Cisco CLI アナライザ
ヘルプ ガイド

バージョン 3.2

2017 年 2 月 1 日

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

Cisco CLI アナライザ ユーザ ガイド

目次

新機能

このバージョンの Cisco CLI アナライザでは、次の新機能が追加されています。

- ケースの作成：対象デバイスのサポート ケースを作成および更新できます。
- **新しいプラットフォームのサポート：**Wireless LAN Controllers（WLC）の AireOS プラットフォーム
- 新しい分析ツール：
  - **パケット キャプチャ** ツールによって、トラフィックをキャプチャして結果を分析できます。
  - **TAC データ収集**ツールによって、TAC エンジニアから提供されたタスク ID に関連付けられている診断コマンドが自動的に実行されます。
  - WLC の AireOS で、[Show Run Diagnostics]ツールと [Show Tech Diagnostics] ツールを使用できます。
- ジャンプ サーバのサポート：ジャンプ サーバに接続するために必要なクレデンシャルと接続後にサーバで実行するコマンドを含むプロファイルを作成します。
- ミニ サイドバー：サイドバーを折りたたむとアイコンだけが表示され、表示領域が広がります。
- **その他の機能向上：**ターミナル ウィンドウに特殊文字 | と @ を挿入するためのキー シーケンスを定義することができます。[デバイス（Devices）] ページで、シリアル番号順にデバイスを並べ替えることができます。IP ルート分析ツールで NX-OS プラットフォームがサポートされるようになりました。またインターフェイスの細かい要素が改善され、見やすくなりました。

はじめに

Cisco CLI アナライザについて

Cisco CLI アナライザは、サポート対象デバイスの全体的なヘルスのトラブルシューティングとチェックに役立つ、スマートな SSH クライアントです。主な機能は次のとおりです。

- **システム診断：**Cisco TAC のナレッジを活用して、ASA を分析し、システム上の問題、設定ミス、ベスト プラクティス違反などの既知の問題を検出します。
- **トレースバック アナライザ：**ASA でシステム トレースバックが発生した場合に、クラッシュの根本原因と既知のバグを照合します。一致が見つかると、バグを修正済みの ASA のバージョンが提供されます。
- **パケット トレーサ：**管理者が ASA を通じて、シミュレートされたパケットをテストとして送信できます。パケットがドロップされた場合は、パケット ドロップの原因になった可能性がある ASA の設定部分または機能が特定されます。
- **ファイアウォール トップ トーカー：**ASA を通じてトラフィックを送信する、ビット レートが最も高い接続を特定します。
- **未使用ポリシー ディテクタ：**未使用のアクセス リスト、オブジェクト グループ、オブジェクトなど、未使用の設定ポリシーを検出します。検出させた設定ポリシーは設定ミスである可能性があります。このツールでは、**show run** および **show access-list | excl ^ |elem** コマンドの出力が収集されます。出力はシスコにアップロードされて分析されます。このツールの全機能は、リリース 9.x 以上の ASA で利用できます。

- **IP ルート分析:** IPv4 ルーティング テーブルを分析し、ルートの不安定性、ルート集約、サブネット プレフィックス分布、すべてのプロトコルのアドミニストレーティブ ディスタンスに関するサマリーなどのレポートが作成されます。

  注: 分析されるルート数は 100,000 までです。この制限を超えるとツールは機能しません。

- **BGP トップ トーカー:** 送受信されるメッセージ数が最も多い BGP ピアの特定に役立ちます。
- **L2VPN トップ トーカー:** 最大のパケット レートを持つレイヤ 2 VPN ポイントツーポイント回線とブリッジ ドメインを特定できます。
- **LPTS トップ トーカー:** ハードウェアからソフトウェア処理に渡されるトラフィックのタイプとレートを特定できます。
- **コンテキスト ヘルプとハイライト:** コマンド出力に基づいて、情報をインタラクティブに提供します。コンソール ウィンドウでリアルタイム検索機能を利用できます。

注: Cisco CLI アナライザを使用するには、有効な Cisco.com アカウントが必要です。有効な Cisco.com アカウントがない場合は、Cisco.com の登録ページで登録を行い、Cisco.com プロファイルにサービス契約を関連付ける必要があります。

システム要件

Cisco CLI アナライザを実行するための、ソフトウェアとハードウェアの最小要件は次のとおりです。

ソフトウェア

- Windows 7（32 ビットまたは 64 ビット）
- Mac OS X バージョン 10.9（Mavericks）以降

ハードウェア

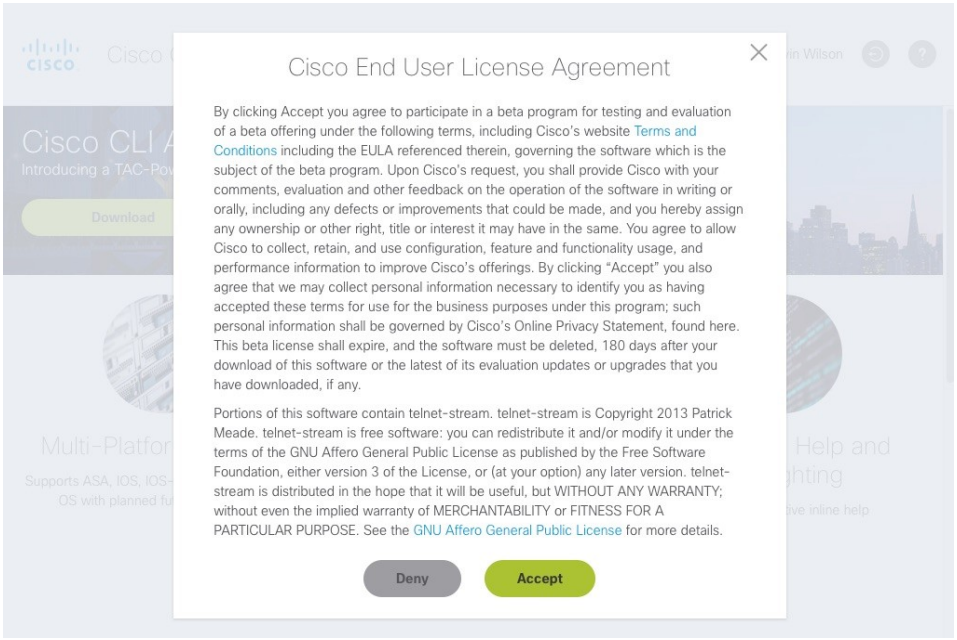
- 2 ギガバイト（GB）の RAM
- 512 メガバイト（MB）のハード ディスク空き容量

Cisco CLI アナライザのダウンロードとインストール

Cisco CLI アナライザをダウンロードしてインストールするには、次の手順を実行します。

1. ブラウザで [シスコのツールおよびリソース（Cisco Tools & Resources）] ページを開き、[Cisco CLI アナライザ（Cisco CLI Analyzer）] をクリックします。
2. Cisco CLI アナライザの Web ページでベータ版の利用規約を読み、[Cisco CLI アナライザを試す（Try the Cisco CLI Analyzer）] をクリックします。

   [シスコ エンド ユーザ ライセンス契約（Cisco End User License Agreement）]ページが表示されます。



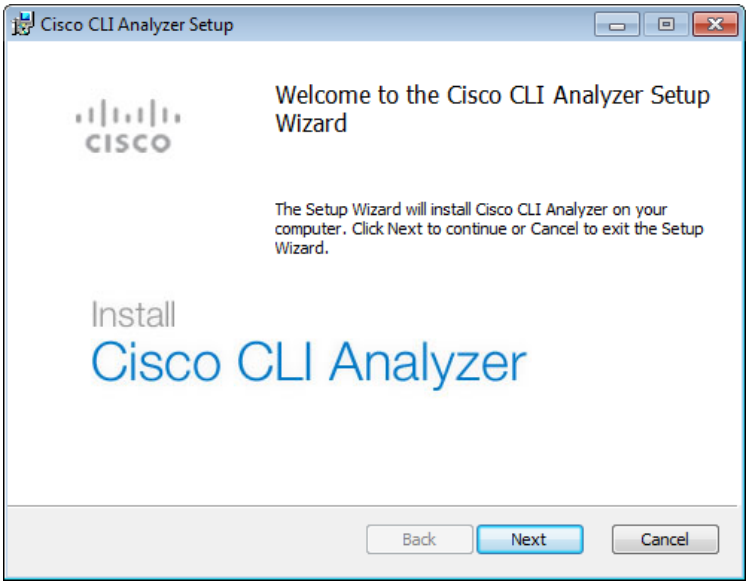
3. [同意(Accept)] をクリックします。

   [Cisco File Exchange]ページが表示されます。

4. [Cisco File Exchange]ページで、使用中のオペレーティング システムに対応するリンクをクリックします。

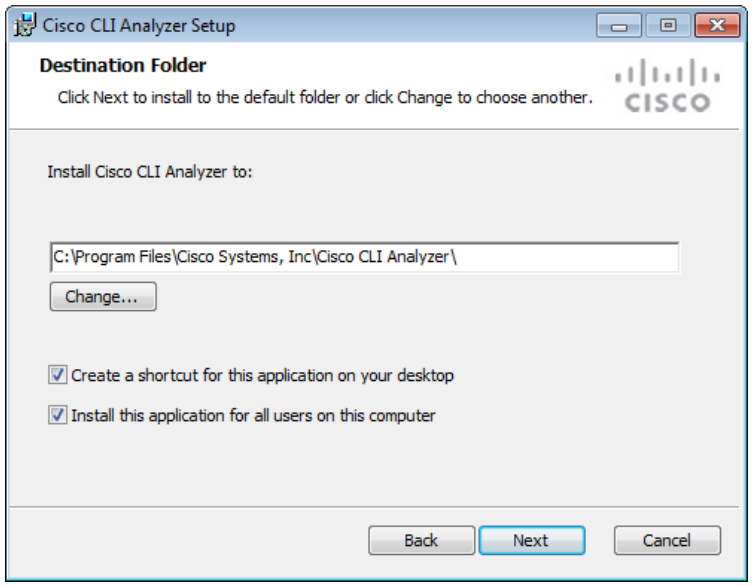
5. ファイルがダウンロードされたら、実行ファイルをダブルクリックしてインストールを開始します。

   [Cisco CLI アナライザ セットアップ ウィザード(Cisco CLI Analyzer Setup Wizard)]が表示されます。



6. [次へ(Next)] をクリックします。

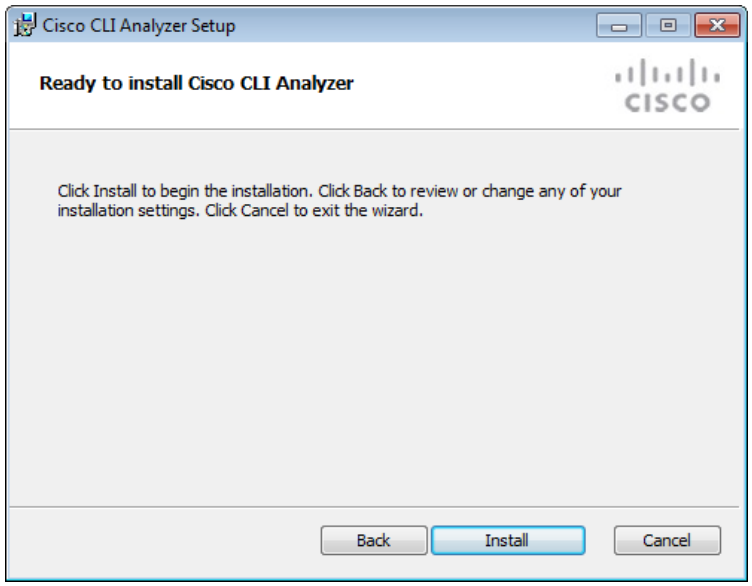
   [インストール先フォルダ(Destination Folder)]ダイアログ ウィンドウが表示されます。



デフォルトのフォルダ以外の場所にインストールするには、[変更(Change)] をクリックして、新しいインストール先フォルダを指定します。

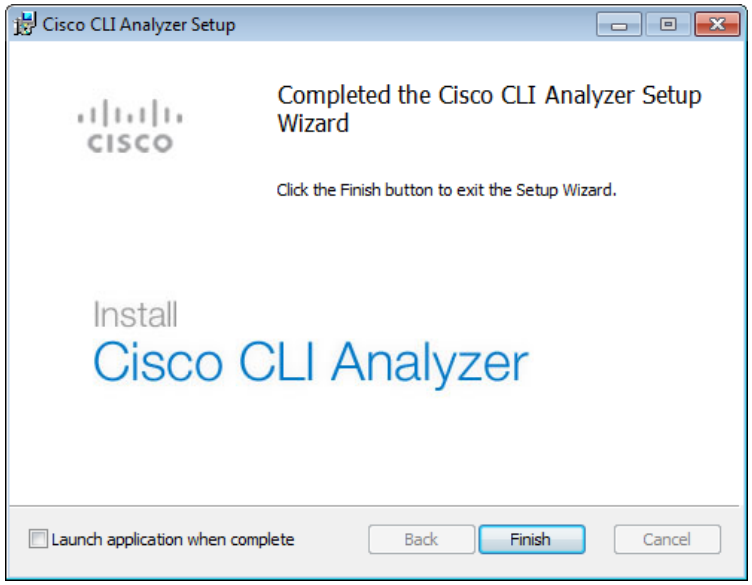
7. デスクトップ ショートカットを追加するには、[デスクトップにこのアプリケーションのショートカットを作成する(Create a shortcut for this application on your desktop)] チェックボックスをオンにします。
8. [次へ(Next)] をクリックします。

   [Cisco CLI アナライザのインストール準備が完了しました(Ready to install Cisco CLI Analyzer)]ダイアログ ウィンドウが表示されます。



9. [Cisco CLI アナライザのインストール準備が完了しました(Ready to install Cisco CLI Analyzer)] ダイアログ ウィンドウで、[インストール(Install)] をクリックします。

   インストールが完了すると、[Cisco CLI アナライザ セットアップ ウィザードが完了しました(Completed the Cisco CLI Analyzer Setup Wizard)]ダイアログ ウィンドウが表示されます。



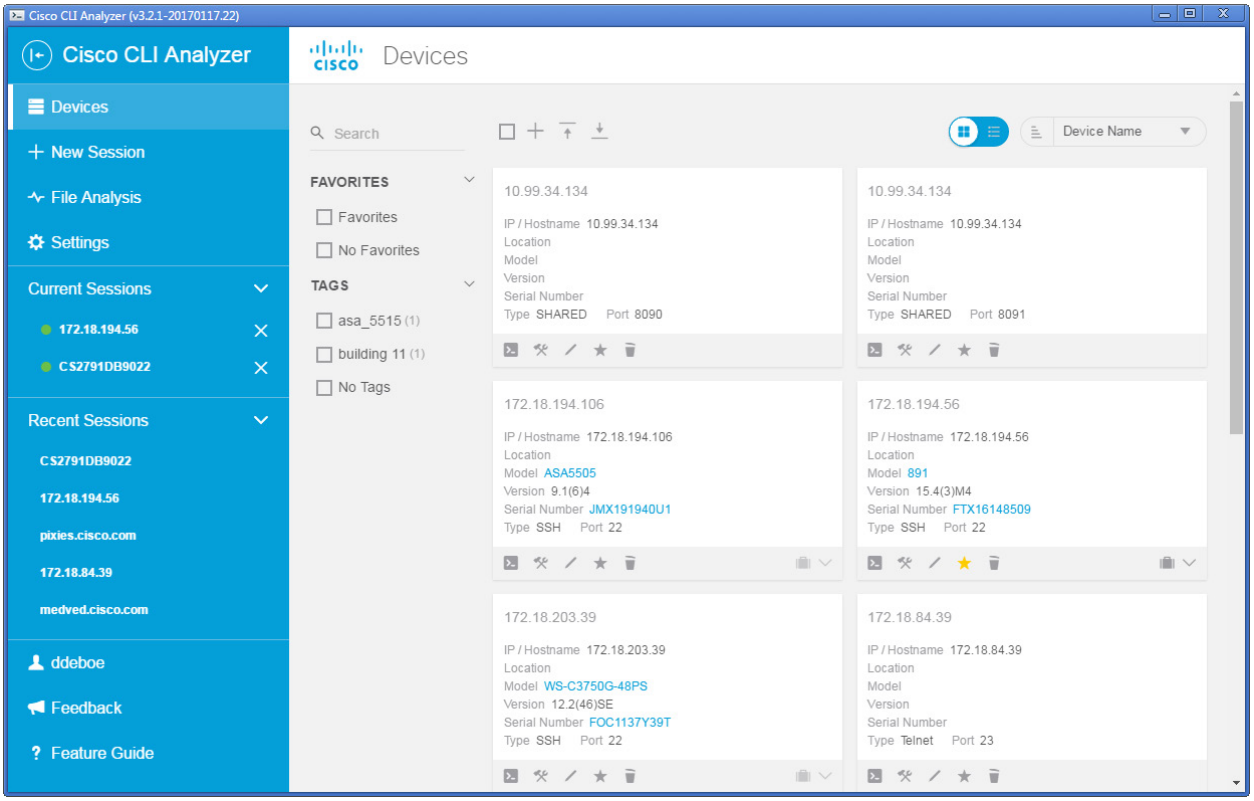
10. ウィンドウを閉じてアプリケーションを起動するには、[完了したらアプリケーションを起動する(Launch application when complete)] チェックボックスをオンにします。
11. [終了(Finish)] をクリックすると、Cisco CLI アナライザ セットアップ ウィザードが終了します。

注:インストール後に Cisco CLI アナライザの実行ファイルを再度実行すると、アプリケーションの修復または削除を行うことができます。

Cisco CLI アナライザへのアクセス

Cisco CLI アナライザのインストール後に [Cisco CLI アナライザ(Cisco CLI Analyzer)] アイコンをクリックすると、Cisco CLI アナライザ インターフェイスが表示されます。

Cisco CLI アナライザ インターフェイスは、[デバイス(Devices)]タブが選択された状態で表示されます。



[デバイス(Devices)] タブでは次の機能を使用できます。

- [現在のセッション(Current Sessions)]:いずれかのデバイスをクリックすると、そのデバイスのコンソール ウィンドウに切り替わります。接続がアクティブになっているデバイスの横には緑色の丸が表示され、切断されているデバイスの横には赤い丸が表示されます。デバイスの横の [X]をクリックすると現在のセッションが終了し、リストから削除されます。
- [最近のセッション(Recent Sessions)]:デバイスをクリックすると、[セッション ログイン(SessionLogin)]画面が表示されます。デバイスの上にポインタを置くと、そのデバイスについて、前回のアクティブ セッションの日付と時刻が表示されます。デバイスの横の [X]をクリックすると、最近のセッションがリストから削除されます。
- **ツールバー**:ツールバーには、デバイス リストの検索と並べ替え、選択したデバイスに対する一括操作、さらにデバイスの追加、インポート、エクスポートを行うオプションがあります。
- **フィルタ**:フィルタのチェックボックスをオンにすると、フィルタ条件に一致しないデバイスが非表示になります。お気に入りとしてマークしたデバイス、またはデバイスに追加したタグに基づいてフィルタリングできます。
- **折りたたみ可能サイドバー**: ボタンをクリックするとサイドバーが折りたたまれ、アイコンだけが表示されます。 ボタンをクリックすると、サイドバーが元の幅に戻り、テキスト ラベルが表示されます。

