



Monitoring and Report Viewer を使用した ACS のトラブルシューティング

この章では、Monitoring and Report Viewer が提供する Cisco Secure Access Control System 用の診断ツールおよびトラブルシューティング ツールについて説明します。

この章の内容は、次のとおりです。

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テストの実行 \(14-3 ページ\)](#)
- [診断情報向け ACS サポート バンドルのダウンロード \(14-4 ページ\)](#)
- [Expert Troubleshooter での作業 \(14-6 ページ\)](#)

利用可能な診断ツールおよびトラブルシューティング ツール

Monitoring and Report Viewer には、次のツールが用意されています。

- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

接続テスト

認証に問題がある場合は、接続テストを実行して、接続に関する問題をチェックできます。接続先のネットワーク デバイスのホスト名または IP アドレスを入力して、Web インターフェイスから **ping**、**traceroute**、および **nslookup** コマンドを実行できます。

Monitoring and Report Viewer に、これらのコマンドの出力が表示されます。接続テストの実行方法の詳細な手順については、[接続テストの実行 \(14-3 ページ\)](#) を参照してください。

ACS サポート バンドル

ACS サポート バンドルを使用して、TAC が ACS の問題をトラブルシューティングするための診断情報を準備できます。

通常、サポートバンドルには、ACS データベース、ログ ファイル、コア ファイル、および Monitoring and Report Viewer のサポート ファイルが含まれています。ACS ノードごとに、サポートバンドルから特定のファイルを除外できます。サポートバンドルは、ローカルコンピュータにダウンロードできます。ブラウザに、(設定に応じて) ダウンロードの進行状況が表示され、適切な場所にサポートバンドルを保存するように要求するプロンプトが表示されます。

- ACS サーバがプライマリ インスタンスである場合、サポートバンドルには、ACS 設定のエクスポートが含まれています。
- ACS サーバがセカンダリ インスタンスである場合、ACS データベースは含まれていません。
- ACS サーバがログ コレクタである場合、サポートバンドルには、監視およびレポートの設定のエクスポート、および収集された AAA の監査ログと診断ログが含まれています。
- ACS サーバがログ コレクタでない場合、サポートバンドルには、監視およびレポートの設定は含まれていません。ACS サポートバンドルのダウンロード方法の詳細な手順については、[診断情報向け ACS サポートバンドルのダウンロード \(14-4 ページ\)](#) を参照してください。

Expert Troubleshooter

Expert Troubleshooter は、展開されている ACS の問題の診断およびトラブルシューティングに役立つ、Web ベースの使いやすいトラブルシューティングユーティリティです。このユーティリティを使用すると、問題を診断する時間を短縮でき、問題の解決方法の詳細な手順が提供されます。

Expert Troubleshooter を使用して、成功した認証および失敗した認証を診断およびトラブルシューティングできます。たとえば、ユーザがネットワークへのアクセス権を取得できない場合、Expert Troubleshooter を使用して、問題の原因を診断できます。

Expert Troubleshooter では、ACS Web インターフェイスから任意のネットワーク デバイス上で **show** コマンドを実行できます。**show** コマンドの出力は、コンソールへの出力とまったく同じ形式で返されます。

Expert Troubleshooter を使用して、任意のネットワーク デバイスの設定を評価し、問題を引き起こすような矛盾が存在しないかどうかを確認できます。ACS 5.8 は、IPv4 と IPv6 を介したネットワーク デバイスとの通信の評価をサポートします。

さらに、Expert Troubleshooter には Security Group Access デバイス関連の問題をトラブルシューティングするための 4 つの診断ツールが用意されています。

Expert Troubleshooter によって、問題の原因が特定され、問題を解決するために実行可能な一連のアクションが示されます。Expert Troubleshooter に用意されているさまざまなツールの詳細については、[Expert Troubleshooter での作業 \(14-6 ページ\)](#) を参照してください。

