操作のユーザ インターフェイスのリファレンス

RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [RADIUS ライブ ログ（RADIUS Live Logs）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]** です。RADIUS ライブ ログはプライマリ PAN だけで表示されます。

表 *1 : RADIUS* ライブ ログ

オプション	使用上のガイドライン
時刻（Time）	モニタリングおよび収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。

オプション	使用上のガイドライン
繰り返し回数（Repeat Count）	ID、ネットワーク デバイス、および許可のコンテキストで変更がなく、直近の24時間で認証要求が繰り返された回数を表示します。
ID（Identity）	ログイン済みの認証に関連付けられているユーザ名を示します。
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
エンドポイント プロファイル（Endpoint Profile）	プロファイリングされるエンドポイントのタイプを示します（たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます）。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル	認証に使用された許可プロファイルを表示します。
[IPアドレス（IP Address）]	エンドポイントデバイスの IP アドレスを表示します。
ネットワーク デバイス（Network Device）	ネットワーク アクセス デバイスの IP アドレスを表示します。
デバイス ポート（Device Port）	エンドポイントが接続されているポート番号を表示します。
ID グループ	ログの生成対象となるユーザまたはエンドポイントに割り当てられる ID グループを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
サーバ	ログの生成元になったポリシー サービスが示されます。
MDMサーバ名（MDM Server Name）	MDM サーバの名前を表示します。
イベント	イベント ステータスを表示します。

オプション	使用上のガイドライン
失敗の理由（Failure Reason）	認証が失敗した場合、その失敗の詳細な理由を表示します。
認証方式（Auth Method）	Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2（MS-CHAPv2）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や拡張認証プロトコル（EAP）など、使用される認証プロトコルを表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
セッション ID	セッション ID を表示します。

（注） [RADIUS ライブ ログ（RADIUS Live Logs）] と [TACACS+ ライブ ログ（TACACS+ Live Logs）] 詳細ペインでは、各ポリシー許可ルールの 1 番目の属性として [照会済み PIP（Queried PIP）] が表示されます。許可ルール内のすべての属性が、以前のルールについてすでに照会されているディクショナリに関連している場合、これ以外に [照会済み PIP（Queried PIP）] エントリは表示されません。

[RADIUS ライブ ログ（RADIUS Live Logs）] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタム フィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

関連トピック

ライブ認証のモニタ
ライブ認証

RADIUS ライブ セッション

次の表では、ライブ認証が表示される [RADIUS ライブ セッション（RADIUS live sessions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [RADIUS] > [ライブ セッション（Live Sessions）]** です。 RADIUS ライブ セッションはプライマリ PAN でしか表示できません。

表 *2 : RADIUS* ライブ セッション

フィールド	説明
開始（Initiated）	セッション開始時のタイムスタンプを表示します。
更新しました	何らかの変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（Account Session Time）	ユーザ セッションの期間（秒単位）を表示します。
セッション ステータス（Session Status）	エンドポイント デバイスの現在のステータスを表示します。
アクション（CoA Action）	アクティブな RADIUS セッションを再認証するか、またはアクティブな RADIUS セッションを切断するには、[アクション（Actions）] アイコンをクリックします。
繰り返し回数（Repeat Count）	ユーザまたはエンドポイントの再認証回数を示します。
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
ID（Identity）	エンドポイント デバイスのユーザ名を表示します。
[IPアドレス（IP Address）]	エンドポイントデバイスの IP アドレスを表示します。
監査セッション ID（Audit Session ID）	固有のセッション ID を表示します。
アカウント セッション ID（Account Session ID）	ネットワーク デバイスから提供された固有 ID を表示します。
エンドポイント プロファイル（Endpoint Profile）	デバイスのエンドポイント プロファイルを表示します。

フィールド	説明
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
サーバ	ログを生成したポリシーサービスを示します。
認証方式（Auth Method）	パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や拡張認証プロトコル（EAP）など、使用される認証プロトコルを表示します。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル	認証に使用された許可プロファイルを表示します。
NAS IP アドレス	ネットワーク デバイスの IP アドレスを表示します。
デバイス ポート（Device Port）	ネットワーク デバイスに接続されたポートを表示します。
PRA アクション（PRA Action）	ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。
ANCステータス（ANC Status）	[隔離（Quarantine）]、[隔離解除（Unquarantine）]、または [シャットダウン（Shutdown）] としてデバイスの適応型ネットワーク制御のステータスを表示します。

