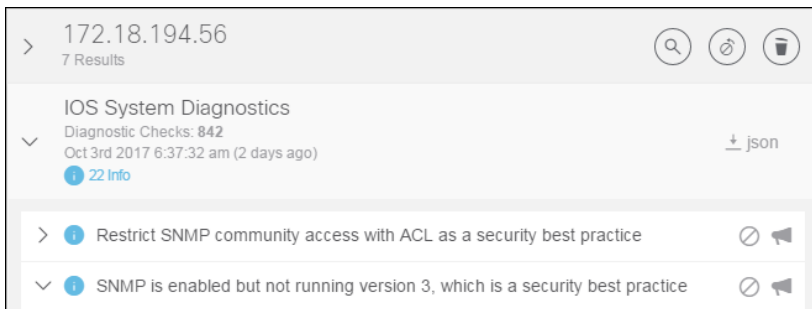
Select the event(s) that you want to show and click the **Unhide** button.
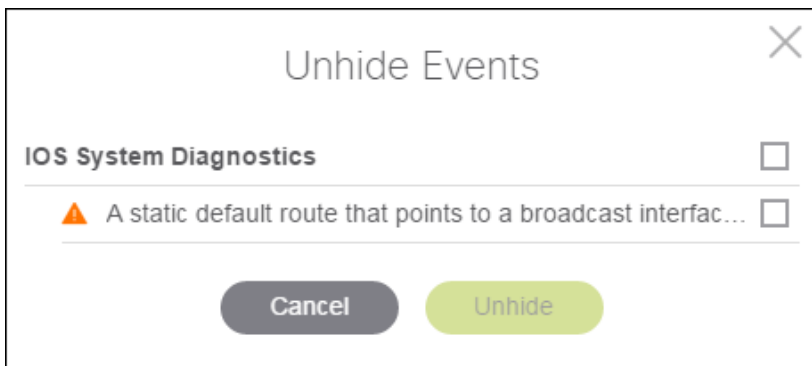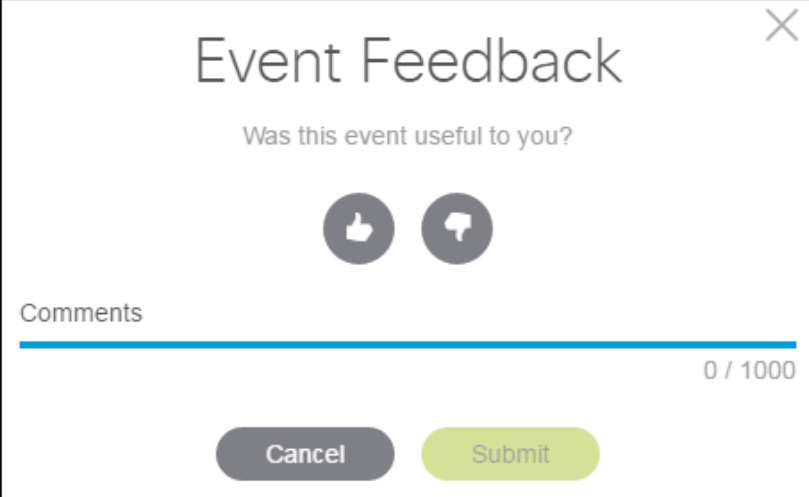
Send Feedback About Diagnostic Events

If your contract permits it, you can send feedback about the events the diagnostic tools report. This feedback helps Cisco improve the usefulness of the information the diagnostic tools provide.

The following tools support feedback.

- ASA System Diagnostics
- IOS System Diagnostics
- IOS-XE System Diagnostics
- IOS-XR System Diagnostics
- NX-OS System Diagnostics
- WLC Show Run Diagnostics
- WLC Show Tech Diagnostics

To send feedback for an event in the Tool Results window, click the Feedback icon (📣) beside that event. Type your feedback and click the **Submit** button.

Search the Command Output

The Cisco CLI Analyzer includes a highlight feature that enables real-time search capabilities in the console window to search command output. (See a [demonstration video](#) of this feature.)

Complete these steps to search the command output.

1. Hover over the Highlight icon (✎) and check the tooltip to ensure that search result highlights are enabled. If highlights are disabled, click the icon to enable highlights.