表 14-1 に、ACS 5.8 に用意されている診断ツールを示します。

表 14-1 Expert Troubleshooter : 診断ツール

診断ツール	説明
RADIUS Authentication Troubleshooting	RADIUS 認証をトラブルシューティングします。詳細については、「 RADIUS 認証のトラブルシューティング (14-6 ページ) 」を参照してください。
Execute Network Device Command	ネットワーク デバイス上で任意の show コマンドを実行します。詳細については、「 ネットワーク デバイス上での show コマンドの実行 (14-10 ページ) 」を参照してください。
Evaluate Configuration Validator	ネットワーク デバイスの設定を評価します。詳細については、「 ネットワーク デバイスの設定の評価 (14-11 ページ) 」を参照してください。

表 14-1 Expert Troubleshooter : 診断ツール (続き)

診断ツール	説明
TrustSec ツール	
Egress (SGACL) Policy	ネットワーク デバイスと ACS との間で出力ポリシー (SGACL) を比較します。詳細については、「 ネットワーク デバイスと ACS との間での SGACL ポリシーの比較 (14-12 ページ) 」を参照してください。
SXP-IP Mappings	デバイスとピアとの間で SXP マッピングを比較します。詳細については、「 デバイスとそのピアとの間での SXP-IP マッピングの比較 (14-13 ページ) 」を参照してください。
IP User SGT	デバイスの IP-SGT を、ACS 認証で割り当てられたユーザ IP-SGT レコードと比較します。詳細については、「 デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較 (14-15 ページ) 」を参照してください。
Device SGT	デバイスの SGT を、ACS によって割り当てられた SGT と比較します。詳細については、「 デバイス SGT と ACS によって割り当てられたデバイス SGT との比較 (14-16 ページ) 」を参照してください。

接続テストの実行

ネットワーク デバイスのホスト名または IP アドレスを使用して、デバイスへの接続をテストできます。たとえば、接続テストを実行することによって、ID ストアへの接続を確認できます。ACS 5.8 では、リモート マシンの接続もテストできます。

ACS と、デバイスのホスト名または IP アドレスとの間の接続をテストするには、次の手順を実行します。

- ステップ 1 [Monitoring and Reports] > [Troubleshooting] > [Connectivity Tests] を選択します。
[Connectivity Tests] ページが表示されます。
- ステップ 2 適切な IP アドレスの種類を選択するために [IPv4] または [IPv6] オプション ボタンをクリックします。
- ステップ 3 表 14-2 の説明に従って、[Connectivity Tests] ページのフィールドを変更します。

表 14-2 Connectivity Tests

オプション	説明
[Hostname] または [IP Address]	テストする接続のホスト名または IP アドレスを入力します。入力したホスト名または IP アドレスをクリアするには、[Clear] をクリックします。
ping	送受信されたパケット、パケット損失 (存在する場合)、およびテストが完了するまでの時間を示す ping コマンドの出力を確認する場合にクリックします。
tracert	ACS とテスト対象のホスト名または IP アドレスとの間の中間 IP アドレス (ホップ)、および各ホップ完了までの時間を示す tracert コマンドの出力を確認する場合にクリックします。
nslookup	テスト対象のホスト名または IP アドレスをドメイン ネーム サーバに問い合わせた結果としてのサーバ名および IP アドレスを示す nslookup コマンドの出力を確認する場合にクリックします。

ステップ 4 実行するテストに応じて、[ping]、[tracert]、または [nslookup] をクリックします。
[ping]、[tracert]、または [nslookup] コマンドの出力が表示されます。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポートバンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

診断情報向け ACS サポートバンドルのダウンロード

ACS サポートバンドルを作成およびダウンロードするには、次の手順を実行します。

ステップ 1 [Monitoring and Reports] > [Troubleshooting] > [ACS Support Bundle] を選択します。
[ACS Support Bundle] ページが表示され、表 14-3 で説明されているフィールドが表示されます。

表 14-3 [ACS Support Bundle] ページ

オプション	説明
Server	ACS ノード インスタンスの名前。ACS ノード インスタンスの ACS サポートバンドルを作成およびダウンロードするための [Download Parameters for the Server] ページを表示する場合にクリックします。
IP Address	表示のみ。関連する ACS ノードの IP アドレスを示します。
Node Designation	表示のみ。関連する ACS ノードのプライマリ インスタンスまたはセカンダリ インスタンスを示します。

ステップ 2 サーバを選択して、[Get Support Bundle] をクリックします。
[Download Parameters for the Server] ページが表示されます。関連する ACS ノード インスタンスの ACS サポートバンドルを作成およびダウンロードできます。



