

Soliton Net'Attest EPS Ver3.6.2 の設定例

エスアイアイ・ネットワーク・システムズ株式会社

Soliton Net'Attest EPS Ver3.6.2 の設定例を以下に記載します。

この設定例は参考情報としてお取り扱いください。

Net'Attest EPS のインストール方法や設定の詳細は、製品ドキュメントをご参照ください。

なお、SmartCS NS-2240 シリーズの設定例は取扱説明書「4.8 章 設定事例」に記載しております。そちらもあわせてご参照ください。

■ RADIUS サーバー情報

Net'Attest EPS は以下で動作します。

製品形態	アプライアンス製品 (BOX 型)
設定方法	HTTPS
Auth ポート番号	UDP 1812 (デフォルト) 変更可
Acct ポート番号	UDP 1813 (デフォルト) 変更可

■ クライアントの登録方法

・ RADIUS サーバー基本設定

「RADIUS 認証サーバー設定」の「基本設定」で、認証ポートと EAP 認証ポートタイプを設定します。認証ポートは SmartCS NS-2240 シリーズに設定した認証ポートにあわせて設定します。EAP 認証タイプは工場出荷値の TTLS/MD5 のままで結構です。

Soliton Net'Attest EPS - Microsoft Internet Explorer

アドレス https://105.31.229.2181/admin/top.cgi

Net'Attest EPS Soliton

eps.local

RADIUS RADIUSサーバー 基本設定

認証ポート
※ポート番号を変更した場合、RADIUSサービスの再起動が行われます。

ログにパスワードを表示する (PAP 認証のみ)

EAP 認証タイプ

優先順位	認証タイプ
1	TTLS
2	MD5
3	----
4	----
5	----

EAP-TLS/TTLS/PEAP 設定

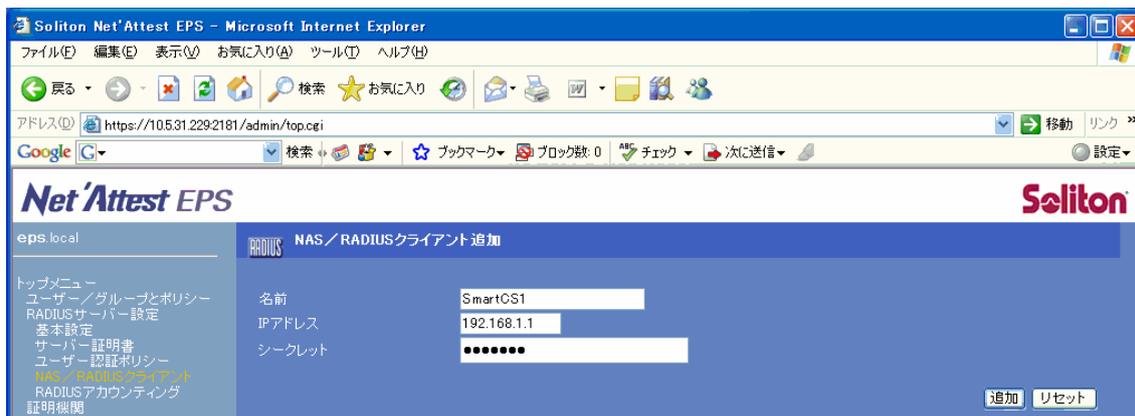
メッセージフラグメントサイズ バイト

メッセージの長さ情報、フラグメントされた

設定 リセット

- ・クライアント(SmartCS NS-2240 シリーズ)とシークレットキーの登録

「RADIUS サーバー設定」の「NAS/RADIUS クライアント」で、クライアントの情報を登録します。このページで SmartCS NS-2240 シリーズのホスト名と IP アドレス、シークレットキーを登録します。シークレットキーは SmartCS NS-2240 シリーズに登録したキーと同じものを設定します。

