操作のユーザ インターフェイス リファレンス

この章は、Cisco Identity Services Engine（ISE）で提供されるユーザ インターフェイス要素のリファレンスで、次の機能の設定が含まれます。

最近の RADIUS 認証

次の表に、最近の RADIUS 認証を表示する [認証（Authentications）] 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）] > [認証（Authentications）] > [ライブ認証（Live Authentications）] です。

表 C-1　　ライブ認証

オプション	使用上のガイドライン
設定が誤っているサプリカント（Misconfigured Supplicants）	直近の 24 時間で設定が誤っているサプリカントが検出された回数を示します。
設定が誤っているネットワーク デバイス（Misconfigured Network Devices）	直近の 24 時間で設定が誤っているネットワーク デバイスが検出された回数を示します。
RADIUS ドロップ（RADIUS Drops）	直近の 24 時間で RADIUS 要求がドロップされた回数を示します。 **（注）** このオプションが表示するドロップされた RADIUS 要求には、RADIUS アカウンティング要求に対応するドロップ カウントは含まれていません。RADIUS アカウンティング要求に対応する詳細は、RADIUS エラー レポートで表示できます。RADIUS エラー レポートの詳細については、「使用可能なレポート」（P.26-7）を参照してください。
クライアントが停止した応答（Client Stopped Responding）	直近の 24 時間でクライアントが応答を停止した回数を示します。
リピート カウンタ（Repeat Counter）	ID、ネットワーク デバイス、および許可のコンテキストが変更されずに、直近の 24 時間で認証要求が繰り返された回数を示します。
時間（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。選択解除はできません。

表 C-1　ライブ認証 （続き）

オプション	使用上のガイドライン
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。選択解除はできません。
ユーザ名（Username）	認証に関連付けられたユーザ名を表示します。
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。
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が表示されます。
許可プロファイル（Authorization Profiles）	認証に使用された許可プロファイルを表示します。
ID グループ（Identity group）	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。
イベント（Event）	イベント ステータスが表示されます。
障害理由（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。
サーバ（Server）	ログ生成のもとになったポリシー サービスが表示されます。
セッション ID（Session ID）	セッション ID を示します

関連項目

「ライブ認証のモニタリング」（P.25-13）

ライブ セッションの表示

次の表に、ライブ認証セッションを表示するライブ セッション 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）] > [認証（Authentications）] > [ライブ セッションの表示（Show Live Sessions）] です。

表 C-2　ライブ セッション

フィールド	説明
リセット リピート カウント（Reset Repeat Counts）	すべてのエンドポイントに対して再試行オプションをリセットする場合にクリックします。
開始時（Initiated）	認証セッションが開始されたときのタイムスタンプを表示します。
更新時（Updated）	CoA アクションなどの変更のため、セッションが最後に更新されたときのタイム スタンプを表示します。
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。
CoA アクション（CoA Action）	アクティブな RADIUS セッションの許可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合にこれを使用します。
リピート カウント（repeat count）	セッションが再試行された回数を表示します。
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	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。
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。
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（Server）	ログ生成のもとになったポリシー サービスが表示されます。
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。
NAS IP アドレス（NAS IP Address）	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。

ライブ認証の詳細（Live Authentication Details）

次の表に、ライブ認証の詳細ドリル ダウン 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）] > [認証（Authentications）] > [ライブ認証（Live Authentications）] > [詳細アイコン（Details Icon）] です。このページには、セッション エントリと成功した認証エントリ間のリンクを説明するテキストも表示されます。

表 C-3　ライブ認証のドリル ダウン

フィールド	説明
イベント（Event）	成功した認証イベントの数を表示します。
ユーザ名（Username）	認証に関連付けられたユーザ名を表示します。
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）	デバイスのエンドポイント プロファイルを表示します。
許可プロファイル（Authorization Profiles）	認証に使用された許可プロファイルを表示します。
AuthorizationPolicyMatchedRule	認証に使用される認可ポリシー ルールを表示します。
ISEPollicySetName	ISE ポリシー セットの名前を表示します。
IdentitySelectionMatchedRule	認証に使用される ID 選択ルールを表示します。
ソース タイムスタンプ（Source Timestamp）	ソースのタイム スタンプを表示します。
受信タイムスタンプ（Recieved Timestamp）	許可イベントが受信された時間を表示します。
ポリシー サーバ（Policy Server）	ポリシー サーバ名を表示します。
障害理由（Failure Reason）	認証失敗の理由を表示します。