(注) ACS 5.8 では、IPv6 URL で指定された宛先にサポートバンドルをダウンロードすることができます。

ステップ 3 ACS support.tar.gz ファイルに統合するダウンロード オプションを選択します。
ファイルのサイズが非常に大きい場合には、サポートバンドルのダウンロードに時間がかかる場合があります。ダウンロード時間を短縮するためには、サポートバンドルにコアファイルおよび Monitoring & Report Viewer のサポートファイルを含めないでください。

次のオプションがあります。

- **Encrypt Support Bundle** : サポートバンドルを暗号化するには、このチェックボックスをオンにします。[Passphrase] に復号化用のパスワードを指定し、[Confirm Passphrase] でそのパスワードを確認します。

- **Include full configuration database** : サポートバンドルにデータベース全体を組み込む場合にこのチェックボックスをオンにします。このオプションがオフの場合、サポートバンドルには、データベースのサブセットだけが組み込まれます。ログに機密情報を含めるかどうかを指定するには、[Include sensitive information] または [Exclude sensitive information] をクリックします。

機密情報には、暗号化されたパスワードや、ACS 設定データなどがあります。

- **Include debug logs** : デバッグログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Recent] をクリックして、組み込むデバッグログの範囲を [file(s)] フィールドに 1 ~ 999 の値を入力します。
- **Include local logs** : ローカルログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Recent] をクリックして、組み込むローカルログの範囲を [file(s)] フィールドに 1 ~ 999 の値を入力します。
- **Include core files** : コアファイルを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Include files from the last] をクリックして、[day(s)] フィールドに 1 ~ 365 の値を入力します。
- **Include monitoring and reporting logs** : 監視ログおよびレポートログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Include files from the last] をクリックして、[day(s)] フィールドに 1 ~ 365 の値を入力します。

次のどの監視ログおよびレポートログを組み込むかを指定します。

- AAA Audit
 - AAA Diagnostics
 - System Diagnostics
 - AAA Accounting
 - Administrative and Operational Audit
- **Include system logs** : システムログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Recent] をクリックして、[file(s)] フィールドに 1 ~ 999 の値を入力します。
- 必要に応じて、[Description] フィールドに説明を入力できます。

ステップ 4 次のいずれかをクリックします。

- 指定したオプションを使用してサポートバンドルをダウンロードするには、[Download] をクリックします。サポートバンドルが作成およびダウンロードされます。
- 行った変更をクリアして、デフォルト設定に戻すには、[Restore Defaults] をクリックします。



(注)

ACS は、デフォルトで関連する ACS ノードインスタンスのサポートバンドルを作成またはダウンロードする際にコアファイルを選択しません。サポートバンドルにコアファイルを含める場合は、[Include core files] チェックボックスをオンにできます。[Encrypt Support Bundle] チェックボックスをオンにすると、ACS のサポートバンドルを暗号化できます。これにより、コアファイルが暗号化され、サポートされているバンドルに含まれます。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)

- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

Expert Troubleshooter での作業

次の項では、Expert Troubleshooter 診断ツールの使用方法について説明します。

- [RADIUS 認証のトラブルシューティング \(14-6 ページ\)](#)
- [ネットワーク デバイス上での show コマンドの実行 \(14-10 ページ\)](#)
- [ネットワーク デバイスの設定の評価 \(14-11 ページ\)](#)
- [ネットワーク デバイスと ACS との間での SGACL ポリシーの比較 \(14-12 ページ\)](#)
- [デバイスとそのピアとの間での SXP-IP マッピングの比較 \(14-13 ページ\)](#)
- [デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較 \(14-15 ページ\)](#)
- [デバイス SGT と ACS によって割り当てられたデバイス SGT との比較 \(14-16 ページ\)](#)

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

RADIUS 認証のトラブルシューティング

RADIUS Authentication Troubleshooting 診断ツールを使用すると、RADIUS 認証に関する問題をトラブルシューティングできます。これを行うには、次の手順を実行します。