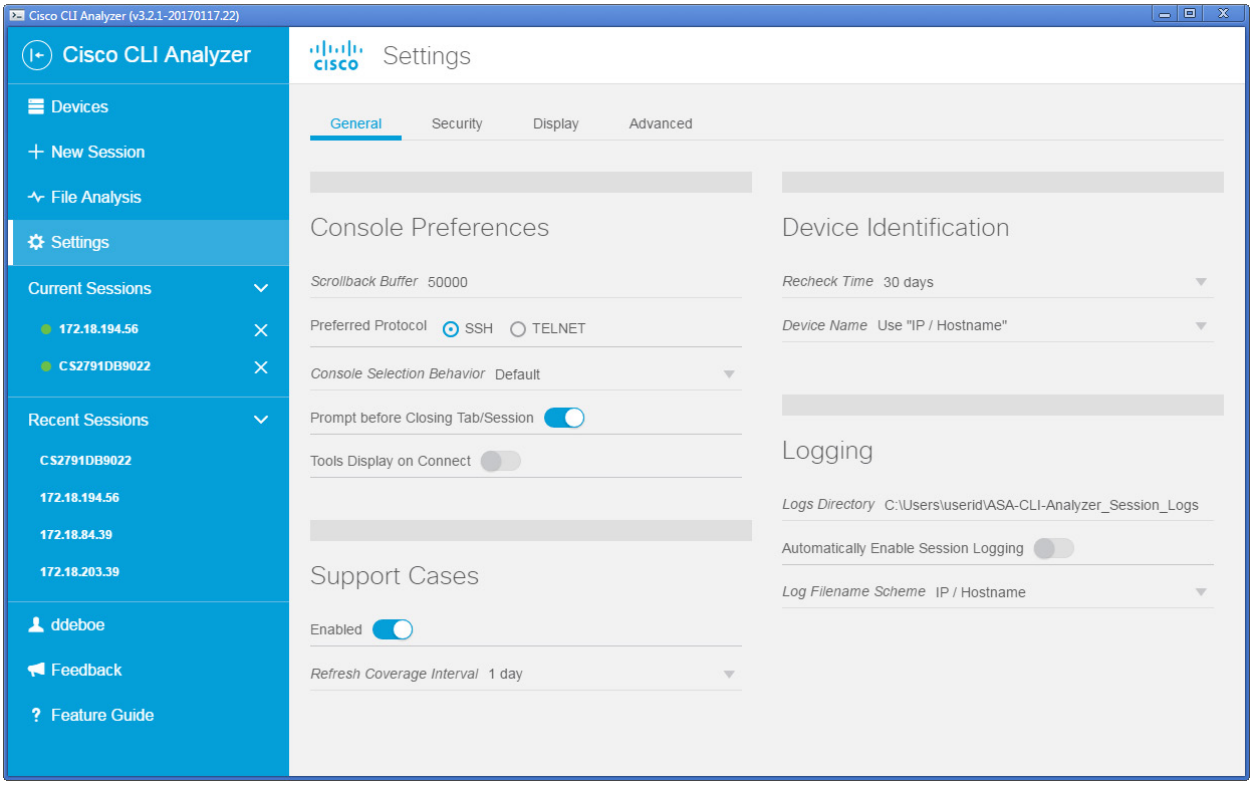
アプリケーション設定

[設定(Settings)]タブをクリックすると、グローバル コンソール設定にアクセスできます。これらの設定は、すべてのデバイス セッションに適用されます。

設定では、[全般(General)]、[セキュリティ(Security)]、[表示(Display)]、[詳細設定(Advanced)] の 4 つのタブが表示されます。

[全般(General)] タブ

これらの設定は、複数の機能に適用されます。



[コンソール設定(Console Preferences)]

- [スクロールバック バッファ(Scrollback Buffer)]:メモリに保持されるコマンドラインの数を設定できます。スクロールバック バッファを設定するには、100 ～ 50,000 の数値を入力します。
- [優先プロトコル(Preferred Protocol)]:最も頻繁に使用するプロトコル(SSH または Telnet)を選択します。このプロトコルは、新しい接続を確立するとデフォルトで選択されます。
- [コンソール選択動作(Console Selection Behavior)]:コンソール ウィンドウ内でマウスを使用してテキストを選択した場合の動作を選択します。デフォルトのテキスト選択動作に加えて、PuTTY または SecureCRT の動作をエミュレートすることもできます。
- [タブ/セッションを閉じる前にプロンプトを表示(Prompt before Closing Tab/Session)]:トグル ボタンをクリックすると、[セッションを終了(End Session)]ダイアログ ウィンドウを有効または無効にすることができます。このウィンドウは現行のセッションのタブを閉じた場合に表示され、セッションを閉じるかどうか確認するように求められます。

- [接続時にツールを表示（Tools Display on Connect）]：トグル ボタンをクリックすると、新しいデバイス セッションで分析ツールの表示または非表示を切り替えることができます。セッションを開いたときにデフォルトでツールが非表示になっている場合は、[ツール（Tools）] ボタン（）をクリックしてツールを表示させることができます。

[サポート ケース（Support Cases）]

- [有効（Enabled）]：トグルボタンをクリックすると、サポート ケースの作成を有効または無効にすることができます。この機能はデフォルトで有効になっています。
- [カバレッジ間隔の更新（Refresh Coverage Interval）]：CLI アナライザがデバイスのサポート カバレッジをチェックし、デバイス リストの情報を更新する頻度を選択します。[一括操作（Bulk Actions）]ボタンを使用して、選択したデバイスのカバレッジを手動で更新することもできます。

[デバイスの識別（Device Identification）]

- [再確認時間（Recheck Time）]：`show version` コマンド（または適切なコマンド）を自動的で実行する間隔を日数で選択します（デフォルト = 30 日）。[常に確認（Always Check）]を選択すると、デバイス セッションが開始されるたびに自動で確認されます。
- [デバイス名（Device Name）]：リストに新しく追加したデバイスの名前を、IP アドレスとルータのデバイス名のどちらにするかを選択できます。

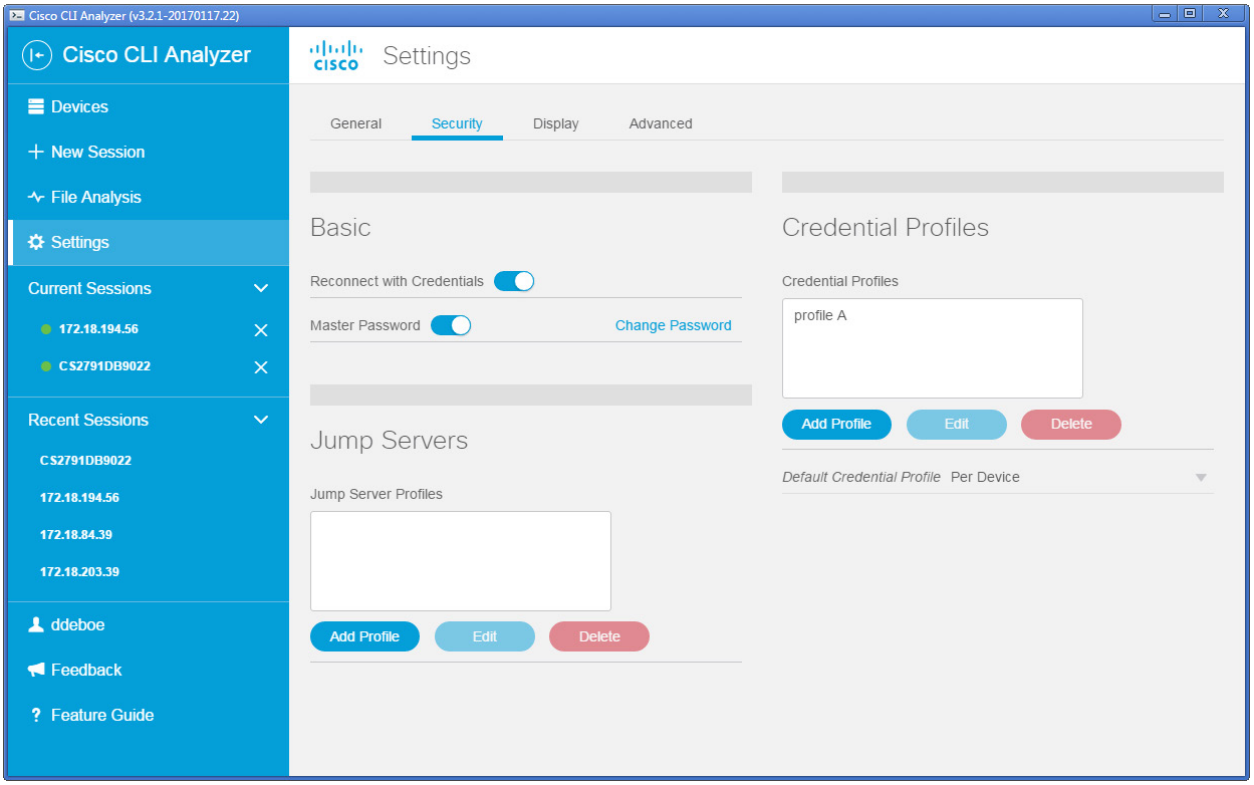
[ロギング（Logging）]

- [ログ ディレクトリ（Logs Directory）]：デフォルトでは、次の場所にログ ファイルが保存されます。
  - **Windows：**C:\Users\<userid>\Cisco-CLI-Analyzer_Session_Logs
  - **Mac OS X：**/Users/<userid>/Cisco-CLI-Analyzer_Session_Logs

  別のフォルダを選択するには、現在表示されているパスをクリックします。目的のフォルダを参照して選択し、[OK]をクリックします。
- [セッションのロギングを自動的に有効にする（Automatically Enable Session Logging）]：トグルボタンをクリックすると、自動セッション ログを有効または無効にすることができます。有効にすると、デバイスに接続したときにデフォルトでアクティビティがログに記録され、切断するとログ ファイルが自動的に保存されます。セッションのロギングは、コンソール内で手動で開始または停止することもできます。詳細については、「現行セッションのログ」を参照してください。
- [ログ ファイル名のスキーム（Log Filename Scheme）]：ログ ファイルの名前を、デバイスの IP アドレスとルータのデバイス名のどちらにするかを選択できます。

[セキュリティ(Security)] タブ

これらの設定は、デバイスとの接続に使用するクレデンシャルに影響します。



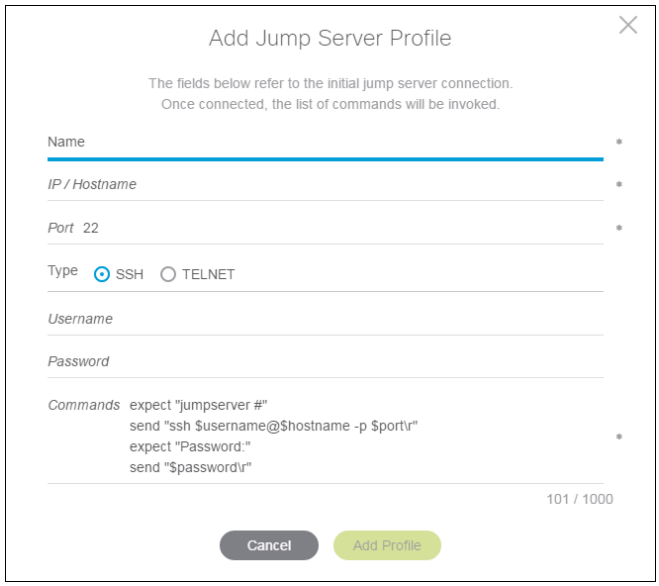
- [クレデンシャルによる再接続(Reconnect with Credentials)]:トグルボタンをクリックすると、以前に入力したログイン クレデンシャルを使用して再接続できる機能を、有効または無効にすることができます。有効にすると、セッション タブを閉じるまで、各セッション タブのログイン クレデンシャルが維持されます。
- [マスター パスワード(Master Password)]:チェックボックスをオンにすると、Cisco CLI アナライザでマスターパスワードを保存できるようになります。マスター パスワードを使用すれば、個々のデバイスのクレデンシャルを保存できるため、クレデンシャルを毎回入力する必要がありません。CLI アナライザではセキュア ハッシュ アルゴリズム 3(SHA-3)を使用することで、パスワードをハッシュ値としてデータベースに安全に保存します。

  この機能を有効にすると、Cisco CLI アナライザを開いたときに、マスター パスワードを入力するように求められます。マスター パスワードを入力しない場合は、個々のデバイス セッションに対してクレデンシャルを入力する必要があります。

  パスワードを変更するには、[パスワードの変更(Change Password)]をクリックします。古いマスター パスワードと新しいマスター パスワードを入力します。
- [クレデンシャル プロファイル(Credential Profiles)]:デバイス セッションの開始に使用するユーザプロファイルを作成および管理します。プロファイルを作成するには、[プロファイルの追加(Add Profile)]をクリックしてプロファイル名を入力し、デバイスにアクセスするためのクレデンシャルを入力します。デバイスでプロファイルを使用できるようにするには、デバイスを編集し、デバイスが承認するクレデンシャル プロファイルを選択します。

  注:一括操作機能を使用して、複数のデバイスにクレデンシャル プロファイルを割り当てることもできます。デバイスを選択し、[一括操作(Bulk Actions)]ボタンをクリックして、[クレデンシャル プロファイルの適用(Apply Credential Profile)] を選択します。

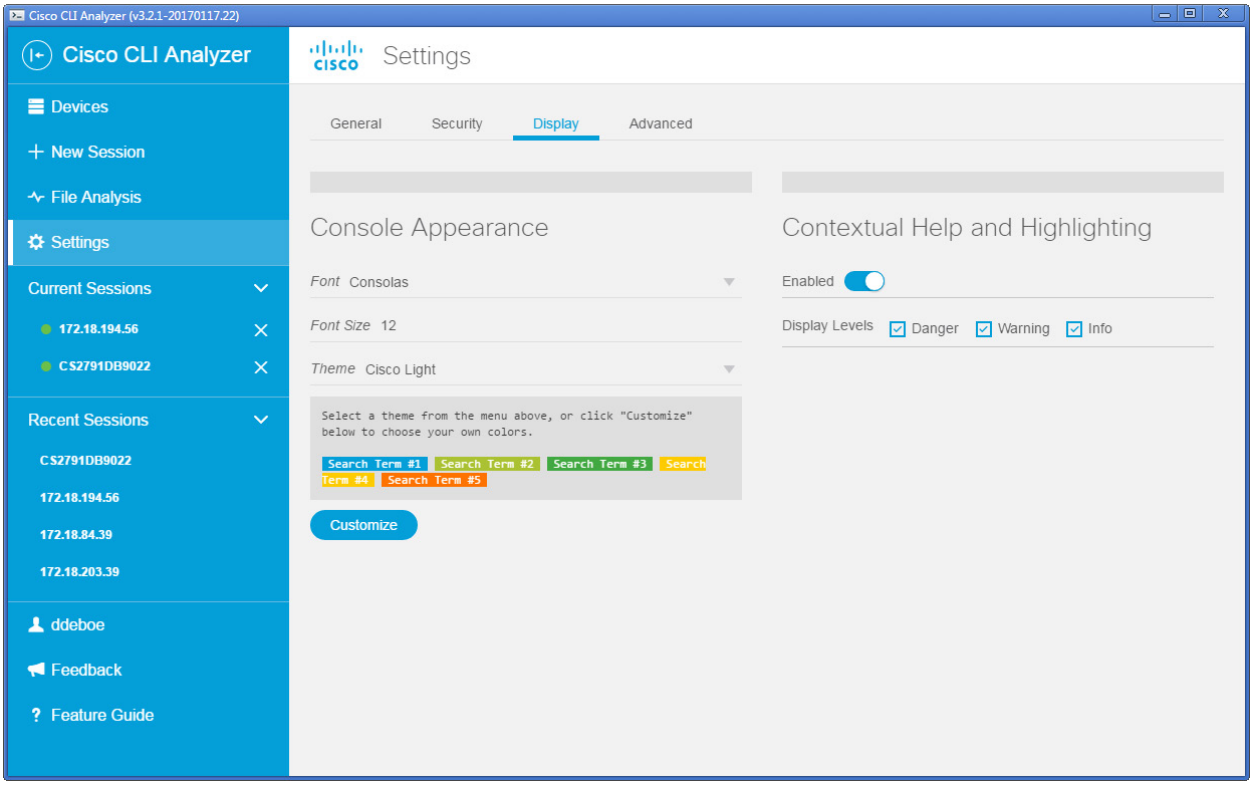
- [デフォルトのクレデンシャル プロファイル（Default Credential Profile）]：デフォルトで使用するプロファイルを選択します。[デバイスごと（Per Device）]を選択し、デフォルトのプロファイルが設定されておらず、かつデバイスがデフォルトのプロファイルを受け入れるように設定されている場合は、代わりにデバイス固有のクレデンシャルだけが承認されます。
- [ジャンプ サーバのプロファイル（Jump Server Profiles）]：ジャンプサーバに接続するために必要なクレデンシャルと接続後にサーバで実行するコマンドを含むプロファイルを作成します。プロファイルを作成するには、[プロファイルの追加（Add Profile）]をクリックします。



ジャンプ サーバの名前と IP アドレス、使用するポート番号と接続タイプ、ユーザ名とパスワードが表示されます。[コマンド（Commands）]領域で、実行するコマンドを入力します。

[表示(Display)] タブ

これらの設定は、テキスト、背景色、ハイライトの表示に影響します。



[コンソールの外観(Console Appearance)]

- [フォント(Font)]:ドロップダウンリストから、任意のフォント タイプを選択します。
- [フォント サイズ(Font Size)]:フィールド内をクリックし、8 ～ 20 のフォントサイズを入力するか、上下の矢印をクリックしてフォント サイズを変更します。
- [テーマ(Theme)]:事前定義されたカラーテーマを選択するか、[カスタマイズ(Customize)] をクリックして、独自に色を選択します。

  [カスタマイズ(Customize)]を選択すると、テキストと背景色の複数のボタンが表示されます。カラー ボタンをクリックするとカラー パレットが表示され、カラーを選択できます。[プレビュー(Preview)] ウィンドウには、現在選択しているテーマまたはカラーのプレビューが表示されます。

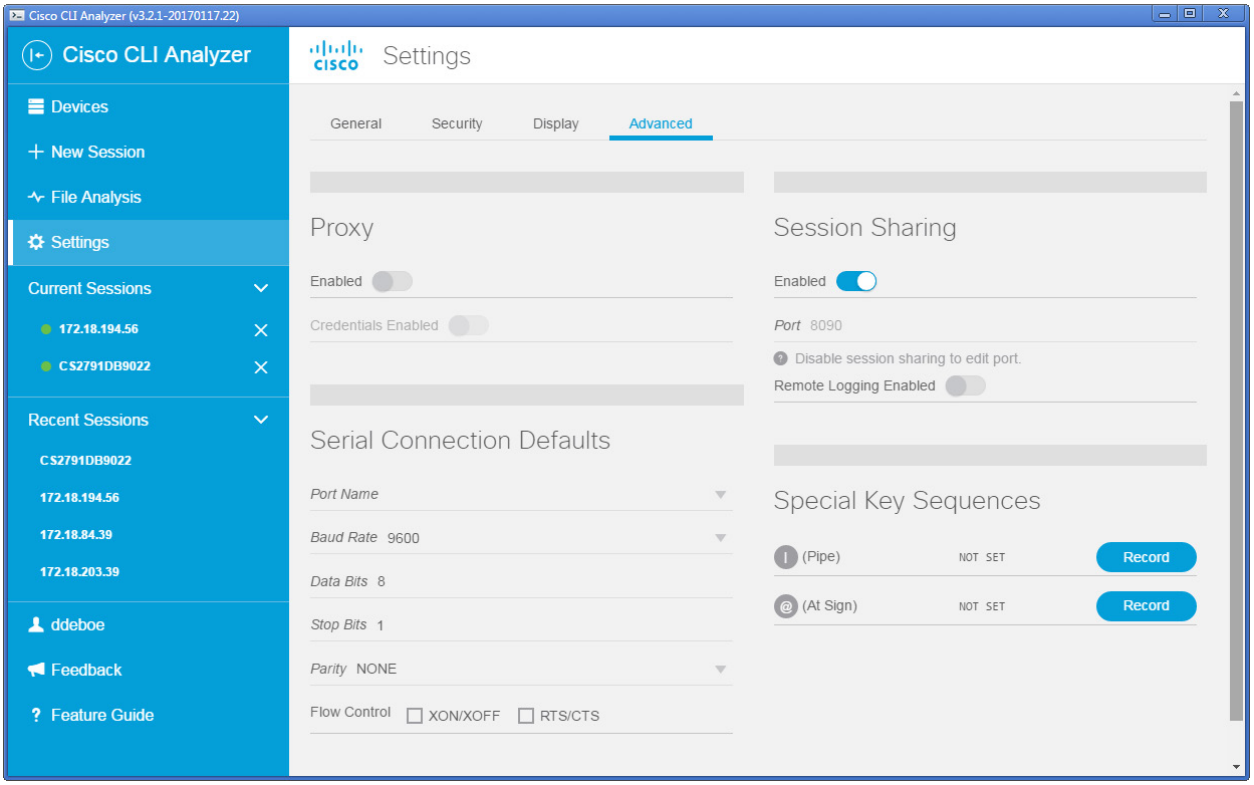
  注:検索条件では、独自のテキストと背景色が使用されます。検索方法の詳細については、「コマンド出力の検索」を参照してください。

[コンテキスト ヘルプとハイライト(Contextual Help and Highlighting)]