2. Enter a term in the search field, then press **Enter** or **Tab**. You can add up to five terms for a search query.

The specified search terms appear beside the search field along with the number of results for each term. Search results appear highlighted in the command window.
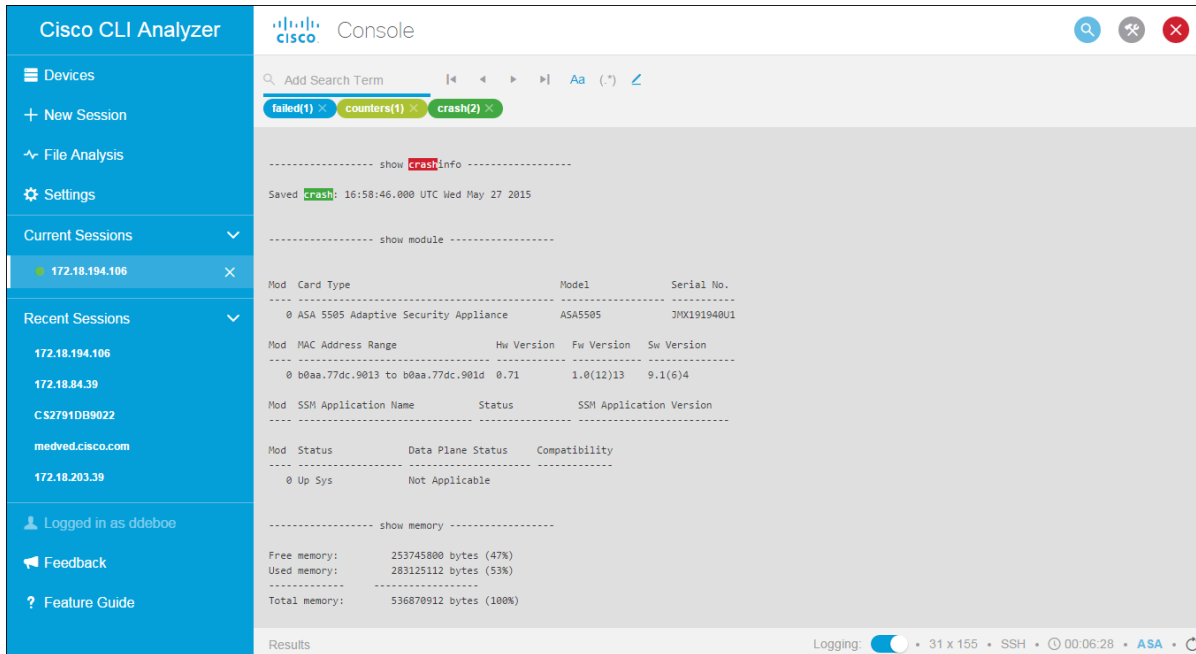
Note: Results are highlighted according to the colors assigned to each search term on the Display tab of the Settings window. The search term that is currently selected is highlighted in red.

3. Use the arrow buttons beside the search box to jump to the first, previous, next, or last occurrence of the search term in the Tool Results window.

4. To restrict search results to case-sensitive matches, click the **Case Sensitive** icon (Aa).

5. To enable or disable regular expressions, click the **RegEx** icon ((.*)).

6. **Note:** RegEx is used to create wildcards or substitutions in your searches. This feature supports a specific set of expressions and characters.

7. To remove a search term, click the **X** for the search term in the search field.

Create a Backup Copy of the Running Configuration

From within a device session, you can save a text file that contains a copy of the device's running configuration. This feature is available on ASA, IOS, IOS-XE, IOS-XR, NX-OS, and WLC platforms.

On the toolbar of the device session window, click the **Back Up** icon ( ). The device executes the **show running-config** command. Navigate to the folder where you want to save the backup file and click **Save**.

Create and Update Support Cases

You can open a support case for an eligible device on the Devices list. (See demonstration videos showing how to create a support case and how to attach a file to a support case.)

Devices with support coverage have a Support Cases icon ( ) displayed in the Actions column (List view) or the Actions bar of the device tile (Grid view). A dark gray icon indicates that the device has support

coverage. A light gray icon indicates that the device is not covered or that your user account does not have permission to perform support case actions for the device.

Complete these steps to create a new support case for a device.

1. Click the Support Cases icon (▮) for the device, then choose **Open a new Case** from the drop-down menu.

2. Click the icon for the type of support you need: Fix my Problem, Answer my Question, or Request an RMA.

3. From the Technology drop-down menu, choose the category of technology for the case.

4. From the Sub-Technology drop-down menu, choose the sub-category of technology for the case.

5. From the Problem drop-down menu, choose the category that best describes the type of problem.

6. On the Description line, enter a short description of the issue. (If you selected Answer my Question, enter your question in this box.)

7. Click the **Submit** button to see a summary of the case, including a case number. You can click the case number to view the case on the Cisco Support Website.

Complete these steps to review or update a support case.

1. Click the Support Cases icon (▮) for the device, then choose the case number that you want to review or update.

2. Click the icon for the action that you want to perform: Collect Data, Add Note, or Attach File.

   - **Collect Data**: If you are creating a new case, you should perform this step if the device platform supports it. If you are updating a case, perform this action if a TAC engineer instructs you to do so. Click **Continue** on the Collect Data dialog and then follow the normal procedure to connect to a device session.

   - **Add Note**: Enter a short description of the note in the Title box, and enter the body of the note in the Details box. Click the **Submit** button to create the note.

   - **Attach File**: Drag a file from Windows Explorer onto the drop area of the Attach Files dialog, or click inside the area and use the Open dialog to select a file to attach. Click the **Submit** button to attach the file.

3. Click the **Done** button when you are finished.

Collect TAC Data

The TAC Data Collection tool allows a TAC engineer to specify one or more diagnostic commands to run on a device. The tool runs the commands and uploads the results to the support case. (See a demonstration video of this feature.)

The TAC engineer sends an email to you that contains a TaskID. The TaskID appears in the subject line of the email and takes the format of **#TAC-X1Y2-3456**.

The image below shows an example email:

Dear Customer,

In order to move things forward in SR **681631261**, I need your assistance to collect a few CLI outputs from the device you opened the SR on.

This will help assess the technical direction to take.

You have a couple of options to provide the CLI outputs.

Option 1: Use Cisco CLI Analyzer to collect required CLI commands automatically.

- Step 1. Download CLI Analyzer for your platform (Win/Mac): https://cway.cisco.com/go/sa/

  Note: If you already have CLI Analyzer 3.2 or greater installed proceed to Step 2.