- ステップ 1** [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。
[Expert Troubleshooter] ページが表示されます。
- ステップ 2** トラブルシューティング ツールのリストから、[RADIUS Authentication Troubleshooting] を選択します。
[RADIUS Authentication Troubleshooter] ページが表示されます。
- ステップ 3** [表 14-4](#) に示すようにフィールドを変更して、トラブルシューティング対象の RADIUS 認証をフィルタリングします。

表 14-4 [RADIUS Authentication Troubleshooter] ページ

オプション	説明
トラブルシューティング対象の RADIUS 認証の検索および選択	
Username	認証をトラブルシューティングするユーザのユーザ名を入力するか、または [Select] をクリックしてリストからユーザ名を選択します。ユーザ名をクリアするには、[Clear] をクリックします。

表 14-4 [RADIUS Authentication Troubleshooter] ページ (続き)

オプション	説明
MAC Address	トラブルシューティングするデバイスの MAC アドレスを入力するか、または [Select] をクリックしてリストから MAC アドレスを選択します。MAC アドレスをクリアするには、[Clear] をクリックします。
Audit Session ID	トラブルシューティングする監査セッション ID を入力します。監査セッション ID をクリアするには、[Clear] をクリックします。
NAS IP	NAS IP アドレスを入力するか、または [Select] をクリックしてリストから NAS IP アドレスを選択します。NAS IP アドレスをクリアするには、[Clear] をクリックします。
NAS Port	NAS ポート番号を入力するか、または [Select] をクリックしてリストから NAS ポート番号を選択します。NAS ポート番号をクリアするには、[Clear] をクリックします。
Authentication Status	[Authentication Status] ドロップダウン リスト ボックスから、RADIUS 認証のステータスを選択します。次のオプションを使用できます。 <ul style="list-style-type: none"> • Pass or Fail • Pass • Fail
Failure Reason	失敗理由を入力するか、または [Select] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[Clear] をクリックします。
Time Range	[Time Range] ドロップダウン リスト ボックスから期間を定義します。Monitoring and Report Viewer によって、この期間に作成された RADIUS 認証レコードが取得されます。次のオプションを使用できます。 <ul style="list-style-type: none"> • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time	([Time Range] として [Custom] を選択した場合だけ) 開始日時を入力するか、またはカレンダー アイコンをクリックして開始日時を選択します。日付は mm/dd/yyyy 形式、時刻は hh:mm 形式である必要があります。
End Date-Time	([Time Range] として [Custom] を選択した場合だけ) 終了日時を入力するか、またはカレンダー アイコンをクリックして終了日時を選択します。日付は mm/dd/yyyy 形式、時刻は hh:mm 形式である必要があります。
Fetch Number of Records	Monitoring and Report Viewer で一度に取得するレコード数を [Fetch Number of Records] ドロップダウン リストから選択します。使用可能なオプションは、[10]、[20]、[50]、[100]、[200]、および [500] です。
Active Directory Domain Name	Active Directory ドメイン名を入力します。AD レコードは、AD の詳細が提供されたときにのみ取得されます。
Active Directory Domain Admin Name	Active Directory ドメイン管理者の名前を入力します。AD レコードは、AD の詳細が提供されたときにのみ取得されます。
Active Directory Domain Admin Password	Active Directory ドメイン管理者のパスワードを入力します。AD レコードは、AD の詳細が提供されたときにのみ取得されます。


- ステップ 4** [Search] をクリックして、検索条件に一致する RADIUS 認証を表示します。
- [Search Result] テーブルに、検索結果が読み込まれます。このテーブルには、[Time]、[Status]、[Username]、[MAC Address]、[Audit Session ID]、[Network Device IP]、[Failure Reason]、および [Access Service] というフィールドがあります。
- ステップ 5** このテーブルから、トラブルシューティングする RADIUS 認証レコードを選択して、[Troubleshoot] をクリックします。
- Expert Troubleshooter によって、RADIUS 認証のトラブルシューティングが開始されます。必要に応じて、Monitoring and Report Viewer によって追加入力が要求されます。
- たとえば、Expert Troubleshooter からネットワーク デバイスへの接続が必要な場合は、接続パラメータおよびログイン クレデンシャルの入力を要求するプロンプトが表示されます。
-  **(注)** RADIUS 認証が AD に対して実行された場合、ACS はトラブルシューティング プロセスを開始する前に AD 証明書を要求します。これらのレポートにアクセスするたびに AD クレデンシャルを入力する必要があります。
- ステップ 6** [User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。
- ステップ 7** [Submit] をクリックします。
- [Progress Details] ページが表示されます。このページには概要が表示されます。また、必要に応じて追加入力を要求するプロンプトが表示されます。Monitoring and Report Viewer で追加入力を必要とする場合は、[Click User Input Required] ボタンをクリックする必要があります。ダイアログボックスが表示されます。
- ステップ 8** 表 14-5 の説明に従ってダイアログボックスのフィールドを変更して、[Submit] をクリックします。