- [有効(Enabled)]:トグルボタンをクリックすると、コンテキスト ヘルプとハイライトを有効または無効にすることができます。この機能はデフォルトで有効になっています。詳細については、「コンテキスト ヘルプとハイライト」を参照してください。
- [表示レベル(DisplayLevels)]:表示する通知のタイプ([危険(Danger)]、[警告(Warning)]、[情報(Info)])を選択します。除外する(無効にする)通知タイプの横にあるチェックボックスをオフにします。

[詳細設定(Advanced)] タブ

これらの設定は、プロキシ サーバ、シリアル接続、共有セッションに適用されます。



[プロキシ(Proxy)]

- [有効(Enabled)]:トグルボタンをクリックすると、アウトバウンド Web 接続におけるプロキシ サーバの使用を有効にします。

  [プロキシ設定の有効化(Enable Proxy Settings)]ウィンドウが自動的に開きます。以下のフィールドに入力します。

  - [プロトコル(Protocol)]:フィールド内をクリックし、ドロップダウンリストからプロトコルを選択します。サポートされているプロトコルとしては、HTTP、HTTPS、Socks、Socks5 などがあります。
  - [ホスト(Host)]:プロキシサーバの IP アドレスを入力します。
  - [ポート(Port)]:使用するポート番号を入力します。

  注:プロキシ設定をアクティブにするには、*アプリケーションを再起動*する必要があります。

- [クレデンシャルの有効化(Credentials Enabled)]:トグルボタンをクリックして、プロキシ サーバのユーザ名とパスワードを入力します。

シリアル接続のデフォルト

注:TAC ツールは、シリアル接続を行うデバイス セッションでは使用できません。

- [ポート名(Port Name)]:シリアル接続で使用する COM ポートを選択するか、ポート番号を手動で入力します。ドロップダウン リストには、システムで検出されたアクティブな COM ポートだけが表示されます。
- [ボー レート(Baud Rate)]:シリアル接続で使用するボーレートを選択します。コンソール ウィンドウにコンテンツが正しく表示されないときは、この値を調整すると正しく表示される場合があります。

- [データ ビット(Data Bits)]:使用するデータビット数を入力するか、上下の矢印をクリックしてビット数を調整します。
- [ストップ ビット(Stop Bits)]:使用するストップビット数を入力するか、上下の矢印をクリックしてビット数を調整します。
- [パリティ(Parity)]:シリアル接続で使用するパリティタイプを選択します。
- [フロー制御(Flow Control)]:シリアル接続で使用するフロー制御のタイプを選択します。

セッション共有

注: セッション共有では AES-256 暗号化が使用されます。

- [有効化(Enabled)]:トグルボタンをクリックすると、共有デバイス セッションが有効になります。
- [ポート(Port)]:共有デバイスセッションで使用するポート番号を入力します(ポート番号を変更するには、セッション共有を無効にする必要があります)。共有セッションへの接続を求めるリモート ユーザには、このポート番号を通知する必要があります。
- [リモート ロギングの有効化(Remote Logging Enabled)]:有効にすると、リモートユーザはデバイス セッションのログを記録するオプションを選択できます。

特殊なキー シーケンス

ターミナル ウィンドウに特殊文字「|」と「@」を挿入するためのキーの組み合わせを指定することができます。

キー シーケンスを設定するには、[記録(Record)]ボタンをクリックし、目的のキーの組み合わせを押して、[設定(Set)]をクリックします。記録されたキー シーケンスを削除するには、シーケンスの横の [X] をクリックします。

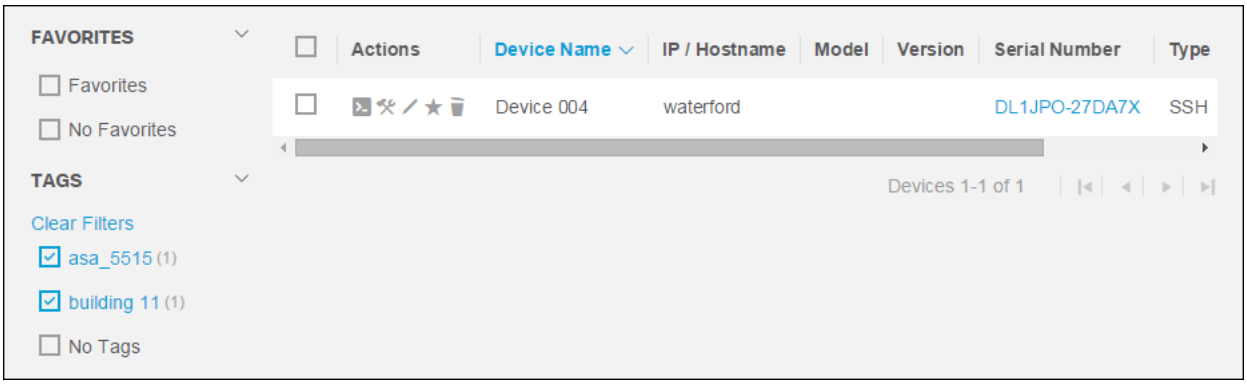
デバイスの管理

デバイスの検索

デバイス リスト内の特定のデバイスを見つけるには、フィルタと検索を使用します。

フィルタ

フィルタは、タグとお気に入りステータスに基づいて設定できます。デバイス リストの左側のフィルタ ボックスをオンにすると、選択したタグまたは選択したお気に入りステータス(お気に入りまたはお気に入り以外)が設定されたデバイスだけが表示されます。

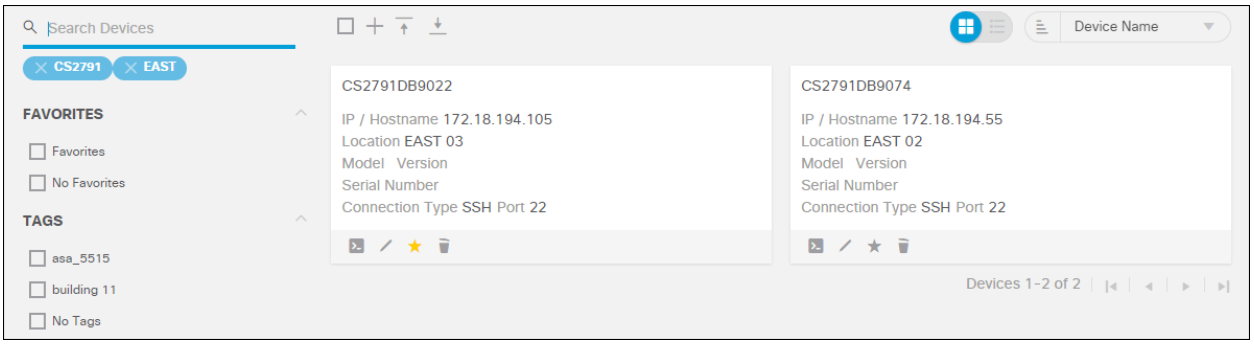


アクティブなフィルタをすべて削除するには、フィルタ チェックボックスの上の [フィルタのクリア(Clear Filters)]をクリックします。デバイス リストにすべてのデバイスが表示されます。

検索

プロパティに特定のキーワードが含まれているデバイスだけがデバイス リストに表示されるようにするには、[検索(Search)] ボックスにキーワードを入力して **Enter** を押します。

[検索(Search)]ボックスの下のバブルにキーワードが表示されます。アクティブ フィルタは保持され、他のフィルタ選択と組み合わせることができます。アクティブ フィルタからキーワードを削除するには、キーワード バブルの [X] をクリックします。



デバイスの並べ替え

表示されたリスト ビューで列ヘッダーをクリックすると、そのプロパティでリストを並べ替えることができます。列ヘッダーをもう一度クリックすると、並べ替えの昇順と降順が切り替わります。

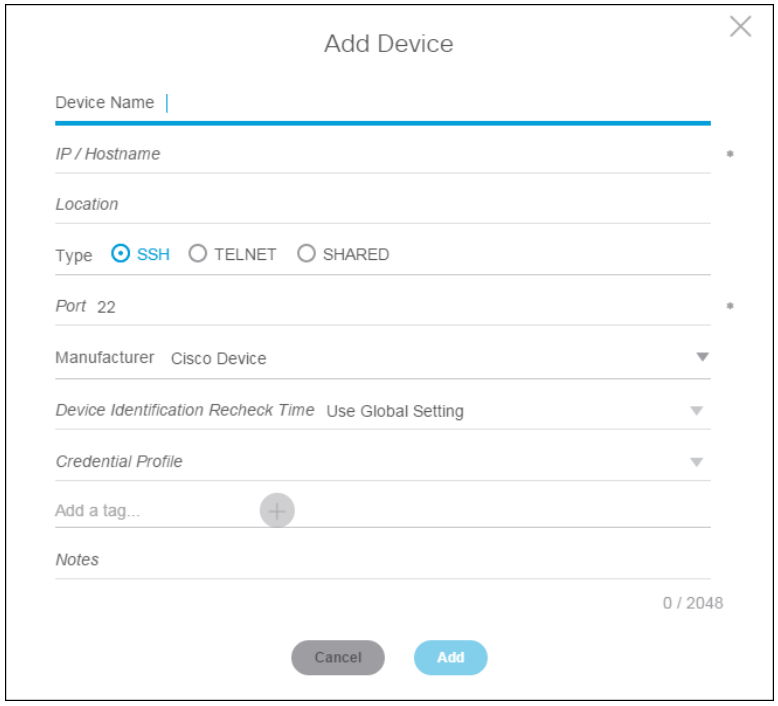
リスト ビューまたはグリッド ビューが表示されている場合は、[並べ替え基準(Sort By)] ボタン(Activity Date)をクリックすると、ドロップダウン リストから並べ替え順序を選択できます。[並べ替え(Sort)] ボタン( )をクリックすると、昇順と降順を切り替えることができます。

デバイス リストへのデバイスの追加

デバイス リストにデバイスを追加するには、以下の手順に従います。

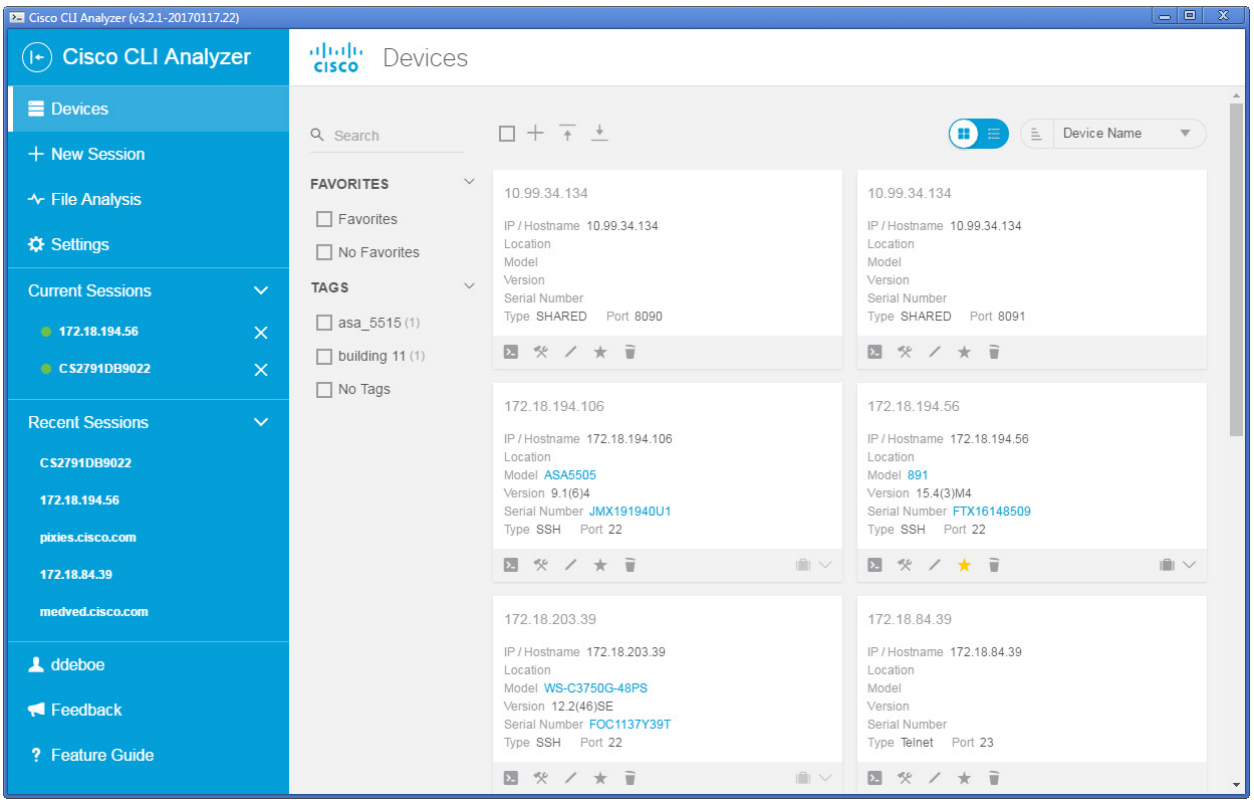
1. Cisco CLI アナライザで、[デバイス(Devices)] タブをクリックし、[クイック接続(Quick Connect)] ボックスの下にあるデバイス リスト ツールバーの [デバイスの追加(Add Device)] ボタン(+)をクリックします。

   [デバイスの追加(Add Device)]ダイアログ ウィンドウが表示されます。



2. [デバイス名(Device Name)] フィールドにデバイスの名前を入力します。
3. [IP/ホスト名(IP/Hostname)]フィールドに、IP アドレスまたはホスト名を入力します。
4. [ロケーション(Location)] フィールドに、デバイスの物理的な場所を入力します。
5. 使用する接続タイプ(**SSH**、**TELNET**、**SHARED**)のオプション ボタンをクリックします。
6. 非標準のポート番号を使用する場合は、[ポート(Port)] フィールドに入力します。
7. [製造元(Manufacturer)]フィールドで、[シスコ デバイス(Cisco Device)] または [シスコ以外のデバイス(Non-Cisco Device)] を選択します。
8. [デバイス識別の再確認時間(Device Identification Recheck Time)]フィールドで、デバイスとの接続時に `show version` コマンドを実行する頻度を選択します。[設定(Settings)]ページの [全般(General)] タブで定義したグローバル設定を使用するか、デバイスに対して個別の設定を選択します。
9. [クレデンシャル プロファイル(Credential Profile)]フィールドで、デバイスとの接続に使用するプロファイルを選択します。デバイスでユーザ クレデンシャル プロファイルが承認されないようにするには、[デバイスごと(Per Device)]を選択します。
10. デバイスについて説明するタグを 1 つ以上割り当てます。[タグを追加...(Add a tag...)] をクリックしてタグを入力し、 + ボタンをクリックします。
11. 必要に応じて、デバイスに関する追加情報を [注記(Notes)]フィールドに入力します。
12. [追加(Add)] をクリックします。

デバイス リストにデバイスが追加されます。



デバイス リストにデバイスを追加すると、次のアクションが可能になります。

- デバイスの下の [接続(Connect)] ボタン( )をクリックすると、そのデバイスに接続できます。
- デバイスの下の [ツール(Tools)] ボタン( )をクリックすると、[ツールの結果(Tools Results)] ウィンドウに、そのデバイスのツールの結果が表示されます。
- デバイスの下の [編集(Edit)] ボタン( )をクリックすると、[デバイスの編集(Edit Device)] ウィンドウが開き、デバイス情報を更新できます。
- デバイスの下の [お気に入り(Favorites)] ボタン( )をクリックすると、そのデバイスがお気に入りに追加されます。ボタン アイコンがオレンジ色のスター( )に変わります。ボタンを再度クリックすると、そのデバイスがお気に入りから削除されます。
- デバイスのシリアル番号のハイパーリンクをクリックすると、デバイスのサービス契約のステータスを確認できます。ブラウザ ウィンドウで Cisco Device Coverage Checker ツールが開きます。

デバイス リストにデバイスを追加したら、次のアクションでリスト内を移動できます。

- デバイスにポインタを合わせて [選択(Select)] ボタン( )をクリックし、デバイスを選択します。デバイスがハイライトされ、[一括操作(Bulk Actions)]ボタンが有効になります。デバイスの選択を解除するには、デバイスの任意の場所をクリックします。
- [すべて選択(Select All)] ボタン( )をクリックすると、リスト内のすべてのデバイスが選択されます。ボタン アイコンが( )に変わり、すべてのデバイスが選択されていることを示します。[一括操作(Bulk Actions)] ボタンが有効になります。
- 1 つ以上のデバイスを選択し、[一括操作(Bulk Actions)] ボタン(Bulk Actions)をクリックします。次にドロップダウン リストからオプションをクリックして、アクション([接続(Connect)]、[カバレッジのチェック(Check Coverage)]、[クレデンシャル プロファイルの適用(Apply Credential Profile)]、[カバレッジの更新(Refresh Coverage)]、[デバイスの削除(Delete Devices)]、[タグの追加(Add Tags)]、[タグの削除(Delete Tags)])を実行します。

- [並べ替え基準(Sort By)] ボタン(Activity Date)をクリックし、ドロップダウン リストからプロパティを選択すると、選択したプロパティでデバイス リストを並べ替えることができます。
- [並べ替え(Sort)] ボタン( )をクリックすると、並べ替え順序が降順から昇順に変わります。ボタン アイコンが昇順( )に変わります。
- フィルタ チェックボックスをオンにすると、選択したフィルタに一致するデバイスだけが表示されます(たとえば [お気に入り以外(No Favorites)] チェックボックスをオンにすると、お気に入りとしてマークされていないデバイスだけが表示されます)。
- デバイス リストを検索するには、[デバイスの検索(Search Devices)] フィールドに検索条件を入力して **Enter** を押します。

CSV ファイルからのデバイスのインポート

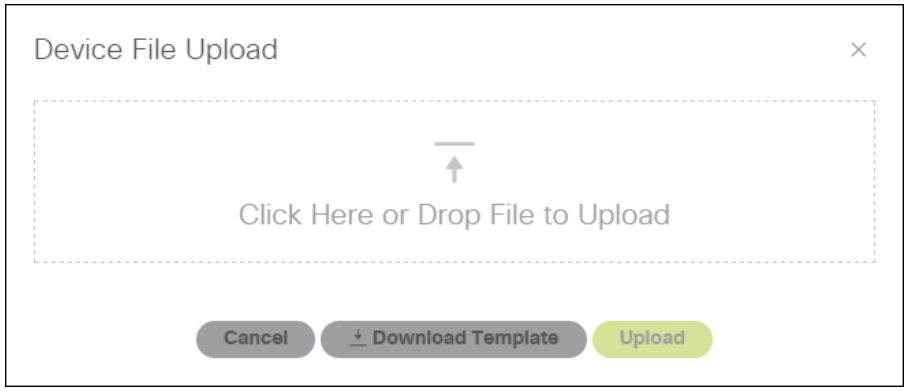
CSV ファイルからデバイス リストにデバイスをインポートできます。

注: インポートされたデバイスは、[設定(Settings)] ページの [セキュリティ(Security)]タブで選択された、デフォルトのクレデンシャル プロファイルを承認するように設定されています。デフォルトのクレデンシャル プロファイル設定が [デバイスごと(Per Device)]である場合、インポートされたデバイスでは個別のクレデンシャルだけが承認されます。

CSV ファイルをインポートするには、次の手順を実行します。

1. Cisco CLI アナライザの [デバイス(Devices)] タブで、([クイック接続(Quick Connect)] 領域の下にある)デバイス リスト ツールバーの [アップロード(Upload)] ボタン( )をクリックします。ドロップダウン メニューから [CSV からインポート(Import from CSV)] を選択します。

   [デバイス ファイルのアップロード(Device File Upload)]ダイアログ ウィンドウが表示されます。



2. 次のいずれかの手順を実行します。
   - [アップロードするファイルをクリックまたはドロップ(Click or drop file to upload)]をクリックします。[開く(Open)] ダイアログで、インポートする CSV ファイルに移動して選択し、[開く(Open)] をクリックします。
   - [アップロードするファイルをクリックまたはドロップ(Click or drop file to upload)] のテキストの上に、別のウィンドウから CSV ファイルをドラッグします。ポインタの下のアイコンが、ファイルが移動されることを示していることを確認して、マウス ボタンを放してファイルをドロップします。
3. [アップロード(Upload)] をクリックします。