- Step 2. Use the CLI Analyzer to connect to the device.

- Step 3. Click on the Tools button (top right corner) and run the "TAC Data Collection" tool.

- Step 4. Select TaskID **#TAC-D0A6-2561** from the dropdown or paste it.

Option 2: If you prefer to collect data manually, please collect the following outputs:

```
admin show platform
show install active summary
show run
show log
```

For option 2, you can use https://cway.cisco.com/csc/index.html?requestID=681631261 for diagnostic data upload.

Thank you.

After you receive the email, complete the following steps to collect the required data.

1. Connect to the device that the TAC engineer specified. If the Tools panel is hidden, click the Tools icon (✶) to display the panel.

2. Click the **Run** icon (▶) for the TAC Data Collection tool to open the data collection dialog.

Provide data collection Task ID ✕

Select a recent TaskID from the dropdown list or enter the TaskID (e.g. #TAC-5ABC-1234) specified in the email from Cisco TAC. After clicking Continue, commands to be run will be shown to the user for confirmation.

Select recent TaskID: SR 681133827: #TAC-01A2-7531   ▼ •

Enter TaskID manually:

Cancel   Continue
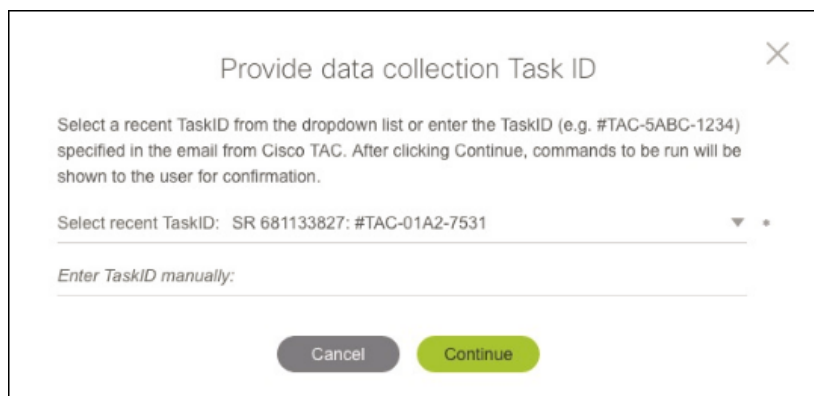
3. Enter the TaskID from the TAC email.

   o If your CCO ID is the case contact, choose the TaskID from the drop-down menu.

   o If you are not the case contact, then your username is not associated with the service request. Enter the TaskID manually by typing or pasting it.

   Note: A TaskID entered manually takes priority over one chosen from the drop-down menu.

4. Click **Continue**.

5. The Cisco CLI Analyzer retrieves the list of commands and displays them. The first command always sets the terminal length to zero, and the last command always restores the original length. The other commands collect the data required by the TAC engineer.
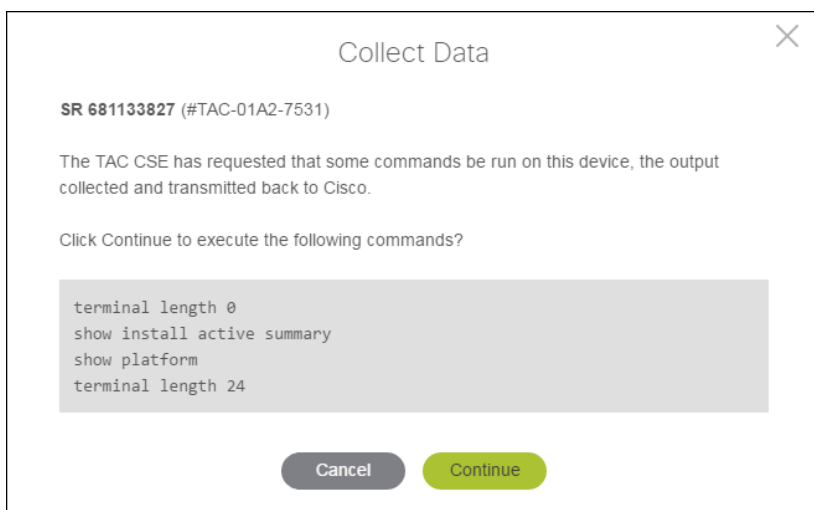
6. Click **Continue** to execute the listed commands and upload the output to the TAC case.

7. The Tool Results window displays the TaskID, the case number, and a link to download the collected outputs. The TAC engineer is notified of the collection and will communicate the analysis and action plan to you.
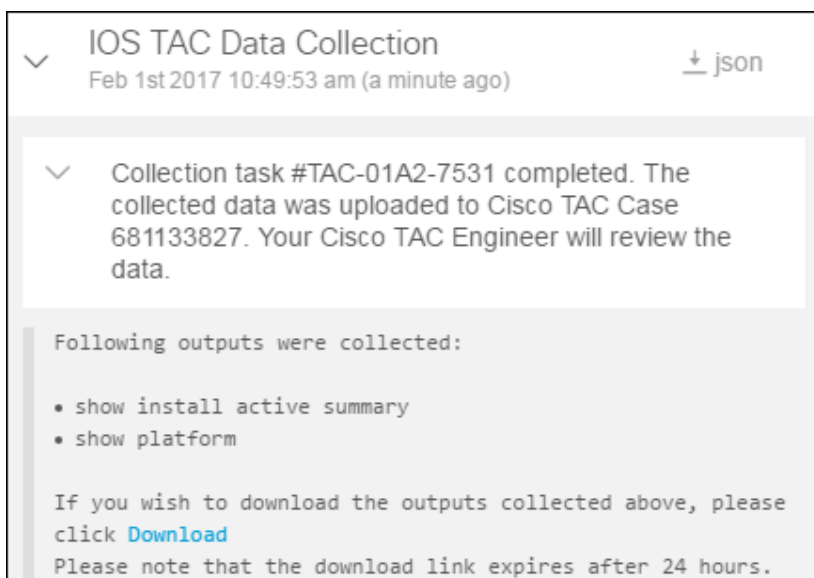
Analyze Offline Files