フィールド	説明
WLC ローミング（WLC Roam）	エンドポイントがローミング中にWLC間でハンドオフされたことを追跡するために使用されるブール値（Y/N）を表示します。cisco-av-pair=nas-update の値は Y または N です。
パケット入力	受信したパケットの数を表示します。
パケット出力	送信したパケットの数を表示します。
受信バイト数（Bytes In）	受信したバイト数を表示します。
送信バイト数（Bytes Out）	送信したバイト数を表示します。
セッション送信元（Session Source）	RADIUS セッションまたは PassiveID セッションのいずれであるかを示します。
ユーザドメイン名（User Domain Name）	ユーザの登録済み DNS 名を示します。
ホストドメイン名（Host Domain Name）	ホストの登録済み DNS 名を示します。
ユーザNetBIOS名（User NetBIOS Name）	ユーザの NetBIOS 名を示します。
ホストNetBIOS名（Host NetBIOS Name）	ホストの NetBIOS 名を示します。
ライセンスのタイプ（License Type）	使用されているライセンスのタイプ（Base、Plus、Apex、または Plus and Apex）を表示します。
ライセンスの詳細（License Details）	ライセンスの詳細を表示します。

フィールド	説明
プロバイダー	エンドポイント イベントはさまざまな syslog ソースから学習されます。これらの syslog ソースはプロバイダーと呼ばれます。 • Windows Management Instrumentation（WMI）：WMI は、オペレーティング システム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクト モデルを提供する Windows サービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベント メッセージを送信するロギング サーバ。 • REST：クライアントはターミナルサーバで認証されます。この syslog ソースの場合、[TS エージェント ID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）] の値が表示されます。 • SPAN：ネットワーク情報は SPAN プローブを使用して検出されます。 • DHCP：DHCP イベント。 • エンドポイント（Endpoint） 異なるプロバイダーからの 2 つのイベントがエンドポイントセッションから学習されると、ライブ セッション ページにこれらのプロバイダーがカンマ区切り値として表示されます。
MAC アドレス（MAC Address）	クライアントの MAC アドレスを表示します。
[エンドポイント チェック時刻（Endpoint Check Time）]	エンドポイント プローブによってエンドポイントが最後にチェックされた時刻を表示します。

フィールド	説明
[エンドポイント チェック結果（Endpoint Check Result）]	エンドポイント プローブの結果が表示されます。設定可能な値は次のとおりです。 • 到達不要 • [ユーザ ログアウト（User Logout）] • [アクティブ ユーザ（Active User）]
[送信元ポートの開始（Source Port Start）]	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
[送信元ポートの終了（Source Port End）]	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
[最初の送信元ポート（Source First Port）]	（REST プロバイダーの場合にのみ値が表示されます。）ターミナル サーバ（TS）エージェントにより割り当てられた最初のポートを示します。 ターミナル サーバ（TS）は、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数エンドポイントが LAN ネットワークに接続できるようにするサーバまたはネットワーク デバイスです。複数のエンドポイントに同一 IP アドレスが割り当てられている場合は、特定ユーザの IP アドレスを識別することが困難になります。このため、特定ユーザを識別する目的で TS エージェントがサーバにインストールされ、各ユーザにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザのマッピングが作成されます。
[TS エージェント ID（TS Agent ID）]	（REST プロバイダーの場合にのみ値が表示されます。）エンドポイントにインストールされているターミナル サーバ（TS）エージェントの一意の ID を表示します。
[AD ユーザ解決 ID（AD User Resolved Identities）]	（AD ユーザの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。

フィールド	説明
[AD ユーザ解決 DN（AD User Resolved DNs）]	（AD ユーザの場合にのみ値が表示されます。）AD ユーザの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

関連トピック

RADIUS セッションの許可の変更

Cisco ISE のアクティブな RADIUS セッション

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブ ログ（TACACS Live Logs）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [TACACS ライブ ログ（TACACS Live Logs）]** です。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 *3 : TACACS* ライブ ログ

フィールド	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。

フィールド	使用上のガイドライン
[ユーザ名（Username）]	デバイス管理者のユーザ名を示します。このカラムは必須です。選択解除することはできません。
タイプ（Type）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、またはその両方を通過または失敗したユーザ名を示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（ISE Node）	アクセス要求が処理される ISE ノードの名前を示します。
ネットワークデバイス名（Network Device Name）	ネットワーク デバイスの名前を示します。
ネットワーク デバイス IP（Network Device IP）	アクセス要求を処理するネットワーク デバイスの IP アドレスを示します。
ネットワーク デバイス グループ（Network Device Groups）	ネットワーク デバイスが属する対応するネットワーク デバイス グループの名前を示します。
デバイスタイプ（Device Type）	異なるネットワーク デバイスからのアクセス要求の処理に使用されるデバイス タイプ ポリシーを示します。
参照先	ネットワーク デバイスからのアクセス要求の処理に使用されるロケーション ベースのポリシーを示します。
デバイス ポート（Device Port）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（Failure Reason）	ネットワーク デバイスによって行われたアクセス要求を拒否した理由を示します。
リモート アドレス（Remote Address）	エンドステーションを一意に識別する IP アドレス、MAC アドレス、またはその他の任意の文字列を示します。