表 14-5 [Progress Details Page - User Input] ダイアログボックス

オプション	説明
ネットワーク デバイス a.b.c.d の接続パラメータの指定	
Username	ネットワーク デバイスにログインするためのユーザ名を入力します。
Password	パスワードを入力します。
Protocol	[Protocol] ドロップダウン リストからプロトコルを選択します。有効なオプションは次のとおりです。 <ul style="list-style-type: none"> • Telnet • SSHv2 [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続をイネーブルにする必要があります。
Port	ポート番号を入力します。
Enable Password	イネーブル パスワードを入力します。
Same As Login Password	イネーブル パスワードがログイン パスワードと同じ場合は、このチェックボックスをオンにします。
Use Console Server	コンソール サーバを使用する場合にこのチェックボックスをオンにします。
Console IP Address	([Use Console Server] チェックボックスをオンにした場合だけ) コンソールの IP アドレスを入力します。

表 14-5 [Progress Details Page - User Input] ダイアログボックス

オプション	説明
高度なオプション (「Expect timeout error」が表示される場合や、デバイスから非標準のプロンプト文字列が返される場合に使用)	高度なオプションは、一部のトラブルシューティング ツールに対してだけ表示されます。
Username Expect String	Username: や Login: などの、ネットワーク デバイスによってユーザ名入力用プロンプトとして使用される文字列を入力します。
Password Expect String	Password: などの、ネットワーク デバイスによってパスワード入力用プロンプトとして使用される文字列を入力します。
Prompt Expect String	ネットワーク デバイスで使用されるプロンプトを入力します。たとえば、#、>、@ を入力します。
Authentication Failure Expect String	Incorrect password や Login invalid などの、認証エラーが発生した場合にネットワーク デバイスから返される文字列を入力します。

ステップ 9 [Done] をクリックして、[Expert Troubleshooter] に戻ります。

[Progress Details] ページは定期的に更新されて、トラブルシューティングの進行中に実行されたタスクが表示されます。トラブルシューティングが完了すると、[Show Results Summary] ボタンが表示されます。

ステップ 10 [Show Results Summary] をクリックします。

[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。

表 14-6 [Results Summary] ページ

オプション	説明
Diagnosis and Resolution	
Diagnosis	問題の診断がここに表示されます。
Resolution	問題の解決手順がここに詳細に表示されます。
Troubleshooting Summary	
Summary	トラブルシューティング情報の各ステップの概要がここに表示されます。任意のステップを展開して、詳細を表示できます。 すべての設定エラーが赤いテキストで示されます。

ステップ 11 [Done] をクリックして、[Expert Troubleshooter] に戻ります。

Monitoring and Report Viewer によって、診断、問題の解決手順、および問題の解決に役立つトラブルシューティング概要が提供されます。



(注) RADIUS Authentication Troubleshooting は、RADIUS 認証レポート ページからも起動できます。この診断ツールを起動する場合は、特定の RADIUS 認証の詳細ページまでドリルダウンする必要があります。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

ネットワーク デバイス上での **show** コマンドの実行

Execute Network Device Command 診断ツールを使用すると、ACS Web インターフェイスからネットワーク デバイス上で任意の **show** コマンドを実行できます。**show** コマンドの結果は、コンソールに表示される場合とまったく同じ形式であり、デバイス設定の問題を特定するために使用できます。任意のネットワーク デバイス上で **show** コマンドを実行するには、次の手順を実行します。

- ステップ 1 [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。
- ステップ 2 トラブルシューティング ツールのリストから、[Execute Network Device Command] を選択します。[Expert Troubleshooter] ページが更新され、表 14-7 で説明されているフィールドが表示されます。