The Cisco CLI Analyzer can analyze a text file (with an extension of .text or .txt) that contains the command output from a previous device session. The text file can also be compressed with supported compression formats that include ZIP (.zip), GZIP (.gz), 7-ZIP (.7z), and RAR (.rar). (See a demonstration video of this feature.)

Note: The maximum file size you can upload, whether compressed or uncompressed, is 1 GB.

Include the following content in the text file.

- The command (such as **# show version**) that generated each output in the file

- Output from the **show version** command

- Optional: Output from the **show tech-support** command (This is required to perform a full analysis.)

- Optional: Output from other supported commands

Complete these steps to analyze a command output file.

1. Ensure that you are logged in using your Cisco account.

2. Click **File Analysis** on the sidebar.

3. Perform one of the following steps to provide the text to analyze:

   o Click **Click Here or Drop File to Analyze**. In the Open dialog, navigate to the text file you want to import, select it, and click **Open**.

   o Drag the CSV file from a separate window onto the drop area. 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.

   o Copy the command output text and paste inside the Command Output area.
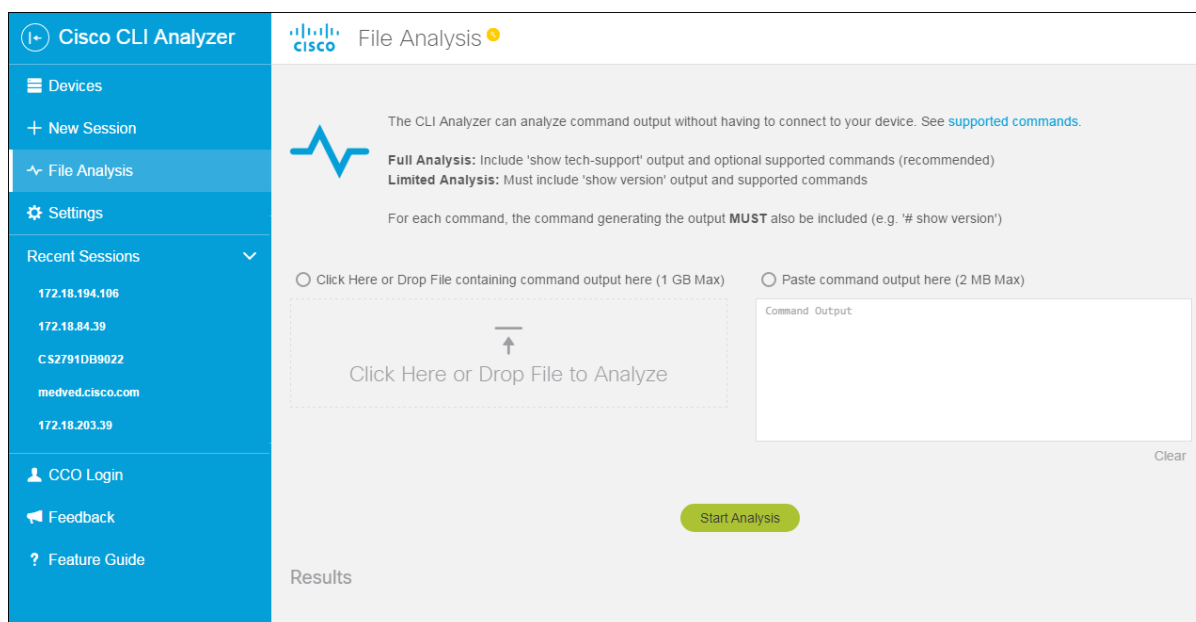
4. Click the **Start Analysis** button.

5. Analysis results appear in the Tool Results window.

Compare Configuration Differences

Use the Config Diff tool to identify differences between the startup and running configurations of a device.

1. Open a session with a supported device (ASA, IOS, or IOS-XR).

2. Click the **Config Diff** tool in the device session window.

3. In the Tool Results window, expand the entry for the Config Diff tool and click **View Config Diff** to open the Configuration Diff window.

The startup configuration and running configuration appear side by side with their differences highlighted.

- Red text indicates a line that is missing or different in the other file.

- Orange text indicates the context in which differences appear: the header or footer of a section that contains red lines. When you open the configuration file to reconcile differences, search for text in the header or footer to locate the relevant area of the file quickly.

- Blue icons indicate that lines within a section have been reordered. In most cases, the order of lines within a section does not matter, but there are exceptions, such as old IOS access lists or IOS-XR route policies.

