The Guaranteed Network

いちばん近くで、もっと先へ。

SECUREMATRIX®とAXシリーズによる認証連携 評価報告書

2013年7月19日

アラクサラネットワークス株式会社
ネットワークテクニカルサポート

資料No. NTS-13-R-007 Rev. 0

The Guaranteed Network

AlaxalA

はじめに

■ 注意事項

本資料に記載の内容は、弊社が特定の環境において、基本動作や接続動作を確認したものであり、すべての環境で機能・性能・信頼性を保証するものではありません。

■ 輸出時の注意

AXシリーズに関し、本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをおとりください。なお、不明な場合は、弊社担当営業にお問い合わせ下さい。

■ 商標一覧

・アラクサラの名称及びロゴマークは、アラクサラネットワークス株式会社の商標及び登録商標です。

・ SECUREMATRIX及びマトリクス認証は、株式会社シー・エス・イーの登録商標です。

・そのほかの記載の会社名，製品名は、それぞれの会社の商標もしくは登録商標です。

■ 関連資料

・AXシリーズ 製品マニュアル
(http://www.alaxala.com/jp/techinfo/manual/index.html)

・AXシリーズ認証ソリューションガイド
(http://www.alaxala.com/jp/techinfo/guide/index.html#01)

・ SECUREMATRIX®について
(http://www.cseltd.co.jp/smx/)

目次

1. SECUREMATRIXとAXシリーズの連携概要

1.1 概要

■SECUREMATRIXとAXシリーズの認証連携の特徴

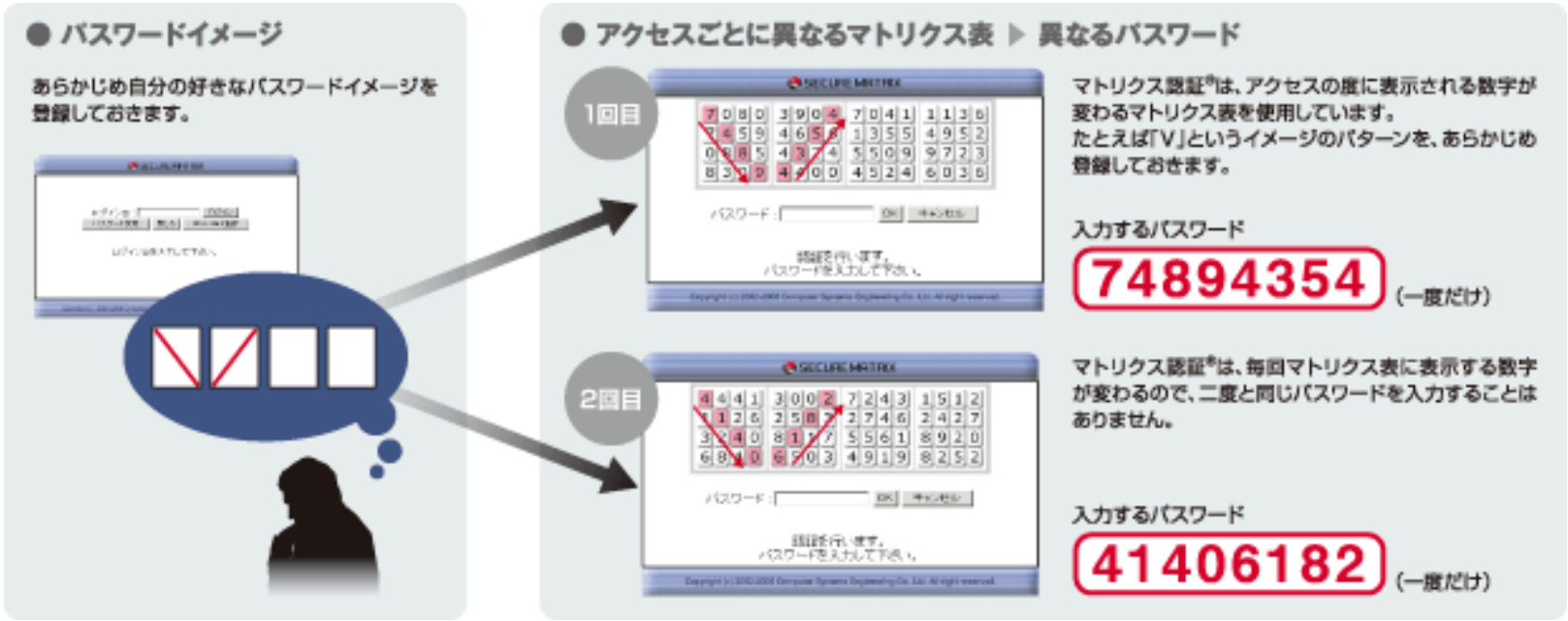
1. SECUREMATRIXのワンタイムパスワードと、AXシリーズのWeb認証を使ってセキュリティの高いユーザ認証を行うことが可能です。
2. AXシリーズのダイナミックVLAN、ダイナミックACL機能と連携可能です。