表 14-7 ネットワーク デバイス上での **show** コマンドの実行

オプション	説明
情報の入力	
Network Device IP	show コマンドを実行するネットワーク デバイスの IPv4 または IPv6 アドレスを入力します。
Command	実行する show コマンドを入力します。

- ステップ 3 [Run] をクリックして、指定したネットワーク デバイスで **show** コマンドを実行します。[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が必要です。
- ステップ 4 [User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。
- ステップ 5 [Submit] をクリックして、ネットワーク デバイス上で **show** コマンドを実行し、出力を表示します。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

ネットワーク デバイスの設定の評価

この診断ツールを使用して、ネットワーク デバイスの設定を評価し、不足している設定や誤っている設定を特定できます。Expert Troubleshooter によって、デバイスの設定が標準設定と比較されます。目的

- ステップ 1** [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。
- ステップ 2** トラブルシューティング ツールのリストから、[Evaluate Configuration Validator] をクリックします。
[Expert Troubleshooter] ページが更新され、表 14-8 で説明されているフィールドが表示されます。

表 14-8 Evaluate Configuration Validator

オプション	説明
情報の入力	
Network Device IP	設定を評価するネットワークの IPv4 または IPv6 アドレスを入力します。
推奨テンプレートと比較する設定項目を、次のうちから選択します。	
AAA	デフォルトはオンです。
RADIUS	デフォルトはオンです。
Device Discovery	デフォルトはオンです。
Logging	デフォルトはオンです。
Web Authentication	Web 認証設定を比較する場合にこのチェックボックスをオンにします。
Profiler Configuration	Profiler 設定を比較する場合にこのチェックボックスをオンにします。
SGA	Security Group Access 設定を比較する場合にこのチェックボックスをオンにします。
802.1X	802.1X 設定を比較する場合にこのチェックボックスをオンにします。次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> open モード Low Impact Mode (Open Mode + ACL) High Security Mode (Closed Mode)

- ステップ 3** [Run] をクリックします。
[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。
- ステップ 4** [User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。
[Troubleshooting Progress Details] ページが表示されます。Expert Troubleshooter によって、ネットワーク デバイスから CLI 応答が取得されます。新しいウィンドウが表示されて、インターフェイス設定を分析するインターフェイスの選択を要求するプロンプトが表示されます。
- ステップ 5** 分析するインターフェイスのチェックボックスをオンにして [Submit] をクリックし、インターフェイスの設定を評価します。
[Progress Details] ページが表示され、概要が示されます。

- ステップ 6 [Show Results Summary] をクリックして、トラブルシューティング概要を表示します。
[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。不足している設定は赤色で表示されます。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

ネットワーク デバイスと ACS との間での SGACL ポリシーの比較

Security Group Access 対応デバイスでは、ACS に設定した出力ポリシー マトリクスに基づいて、ACS によって送信元 SGT と宛先 SGT の各ペアに対して SGACL が割り当てられます。Egress Policy 診断ツールでは、次の処理が実行されます。

1. IP アドレスを指定したデバイスに接続して、送信元 SGT と宛先 SGT の各ペアに対する ACL が取得されます。
2. ACS に設定された出力ポリシーがチェックされ、送信元 SGT と宛先 SGT の各ペアに対する ACL が取得されます。
3. ネットワーク デバイスから取得された SGACL ポリシーと、ACS から取得された SGACL ポリシーが比較されます。
4. ポリシーが一致しない送信元 SGT と宛先 SGT のペアが表示されます。また、追加情報として、一致するエントリも表示します。

ネットワーク デバイスと ACS との間で SGACL ポリシーを比較するには、次の手順を実行します。

- ステップ 1 [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。
- ステップ 2 トラブルシューティング ツールのリストから、[Egress (SGACL) Policy] を選択します。
[Expert Troubleshooter] ページが更新され、[Network Device IP] フィールドが表示されます。
- ステップ 3 ACS と SGACL ポリシーを比較する Security Group Access デバイスの IP アドレスを入力します。
- ステップ 4 [Run] をクリックして、ACS とネットワーク デバイスとの間で SGACL ポリシーを比較します。
[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が必要とされます。
- ステップ 5 [User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。
- ステップ 6 [Submit] をクリックします。
[Progress Details] ページが表示され、結果概要が表示されます。
- ステップ 7 [Show Results Summary] をクリックして、診断および解決手順を表示します。
[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