フィールド	使用上のガイドライン
一致したコマンドセット（Matched Command Set）	MatchedCommandSet 属性値が存在する場合はその値を示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を示します。
シェルプロファイル（Shell Profile）	ネットワーク デバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACS ライブログ（TACACS Live Logs）] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタム フィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

関連トピック

TACACS+ デバイス管理
TACACS+ のグローバル設定

診断ツール

RADIUS 認証のトラブルシューティングの設定

次の表では、RADIUS 認証の問題を認識し、解決できる [RADIUS 認証のトラブルシューティング（RADIUS authentication troubleshooting）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [RADIUS 認証のトラブルシューティング（RADIUS Authentication Troubleshooting）]** です。

表 *4 : RADIUS* 認証のトラブルシューティングの設定

オプション	使用上のガイドライン
[ユーザ名（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します。
MAC アドレス（MAC Address）	トラブルシューティングするデバイスのMACアドレスを入力します。
監査セッション ID（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。
NAS IP	NAS の IP アドレスを入力します。
NAS ポート（NAS Port）	NAS のポート番号を入力します。
認証状況（Authentication Status）	RADIUS 認証のステータスを選択します。
失敗の理由（Failure Reason）	失敗理由を入力するか、または [選択（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、[クリア（Clear）] をクリックします。
時間範囲（Time Range）	時間範囲を選択します。この時間範囲に作成されたRADIUS認証レコードが使用されます。
開始日時（Start Date-Time）	[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合は、開始日時を入力するか、またはカレンダ 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。
終了日時（End Date-Time）	[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合は、終了日時を入力するか、またはカレンダ 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。
レコード数の取得（Fetch Number of Records）	取得するレコードの数をドロップダウン リストから選択します。10、20、50、100、200、または 500 を選択できます。

関連トピック

予期せぬ RADIUS 認証結果のトラブルシューティング
RADIUS 認証のトラブルシューティング ツール

ネットワーク デバイス コマンドの実行の設定

次の表では、[ネットワークデバイスコマンドの実行（Execute Network Device Command）] ページのフィールドについて説明します。これらのフィールドを使用して、ネットワークデバイス上で **show** コマンドを実行します。このページのナビゲーションパスは、**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[ネットワーク デバイスの実行（Execute Network Device）]** です。

表 *5*：ネットワーク デバイス コマンドの実行の設定

オプション	使用上のガイドライン
情報の入力	
ネットワーク デバイス IP（Network Device IP）	コマンドを実行するネットワーク デバイスの IP アドレスを入力します。
コマンド（Command）	**show** コマンドを入力します。

関連トピック

設定を確認する IOS show コマンドの実行
ネットワーク デバイス ツールの実行

設定バリデータの評価の設定

次の表では、[設定バリデータの評価（Evaluate Configuration Validator）] ページのフィールドについて説明します。これらのフィールドを使用してネットワーク デバイスの設定を評価して、設定の問題を特定します。このページのナビゲーション パスは、**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[設定バリデータの評価（Evaluate Configuration Validator）]** です。

表 *6*：設定バリデータの評価の設定

オプション	使用上のガイドライン
情報の入力	
ネットワーク デバイス IP（Network Device IP）	設定を評価するネットワーク デバイスの IP 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	このオプションは、デフォルトで選択されます。
RADIUS	このオプションは、デフォルトで選択されます。

オプション	使用上のガイドライン
デバイス検出（Device Discovery）	このオプションは、デフォルトで選択されます。
ログ	このオプションは、デフォルトで選択されます。
Web 認証（Web Authentication）	Web 認証の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。
プロファイラ設定（Profiler Configuration）	プロファイラの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。
TrustSec	TrustSec 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。使用可能ないずれかのオプションを選択します。

関連トピック

ネットワーク デバイス設定の問題のトラブルシューティング
設定バリデータ ツールの評価

ポスチャのトラブルシューティングの設定

次の表では、ネットワーク内のポスチャ問題の検出と解決に使用する [ポスチャのトラブルシューティング（Posture troubleshooting）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]** です。