Use Contextual Help and Highlighting

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

See a demonstration video of this feature.
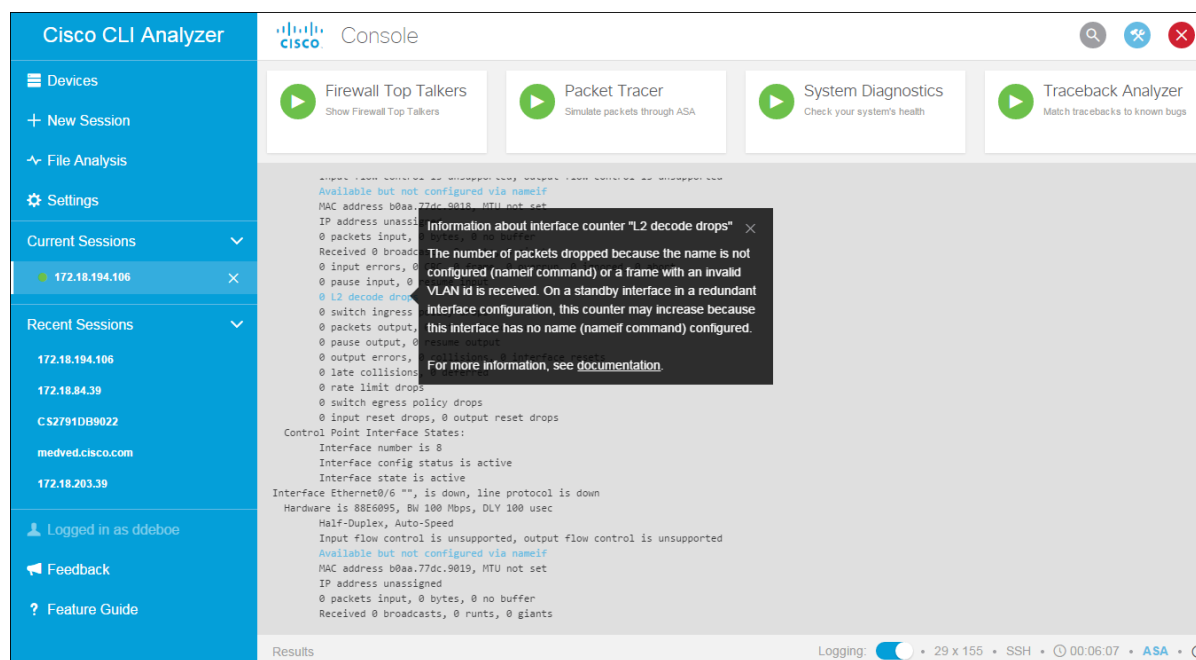
For supported commands on various platforms, refer to the following types.

- ASA Commands

- IOS Commands

- IOS-XE Commands

- IOS-XR Commands

- NX-OS Commands

- UCS Commands

ASA Commands

The Cisco CLI Analyzer supports contextual help and highlighting for the following ASA commands.

packet-tracer

show access-list

show asp drop

show blocks

show capture

show conn

show console-output

show counters

show cpu detailed

show cpu usage

show crypto ikev2 stats

show crypto ipsec sa

show crypto isakmp sa

show crypto isakmp stats

show failover

show failover history

show interface

show kernel cgroup-controller detail

show logging

show memory

show memory detail

show nat

show nat detail

show process

show process cpu-hog

show process cpu-usage

show running-config

show scansafe statistics

show tech-support

show version

write memory

write standby

IOS Commands

The Cisco CLI Analyzer supports contextual help and highlighting for the following 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 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 diagnostic

show ip eigrp neighbors show ip eigrp topology

show ip eigrp traffic

show ip interface

show ip interface brief

show ip nat statistics

show ip nat translations

show ip nat translations verbose

show ip ospf database

show ip ospf database asbr-summary

show ip database external

show ip database network

show ip database nssa-external

show ip database opaque-area

show ospfv3 neighbor

show ospfv3 neighbor detail

show ospfv3 statistic

show ospfv3 statistic detail

show otv

show otv isis rib redistribution mac

show OTV VLAN

show platform

show policy-firewall config

show policy-firewall session

show policy-map interface

show policy-map type inspect zone-pair sessions

show ppp multilink

show ap groups

show ap join stats summary

show ap mac-address H.H.H join stats detailed

show ap summary

show arp

show async status

show atm interface atm

show atm pvc

show atm traffic

show atm vc

show authentication sessions

show bgp

show bgp () X

show bgp (*) (vrf vrf-name)?

show bgp a.b.c.d

show bgp internal

show bgp neighbors

show bgp summary

show bridge-domain

show buffers

show call active voice

show call active voice brief

show call-manager-fallback

show capwap client rcb

show ccm-manager

show ccm-manager music-on-hold

show cdp neighbors detail

show cellular

show diagnostic events

show diagnostic results

show dial-peer voice summary

show dialer

show domain (name) (master|border) site-prefix

show domain (name) (vrf (vrf name)) (master|border) status

show dot11 association all

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 environment status

show etherchannel summary

show fabric

show fex

show fex detail

show frame-relay lmi

show frame-relay map

show frame-relay pvc

show interface atm

show interface multilink

show interface status

show interfaces

show ip database router

show ip database summary

show ip ospf interface

show ip ospf neighbors

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 interface

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 neighbor

show ipv6 ospf statistic

show ipv6 ospf statistic detail

show isdn service

show isdn status

show issu state

show line

show lisp dynamic-eid

show processes cpu

show processes memory

show redundancy

show redundancy states

show route-map

show run interface cellular

show running-config

show sccp connections

show sip-ua calls

show sip-ua status

show spanning-tree

show spanning-tree summary

show stacks

show standby

show stcapp device summary

show switch

show switch stack-ports summary

show tech-support

show tech-support wireless

show telephony-service

show telephony-service all

show version

show vlan

show voice call status

show voice dsp group all

show voice port summary

show voice register global

show cellular intf num radio

show cellular profile

show cem circuit

show clock (detail)