デバイスとそのピアとの間での SXP-IP マッピングの比較

Security Group Access デバイスは、ピアと通信し、その SGT 値を学習します。Security Exchange Protocol (SXP) -IP Mappings 診断ツールは、指定した IP アドレスのデバイスに接続して、ピア デバイスの IP アドレスおよび SGT 値をリストします。

デバイスのピアを 1 つ以上選択する必要があります。このツールは、選択した各ピアに接続し、その SGT 値を取得して、これらの値が以前に取得した値と同じであるかどうかを確認します。

この診断ツールを使用すると、デバイスとそのピアとの間で SXP-IP マッピングを比較できます。目的

-
- ステップ 1** [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。
- ステップ 2** トラブルシューティング ツールのリストから、[SXP-IP Mappings] を選択します。
[Expert Troubleshooter] ページが更新され、[Network Device IP] フィールドが表示されます。
- ステップ 3** ネットワーク デバイスの IP アドレスを入力します。
- ステップ 4** トラブルシューティング ツールのリストで [SXP-IP Mappings] をクリックします。
[Expert Troubleshooter] ページが更新されて、次のフィールドが表示されます。
Network Device IP : ネットワーク デバイスの IP アドレスを入力します。
- ステップ 5** [Run] をクリックします。
[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。
- ステップ 6** [User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。
[Troubleshooting Progress Details] ページが表示されます。Expert Troubleshooter によって、ネットワーク デバイスから SGA SXP 接続が取得されて、ピア SXP デバイスを選択するように再度要求するプロンプトが表示されます。
- ステップ 7** [User Input Required] ボタンをクリックします。
表 14-9 で説明されているフィールドを持つ新しいウィンドウが表示されます。

表 14-9 ピア SXP デバイス

オプション	説明
ピア SXP デバイス	
Peer IP Address	ピア SXP デバイスの IP アドレス。
VRF	ピア デバイスの VRF インスタンス。
Peer SXP Mode	送信者であるかまたは受信者であるかなどの、ピア デバイスの SXP モード。
Self SXP Mode	送信者であるかまたは受信者であるかなどの、ネットワーク デバイスの SXP モード。
Connection State	接続のステータス。

表 14-9 ピア SXP デバイス

オプション	説明
共通接続パラメータ	
User Common Connection Parameters	すべてのピア SXP デバイスの共通接続パラメータを有効にする場合にこのチェックボックスをオンにします。 共通接続パラメータが指定されていない場合、または何らかの理由で共通接続パラメータが機能しない場合には、Expert Troubleshooter によって再度その特定のピア デバイスに対する接続パラメータの入力を要求するプロンプトが表示されます。
Username	ピア SXP デバイスのユーザ名を入力します。
Password	ピア デバイスにアクセスするためのパスワードを入力します。
Protocol	<ul style="list-style-type: none"> [Protocol] ドロップダウン リスト ボックスからプロトコルを選択します。有効なオプションは次のとおりです。 <ul style="list-style-type: none"> - Telnet - SSHv2 <p>[Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続をイネーブルにする必要があります。</p>
Port	<ul style="list-style-type: none"> ポート番号を入力します。デフォルトのポート番号は、Telnet は 23、SSH は 22 です。
Enable Password	イネーブル パスワードがログインパスワードと異なる場合に入力します。
Same as login password	有効パスワードがログインパスワードと同じ場合は、このチェックボックスをオンにします。

ステップ 8 SXP マッピングを比較するピア SXP デバイスのチェックボックスをオンにして、表 14-9 の説明に従って共通接続パラメータを入力します。

ステップ 9 [Submit] をクリックします。
[Progress Details] ページが表示され、結果概要が示されます。

ステップ 10 [Show Results Summary] をクリックして、診断および解決手順を表示します。
[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較

Security Group Access 対応デバイスでは、ACS によって、RADIUS 認証を通して各ユーザに SGT 値が割り当てられます。IP User SGT 診断ツールは、指定した IP アドレスのネットワーク デバイスに接続して、次の処理を行います。