表 *7:* ポスチャのトラブルシューティングの設定

オプション	使用上のガイドライン
トラブルシューティングが必要なポスチャ イベントの検索と選択	
[ユーザ名（Username）]	フィルタリング基準として使用するユーザ名を入力します。
MAC アドレス（MAC Address）	フィルタリング基準として使用する MAC アドレスを、xx-xx-xx-xx-xx-xx 形式で入力します。
ポスチャ ステータス（Posture Status）	フィルタリング基準として使用する認証ステータスを選択します。

オプション	使用上のガイドライン
失敗の理由（Failure Reason）	失敗理由を入力するか、または [選択（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、[クリア（Clear）] をクリックします。
時間範囲（Time Range）	時間範囲を選択します。この時間範囲に作成された RADIUS 認証レコードが使用されます。
開始日時：（Start Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）開始日時を入力するか、またはカレンダ 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。
終了日時：（End Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）終了日時を入力するか、またはカレンダ 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。
レコード数の取得（Fetch Number of Records）	表示するレコードの数を選択します。10、20、50、100、200、または 500 を選択できます。
検索結果	
時刻（Time）	イベントの時刻
ステータス（Status）	ポスチャ ステータス
[ユーザ名（Username）]	イベントに関連付けられたユーザ名
MAC アドレス（MAC Address）	システムの MAC アドレス
失敗の理由（Failure Reason）	イベントの障害理由

関連トピック

エンドポイント ポスチャの障害のトラブルシューティング
ポスチャのトラブルシューティング ツール

TCP ダンプの設定

次の表では、ネットワーク インターフェイスのパケットの内容をモニタし、ネットワークで問題が発生したときにはトラブルシューティングするために使用する **tcpdump** ユーティリティ ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作**

（**Operations**）] > [トラブルシューティング（**Troubleshoot**）] > [診断ツール（**Diagnostic Tools**）] > [一般ツール（**General Tools**）] > [TCP ダンプ（**TCP Dump**）] です。

表 *8 : TCP* ダンプの設定

オプション	使用上のガイドライン
ステータス（Status）	• [停止済み（Stopped）] : tcpdump ユーティリティは実行されていません。 • [開始（Start）] : tcpdump ユーティリティによるネットワークのモニタリングを開始する場合にクリックします。 • [停止（Stop）] : tcpdump ユーティリティを停止する場合にクリックします。
ホスト名（Host Name）	モニタするホストの名前をドロップダウン リストから選択します。
ネットワーク インターフェイス（Network Interface）	モニタするネットワーク インターフェイスの名前をドロップダウンリストから選択します。 （注） IPv4 アドレスまたは IPv6 アドレスを持つすべてのネットワーク インターフェイス カード（NIC）を Cisco ISE 管理者ポータルに表示されるように設定する必要があります。
無差別モード（Promiscuous Mode）	• [オン（On）] : 無差別モードを有効にする場合にクリックします（デフォルト）。 • [オフ（Off）] : 無差別モードを無効にする場合にクリックします。 無差別モードがデフォルトのパケット スニッフィング モードです。有効に設定しておくことを推奨します。このモードでは、ネットワーク インターフェイスはすべてのトラフィックをシステムの CPU に渡します。
フィルタ	フィルタリング基準として使用するブール式を入力します。サポートされている標準 tcpdump フィルタ式 : ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123

オプション	使用上のガイドライン
フォーマット（Format）	tcpdump ファイルのフォーマットを選択します。

ダンプ ファイル（Dump File）	最後のダンプ ファイルに記録された、次のようなデータを表示します。
	Last created on Wed Apr 27 20:42:38 UTC 2011 by admin
	`File size: 3,744 bytes`
	`Format: Raw Packet Data`
	`Host Name: Positron`
	`Network Interface: GigabitEthernet 0`
	`Promiscuous Mode: On`
	• [ダウンロード（Download）]：最新のダンプ ファイルをダウンロードする場合にクリックします。
	• [削除（Delete）]：最新のダンプ ファイルを削除する場合にクリックします。

関連トピック

ネットワーク トラフィックのモニタリングでの TCP ダンプの使用
TCP ダンプ ファイルの保存
着信トラフィックを検証する TCP ダンプ ユーティリティ

SXP-IP マッピング

次の表では、デバイスとそのピア間のマッピングを比較するために使用する [SXP-IP マッピング（SXP-IP mappings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（Trustsec Tools）] > [SXP-IP マッピング（SXP-IP mappings）]** です。

ピア SXP デバイス

表 9：SXP-IP マッピングのピア SXP デバイス

オプション	使用上のガイドライン
ピア SXP デバイス（Peer SXP Devices）	
ピア IP アドレス（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。