診断ツール

ここでは、次の内容について説明します。

- 「デバイス SGT の設定」（P.C-10）
- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）

RADIUS 認証トラブルシューティングの設定

次の表に、RADIUS 認証の問題を識別し、解決できるようにする RADIUS 認証トラブルシューティング 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 認証トラブルシューティング（RADIUS Authentication Troubleshooting）] です。

表 C-4　RADIUS 認証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。
障害理由（Failure Reason）	障害理由を入力するか、または [選択（Select）] をクリックしてリストから障害理由を選択します。障害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。この期間に作成された 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、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、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。
取得レコード数（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。

関連項目

「予期しない RADIUS 認証の結果のトラブルシューティング」（P.25-18）

ネットワーク デバイス コマンドの実行の設定

次の表に、ネットワーク デバイス上で **show** コマンドを実行するために使用する [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）] > [ネットワーク デバイス コマンドの実行（Execute Network Device Command）] です。

表 C-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。

関連項目

「設定を確認するための IOS Show コマンドの実行」（P.25-19）

設定評価バリデータの設定

次の表に、ネットワーク デバイスの設定を評価し、設定問題を識別する [設定評価バリデータ（Evaluate Configuration Validator）] 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）] > [設定評価バリデータ（Evaluate Configuration Validator）] です。

表 C-6　設定評価バリデータの設定

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。
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（Logging）	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	セキュリティ グループ アクセス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、使用可能ないずれかのオプションを選択します。

関連項目

「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」（P.25-20）

ポスチャのトラブルシューティングの設定

次の表に、ネットワーク上のポスチャ問題を見つけて解決するために使用するポスチャのトラブルシューティング 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 C-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。
障害理由（Failure Reason）	障害理由を入力するか、または [選択（Select）] をクリックしてリストから障害理由を選択します。障害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。この期間に作成された 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。
取得レコード数（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	
時間（Time）	イベントの日時。
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
障害理由（Failure Reason）	イベントの障害理由

関連項目

「エンドポイントのポスチャ障害のトラブルシューティング」（P.25-21）

TCP ダンプ設定

次の表に、ネットワーク インターフェイス上のパケットの内容をモニタし、ネットワーク上で発生した問題を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 C-8　TCP ダンプ設定

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。 **（注）** インライン ポスチャ ノードは、サポートされていません。
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）** Cisco ISE 管理者ポータルに表示されるように、IPv4 または IPv6 アドレスですべてのネットワーク インターフェイス カード (NICs) を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 に渡しています。
フィルタ（Filter）	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。標準の tcpdump フィルタ式がサポートされます。
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。

関連項目

「TCP ダンプを使用したネットワーク トラフィックのモニタリング」（P.25-22）

SXP-IP マッピング（SXP-IP Mappings）

次の表に、デバイスと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 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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [SXP-IP マッピング（SXP-IP Mappings）] です。

ピア SXP デバイス

表 C-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。
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	
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（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 接続をイネーブル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。
イネーブル パスワード（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。

関連項目

「SXP-IP マッピングを使用した SGA 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」（P.25-24）

IP User SGT

次の表に、デバイスの IP-SGT 値を ISE によって割り当てられた SGT と比較するために使用する [IP User SGT] 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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [IP User SGT] です。

表 C-10　IP User 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。
フィルタ結果	
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。

関連項目

「IP-SGT マッピングを使用した SGA 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」（P.25-24）

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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [デバイス SGT（Device SGT）] です。

表 C-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	

表 C-11　デバイス SGT の設定 （続き）

オプション	使用上のガイドライン
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 接続をイネーブル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。
イネーブル パスワード（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。

関連項目

「デバイスの SGT マッピングの比較による SGA 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」（P.25-25）

進捗詳細の設定

次の表に、すべての診断ツールの [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 [進捗詳細（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）] > [すべての診断ツール（Any Diagnostic Tool）] です。

表 C-12　進捗詳細の設定

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（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 接続をイネーブル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。
イネーブル パスワード（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。

表 C-12　進捗詳細の設定 （続き）

オプション	使用上のガイドライン
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。	
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。

結果概要（Results Summary）

次の表に、診断ツールを使用する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 C-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。
解決策（Resolution）	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概要（Troubleshooting Summary）	
< *概要*>（<*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。