show controllers

show controllers cellular

show controllers dot11Radio 0

show controllers e1

show controllers e3

show controllers ethernet-controller(fastethernet|gigabitethernet)

show controllers pos

show controllers serial

show controllers SHDSL

show controllers t1

show controllers t3

show controllers vdsl

show interfaces counters

show interfaces counters error

show interfaces INT counters

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 interfaces detail

show logging

show mab

show mac address-table

show mac-address-table

show macsec

show memory

show memory statistics

show mgcp

show mls cef exception status

show module

show netdr captured-packets

show network-clocks sync

show ntp associations detail

show ospfv3 interface

show voip rtp connections

show vpdn tunnel

show vslp lmp neighbors

show vtp password

show vtp status

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-XE Commands

The Cisco CLI Analyzer supports contextual help and highlighting for the following IOX-XE 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 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 diagnostic

show ip database network

show ip database nssa-external

show ip database opaque-area

show ip database router

show ip database summary

show ip ospf interface

show ip ospf neighbors

show platform hardware qfp active statistics drop

show platform hardware qfp active tcam resource-manager usage

show platform hardware slot (#) serdes statistics

show platform health

show platform ptp all

show platform punt client

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 arp

show async status

show atm interface atm

show atm pvc

show atm traffic

show atm vc

show authentication sessions

show bgp

show bgp () X

show bgp (*) (vrf vrf-name)?

show bgp a.b.c.d

show bgp internal

show bgp neighbors

show bgp summary

show bridge-domain

show buffers

show call active voice

show call active voice brief

show diagnostic events

show diagnostic results

show dial-peer voice summary

show dialer

show domain (name) (master|border) site-prefix

show domain (name) (vrf (vrf name)) (master|border) status

show dot11 association all

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 environment status

show etherchannel summary

show fabric

show fex

show fex detail

show frame-relay lmi

show frame-relay map

show frame-relay pvc

show interface atm

show interface multilink

show interface status

show interfaces

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 interface

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 neighbor

show ipv6 ospf statistic

show ipv6 ospf statistic detail

show isdn service

show isdn status

show issu state

show line

show lisp dynamic-eid

show logging

show mab

show mac address-table

show mac-address-table

show platform software status control-processor brief

show policy-firewall config

show policy-firewall session

show policy-map interface

show policy-map type inspect zone-pair sessions

show ppp multilink

show processes cpu

show processes memory

show redundancy

show redundancy states

show route-map

show run interface cellular

show running-config

show sccp connections

show sip-ua calls

show sip-ua status

show spanning-tree

show spanning-tree summary

show stacks

show standby

show stcapp device summary

show switch

show switch stack-ports summary

show tech-support

show tech-support wireless

show call-manager-fallback

show capwap client rcb

show ccm-manager

show ccm-manager music-on-hold

show cdp neighbors detail

show cellular

show cellular intf num radio

show cellular profile

show cem circuit

show clock (detail)

show controllers

show controllers cellular

show controllers dot11Radio 0

show controllers e1

show controllers e3

show controllers ethernet-controller(fastethernet|gigabitethernet)

show controllers pos

show controllers serial

show controllers SHDSL

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 interfaces counters

show interfaces counters error

show interfaces INT counters

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 interfaces detail

show ip eigrp neighbors show ip eigrp topology

show ip eigrp traffic

show ip interface

show ip interface brief

show ip nat statistics

show ip nat translations

show ip nat translations verbose

show ip ospf database

show ip ospf database asbr-summary

show ip database external

show macsec

show memory

show memory statistics

show mgcp

show mls cef exception status

show module

show netdr captured-packets

show network-clocks sync

show ntp associations detail

show ospfv3 interface

show ospfv3 neighbor

show ospfv3 neighbor detail

show ospfv3 statistic

show ospfv3 statistic detail

show otv

show otv isis rib redistribution mac

show OTV VLAN

show platform

show platform hardware qfp active feature firewall drop

show platform hardware qfp active feature ipsec datapath drops

show platform hardware qfp active feature nat datapath stats

show platform hardware qfp active infrastructure exmem statistics

show telephony-service

show telephony-service all

show version

show vlan

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 vslp lmp neighbors

show vtp password

show vtp status

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

show crypto gdoi ks

IOS-XR Commands

The Cisco CLI Analyzer supports contextual help and highlighting for the following 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

The Cisco CLI Analyzer supports contextual help and highlighting for the following 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 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 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 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 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 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

UCS Commands

The Cisco CLI Analyzer supports contextual help and highlighting for the following UCS commands.