CSV ファイルからインポートされたデバイスがデバイス リストに表示されます。

PuTTY からのデバイスのインポート

PuTTY エクスポート ファイルからデバイス リストにデバイスをインポートできます。インポートするには、Windows レジストリの設定で自動的に行う方法と、作成した設定ファイルから手動で行う方法の 2 通りがあります。

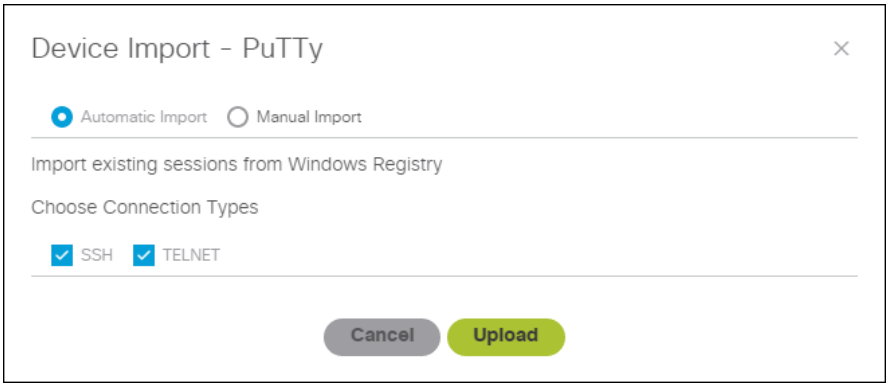
注: インポートされたデバイスは、[設定(Settings)] ページの [セキュリティ(Security)]タブで選択された、デフォルトのクレデンシャル プロファイルを承認するように設定されています。デフォルトのクレデンシャル プロファイル設定が [デバイスごと(Per Device)]である場合、インポートされたデバイスでは個別のクレデンシャルだけが承認されます。

必要に応じて、自動インポートと手動インポートのどちらかの手順に従います。

自動インポート

1. Cisco CLI アナライザの [デバイス(Devices)] タブで、([クイック接続(Quick Connect)] 領域の下にある) デバイス リスト ツールバーの [アップロード(Upload)] ボタン( )をクリックします。ドロップダウン メニューから [PuTTY からインポート(Import from PuTTY)] を選択します。

   [デバイスのインポート - PuTTY(Device Import - PuTTY)]ダイアログ ウィンドウが表示されます。



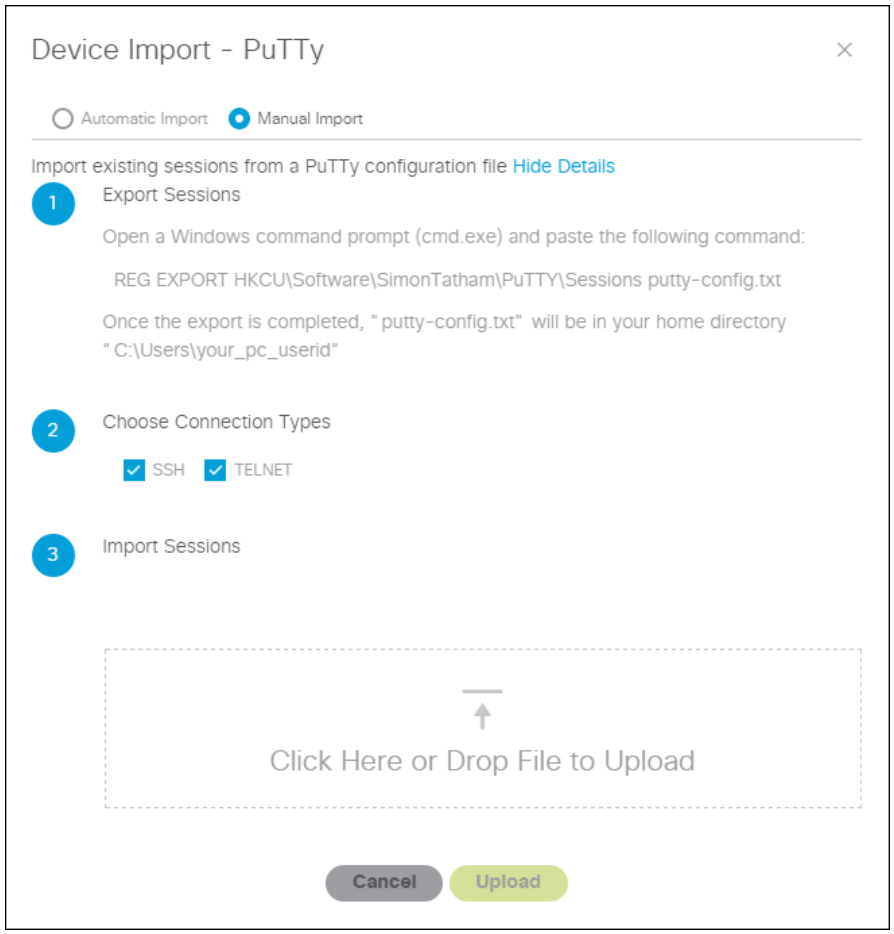
2. インポートする接続タイプ([SSH] と [Telnet]のいずれかまたは両方)を選択します。デフォルトでは両方のチェックボックスがオンになっています。
3. [アップロード(Upload)]をクリックし、アップロード プロセスが完了するまで待ちます。アップロード中に発生したエラーについては、アプリケーションの右下隅に表示されます。

手動インポート

1. Cisco CLI アナライザの [デバイス(Devices)] タブで、([クイック接続(Quick Connect)] 領域の下にある) デバイス リスト ツールバーの [アップロード(Upload)] ボタン( )をクリックします。ドロップダウン メニューから [PuTTY からインポート(Import from PuTTY)] を選択します。

   [デバイスのインポート - PuTTY(Device Import - PuTTY)]ダイアログ ウィンドウが表示されます。

2. ウィンドウの上部にある [手動インポート(Manual Import)] を選択します。
3. [詳細を表示(View Details)] をクリックすると、ウィンドウが拡張され、詳細な手順が表示されます。



4. コマンド シェル ウィンドウを開きます。コマンド プロンプトで、次のテキストを入力するか、コピーして貼り付けます。

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

5. Enter を押します。ホーム ユーザ ディレクトリに `putty-config.txt` ファイルが作成されます。

   C:\Users\<your_user_name>

6. [デバイスのインポート - PuTTY（Device Import - PuTTY）] ダイアログ ウィンドウで、インポートに使用する接続タイプ（[SSH] と [Telnet] のいずれかまたは両方）を選択します。デフォルトでは両方のチェックボックスがオンになっています。

7. 次のいずれかの方法で、PuTTY エクスポート ファイル `putty-config.txt` をアップロードします。

   - Windows Explorer で、エクスポート ファイルが含まれているフォルダを開きます。Windows Explorer からファイルをドラッグし、[デバイスのインポート（Import Devices）] ダイアログ ウィンドウの [ここをクリックするか、アップロードするファイルをドラッグ アンド ドロップする（Click here or drag & drop the file to upload）] にドロップします。
   - [デバイスのインポート（Import Devices）] ダイアログ ウィンドウで、[ここをクリックするか、アップロードするファイルをドラッグ アンド ドロップする（Click here or drag & drop the file to upload）]をクリックします。PuTTY エクスポート ファイルが含まれているフォルダを参照し、ファイルを選択して、[開く（Open）] をクリックします。

8. [アップロード（Upload）]をクリックし、アップロード プロセスが完了するまで待ちます。アップロード中に発生したエラーについては、アプリケーションの右下隅に表示されます。

SecureCRT からのデバイスのインポート

SecureCRT エクスポート ファイルからデバイス リストにデバイスをインポートできます。

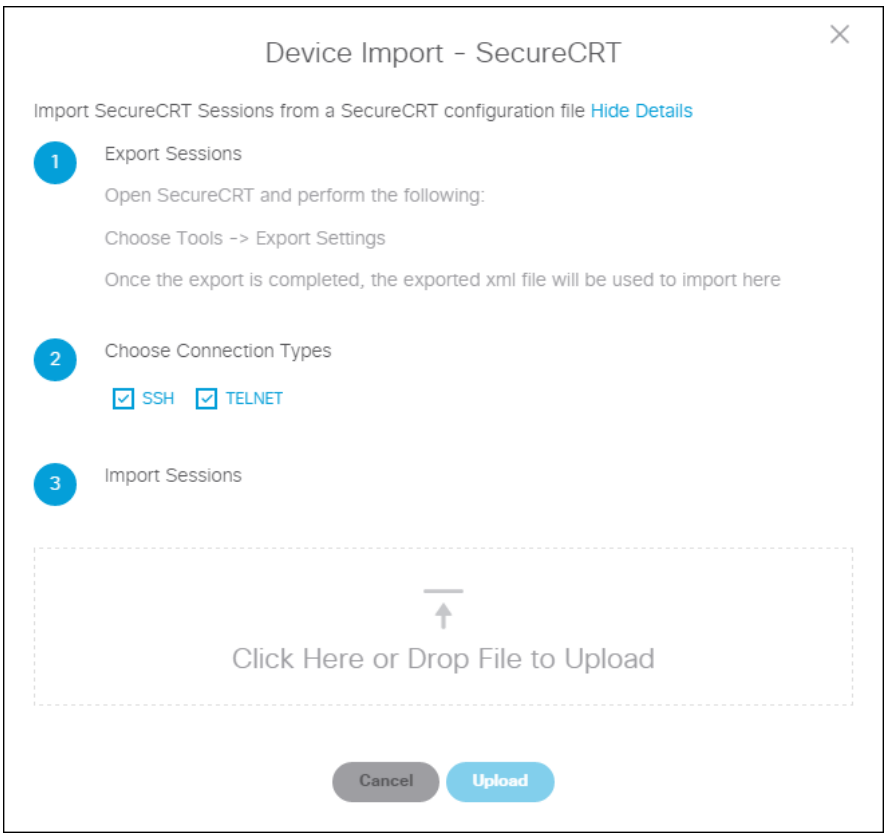
注:インポートされたデバイスは、[設定(Settings)] ページの [セキュリティ(Security)]タブで選択された、デフォルトのクレデンシャル プロファイルを承認するように設定されています。デフォルトのクレデンシャル プロファイル設定が [デバイスごと(Per Device)]である場合、インポートされたデバイスでは個別のクレデンシャルだけが承認されます。

ファイルを作成してインポートするには、次の手順を実行します。

1. Cisco CLI アナライザの [デバイス(Devices)] タブで、([クイック接続(Quick Connect)] 領域の下にある)デバイス リスト ツールバーの [アップロード(Upload)] ボタン( )をクリックします。ドロップダウン メニューから [SecureCRT からインポート(Import from SecureCRT)] を選択します。

   [デバイスのインポート - SecureCRT(Device Import - SecureCRT)]ダイアログ ウィンドウが表示されます。

2. [詳細を表示(View Details)] をクリックすると、ウィンドウが拡張され、詳細な手順が表示されます。



3. SecureCRT を開きます。[ツール(Tools)] メニューから [設定のエクスポート(Export Settings)]を選択します。エクスポート プロセスを実行し、エクスポート ファイルの場所をメモします。

4. [デバイスのインポート - SecureCRT(Device Import - SecureCRT)] ダイアログ ウィンドウで、インポートに使用する接続タイプ([SSH] と [Telnet] のいずれかまたは両方)を選択します。デフォルトでは両方のチェックボックスがオンになっています。

5. 次のいずれかの方法で、SecureCRT エクスポート ファイルをアップロードします。
   - Windows Explorer で、エクスポート ファイルが含まれているフォルダを開きます。Windows Explorer からファイルをドラッグし、[デバイスのインポート(Import Devices)] ダイアログ ウィンドウの [ここをクリックするか、アップロードするファイルをドラッグ アンド ドロップする(Click here or drag & drop the file to upload)] にドロップします。
   - [デバイスのインポート(Import Devices)] ダイアログ ウィンドウで、[ここをクリックするか、アップロードするファイルをドラッグ アンド ドロップする(Click here or drag & drop the file to upload)]をクリックします。SecureCRT エクスポート ファイルが含まれているフォルダを参照し、ファイルを選択して、[開く(Open)] をクリックします。
6. [アップロード(Upload)]をクリックし、アップロード プロセスが完了するまで待ちます。アップロード中に発生したエラーについては、アプリケーションの右下隅に表示されます。

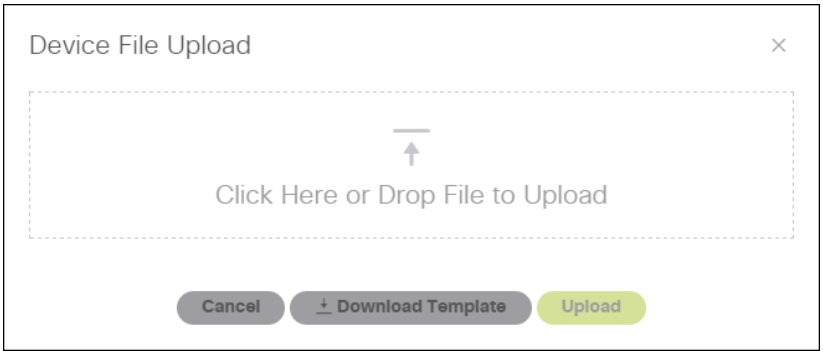
デバイスの CSV ファイルの作成

デバイス情報の CSV ファイルを作成し、任意のワークステーションの Cisco CLI アナライザにインポートできます。

CSV ファイルを作成するには、次の手順を実行します。

1. Cisco CLI アナライザの [デバイス(Devices)] タブで、([クイック接続(Quick Connect)] 領域の下にある)デバイス リスト ツールバーの [アップロード(Upload)] ボタン( )をクリックします。

   [デバイス ファイルのアップロード(Device File Upload)]ダイアログ ウィンドウが表示されます。



2. [テンプレートのダウンロード(Download Template)] をクリックします。

   [名前を付けて保存(Save As)]ダイアログ ウィンドウが表示されます。
3. CSV テンプレートを保存する場所に移動し、[保存(Save)] をクリックします。
4. 任意のアプリケーションで CSV ファイルを開きます。
5. 各デバイスの情報をそれぞれ別の行に入力します。次の情報は必須です。
   - IP アドレスまたはホスト名 (DNS)
   - プロトコル

   その他のデバイス情報は、Cisco CLI アナライザから任意で追加できます。

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

6. 完了したら、[保存(Save)] をクリックします。

デバイスのエクスポート

デバイス リストのデバイス情報を CSV ファイルにエクスポートできます。それにより、別のワークステーションに情報をインポートできます。

デバイス情報を CSV ファイルにエクスポートするには、次の手順を実行します。

1. Cisco CLI アナライザの [デバイス(Devices)] タブで、([クイック接続(Quick Connect)] 領域の下にある) デバイス リスト ツールバーの [エクスポート(Export)] ボタン( )をクリックします。

   [名前を付けて保存(Save As)]ダイアログ ウィンドウが表示されます。

2. コンピュータの任意の場所に移動し、必要に応じて CSV ファイルのファイル名を変更して、[保存(Save)] をクリックします。

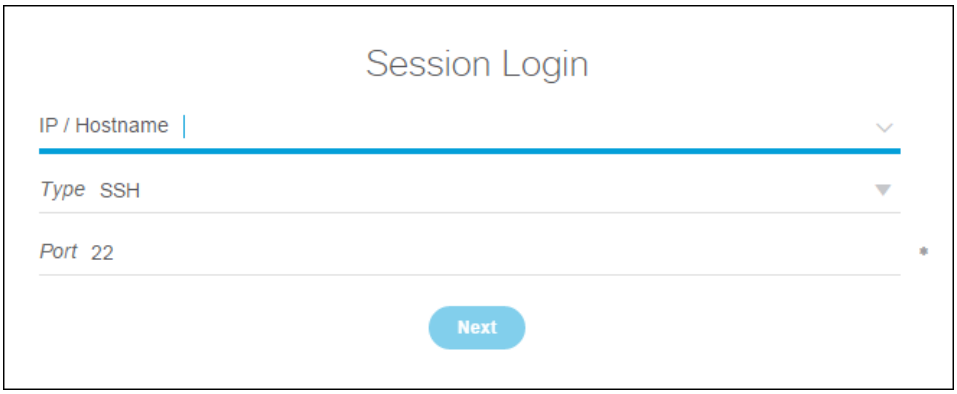
デバイスとの接続(SSH または Telnet)

SSH または Telnet 接続タイプを使用してデバイスに接続するには、次の手順を実行します。

1. [デバイス(Devices)] タブで、次のいずれかのアクションを実行して新しいセッションを開始します。
   - 左パネルの [新規セッション(New Session)] をクリックします。
   - [最近のセッション(Recent Sessions)] リスト内のデバイスをクリックします。
   - デバイス リスト内のデバイス エントリで、 ボタンをクリックします。

   新しいセッション タブが表示され、[セッション ログイン(Session Login)]画面が開きます。

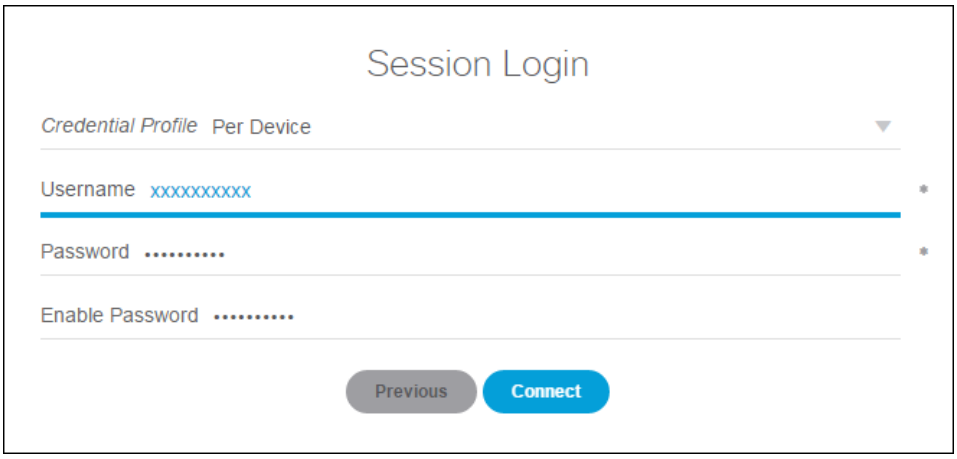
2. デバイスの基本的な接続情報を入力するように求められたら、必要な情報を入力し、[次へ(Next)]をクリックします。その他の場合は、このステップをスキップしてステップ 3 に進みます。
   - [IP/ホスト名(IP/Hostname)]フィールドに、デバイスの IP アドレスまたはホスト名を入力します。このフィールドの横の矢印をクリックして、最近のセッションで接続したデバイスを選択することもできます。
   - 使用する接続タイプ([SSH] または [TELNET])を選択します。
   - [ポート(Port)] フィールドに適切なポート番号を入力します。



   Cisco CLI アナライザがデバイスとの接続をチェックします。デバイスが見つかった場合は、ログイン情報を承認する画面に変わります。

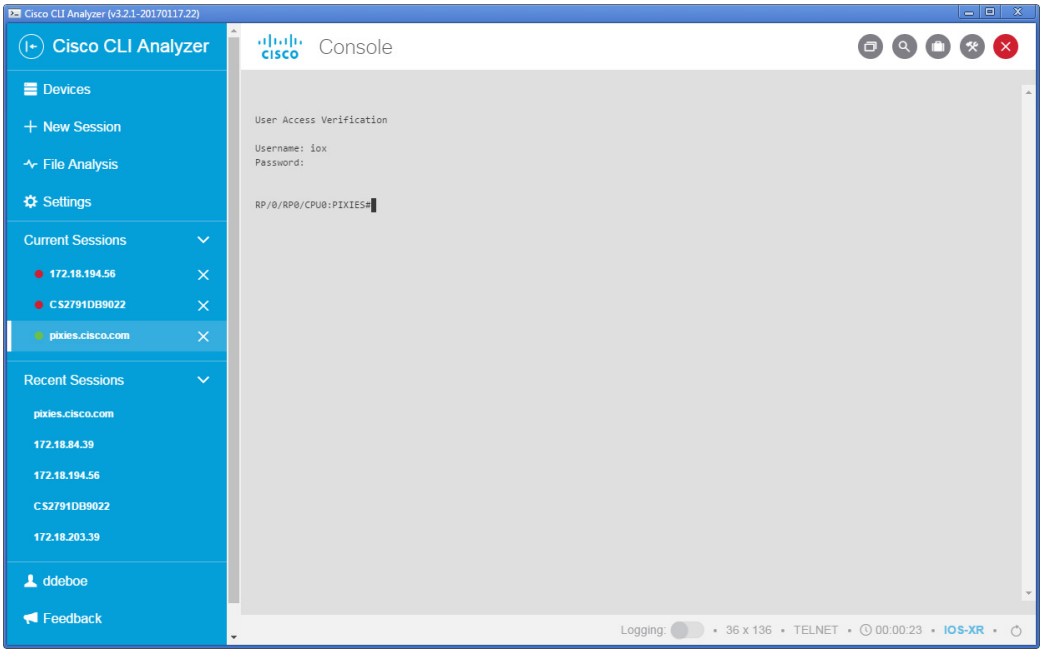
3. 表示されたフィールドに、デバイスへのアクセスに必要なユーザ名とパスワードを入力します。