■評価試験結果

SECUREMATRIXのワンタイムパスワードと、AXシリーズのWeb認証との連携評価を実施して、問題なく動作する事を確認しました。

1.2　SECUREMATRIXの概要

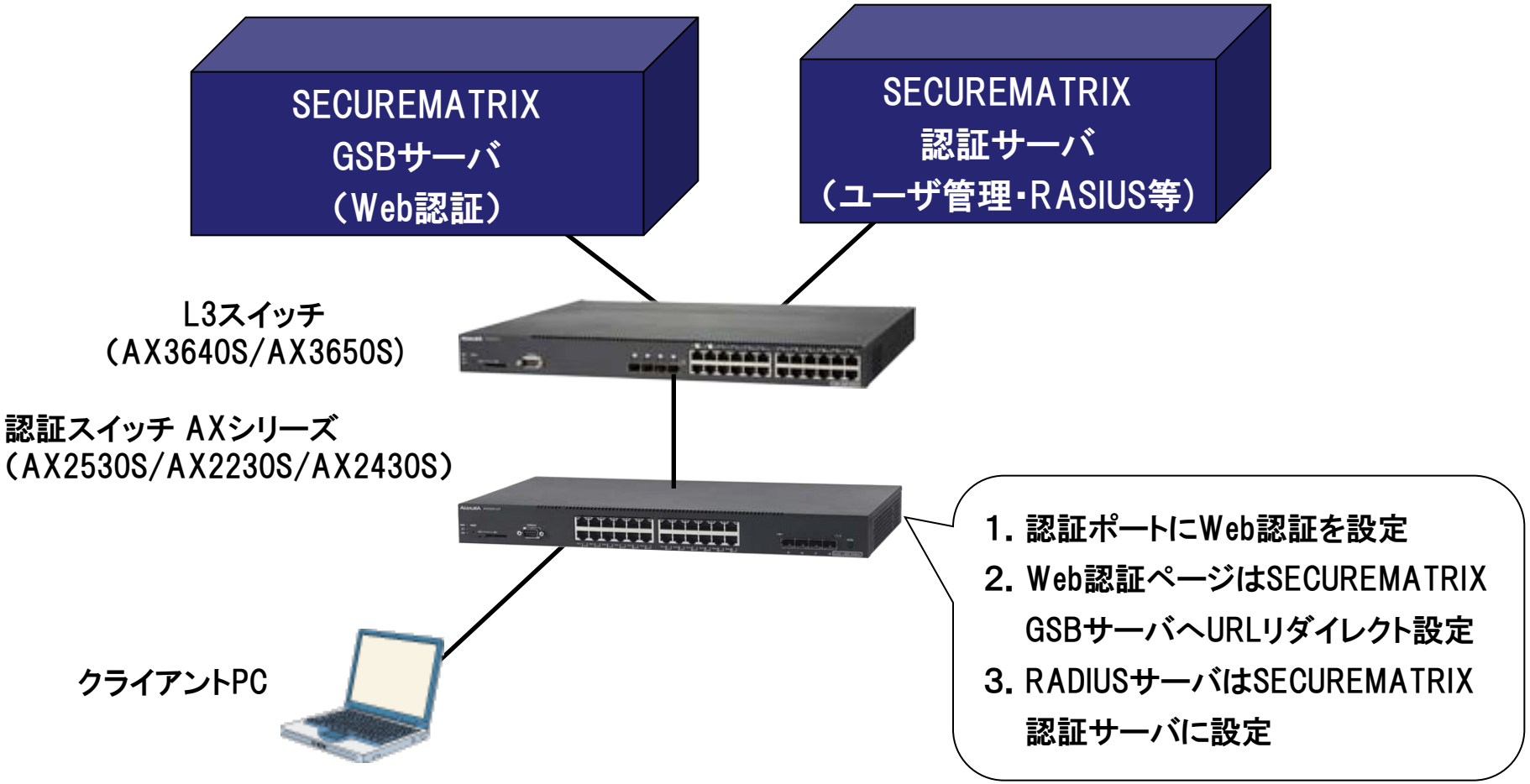
「SECUREMATRIX」はワンタイムパスワードシステムです。



SECUREMATRIXは、64個の数字が並ぶマトリクス表からユーザが決めた位置と順番を選んだ形がパスワードになります。認証のたびにランダムな数字が表示されるマトリクス表にパスワードとなる形を頭の中で重ね、合わさった箇所の数字をパスワード欄に入力することで認証が完了します。この認証方式を「マトリクス認証」方式と言います。マトリクス表の数字が毎回ランダムに表示されることでワンタイムパスワードを実現しています。