オプション	使用上のガイドライン
ピア SXP モード（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。
セルフ 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。
接続状態（Connection State）	接続のステータス。
共通接続パラメータ（Common Connection Parameters）	
ユーザ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。 （注） 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。
[ユーザ名（Username）]	ピア SXP デバイスのユーザ名を入力します。
[パスワード（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。
プロトコル	• プロトコルを選択します。 （注） [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 接続を有効にする必要があります。
[ポート（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。
パスワードを有効にする（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。
ログイン パスワードと同じ（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。

関連トピック

SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

SXP のサポート

IP ユーザ SGT

次の表では、[IP ユーザ SGT（IP User SGT）] ページのフィールドについて説明します。これらのフィールドを使用して、デバイス上の IP-SGT 値を ISE が割り当てた SGT と比較します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（TrustSec Tools）] > [IP ユーザ SGT（IP User SGT）]** です。

表 *10 : IP* ユーザ *SGT*

オプション	使用上のガイドライン
情報の入力	
ネットワーク デバイス IP（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。
結果のフィルタリング	
[ユーザ名（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。
ユーザ IP アドレス（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。

関連トピック

IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

セキュリティ グループの設定

デバイス SGT の設定

次の表に、デバイス SGT を、割り当てられた最新の SGT 値と比較するために使用する [デバイス SGT（Device SGT）] ページのフィールドを示します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（Trustsec Tools）] > [デバイス SGT（Device SGT）]** です。

表 *11*：デバイス *SGT* の設定

オプション	使用上のガイドライン
情報の入力	
ネットワーク デバイス IP（Network Device IPs）（カンマ区切りのリスト）	ISE 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 SGT のネットワーク デバイス IP アドレスをカンマで区切って入力します。
共通接続パラメータ（Common Connection Parameters）	
共通接続パラメータを使用（Use Common Connection Parameters）	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。 • [ユーザ名（Username）]：ネットワーク デバイスのユーザ名を入力します。 • [パスワード（Password）]：パスワードを入力します。 • [プロトコル（Protocol）]：プロトコルを選択します。 （注） [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 接続を有効にする必要があります。 • [ポート（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。
パスワードを有効にする（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。
ログイン パスワードと同じ（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。

関連トピック

デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング

デバイス SGT ツール

進行状況の詳細の設定

次の表では、いずれかの診断ツールの [ユーザ入力必須（User Input Required）] ボタンをクリックすると表示される [進行状況詳細（Progress Details）] ページのフィールドについて説明します。このページには、詳細なトラブルシューティング情報が表示されます。このページへのナビゲーション パスは、**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[任意の診断ツール（Any Diagnostic Tool）]** です。

表 *12 :* 進行状況の詳細の設定

オプション	使用上のガイドライン
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	
[ユーザ名（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。
[パスワード（Password）]	パスワードを入力します。
プロトコル	プロトコルを選択します。 （注） [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 接続を有効にする必要があります。
[ポート（Port）]	ポート番号を入力します。
パスワードを有効にする（Enable Password）	イネーブル パスワードを入力します。
ログイン パスワードと同じ（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。
コンソール サーバを使用（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。
コンソール IP アドレス（Console IP Address）	（[コンソール サーバを使用（Use Console Server）] チェックボックスをオンにした場合）コンソールの IP アドレスを入力します。
高度なオプション（「タイムアウトエラー（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） （注） 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。	

オプション	使用上のガイドライン
ユーザ名用文字列（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。
パスワード用文字列（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。
プロンプト用文字列（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。
認証失敗用文字列（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。

関連トピック

- 予期せぬ RADIUS 認証結果のトラブルシューティング
- 設定を確認する IOS show コマンドの実行
- ネットワーク デバイス設定の問題のトラブルシューティング
- SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング
- IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング
- 診断トラブルシューティング ツール

結果概要（Results Summary）

次の表では、診断ツールを使用したときに結果として表示される結果概要ページのフィールドについて説明します。

表 13:[RADIUS 認証のトラブルシューティング（RADIUS Authentication Troubleshooting）]：[結果概要（Results Summary）]

オプション	使用上のガイドライン
診断と解決策（Diagnosis and Resolution）	
診断（Diagnosis）	問題の診断がここに表示されます。
解像度	問題の解決手順がここに詳細に表示されます。
トラブルシューティングの概要（Troubleshooting Summary）	

オプション	使用上のガイドライン
要約	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。

関連トピック

予期せぬ RADIUS 認証結果のトラブルシューティング

RADIUS 認証のトラブルシューティング ツール