4. 必要に応じて、アクセスを有効にするパスワードを [イネーブル パスワード（Enable Password）]フィールドに入力します。フィールドを空白にした場合は、イネーブル アクセスを必要とするスクリプトを実行する前に、コマンド プロンプトでイネーブル コマンドとパスワードを手動で入力する必要があります。



5. [接続（Connect）] をクリックします。

セッション ウィンドウが開き、アクティブ セッションを示す緑色のセッション タブ アイコンが表示されます。



注: ウィンドウ下部のステータス バーには、行と列の数、接続プロトコル、開始時刻、経過時間、デバイス タイプが表示されます。

デフォルトでは、セッションごとに `show version` コマンドまたは適切なコマンドが実行されます。[設定（Settings）] ページの [全般（General）]タブで、このコマンドを実行する頻度を変更できます。個々のデバイスで頻度を編集することもできます。

接続すると、次のアクションを実行できます。

- 現在のセッションのログ
- CLI コマンドの実行
- Cisco CLI アナライザ スクリプトの実行
- コマンド出力の検索

注: デバイスの接続を切断するには、[切断(Disconnect)]をクリックします。セッションがタイムアウトになって自動的に切断された場合は、[再接続(Reconnect)]をクリックします。[デバイス(Devices)]タブの [現在のセッション(Current Sessions)] リストで、セッションをダブルクリックして再接続することもできます。

コマンド ラインから SSH セッションを開始

コマンド ラインから Cisco CLI アナライザを開くと、アプリケーションが開くと同時に SSH デバイス セッションが直ちに開始されるように引数を追加できます。

注: 他に CLI アナライザのインスタンスが開いていないことを確認してから続行してください。

- **Windows:** `C:\Program Files\Cisco Systems, Inc\Cisco CLI Analyzer\nw.exe "--ssh <username>@<deviceIP>"`
- **Mac OS:** `open "/Applications/Cisco CLI Analyzer.app" --args "--ssh <username>@<deviceIP>"`

注: *<username>* はデバイスへのログインに使用するアカウントです。*<deviceIP>* はデバイスの IP アドレスです。

デバイスとの接続(シリアル)

PC をデバイスの COM ポートに接続できます(Bluetooth ワイヤレス シリアル アダプタはサポートされていません)。

シリアル接続は、次の点で SSH/Telnet 接続とは異なります。

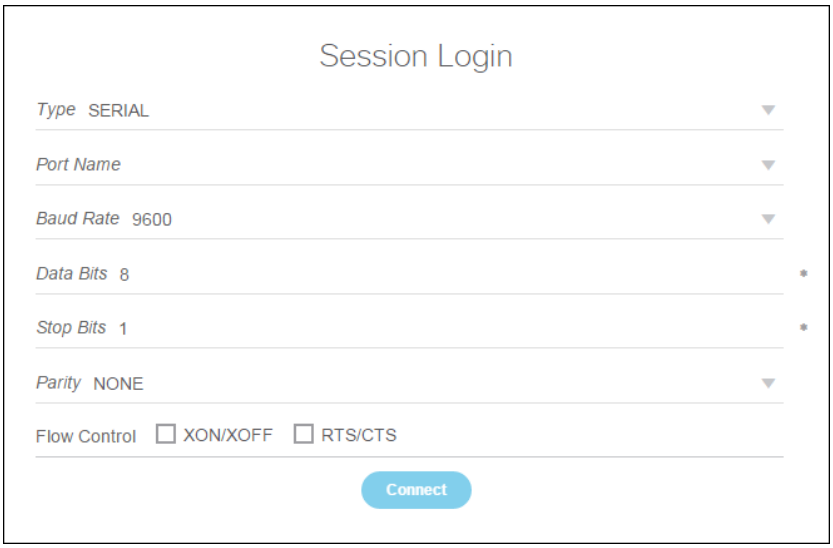
- シリアル接続では、接続したデバイスのエントリがデバイス リスト内に作成されません。
- シリアル接続では、デバイス識別、システム診断ツール、ハードウェア フロー制御はサポートされていません。

シリアル接続タイプを使用してデバイスに接続するには、次の手順を実行します。

1. [デバイス(Devices)] タブで、次のいずれかのアクションを実行して新しいセッションを開始します。
    - 左パネルの [新規セッション(New Session)] をクリックします。
    - [最近のセッション(Recent Sessions)] リスト内のデバイスをクリックします。

    新しいセッション タブが表示され、[セッション ログイン(Session Login)]画面が開きます。
2. [IP/ホスト名(IP/Hostname)]フィールドをスキップします。[タイプ(Type)]フィールドで、ドロップダウン リストから [シリアル(SERIAL)] を選択します。

    画面に複数のフィールドが表示されます。



3. 接続に使用する COM ポートを選択します。
4. 残りのフィールドに情報を入力します(ボー レート、データ ビット、ストップ ビット、パリティ タイプ、フロー制御)。
5. [接続(Connect)] をクリックします。

   セッション ウィンドウが開きます。
6. コマンド プロンプトでユーザ クレデンシャルを入力します(これらのクレデンシャルは保存されないため、シリアル デバイス接続を開くたびに入力する必要があります)。

Send Break

シリアル接続がアクティブである場合は、次のいずれかの方法で「send break」コマンドを入力できます。

- **Ctrl+Shift+s** を押します。
- コンソール ウィンドウ内を右クリックし、コンテキスト メニューから [Send BREAK]を選択します。

注: この機能では、Send Break がサポートされている USB/シリアル アダプタとシスコ デバイスが必要になります。Send Break は、シスコ デバイスの再起動中の適切なタイミングでトリガーする必要があります。

共有デバイス セッション

共有デバイス セッションにより、複数のユーザのトレーニングが可能になります。またピアツーピア接続(IP 間接続)が利用できる場合にはトラブルシューティングにも役立ちます。

セッション イニシエータはセッションの制御を保持し、1 人のリモート ユーザに読み取り/書き込み権限を付与できます。他のリモート ユーザは読み取り専用アクセスに限定されます。

注: 共有セッションは内部ネットワークでのみサポートされます。インターネット、または NAT とファイアウォールを介した共有セッション接続は、まだサポートされていません。

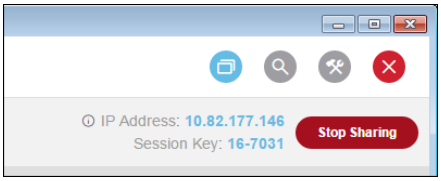
注: 共有セッションでは AES-256 暗号化が使用されます。

共有セッションの作成と管理

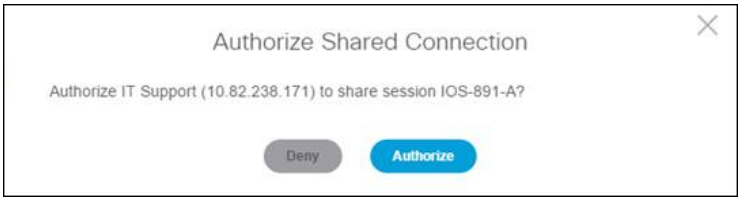
共有デバイス セッションを作成するには、次の手順を実行します。

1. [設定(Settings)]ページの [詳細設定(Advanced)] タブで、共有セッションが有効になっていることを確認します。
2. 通常の方法でデバイスに接続します。接続タイプとして [SSH]または [Telnet] を選択します。
3. セッション ウィンドウで ボタンをクリックすると、[共有セッション(Shared Session)] ツールバーが表示されます。
4. [セッションの共有(Share Session)] をクリックします。

   ツールバーには、デバイスの IP アドレスとセッション キーが表示されます。

5. この情報を、参加を希望するリモート ユーザに提供します。
   - 共有セッションを開始した PC の IP アドレス
   - ポート番号
   - セッション キー
6. リモート ユーザがセッションに参加すると、接続の許可を求める確認ダイアログが表示されます。[許可(Authorize)] をクリックします。

   リモート ユーザの名前がツールバーのボタンに表示されます。ボタンをクリックすると、リモート ユーザのセッション オプションにアクセスできます。

共有セッションがアクティブな場合には、次のアクションを実行できます。

- **リモート ユーザに書き込み権限を与える:**ユーザのボタンをクリックし、[書き込み権限を与える(Give Write Permissions)]を選択します。別のリモート ユーザがこの権限レベルをすでに持っている場合は、権限が新しいユーザに移行されます。
- **書き込み権限を取り消す:**このオプションは、書き込み権限を持つリモート ユーザの場合にのみ表示されます。ユーザのボタンをクリックし、[書き込み権限を取り消す(Revoke Write Permissions)]を選択します。
- **リモート ユーザを切断する:**ユーザのボタンをクリックして、[ユーザを切断(Disconnect User)] を選択します。
- **セッションの共有を停止する:** ツールバーの [共有を停止(Stop Sharing)]ボタンをクリックします。その後同じセッションを再度共有する場合は、リモート ユーザに提供する新しいセッション キーが生成されます。
- **他のデバイス セッションで作業する:**共有セッションを開いたままで、別のセッションに切り替えることができます。書き込み権限を持つリモート ユーザは、共有セッションでの作業を続行できます。[現在のセッション(Current Sessions)] リストには、アクティブな各共有セッションの横に [共有(Shared)]と表示されます。

共有セッションへの参加

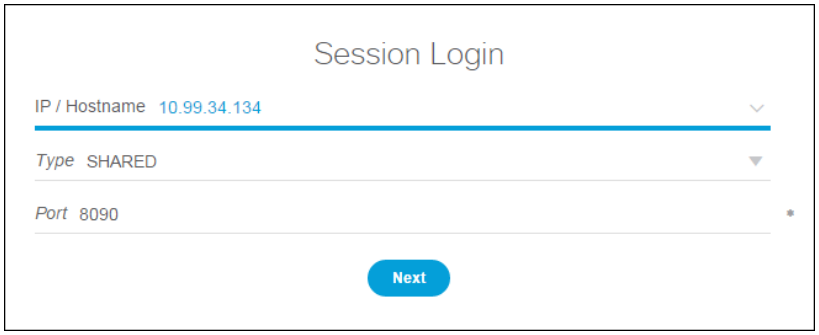
共有セッションに参加するには、セッション イニシエータが提供する次の情報が必要になります。

- CLI アナライザの共有セッションが開始された PC の IP アドレス
- ポート番号（セッション イニシエータが [設定（Settings）]ページの [詳細設定（Advanced）] タブで設定しているポート番号。デフォルトのポートは 8090）
- セッション キー

共有デバイス セッションを作成するには、次の手順を実行します。

1. [デバイス（Devices）] タブで、次のいずれかのアクションを実行して新しいセッションを開始します。
    - 左パネルの [新規セッション（New Session）] をクリックします。
    - [最近のセッション（Recent Sessions）] リスト内のデバイスをクリックします。
    - デバイス リスト内のデバイス エントリで、  ボタンをクリックします。

    新しいセッション タブが表示され、[セッション ログイン（Session Login）]画面が開きます。
2. デバイスの基本的な接続情報を入力するように求められたら、必要な情報を入力し、[次へ（Next）]をクリックします。その他の場合は、このステップをスキップしてステップ 3 に進みます。
    - [IP/ホスト名（IP/Hostname）]フィールドに、デバイスの IP アドレスまたはホスト名を入力します。このフィールドの横の矢印をクリックして、最近のセッションで接続したデバイスを選択することもできます。
    - [共有（Shared）]接続タイプを選択します。
    - セッション イニシエータから提供されたポート番号を入力します。

3. [次へ（Next）]をクリックします。
4. 共有セッションで自分を識別するための名前を入力します。
5. セッション イニシエータから提供されたセッション キーを入力します。
6. [接続（Connect）]をクリックします。

    セッション イニシエータが接続を承認すると、セッション ウィンドウが開きます。

    セッション イニシエータから書き込み権限が与えられると、共有セッションでコマンドを実行し、分析ツールを使用できます。（分析ツールの実行結果は、ユーザのクライアントだけに表示されます。セッション イニシエータは表示できません）。

機能

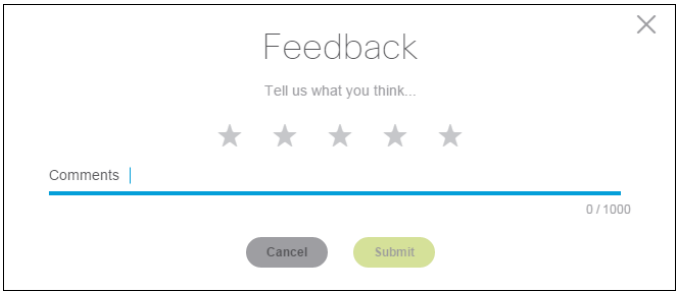
キーボードのショートカット

次の表に、Windows および OS X プラットフォームでサポートされているキーボード ショートカットを示します。オペレーティング システムが指定されていないショートカットは、サポートされているすべてのプラットフォームで使用できます。一部の機能では、すべてのプラットフォームで機能するショートカットや、特定のオペレーティング システムで使用できる追加のショートカットを利用できます。

機能	ショートカット
新しいセッションの開始	Alt-Q
選択した項目をクリップボードにコピー	▪ Windows：Ctrl-C ▪ OS X：Command-C
コンソールの検索	▪ Windows：Ctrl-F ▪ OS X：Command-F
すべてのテキストを選択	▪ すべてのプラットフォーム：Ctrl-Shift-A ▪ OS X：Command-A
コピーして貼り付け	Ctrl-Shift-B
前のタブに切り替え	Ctrl-Shift-TAB
次のタブに切り替え	Ctrl-Tab
クリップボードの内容を貼り付け	▪ Windows：Ctrl-V ▪ OS X：Command-V
1 ページ下方向にスクロール	Page Down
1 ページ上方向にスクロール	Page Up
全画面表示	▪ すべてのプラットフォーム：Shift-F ▪ Windows：F11 ▪ OS X：Command-F

コメントと質問の送信

Cisco CLI アナライザ ツールに関するコメントや質問を送信するには、左パネルの [フィードバック（Feedback）]をクリックして、[フィードバック（Feedback）]フォームを開きます。表示されたフィールドにコメントを入力します。さらに任意でスター評価を選択できます。終了したら、[送信（Submit）] をクリックしてフィードバックを送信します。



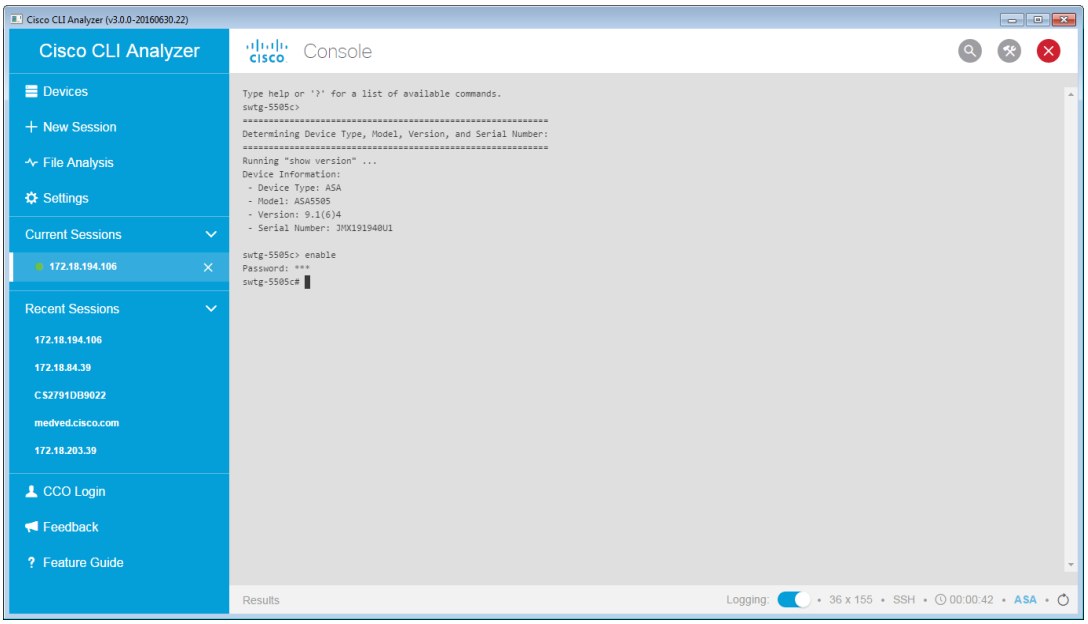
現在のセッションのログ

Cisco CLI アナライザでは、現在のコンソール セッションをキャプチャして、ローカル コンピュータに出力を保存できます。

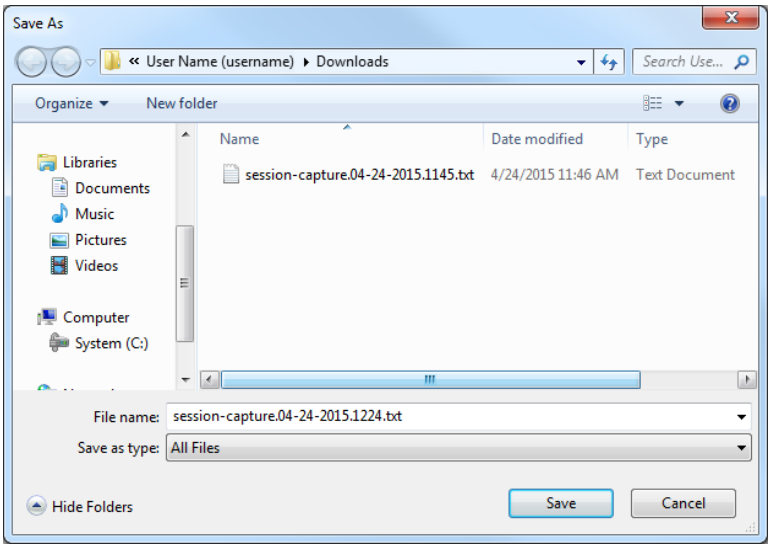
注:[設定(Settings)] ページの [全般(General)]タブのオプションでは、デバイスに接続したときにセッション アクティビティを自動的にログに記録し、切断したときにログ ファイルを自動的に保存することができます。詳細については、「セッションのロギングを自動的に有効にする」を参照してください。

現在のセッションをログに記録するには、次の手順を実行します。

1. 「デバイスとの接続」の説明に従ってデバイスに接続します。
2. [ロギング(Logging)]トグル ボタンの位置が左(オフ)になっている場合は、ボタンをクリックして機能をアクティブにします。
   セッションのログが開始します。



3. セッションが完了したら、[ロギング(Logging)]トグル ボタンをクリックします。
   [名前を付けて保存(Save As)]ダイアログ ウィンドウが表示されます。



デフォルトでは、ログ ファイルは次の場所に保存されます。

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

4. コンピュータ上の任意の場所に移動し、[保存(Save)] をクリックします。

デバイスのタグ付け

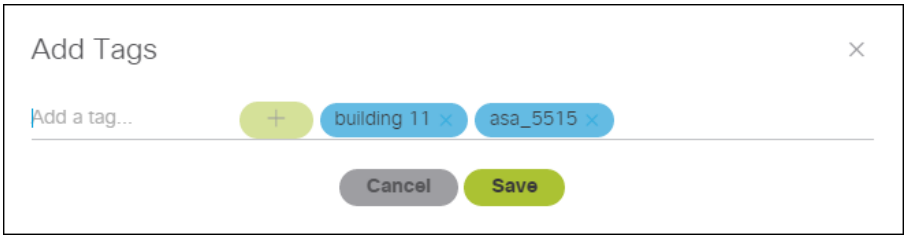
デバイスをタグ付け(テキスト参照)することで、階層ツリー内を移動することなく、デバイスの場所を簡単に特定できます。デバイスのグループをタグ付けすることで、[デバイス(Devices)]タブの整理とフィルタリングが容易になります。