Command	Context	Scope
show fault	UCSM	monitoring
show diagnostic result module	NX-OS	
show ip igmp groups	NX-OS	
show interface trunk	NX-OS	
show interface ethernet	NX-OS	
show interface counters errors	NX-OS	
show running-config	NX-OS	
show interface status err-disabled	NX-OS	
show processes cpu	NX-OS	
show cluster extended-state	local-mgmt	
show interface	NX-OS	
show version	NX-OS	
show fault detail	UCSM	monitoring
show diagnostic result module all	NX-OS	

Command	Context	Scope
show processes log	NX-OS	
show logging logfile	NX-OS	
show diagnostic content module all	NX-OS	
show system reset-reason	NX-OS	
show ip igmp route	NX-OS	
show module	NX-OS	
show pmon state	local-mgmt	
show diagnostic content module	NX-OS	
show system internal flash	NX-OS	
show system internal mts buffers details	NX-OS	
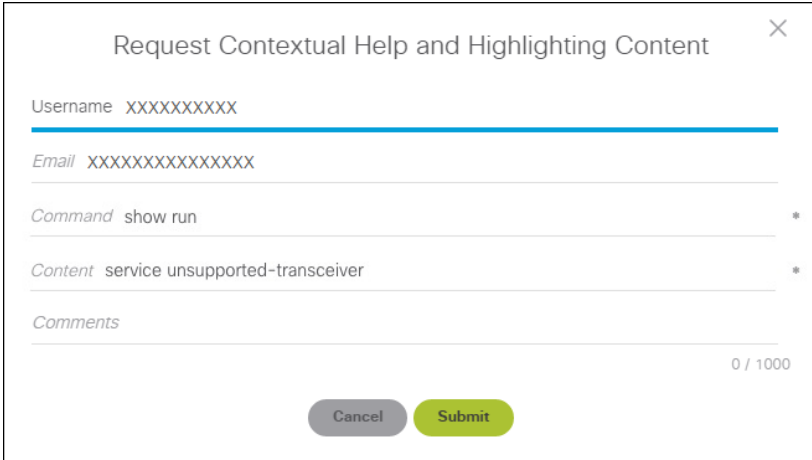
Set Context Menu Options

(See demonstration videos for features on search, ping, and SSH.)

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 into the command prompt as a single action.
- **Select All & Copy:** Copies all the text in the console window.
- **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.
- **Check Device Coverage:** Opens the Cisco Device Coverage Checker tool in a browser window after you select a valid serial number.
- **Request CHH Content:** Opens the *Request Contextual Help and Highlighting Content* dialog window, which you can use to submit a request for additional CHH content.

- **Add Selection to Case**: If a case is open against the device, you can highlight text in the console window and select this menu option to add to the case an attachment that contains the highlighted text.

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.

```
swtg-5505c# ping 172.18.194.105
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.194.105          timeout in 2 seconds:
!!!!!
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
Message #16 : 88E6095 rev 2 Ethernet @ index 03Message #17 :  MAC: b0aa.77dc.9015
Message #18 : 88E6095 rev 2 Ethernet @ index 02Message #19 :  MAC: b0aa.77dc.9014
Message #20 : 88E6095 rev 2 Ethernet @ index 01Message #21 :  MAC: b0aa.77dc.9013
Message #22 : y88acs06 rev16 Gigabit Ethernet @ index 00 MAC: b0aa.77dc.901b
Message #23 : Verify the activation-key, it might take a while...
Message #24 : Running Permanent Message #25 : Activation Key: Message #26 : 0x2136fb7a Message
age #30 : 0x023032a9 Message #31 :
Message #32 :
```

Context menu options shown:
- Copy
- Paste
- Copy & Paste
- Add Search Term
- Search Cisco.com
- Request CHH Content
- Ping 172.18.194.105
- Traceroute 172.18.194.105
- Open SSH Session
- Open Telnet Session

Frequently Asked Questions

Q. Why do I need to log in with my Cisco.com account to use some features of the Cisco CLI Analyzer?

A. To use features that require Cisco access (such as File Analysis, System Diagnostics, and Case Management), you must have a valid Cisco.com account, and your profile must be associated with an active customer or partner contract. If you do not have a Cisco.com account, register on Cisco.com and then associate a service contract to your profile.

When you use these features, the Cisco CLI Analyzer prompts you for your Cisco account credentials. To log in at any time, click the CCO Login icon (⟳) in the sidebar and enter your email address and password.

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

A. Ensure your username 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.

Q. Why am I unable to log in to my CCO account?

A. If you are unable to log in, use this information to help diagnose and resolve the issue.

- Your account might not have sufficient privileges. Contact Cisco Support if you are unsure what level of access your account has.

- Try to log in through the Cisco CLI Analyzer on an open Internet connection. If you are able to log in, the issue might be related to proxy settings on your network. If your network has a proxy server (such as Cisco WSA), you must add the following hosts.

    o id.cisco.com

    o sso.cisco.com

    o apix.cisco.com

    o cway.cisco.com

  After adding these hosts to the proxy server, try again to log in to the Cisco CLI Analyzer and use the tools.