2. SECUREMATRIXとAXシリーズの連携評価

2.1 評価構成



SECUREMATRIXのワンタイムパスワードとAXシリーズのWeb認証との連携評価を実施する。

2.2 試験の設定条件

(1)「SECUREMATRIX」の設定条件

・RADIUSクライアントとしてAXシリーズを登録する
・RADIUSの設定のSSL-VPNシングルサインオン設定でAXシリーズのWeb認証方法を設定する。
・ダイナミックVLAN/ダイナミックACL確認のため、RADIUS設定でアトリビュートを設定する。

(2)認証スイッチ「AXシリーズ」の設定条件

・ クライアントPCを接続する認証ポートは、Web認証ポートに設定する。
（固定VLAN、ダイナミックVLAN、ダイナミックACLを設定）
・ Web認証のRADIUSサーバの設定として「SECUREMATRIX 認証サーバ」の IPアドレスと認証キーを設定する。

・Web認証ページを「SECUREMATRIX GSBサーバ」へURLリダイレクトができるように設定する。
AX2500Sはコンフィグにて設定して、その他機種は認証画面入替え機能を使用して、
「SECUREMATRIX GSBサーバ」へリダイレクトする。
（リダイレクト先のURLはRADIUSクライアント登録のシングルサインオン指定でアクセスパス指定による）
・認証専用アクセスリストに「SECUREMATRIX GSBサーバ」への通信を許可する。

※ 設定の詳細は3章を参照

2.3 評価項目と使用機器

(1)評価項目

◆ SECUREMATRIXとAXシリーズのWeb認証が連携できること
- 認証前のユーザのSECUREMATRIX GSBサーバへのURLリダイレクトできること
- マトリクス認証成功時にAXシリーズのWeb認証が成功し通信許可できること

◆ ユーザごとのダイナミックVLANの指定が可能であること

◆ ユーザごとのダイナミックACL(Filter-ID)の指定が可能であること

(2)使用機器・ソフトウェア

- SECUREMATRIX ® : Version 3.6.1.a
- 認証スイッチ
  - AX1240S/AX2230S : Ver2.4A
  - AX2530S : Ver3.5
  - AX2430S : 11.7F
  - AX3640S/AX3650S : 11.11A
- クライアントPC : Windows 7 SP1 Enterprise
- ブラウザ : Internet Explorer 9
- Java : JRE 1.7.0_25