タグでは次の文字を使用できます。

- 小文字(大文字は自動的に小文字に変換される)
- 数字
- スペース
- ハイフン(-)とアンダースコア(_)

デバイスをタグ付けするには、次の手順を実行します。

1. [デバイス(Devices)] タブで、タグ付けするデバイスごとに [選択(Select)] ボタン( )をクリックします。
2. [一括操作(Bulk Actions)] ボタン(Bulk Actions (3))をクリックします。ドロップダウン メニューから [タグの追加(Add Tags)] を選択します。
3. [タグの追加(Add Tags)] ウィンドウで [タグを追加...(Add a tag...)]をクリックして、選択したデバイスに付加するタグを入力します。 + ボタンをクリックします。付加するタグごとにこのステップを繰り返します。



4. [保存(Save)] をクリックします。

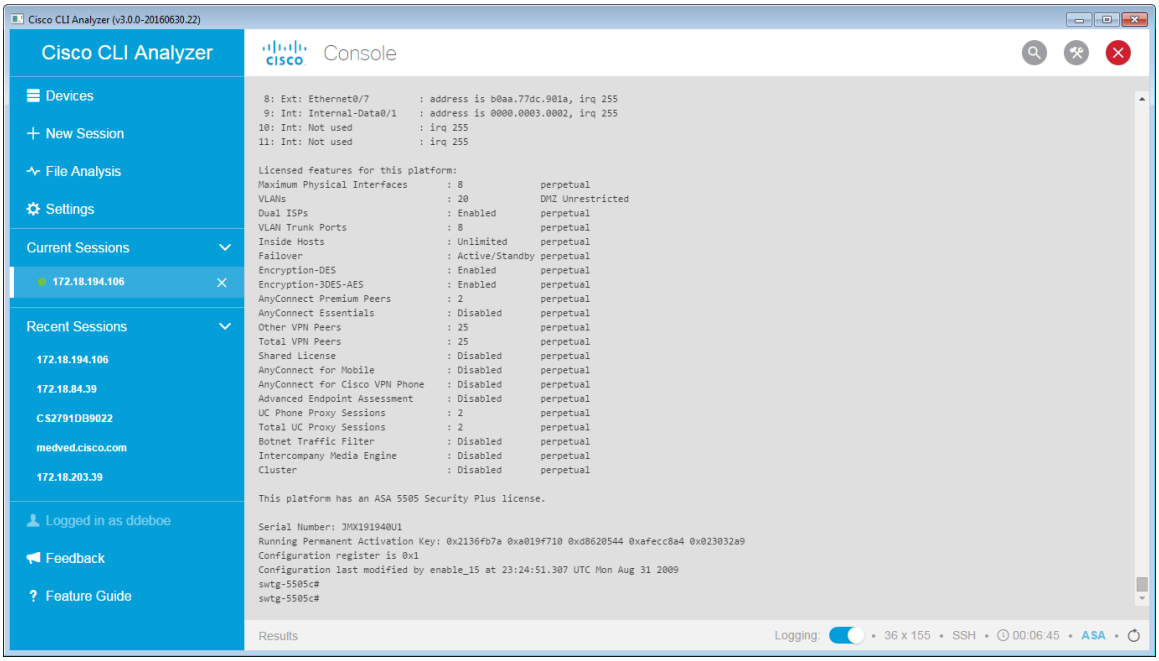
デバイス タグを削除するには、次の手順を実行します。

1. [デバイス(Devices)] タブで、タグを削除する各デバイスの [選択(Select)] ボタン( )をクリックします。
2. [一括操作(Bulk Actions)] ボタン(Bulk Actions (3))をクリックします。ドロップダウン メニューから [タグの削除(Delete Tags)] を選択します。
3. [タグの削除(Delete Tags)]ウィンドウで、削除する各タグの [X] をクリックします。

4. [保存(Save)] をクリックします。

CLI コマンドの実行

CLI コマンドを実行するには、「デバイスとの接続」の説明に従ってデバイスに接続し、コマンド プロンプトにコマンドを入力して、Enter を押します。



Cisco CLI アナライザ スクリプトの実行

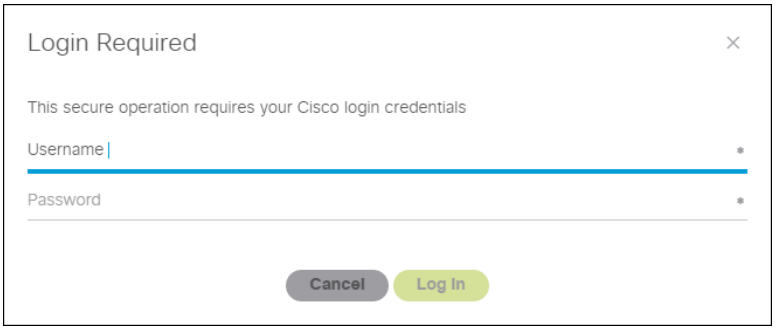
Cisco CLI アナライザでは、ASA、IOS、IOS-XE、または IOS-XR デバイスのサポートで発生する問題の特定、トラブルシューティング、解決に役立つスクリプトを実行できます。これらのスクリプトは、デバイス セッション ウィンドウのツール パネルに表示されます。

CCO ログイン

スクリプト操作の多くは、シスコ アカウントでのログインを必要とします。ログインするには、プロンプトからログインするか、Cisco CLI アナライザ ウィンドウの右上隅にある [ログイン(Login)] をクリックして、ユーザ クレデンシャルを入力します。

注:これらのツールを使用するには、アクティブなカスタマー契約またはパートナー契約にプロファイルを関連付ける必要があります。

CCO ログインに問題がある場合は、「*よく寄せられる質問*」セクションの「CCO アカウントにログインできないのはなぜですか。」を参照してください。



ツールの説明

新しいツールに関するアイデアや、ツールの強化に関するご提案については、「コメントと質問の送信」に従ってフィードバックをお送りください。

システム診断

サポートされているプラットフォーム：ASA、IOS、IOS-XE、IOS-XR

このツールでは、Cisco TAC のナレッジを活用して、シスコがサポートするデバイスを分析し、システムの問題、設定ミス、ベスト プラクティス違反などの既知の問題を検出します。

注：この分析では、**show tech-support** コマンドの出力を処理のためにシスコに送信する必要があります。**IOS-XR** 分析では、「show」コマンドの使用方法が異なります。

ファイアウォール トップ トーカー

サポートされているプラットフォーム：ASA

このツールでは、ASA を通じてトラフィックを送信している接続のうち、特定の期間でビット レートが最も高い接続を判別できます。

そのこのツールでは、数秒差で実行された **show conn** や **show conn all** の 2 つの出力が比較されます。ここではバイト数の差異が計算され、1 番目の出力から 2 番目の出力までの間に各接続で渡されたトラフィック数が確認されます。また、新たな接続（1 番目の出力になく 2 番目の出力だけに存在する接続）が特定されます。

さらに、対象の接続のリストが、トラフィック数で並べ替えられて表示されます。結果は JSON または CSV 形式でエクスポートできます。

トレースバック アナライザ

サポートされているプラットフォーム：ASA

このツールでは、ASA でシステム トレースバックが発生した場合に、クラッシュの根本原因と既知のバグを照合します。一致が見つかると、バグを修正済みの ASA が提供されます。

注：この分析では、**show crashinfo** コマンドの出力を処理のためにシスコに送信する必要があります。ASA ソフトウェアの全バージョンがサポートされています。

パケット トレーサ

サポートされているプラットフォーム：ASA

管理者がこのツールを使うことで、シミュレートされたパケットを ASA を通じてテスト送信できます。パケットがドロップされた場合は、パケット ドロップの原因になった可能性がある ASA の設定部分または機能が特定されます。

注：ASA バージョン 7.2（コマンドが最初に導入されたバージョン）以降がサポートされています。

未使用ポリシー ディテクタ

サポートされているプラットフォーム：ASA

このツールでは、未使用のアクセス リスト、オブジェクト グループ、オブジェクトなど、未使用の設定ポリシーを検出します。検出させた設定ポリシーは設定ミスである可能性があります。このツールでは、**show run** および **show access-list | excl ^ |elem** コマンドの出力が収集されます。出力はシスコにアップロードされて分析されます。このツールの全機能は、リリース 9.x 以上の ASA で利用できます。

BGP トップ トーカー

サポートされているプラットフォーム:IOS-XR

このツールでは、特定の期間で送受信されたメッセージ数が最も多いボーダー ゲートウェイ プロトコル ピアを判別できます。

L2VPN トップ トーカー

サポートされているプラットフォーム:IOS-XR

このツールでは、レイヤ 2 VPN ポイントツーポイント回線とブリッジ ドメインで、特定の期間のパケット レートが最も高かったものが判別されます。

LPTS トップ トーカー

サポートされているプラットフォーム:IOS-XR

このツールでは、ハードウェアからソフトウェア処理に渡されるトラフィックのタイプとレートを特定できます(IOS-XR デバイス専用)。Local Packet Transport Services(LPTS)は、ハンドオフの必要があるトラフィック(Telnet、SSH、SNMP など)を特定し、レートを制限してソフトウェアのオーバーロードを防ぐルータ機能です。

IP ルート分析

サポートされているプラットフォーム:IOS、IOS-XE、NX-OS

このツールでは、IPv4 または IPv6 ルートの分析に基づいて、異なる 4 つのレポートが作成されます(NX-OS プラットフォームでは IPv4 ルートのみサポート)。

- ルートの不安定性:ルーティングの変更を 60 秒間隔でチェック
- ネクスト ホップを記載したルート概要
- ルーティング テーブルのサブネット プレフィックス分布
- すべてのプロトコルのアドミニストレーティブ ディスタンスに関する概要

注:ルーティング テーブルのルート数が 100,000 以上である場合、このツールは機能しません。

パケット キャプチャ

サポートされているプラットフォーム:ASA、IOS、IOS-XE、IOS-XR、NX-OS

このツールでは、パケット キャプチャを設定して実行し、結果を分析できます。デバイス プラットフォームに基づき、キャプチャするパケットの種類を指定し、ターミナル内でキャプチャされたパケットを復号化し、トラフィック分析結果を表示できます。

ケースの作成

サポートされているプラットフォーム:ASA、IOS、IOS-XE、IOS-XR

このツールにより、サポートされているプラットフォームではサポート ケース データの収集が自動化されます。他のプラットフォーム(FX-OS、NX-OS、UCS)のデバイスの場合は、標準のケース作成が可能です。

TAC データの収集

サポートされているプラットフォーム:ASA、IOS、IOS-XE、IOS-XR、NX-OS、UCS、AireOS(ワイヤレス LAN コントローラ)

このツールでは、サポート ケースの解決に必要な診断データの収集が自動化されます。TAC エンジニアから TaskID コードが提供されます。TAC データ収集ツールに TaskID を入力すると、CLI アナライザが診断コマンドを自動的に実行し、出力をサポート ケースにアップロードします。

実行診断の表示

サポートされているプラットフォーム：AireOS（ワイヤレス LAN コントローラ）

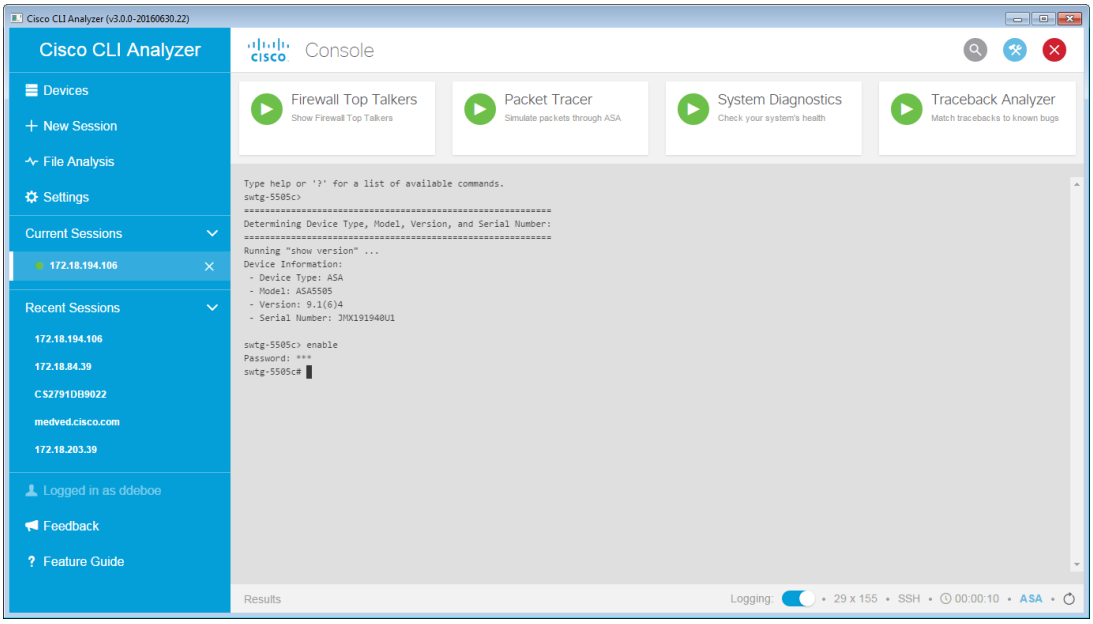
技術診断の表示

サポートされているプラットフォーム：AireOS（ワイヤレス LAN コントローラ）

スクリプトの実行

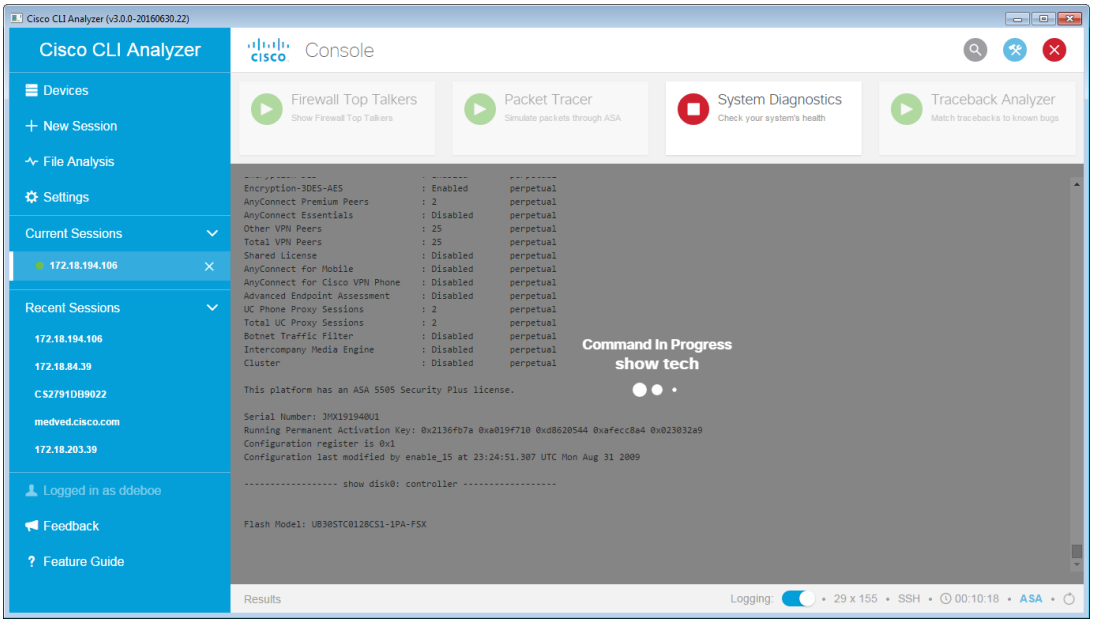
Cisco CLI アナライザ スクリプトを実行するには、次の手順を実行します。

1. 「デバイスとの接続」の説明に従ってデバイスに接続し、[ツール（Tools）] をクリックします。
2. ツール パネルが非表示になっている場合は、ツール アイコン（ ）をクリックするとパネルが表示されます。



3. 実行するスクリプトの [実行（Run）] ボタン（ ）をクリックします。
4. プロンプトが表示されたら、ツールの追加設定を入力します。

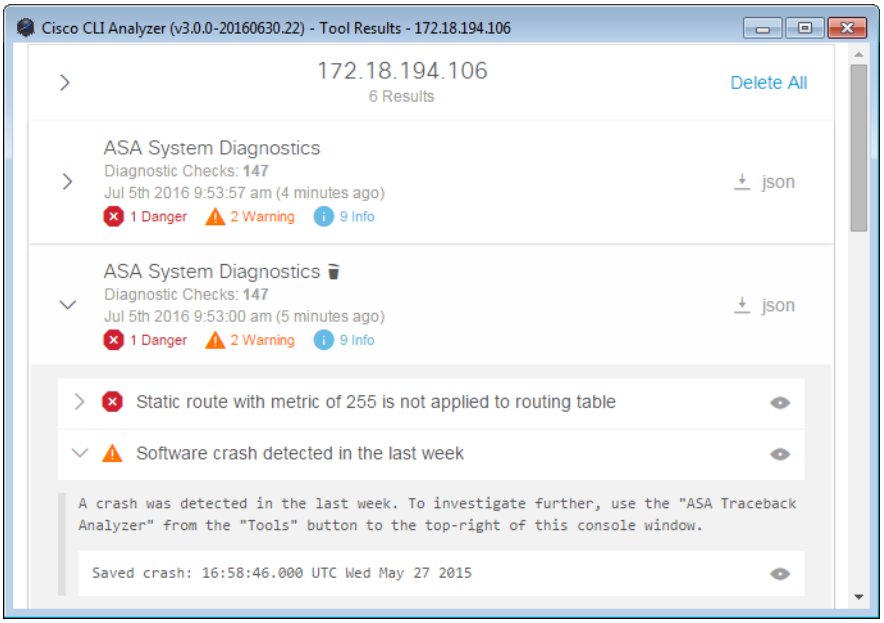
   スクリプトが実行開始します。



注: *イネーブル* アクセスが必要な場合は、スクリプトを実行する前にクレデンシャルを入力するように求められます。

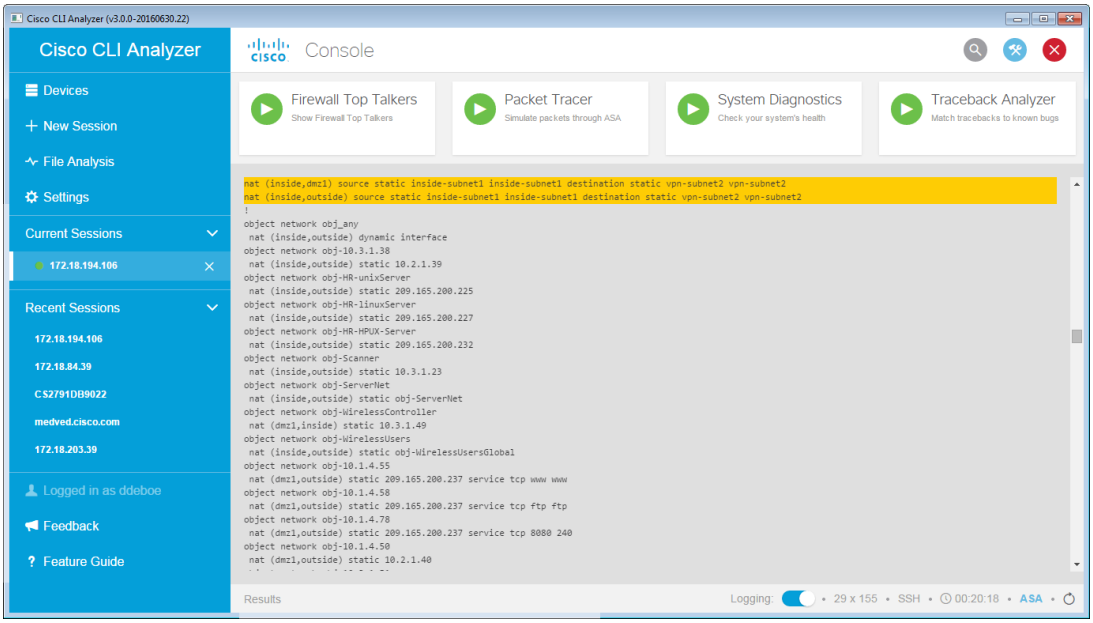
5. スクリプトが完了するまで待つか、[停止(Halt)] ボタン( )をクリックしてスクリプトを停止します。
6. スクリプトが完了すると、セッションが [ツールの結果(Tool Results)] ウィンドウにリストされます。[ツールの結果(Tool Results)] ウィンドウが開いていない場合は、セッション タブの左下隅にある [結果(Results)] をクリックして開きます。