Q. Do I need to allow specific traffic through my firewall or proxy server?

A. Yes, please ensure that you permit the following hosts.
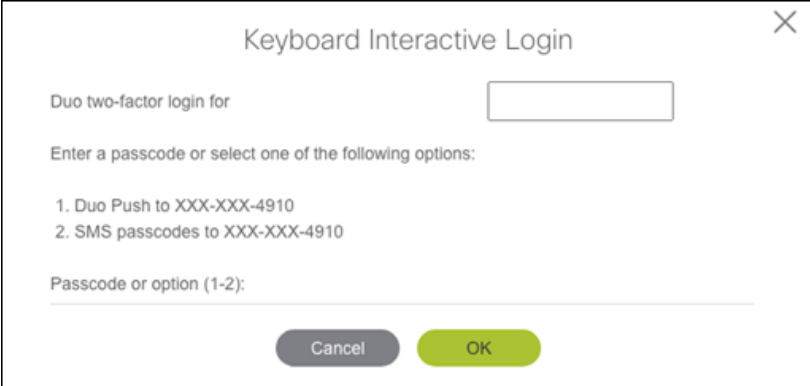
- apix.cisco.com

- apx.cisco.com

- id.cisco.com

- cway.cisco.com

- software.cisco.com

- sso.cisco.com

- storageconnect-prd.cisco.com

Q. When should I use the Keyboard Interactive feature?

A. For most devices and connections, this feature should be off. If you enable Keyboard Interactive for an SSH session that does not support this connection type, the session will fail.

This feature primarily helps manage connections that require a verification code for multifactor authentication (such as Cisco Duo or Google Authenticator). For example, you could enable the Keyboard Interactive feature for a connection using a jump server with Cisco Duo authentication.

When the Keyboard Interactive feature is enabled, you can establish a session with a device that uses multifactor authentication (MFA) by entering the appropriate information and clicking OK to connect to the device.

Q. Which version of the Cisco CLI Analyzer should I use?

A. For the best experience, we recommend running the latest version of the Cisco CLI Analyzer. Check the [Software Download area](#) to ensure that you have installed the current version.

- Starting with version 3.7.1, the Cisco CLI Analyzer uses a new authentication method. All other functionality remains the same, so we recommend discontinuing use of any previous versions.

    - You can still install and run earlier versions, but functionality will be limited.

        - You will be able to connect directly to a device via SSH.

        - You won't be able to use the diagnostic or analytical tools, or any other feature that requires you to log in (such as File Analysis, System Diagnostics, or Case Management).

    - To ensure proper functionality, [check the settings](#) for your firewall or proxy server to confirm that the correct hosts are permitted.

- Check the [version information](#) to ensure that you install the version of the application that works with your system hardware.

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

A. 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 part of the ASA config file. The file cannot be saved if this command is in the config file. To resolve this issue, ensure that this command is not enabled.

Note: To set the default behavior, add the **no crashinfo save disable** command. If a crash file is present, it will be stored in the local flash as crash.txt.

Q. Which operating systems, terminal emulation, and protocols does the Cisco CLI Analyzer support?

A. See [System Requirements](#) for information on operating systems that the Cisco CLI Analyzer supports.

The Cisco CLI Analyzer supports terminal emulator VT100.

The Cisco CLI Analyzer supports Telnet and SSH version 2.

Q. Why did File Analysis report no results or state that it was unable to determine the output provided?

A. Please ensure that the text file you want to analyze includes the following content.

- The command (such as **# show version**) that generated each output in the file

- Output from the **show version** command

- Output from the **show tech-support** command (optional, but required to perform a full analysis)

- Output from other supported commands (optional)

Q. I installed the Cisco CLI Analyzer but can't launch the application. What should I do?

A. Some versions of Windows 10 contain a bug that prevents the Cisco CLI Analyzer from launching. To address this issue, [install Visual Studio 2015-2022,](#) restart your computer, then launch the Cisco CLI Analyzer.

Q. Which expressions and characters are supported in the Cisco CLI Analyzer RegEx search feature?

A. The 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

Q. Can I make a backup copy of my application settings and results?

A. You can back up and restore from a compressed file including the settings, devices, and tool results for your Cisco CLI Analyzer installation.

Q. How do I request features or provide product feedback?

A. To request additional features or provide product feedback, use the feedback form.

Known Issues

See below for information on known behaviors of Cisco CLI Analyzer as well as applicable workaround details.

Issue	When I double-click or triple-click the mouse and then hold/drag to select additional words or lines, Cisco CLI Analyzer copies and pastes only the first word from the selected area.
Workaround	Click the mouse button once, then hold and drag to select the desired text.

Additional Resources

These demonstration videos provide more information about features of the Cisco CLI Analyzer. Each video opens in a separate browser window.

- [Console Themes](#)
- [Console Themes: Customizing](#)
- [Contextual Help and Highlighting](#)
- [Contextual Menu (Ping)](#)
- [Contextual Menu (Search)](#)
- [Contextual Menu (SSH)](#)
- [Credential Profiles](#)
- [Credential Profiles: Default Profile](#)
- [Device Coverage Checker](#)
- [Device Determination](#)
- [Device Tagging](#)
- [Favorite Commands](#)
- [File Analysis](#)

- [Font and Font Sizes](#)
- [IOS-XR Tools](#)
- [Jump Server Profiles](#)
- [Multiple Device Session Windows](#)
- [Multi-Search Highlighting](#)
- [Proxy Authentication](#)
- [Serial Connection](#)
- [Serial Connection: Send Break](#)
- [Shared Device Session](#)
- [Support Case Creation](#)
- [Support Case: Attach File](#)
- [TAC Data Collection](#)
- [Tool Results Window](#)

Submit Comments and Questions

To submit comments and questions about the Cisco CLI Analyzer, click **Feedback** in the left panel of the application. Enter your comments in the field provided, and select a star rating if you wish. Click the **Submit** button to send your feedback.

You can also visit the [Cisco CLI Analyzer Community](#) to ask questions and see comments from other users.