2. 4 評価結果

以下に、SECUREMATRIXのワンタイムパスワードとAXシリーズの連携評価の結果を示します。

SECUREMATRIX： Version 3.6.1.a

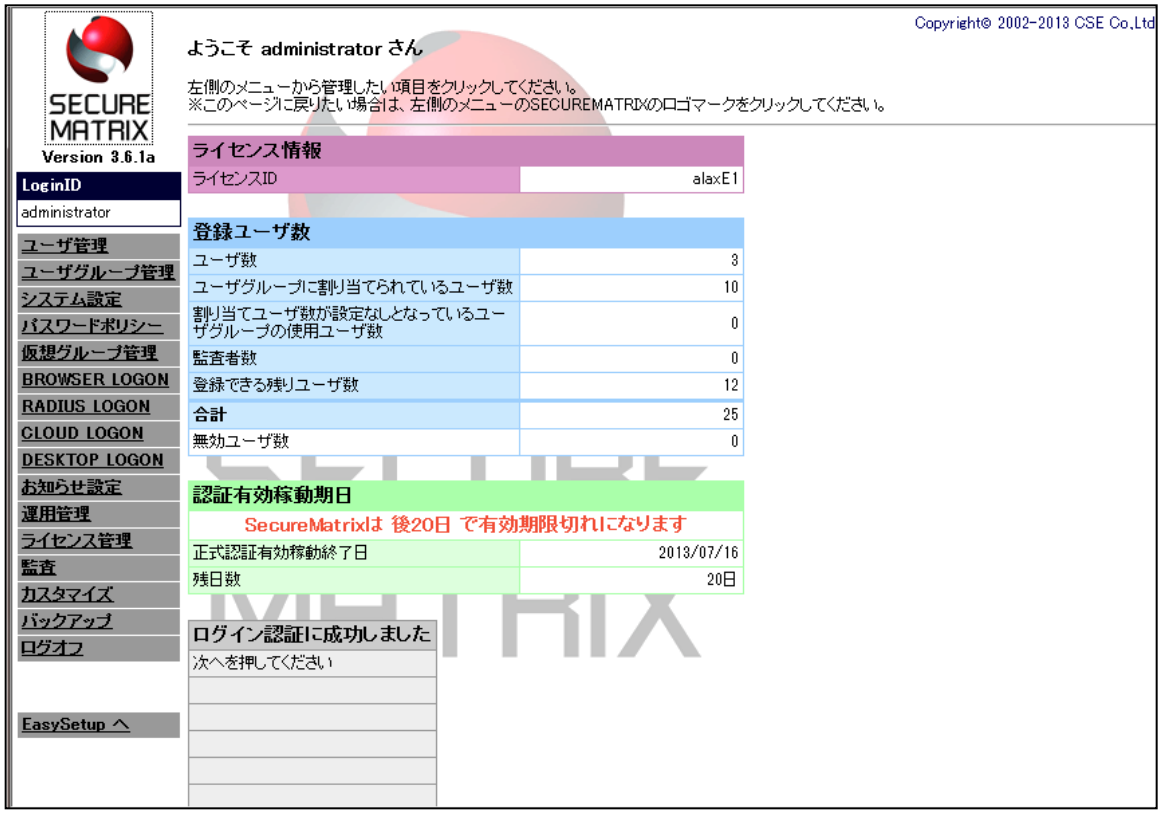
対象機器	機器バージョン	Web認証連携（固定VLAN）	アトリビュート確認ダイナミックVLAN	アトリビュート確認ダイナミックACL
AX2400S	11.7F	○	○	―
AX3600S	11.11A	○	○	―
AX1200S	2.4A	○	○	―
AX2200S	2.4A	○	○	―
AX2500S	3.5	○	○	○

○ ：連携OK

― ：機能未サポート

3.1 SECUREMATRIXの設定

AXシリーズと接続する場合まずRADIUSクライアントとして機器を登録します。



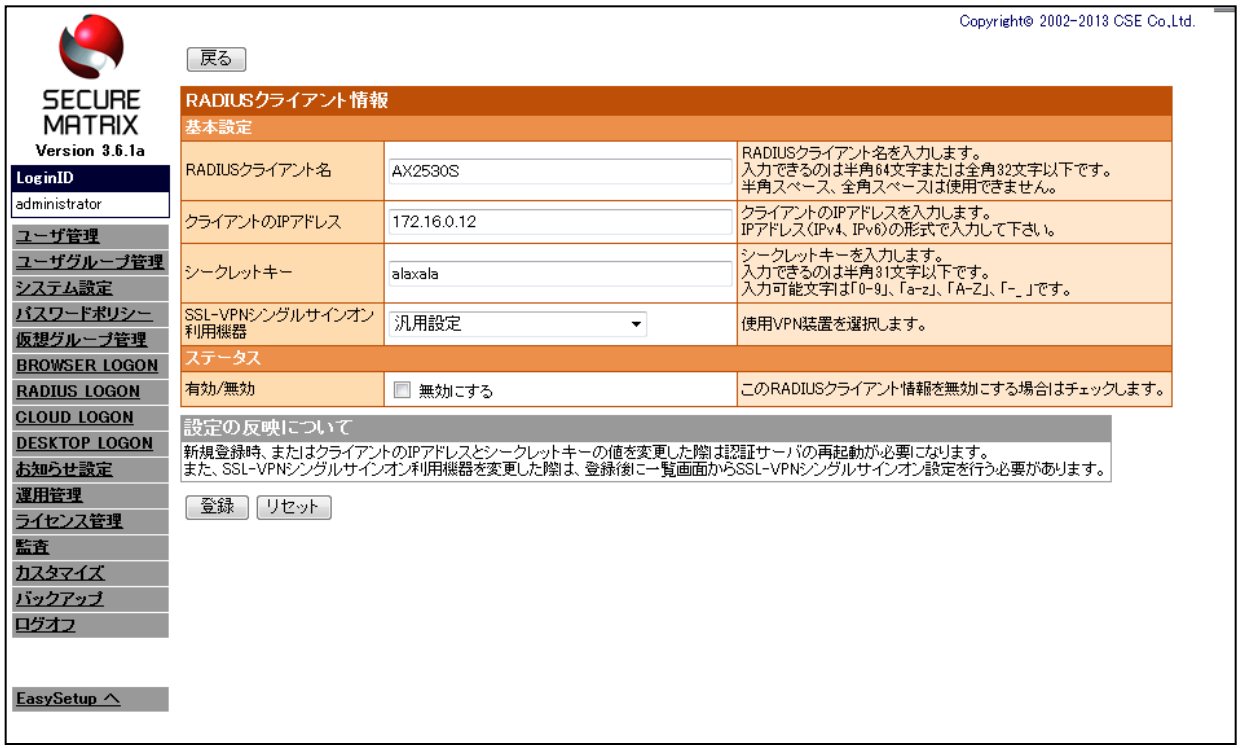
上記画面はSECUREMATRIX認証サーバのTOP画面です。
管理者でログインして「RADIUS LOGON」を開きRADIUSクライアントを登録します。