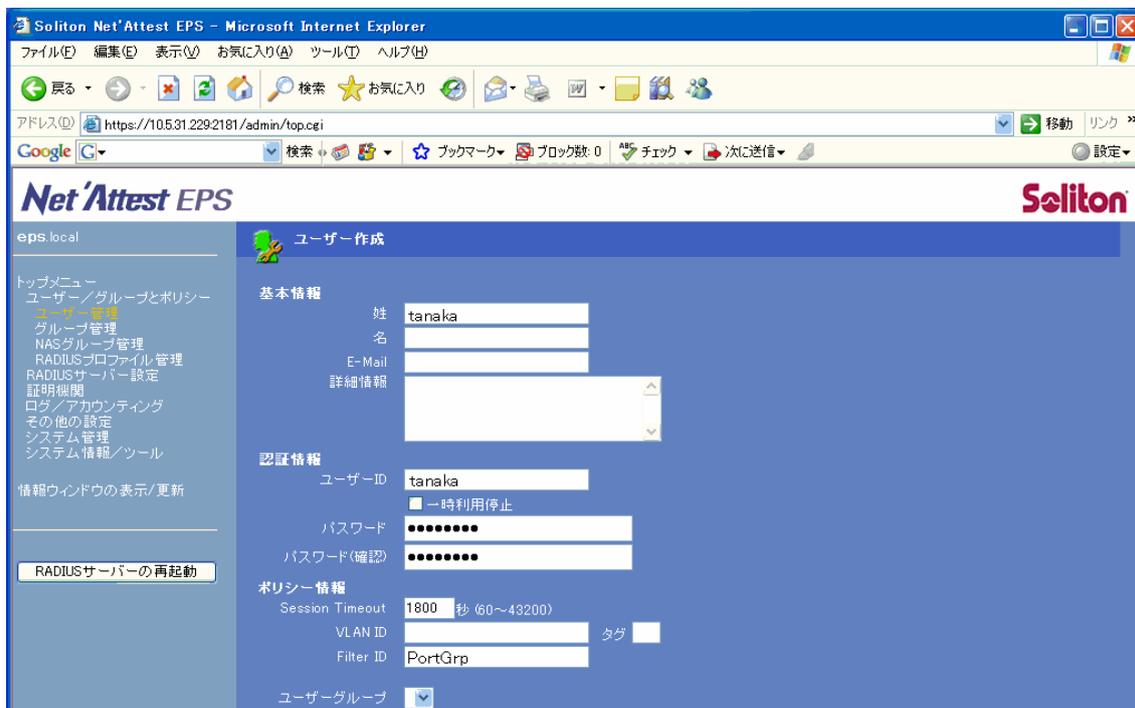


■ 認証ユーザーの登録方法

- ・ユーザーの登録

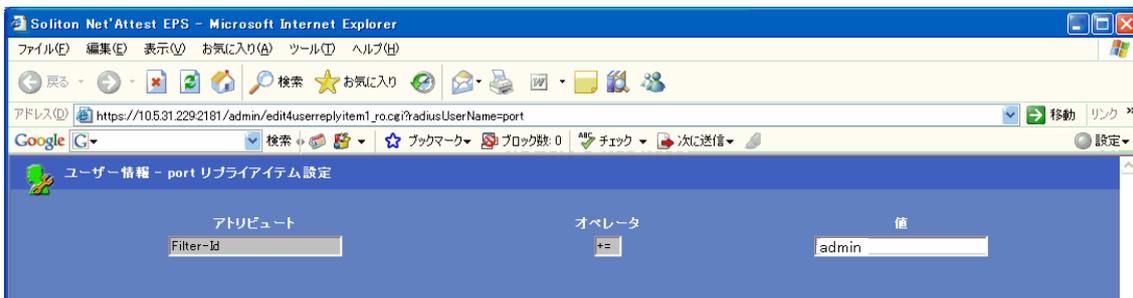
ユーザー情報を Net'Attest EPS に登録します。「ユーザー/グループとポリシー」の「ユーザー管理」で認証するユーザーを登録します。

下記はアクセスグルーピング機能利用時のポートユーザーの登録例です。



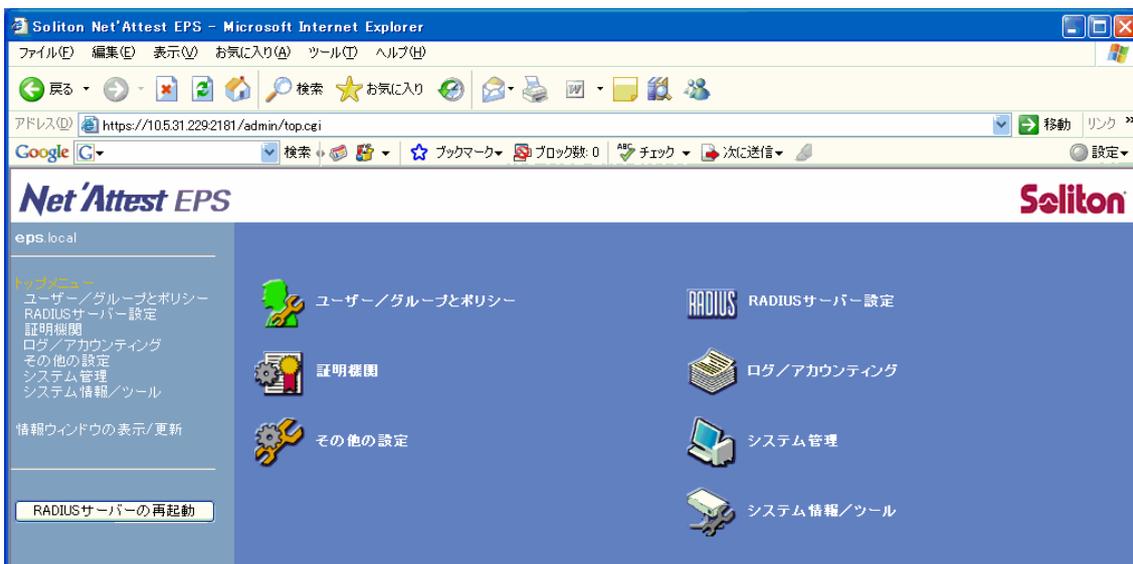
- ・ 複数 Filter-Id アトリビュートの登録

複数の Filter-Id アトリビュートを登録する場合は、「ユーザー情報」の「リプライアイテム設定」で Filter-Id アトリビュートを羅列します。Filter-Id を追加する場合、オペレータは”+=”です。



- 設定の反映

登録したクライアントやユーザーを反映させるには画面左側の「RADIUS サーバーの再起動」を押下して、Net'Attest EPS を再起動させます。



- 注意

- ・ SmartCS NS-2240 シリーズには Net'Attest EPS のコンソールポートを接続しないでください。Net'Attest EPS のコンソールポートは常時接続することを推奨しておりません。

■ 補足情報

- ・アクセスログの保管場所

アカウントログは「トップメニュー」の「ログ/アカウントティング」に保存されます。
アクセスログを確認する場合は上記メニューを参照してください。

- ・トラブルシューティング

SmartCS NS-2240 シリーズで **trace radius level 2** コマンドを実行すると、トラブルシューティングに有用な情報を収集することもできます。
このコマンドの詳細は取扱説明書ならびにコマンドリファレンスを参照してください。

以上