   [ツールの結果(Tool Results)] ウィンドウには、デバイスごとに最新の結果が 25 件表示されます。この情報は、[ツールの結果(Tool Results)] ウィンドウや Cisco CLI アナライザ ウィンドウを閉じても保持されます。



7. [結果(Results)] リスト内の項目をクリックすると、リストが拡張されて詳細が表示されます。

8. [結果(Results)] リスト内の項目の横にある アイコンをクリックすると、セッション ウィンドウ内の関連するテキストまでスクロールし、ハイライト表示されます。**注:**この機能は、システム診断ツールでのみ使用できます。IOS-XR デバイスに接続している場合は、テキストのハイライト機能は使用できないため、 アイコンは表示されません。



9. [結果(Results)] 領域の右上隅にある **json** をクリックすると、json ファイルに結果をエクスポートできます。

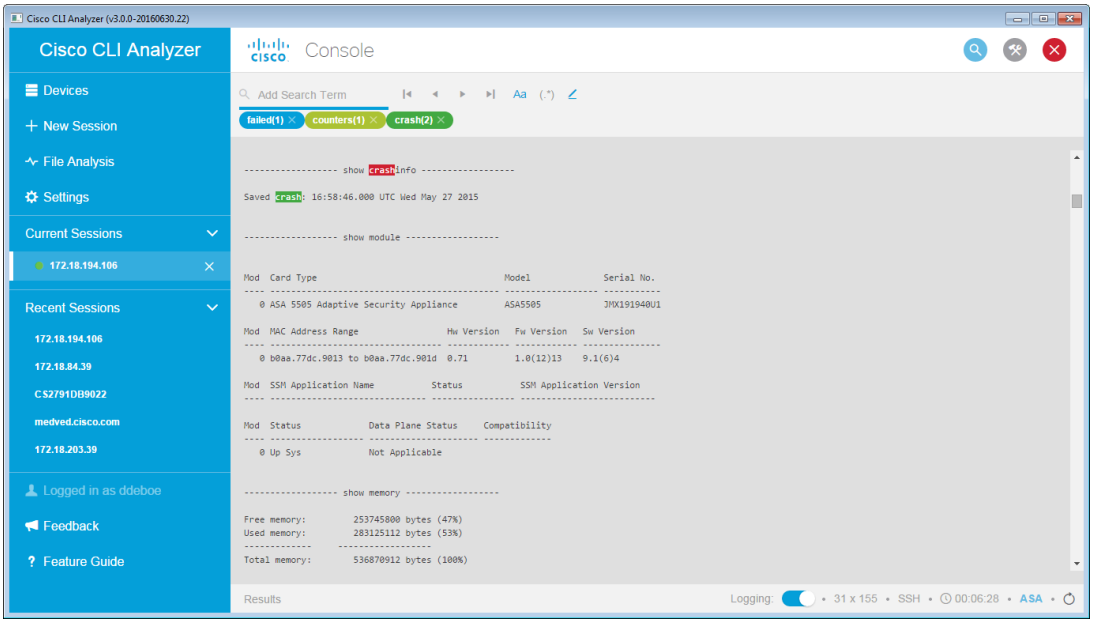
コマンド出力の検索

Cisco CLI アナライザには、コンソール ウィンドウでリアルタイム検索を使用してコマンド出力を検索できる、ハイライト機能があります。

コマンドの出力を検索するには、次の手順を実行します。

1. [ハイライト(Highlight)]ボタン( )をポイントしてツールチップを表示させて、検索結果のハイライトが有効になっていることを確認します。ハイライトが無効になっている場合は、ボタンをクリックして有効にします。
2. 表示されたフィールドに検索条件を入力し、**Enter** または **Tab** を押します。この手順を繰り返して、最大 5 つまで検索条件を入力できます。

   指定された検索条件は、検索フィールドの横に、条件ごとの検索結果数と合わせて表示されます。検索結果は、コマンド ウィンドウにハイライトされて表示されます。



注: 結果は、[設定(Settings)] ページの [表示(Display)]タブで各検索条件に割り当てられた色に従ってハイライトされます。現在選択されている検索条件は、赤でハイライトされます。検索条件にカスタム カラーを割り当てる方法については、「テーマ」を参照してください。

3. 複数の検索結果間を移動するには、次のボタンを使用します。
   - 前(◀):検索条件の前の一致に移動します。
   - 次へ(▶):検索条件の次の一致に移動します。
   - 最初(|◀):出力内の検索条件の最初の一致に移動します。
   - 最後(▶|):出力内の検索条件の最後の一致に移動します。
4. 検索結果を大文字小文字を区別して絞り込むには、[大文字小文字を区別(Case Sensitive)] ボタン(Aa)をクリックします。
5. 正規表現を有効または無効にするには、[正規表現(RegEx)] ボタン((.*))をクリックします。

注: 正規表現は、検索条件にワイルドカードまたは置換を含める際に使用します。サポートされている正規表現については、「正規表現検索機能では、どのような表現と文字がサポートされていますか。」を参照してください。

6. 検索条件を削除するには、検索フィールドの検索条件の [X] をクリックします。

サポート ケースの作成および更新

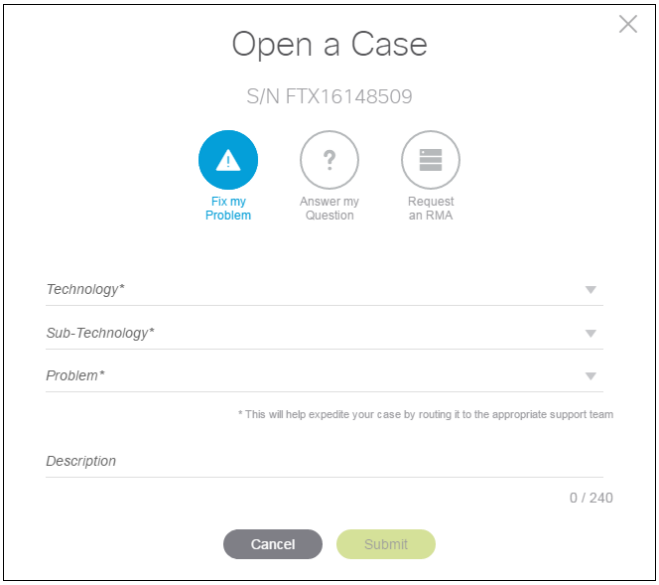
デバイス リストの対象デバイスに対して、サポート ケースをオープンできます。

サポート対象であるデバイスについては、[アクション(Actions)] 列(リスト ビュー)、またはデバイス タイルの [アクション(Actions)] バー(グリッド ビュー)に、ブリーフケース アイコン( )があります。濃いグレーのアイコンは、デバイスがサポート対象であることを示します。薄いグレーのアイコンは、デバイスがサポート対象でないか、ユーザ アカウントにそのデバイスのサポート ケース アクションを実行する権限がないことを示します。

デバイスに新しいサポート ケースを作成するには、次の手順を実行します。

1. デバイスのタイルまたは行の アイコンをクリックします。ドロップダウン メニューから [新規ケースをオープン(Open a new case)]を選択します。

   [ケース オープン(Open a Case)] 画面が表示されます。



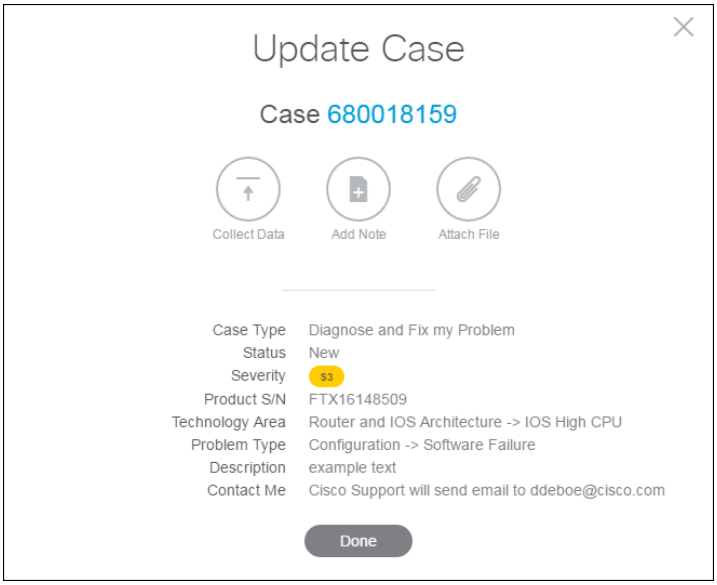
2. [問題の修正を要求(Fix myProblem)]、[質問の回答を要求(Answer my Question)]、または [RMA を要求(Request an RMA)] から、必要なサポートのタイプのボタンを選択します。
3. [テクノロジー(Technology)]フィールド内をクリックします。ドロップダウン メニューから、サポートが必要なテクノロジーのカテゴリを選択します。
4. [サブテクノロジー(Sub-Technology)]フィールド内をクリックします。ドロップダウン メニューから、サポートが必要なテクノロジーのサブカテゴリを選択します。
5. [問題(Problem)]フィールド内をクリックします。ドロップダウン メニューから、問題のタイプを示すカテゴリを選択します。
6. [説明(Description)]ボックスに、問題の簡単な説明を入力します([質問の回答を要求(Answer my Question)]を選択した場合は、このボックスに質問を入力してください)。
7. [送信(Submit)]をクリックします。

   [ケース オープン(Open a Case)] 画面には、ケース番号を含む、ケース概要が表示されます。ケース番号をクリックすると、サポート Web サイトでケースを表示できます。

サポート ケースのレビューまたは更新を行うには、次の手順を実行します。

1. デバイスのタイルまたは行の アイコンをクリックします。ドロップダウン メニューから、レビューまたは更新を行うケース番号を選択します。

   [ケースの更新(Update Case)] 画面が表示されます。



2. [データの収集(Collect Data)]、[メモの追加(AddNote)]、または [ファイルの添付(Attach File)] から、実行するアクションのボタンを選択します。

   - [データの収集(CollectData)]:最初にケースを作成する場合は、この手順を実行することを強くお勧めします(デバイスのプラットフォームでサポートされている場合)。ケースの更新では、TAC エンジニアの指示があれば、このアクションを実行します。[データの収集(Collect Data)] ダイアログで [続行(Continue)]をクリックして、通常の手順に従ってデバイス セッションに接続します。
   - [メモの追加(AddNote)]:[タイトル(Title)] ボックスにメモの簡単な説明を入力し、[詳細(Details)] ボックスにメモの本文を入力します。[送信(Submit)]をクリックするとメモが作成されます。
   - [ファイルの添付(Attach File)]:Windows Explorer から[ファイルの添付(Attach Files)] ダイアログにファイルをドラッグするか、ボックス内をクリックして、[開く(Open)] ダイアログから添付するファイルを選択します。[送信(Submit)]をクリックするとファイルが添付されます。

3. 完了したら [完了(Done)]をクリックします。

TAC データの収集

TAC データ収集ツールでは、TAC エンジニアがデバイスで実行する 1 つ以上の診断コマンドを指定することができます。このツールでコマンドを実行すると、結果がサポート ケースにアップロードされます。

TAC エンジニアから、TaskID が含まれた電子メールが届きます。TaskID は、電子メールの件名欄に **#TAC-X1Y2-3456** の形式で示されます。

次の画像は電子メールのサンプルを示しています。

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:

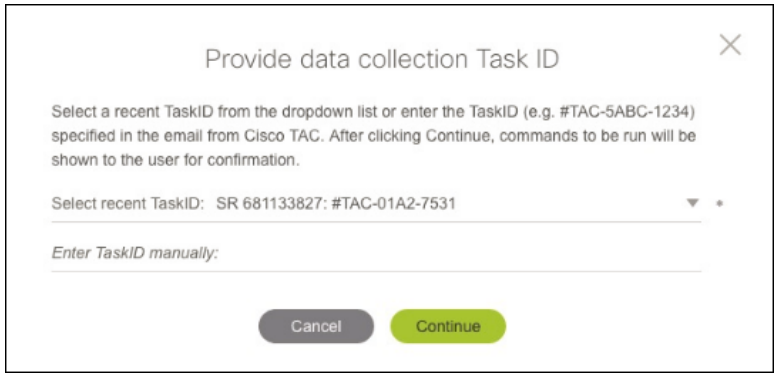
```
admin show platform
show install active summary
show run
show log
```

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

Thank you.

電子メールを受信したら、次の手順で必要なデータを収集します。

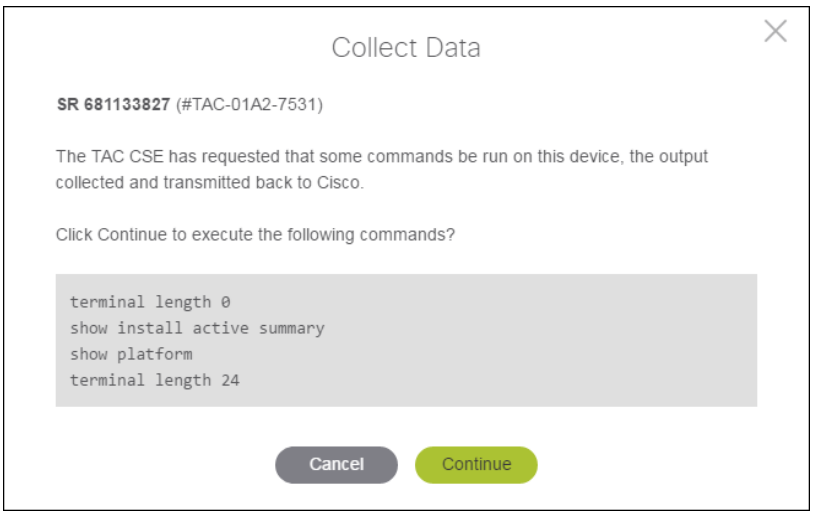
1. TAC エンジニアが指定したデバイスに接続します。
2. ツール パネルが非表示になっている場合は、ツール アイコン( )をクリックするとパネルが表示されます。
3. TAC データ収集ツールで、[実行(Run)] ボタン( )をクリックします。
   [データ収集 TaskID の入力(Provide Data Collection Task ID)] ウィンドウが開きます。



4. TaskID を入力します。
   - ケース担当者の CCO ID である場合は、[最近の TaskID を選択（Select recent TaskID）]フィールドの矢印をクリックして、ドロップダウン リストから TaskID を選択します。
   - ケース担当者でない場合は、ユーザ名がサービス リクエストと関連付けられていないため、TaskID を手動で入力する必要があります。[TaskID の入力（Enter TaskID）]フィールドには、TAC エンジニアから電子メールで提供された TaskID を入力するか貼り付けます。

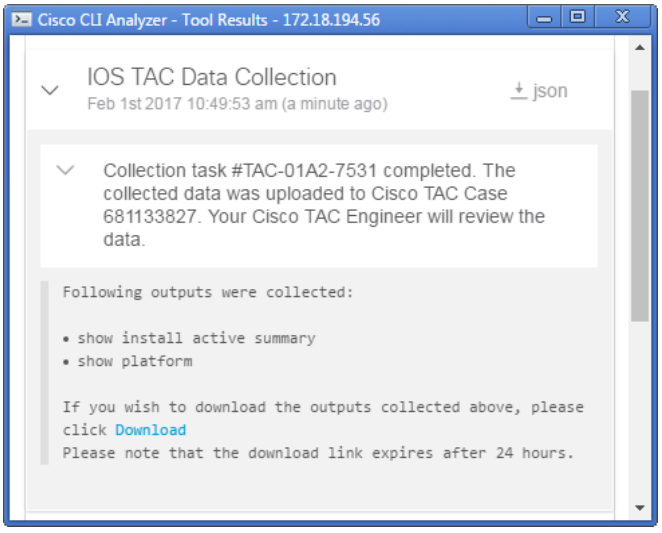
     注：手動で入力した TaskID は、ドロップダウン リストから選択した TaskID よりも優先されます（両方存在する場合）。
5. [続行（Continue）]をクリックします。

   CLI アナライザでコマンドのリストが取得されて表示されます。最初のコマンドではターミナルの長さがゼロに設定され、最後のコマンドでは元の長さが復元されます。他のコマンドでは、TAC エンジニアが要求したデータが収集されます。



6. [続行（Continue）]をクリックして、リストされたコマンドを実行し、出力を TAC ケースにアップロードします。

   [ツールの結果（Tool Results）] ウィンドウに、TaskID、ケース番号、収集された出力をダウンロードできるリンクが表示されます。TAC エンジニアは、収集について通知を受けると、分析とアクションの計画を提供します。



オフライン ファイルの分析

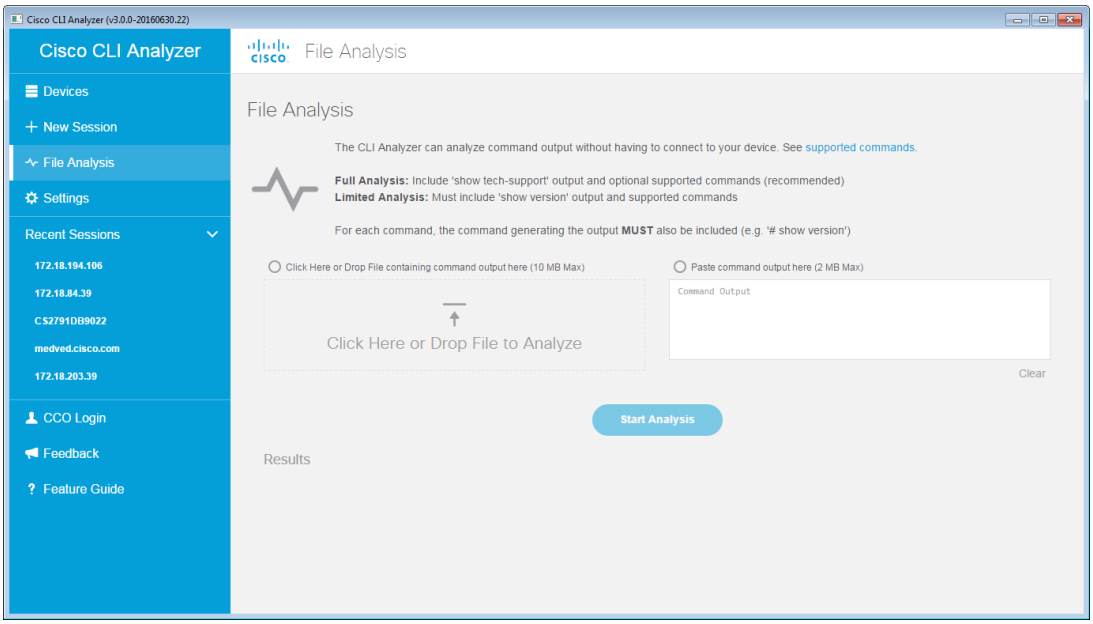
Cisco CLI アナライザでは、以前のデバイス セッションのコマンド出力が含まれたテキスト ファイル（拡張子が `.text` または `.txt`）を分析できます。

テキスト ファイルには次のコンテンツを含めます。

- ファイル内の各出力を生成したコマンド（「`# show version`」など）
- `show version` コマンドによる出力
- （任意）`show tech-support` コマンドの出力。完全な分析を行うために必要になります。
- （任意）サポートされている他のコマンドによる出力