1. ネットワーク デバイス上のすべての IP-SGT 割り当てのリストを取得します。
2. 各 IP-SGT ペアの RADIUS 認証レコードおよびアカウントング レコードをチェックして、ACS によって割り当てられた最新のユーザ IP-SGT 値を確認します。
3. IP-SGT ペアを表形式で表示して、ACS によって割り当てられた最新の SGT 値とデバイス上の SGT 値が同じであるかどうかが特定されます。

この診断ツールを使用すると、デバイスの IP-SGT 値と ACS によって割り当てられた SGT を比較できます。目的

ステップ 1 [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

ステップ 2 トラブルシューティング ツールのリストから、[IP User SGT] をクリックします。

[Expert Troubleshooter] ページが更新され、表 14-10 で説明されているフィールドが表示されます。

表 14-10 IP User SGT

オプション	説明
情報の入力	
Network Device IP	ネットワーク デバイスの IPv4 または IPv6 アドレスを入力します。
結果のフィルタリング	
Username	レコードをトラブルシューティングするユーザのユーザ名を入力します。
User IP Address	レコードをトラブルシューティングするユーザの IP アドレスを入力します。
SGT	ユーザ SGT 値を入力します。

ステップ 3 [Run] をクリックします。

[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。

ステップ 4 [User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

ステップ 5 [Submit] をクリックします。

[Progress Details] ページが表示され、結果概要が示されます。

ステップ 6 [Show Results Summary] をクリックして、診断および解決手順を表示します。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

デバイス SGT と ACS によって割り当てられたデバイス SGT との比較

Security Group Access 対応デバイスでは、ACS によって、RADIUS 認証を通して各ネットワーク デバイスに SGT 値が割り当てられます。Device SGT 診断ツールは、指定した IP アドレスのネットワーク デバイスに接続して、次の処理を行います。

1. ネットワーク デバイスの SGT 値を取得します。
2. RADIUS 認証レコードをチェックして、ACS によって割り当てられた最新の SGT 値を特定します。
3. デバイス SGT ペアを表形式で表示して、SGT 値が同じであるかどうか特定されます。
この診断ツールを使用すると、デバイス SGT を、ACS によって割り当てられたデバイス SGT と比較できます。目的

ステップ 1 [Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。
[Expert Troubleshooter] ページが表示されます。

ステップ 2 トラブルシューティング ツールのリストから、[Device SGT] をクリックします。
[Expert Troubleshooter] ページが更新され、表 14-11 で説明されているフィールドが表示されます。

表 14-11 Device SGT

オプション	説明
情報の入力	
Network Device IPs (カンマ区切りのリスト)	カンマ区切りのネットワーク デバイス IPv4 または IPv6 アドレス (SGT を、ACS によって割り当てられたデバイス SGT と比較するデバイスの場合) を入力します。
共通接続パラメータ	
Use Common Connection Parameters	<p>比較時に次の共通接続パラメータを使用する場合にこのチェックボックスをオンにします。</p> <ul style="list-style-type: none"> • Username : ネットワーク デバイスのユーザ名を入力します。 • Password : パスワードを入力します。 • [Protocol] : [Protocol] ドロップダウン リスト ボックスからプロトコルを選択します。有効なオプションは次のとおりです。 <ul style="list-style-type: none"> - Telnet - SSHv2 <p>[Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続をイネーブルにする必要があります。</p> <ul style="list-style-type: none"> • Port : ポート番号を入力します。デフォルトのポート番号は、Telnet は 23、SSH は 22 です。
Enable Password	イネーブル パスワードがログインパスワードと異なる場合に入力します。
Same as login password	有効パスワードがログインパスワードと同じ場合は、このチェックボックスをオンにします。

ステップ 3 [Run] をクリックします。
[Progress Details] ページが表示され、概要が示されます。

ステップ 4 [Show Results Summary] をクリックして、デバイス SGT 比較の結果を表示します。

[Results Summary] ページが表示されて、診断、解決策、およびトラブルシューティング概要が表示されます。

関連項目

- [利用可能な診断ツールおよびトラブルシューティング ツール \(14-1 ページ\)](#)
- [接続テスト \(14-1 ページ\)](#)
- [ACS サポート バンドル \(14-1 ページ\)](#)
- [Expert Troubleshooter \(14-2 ページ\)](#)