コマンド出力のファイルを分析するには、次の手順を実行します。

1. シスコ アカウントでログインしていない場合は、ここでログインします。
2. [ファイル分析（File Analysis）] タブをクリックします。

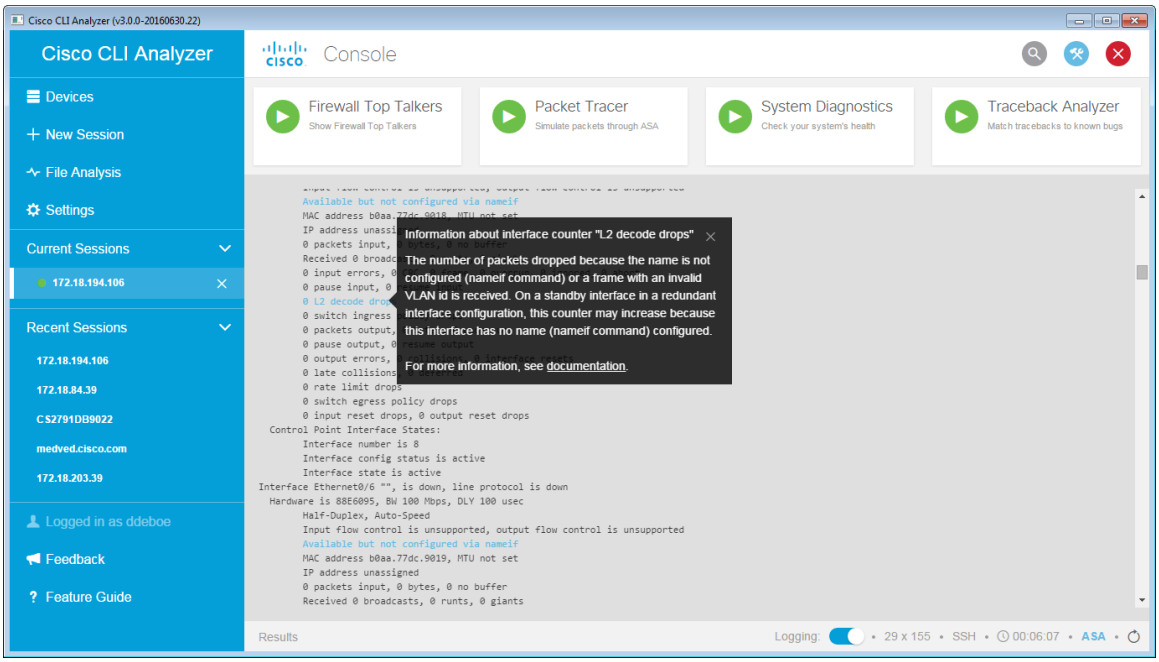


3. 次のいずれかの手順を実行して、分析するテキストを入力します。
   - [ここをクリックするか分析するファイルをドロップ（Click Here or Drop File to Analyze）]領域にテキスト ファイルをドラッグします。
   - [ここをクリックするか分析するファイルをドロップ（Click Here or Drop File to Analyze）]領域内をクリックし、テキスト ファイルを参照して選択して、[開く（Open）] をクリックします。
   - コマンド出力のテキストをコピーし、[コマンド出力（Command Output）]領域内をクリックして、コピーしたテキストを貼り付けます。
4. [分析開始（Start Analysis）]をクリックします。

   [ツールの結果（Tool Results）] ウィンドウに分析結果が表示されます。

[コンテキスト ヘルプとハイライト(Contextual Help and Highlighting)]

Cisco CLI アナライザには、特定のコマンドにコンテキスト ヘルプ機能とハイライト機能が用意されています。この機能では、CLI 出力内の特定のテキストがハイライトされ、テキストに関する追加情報が提供されます。コンテキストヘルプを表示するには、追加情報を表示させるテキストに対応するリンクをクリックします。



コンテキスト ヘルプとハイライトは、次のコマンドでサポートされています。

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

IOS コマンド			
show aaa servers	show controllers vdsl	show ip device tracking	show ospfv3 neighbor
show access-session	show crypto (gdoi|gkm) gm acl	show ip eigrp accounting	show ospfv3 neighbor detail
show ap capwap summary	show crypto call admission statistics	show ip eigrp events	show ospfv3 statistic
show ap config general	show crypto eli	show ip eigrp topology	show ospfv3 statistic detail
show ap dot11 24ghz coverage	show crypto gdoi	show ip eigrp interfaces detail	show otv
show ap dot11 24ghz network	show crypto gdoi gm	show ip eigrp neighbors show ip eigrp topology	show otv isis rib redistribution mac
show ap dot11 24ghz summary	show crypto gdoi ks	show ip eigrp traffic	show OTV VLAN
show ap dot11 24ghz txpower	show crypto gdoi ks coop	show ip interface	show platform
show ap dot11 5ghz coverage	show crypto gdoi ks policy	show ip interface brief	show policy-firewall config
show ap dot11 5ghz network	show crypto ikev2 sa	show ip nat statistics	show policy-firewall session
show ap dot11 5ghz summary	show crypto ikev2 stats	show ip nat translations	show policy-map interface
show ap dot11 5ghz txpower	show crypto ipsec sa	show ip nat translations verbose	show policy-map type inspect zone-pair sessions
show ap groups	show crypto isakmp sa	show ip ospf database	show ppp multilink
show ap join stats summary	show crypto key mypubkey (rsa|ec|all)	show ip ospf database asbr-summary	show processes cpu
show ap mac-address H.H.H join stats detailed	show crypto session	show ip database external	show processes memory
show ap summary	show diagnostic	show ip database network	show redundancy
show arp	show diagnostic events	show ip database nssa-external	show redundancy states
show async status	show diagnostic results	show ip database opaque-area	show route-map
show atm interface atm	show dial-peer voice summary	show ip database router	show run interface cellular
show atm pvc	show dialer	show ip database summary	show running-config
show atm traffic	show domain (name) (master|border) site-prefix	show ip ospf interface	show sccp connections
show atm vc	show domain (name) (vrf (vrf name)) (master|border) status	show ip ospf neighbors	show sip-ua calls
show authentication sessions	show dot11 association all	show ip ospf statistics	show sip-ua status
show bgp	show dot1x	show ip ospf statistics detail	show spanning-tree
show bgp () X	show dspfarm all	show ip route summary	show spanning-tree summary
show bgp (*) (vrf vrf-name)?	show eigrp address-family ipv4 events	show ip traffic	show stacks
show bgp a.b.c.d	show eigrp address-family ipv4 topology	show ip wccp	show standby
show bgp internal	show eigrp address-family ipv6 events	show ip(v6) eigrp traffic	show stcapp device summary
show bgp neighbors	show eigrp address-family ipv6 topology	show ip(v6) ospf interface	show switch
show bgp summary	show environment	show ip(v6) ospf neighbor detail	show switch stack-ports summary
show bridge-domain	show environment status	show ip(v6) protocols	show tech-support
show buffers	show etherchannel summary	show ip(v6) route	show tech-support wireless
show call active voice	show fabric	show ipv6 eigrp events	show telephony-service
show call active voice brief	show fex	show ipv6 eigrp interfaces	show telephony-service all
show call-manager-fallback	show fex detail	show ipv6 eigrp neighbors	show version
show capwap client rcb	show frame-relay lmi	show ipv6 eigrp topology	show vlan
show ccm-manager	show frame-relay map	show ipv6 interface	show voice call status
show ccm-manager music-on-hold	show frame-relay pvc	show ipv6 ospf neighbor	show voice dsp group all
show cdp neighbors detail		show ipv6 ospf statistic	show voice port summary
show cellular		show ipv6 ospf statistic detail	show voice register global
		show isdn service	show voip rtp connections
		show isdn status	show vpdn tunnel
		show issu state	show vslp lmp neighbors
			show vtp password

IOS コマンド			
show cellular intf num radio	show interface atm	show line	show vtp status
show cellular profile	show interface multilink	show lisp dynamic-eid	show wireless client mac-address H.H.H detail
show cem circuit	show interface status	show logging	show wireless client summary
show clock (detail)	show interfaces	show mab	show wireless country configured
show controllers	show interfaces counters	show mac address-table	show wireless detail
show controllers cellular	show interfaces counters error	show mac-address-table	show wireless mobility summary
show controllers dot11Radio 0	show interfaces INT counters	show macsec	show wireless multicast
show controllers e1	show interfaces switching	show memory	show wireless summary
show controllers e3	show ip bgp	show memory statistics	show wireless wps summary
show controllers ethernet-controller(fastethernet |gigabitethernet)	show ip bgp ?	show mgcp	show zone-pair security
show controllers pos	show ip bgp a.b.c.d	show mls cef exception status	
show controllers serial	show ip bgp internal	show module	
show controllers SHDSL	show ip bgp neighbors	show netdr captured-packets	
show controllers t1	show ip bgp summary	show network-clocks sync	
show controllers t3	show ip cef	show ntp associations detail	
		show ospfv3 interface	

IOS-XE コマンド			
show aaa servers	show crypto gdoi	show ip nat translations	show platform hardware qfp active feature firewall drop
show access-session	show crypto gdoi gm	show ip nat translations verbose	show platform hardware qfp active feature ipsec datapath drops
show ap capwap summary	show crypto gdoi ks	show ip ospf database	show platform hardware qfp active feature nat datapath stats
show ap config general	show crypto gdoi ks coop	show ip ospf database asbr-summary	show platform hardware qfp active infrastructure exmem statistics
show ap dot11 24ghz coverage	show crypto gdoi ks policy	show ip database external	show platform hardware qfp active statistics drop
show ap dot11 24ghz network	show crypto ikev2 sa	show ip database network	show platform hardware qfp active tcam resource-manager usage
show ap dot11 24ghz summary	show crypto ikev2 stats	show ip database nssa-external	show platform hardware slot (#) serdes statistics
show ap dot11 24ghz txpower	show crypto ipsec sa	show ip database opaque-area	show platform health
show ap dot11 5ghz coverage	show crypto isakmp sa	show ip database router	show platform ptp all
show ap dot11 5ghz network	show crypto key mypubkey (rsa|ec|all)	show ip database summary	show platform punt client
show ap dot11 5ghz summary	show crypto session	show ip ospf interface	show platform software status control-processor brief
show ap dot11 5ghz txpower	show diagnostic	show ip ospf neighbors	show policy-firewall config
show ap groups	show diagnostic events	show ip ospf statistics	show policy-firewall session
show ap join stats summary	show diagnostic results	show ip ospf statistics detail	show policy-map interface
show ap mac-address H.H.H join stats detailed	show dial-peer voice summary	show ip route summary	show policy-map type inspect zone-pair sessions
show ap summary	show dialer	show ip traffic	
show arp	show domain (name) (master|border) site-prefix	show ip wccp	
show async status	show domain (name) (vrf (vrf name)) (master|border) status	show ip(v6) eigrp traffic	
show atm interface atm	show dot11 association all	show ip(v6) ospf interface	
show atm pvc	show dot1x	show ip(v6) ospf neighbor detail	
	show dspfarm all	show ip(v6) protocols	
		show ip(v6) route	
		show ipv6 eigrp events	

IOS-XE コマンド			
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 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 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 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 topology 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 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 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 cpu packet buffered show platform cpu packet driver show platform cpu packet statistics show platform hardware cef exception status show platform hardware qfp active feature erspan state	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 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

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

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

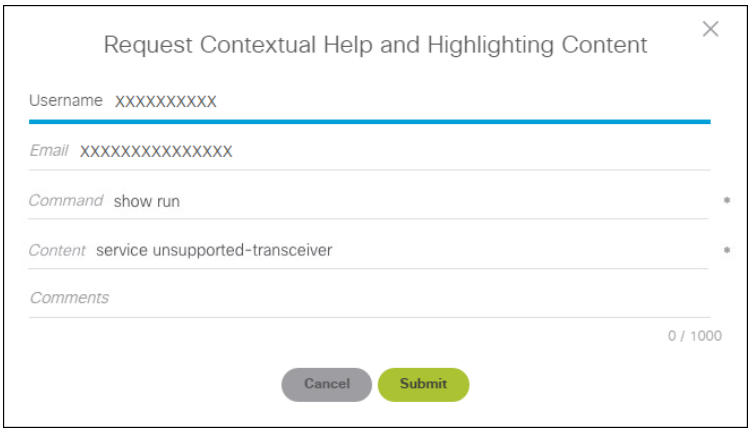
UCS コマンド		
コマンド	コンテキスト	対象範囲
show fault	UCSM	モニタリング
show diagnostic result module	NX-OS	
show ip igmp groups	NX-OS	
show interface trunk	NX-OS	
show interface ethernet	NX-OS	
show interface counters errors	NX-OS	
show running-config	NX-OS	
show interface status err-disabled	NX-OS	
show processes cpu	NX-OS	
show cluster extended-state	local-mgmt	
show interface	NX-OS	
show version	NX-OS	
show fault detail	UCSM	モニタリング
show diagnostic result module all	NX-OS	
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	

コンテキスト メニュー オプション

Cisco CLI アナライザでは、ハイライトしたコンソール テキストに応じた右クリック メニュー オプションを使用できます。

これらのオプションは、コンソール内の任意のテキストをハイライトして右クリックすると表示されます。

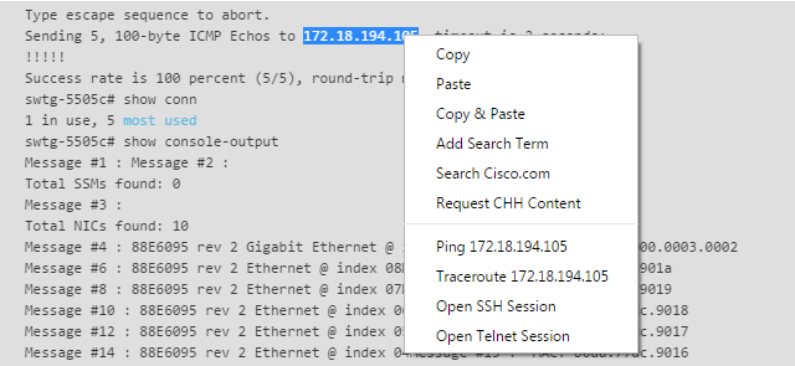
- [コピー(Copy)]:選択したテキストをクリップボードにコピーします。
- [貼り付け(Paste)]:クリップボードにコピーしたテキストをコマンドプロンプトに貼り付けます。
- [コピーして貼り付け(Copy & Paste)]:1 回の操作で、選択したテキストをコピーしてコマンドプロンプトに貼り付けます。
- [すべて選択してコピー(Select All & Copy)]:コンソールウィンドウ内のテキスト全体をコピーします。
- [検索条件の追加(Add Search Term)]:選択したテキストを検索条件として追加してハイライトします。
- [Cisco.com を検索(Search Cisco.com)]:ハイライトしたテキストに関する情報をCisco.com の Web サイトで検索します。
- [デバイスのカバレッジのチェック(Check Device Coverage)]:有効なシリアル番号を選択した後、ブラウザウィンドウで Cisco Device Coverage Checker ツールを開きます。
- [CHH コンテンツのリクエスト(Request CHH Content)]:[コンテキスト ヘルプとコンテンツのハイライトのリクエスト(Request Contextual Help and Highlighting Content)]ダイアログ ウィンドウが開き、追加の CHH コンテンツのリクエストを送信できます。



IP アドレスをハイライトして右クリックすると、次の追加オプションを使用できます。

- [Ping]:選択したIP アドレスで ping コマンドを実行します。
- [トレースルート(Traceroute)]:選択したIP アドレスでトレースルート コマンドを実行します。
- [SSH セッションを開く(Open SSH Session)]:SSHプロトコルで、選択した IP アドレスに対する新しい接続を作成します。
- [Telnet セッションを開く(Open Telnet Session)]:Telnetプロトコルで、選択した IP アドレスに対する新しい接続を作成します。

注:コンソールで語句または IP アドレスをダブルクリックすると、ハイライトするテキストの上にカーソルでドラッグしなくても、すばやく選択できます。


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.194.105
!!!!!
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 @
Message #6 : 88E6095 rev 2 Ethernet @ index 08
Message #8 : 88E6095 rev 2 Ethernet @ index 07
Message #10 : 88E6095 rev 2 Ethernet @ index 0
Message #12 : 88E6095 rev 2 Ethernet @ index 0
Message #14 : 88E6095 rev 2 Ethernet @ index 0
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

よく寄せられる質問（FAQ）

使用する機能によっては、Cisco.com アカウントでログインする必要があるのはなぜですか。

Cisco CLI アナライザを使用するには、有効な Cisco.com アカウントが必要になります。有効な Cisco.com アカウントがない場合は、Cisco.com の登録ページで登録を行い、Cisco.com プロファイルにサービス契約を関連付ける必要があります。

CCO アカウント情報を入力しても Cisco CLI アナライザにアクセスできないのはなぜですか。

ユーザ名とパスワードを正しく入力しており、かつ Cisco.com アカウントにアクティブなサポート契約が関連付けられていることを確認してください。これらの項目を確認した上で Cisco CLI アナライザにアクセスできない場合は、「コメントと質問の送信」の説明に従って、フィードバック フォームでお問い合わせください。

CCO アカウントにログインできないのはなぜでしょうか。

ログインできない場合は、次の情報を基に診断してください。

- 十分なアカウント権限がない可能性があります。アカウントのアクセス レベルが不明である場合は、サポートまでご連絡ください。
- オープンなインターネット接続で Cisco CLI アナライザを通じた CCO ログインを試みてください。ログインできた場合、この問題はネットワークのプロキシ設定に起因している可能性があります。
- ネットワークにプロキシ サーバ（Cisco WSA など）がある場合は、それらのホストをプロキシ サーバに追加する必要があります。

  cloudsso.cisco.com
  sso.cisco.com
  api.cisco.com
  cway.cisco.com

- それらのホストをプロキシ サーバに追加したら、Cisco CLI アナライザに再度ログインしてツールを使用してください。

機能のリクエストや、製品に関するフィードバックはどのように行うことができますか。

追加機能のリクエストや、製品に関するフィードバックを行う場合は、「コメントと質問の送信」の説明に従ってフィードバック フォームを使用してください。

ASA トレースバック デコーダで crash.txt ファイルが見つからないのはなぜですか。

ASA がクラッシュして再起動された場合、ASA トレースバック デコーダで crash.txt ファイルが見つからないとのメッセージが表示されることがあります。

ASA 設定ファイルに crashinfo save disable が追加されない限り、ASA では、クラッシュ情報がデフォルトでフラッシュ メモリに保存されます。このコマンドを設定ファイルに追加すると、ファイルを保存できなくなります。この問題を解決するには、コマンドが無効になっていることを確認してください。

注: デフォルトの動作を設定するには、`no crashinfo save disable` を追加します。クラッシュ ファイルが存在すれば、ローカルのフラッシュに「crash.txt」として保存されます。

Cisco CLI アナライザではどのオペレーティング システムがサポートされていますか。

Cisco CLI アナライザでサポートされているオペレーティング システムについては、「システム要件」を参照してください。

Cisco CLI アナライザではどのようなターミナル エミュレーションがサポートされていますか。

Cisco CLI アナライザでは、ターミナル エミュレータ VT100 がサポートされています。

Cisco CLI アナライザではどのようなプロトコルがサポートされていますか。

Cisco CLI アナライザでは、Telnet および SSH バージョン 2 がサポートされています。

ファイル分析で、結果がレポートされない、または提供された出力を特定できないと表示されるのはなぜですか。

分析するテキスト ファイルに次のコンテンツが含まれていることを確認してください。

- ファイル内の各出力を生成したコマンド(「`# show version`」など)
- `show version` コマンドによる出力
- (任意)`show tech-support` コマンドの出力。完全な分析を行うために必要になります。
- (任意)サポートされている他のコマンドによる出力

正規表現検索機能では、どのような表現と文字がサポートされていますか。

Cisco CLI アナライザの正規表現検索機能では、Javascript RegExp の角カッコ、メタ文字、数量詞を使用できます。

角カッコ	説明
[abc]	角カッコの間にある文字を検索する
[^abc]	角カッコの間にない文字を検索する
[0-9]	角カッコの間で指定された範囲内の数字を検索する
[^0-9]	角カッコの間で指定された範囲内にない数字を検索する
(x|y)	指定された文字を検索する

メタ文字	説明
.	1 つの文字(改行記号または行末記号)を検索する
\w	単語文字を検索する
\W	単語文字以外を検索する
\d	数字を検索する
\D	数字以外を検索する
\s	空白文字を検索する
\S	空白文字以外を検索する
\b	単語の先頭または末尾の一致を検索する
\B	単語の先頭または末尾以外での一致を検索する
\0	NUL 文字を検索する
\n	改行文字を検索する
\f	フォーム フィード文字を検索する
\r	CR 文字を検索する
\t	タブ文字を検索する
\v	垂直タブ文字を検索する
\xxx	8 進数 xxx で指定された文字を検索する
\xdd	16 進数 dd で指定された文字を検索する
\uxxxx	16 進数 xxxx で指定された Unicode 文字を検索する

数量詞	説明
n+	少なくとも 1 つの n を含む文字列に一致する
n*	0 または 1 つ以上の n を含む文字列に一致する
n?	0 または 1 つの n を含む文字列に一致する
n{X}	連続する X 個の n を含む文字列に一致する
n{X,Y}	連続する X 個から Y 個までの n を含む文字列に一致する
n{X,}	連続する X 個以上の n を含む文字列に一致する
n$	末尾が n である文字列に一致する
^n	先頭が n である文字列に一致する
?=n	特定の文字列 n が後に続く文字列に一致する
!=n	特定の文字列 n が後に続かない文字列に一致する