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ RADIUSクライアントの登録

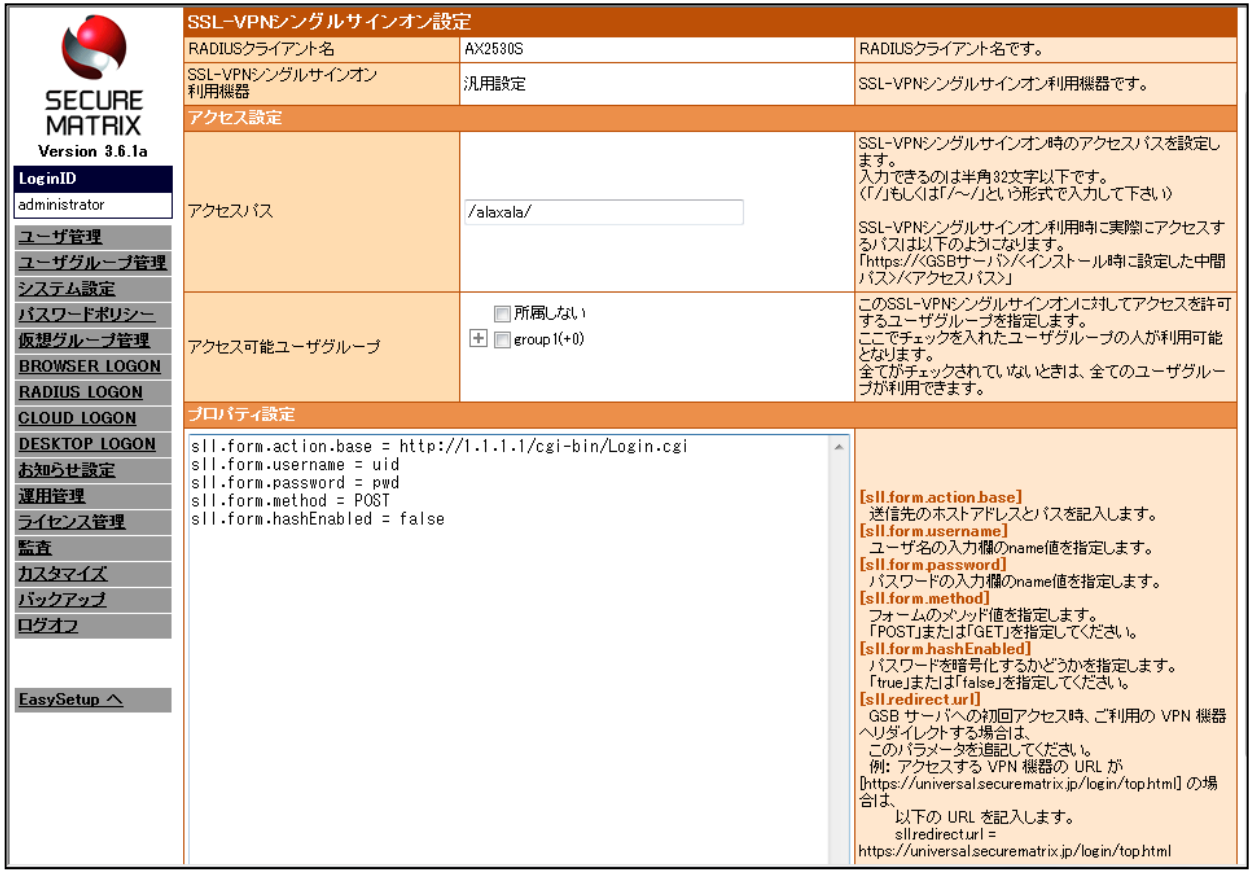
① AXシリーズの連携設定は、RADIUSクライアント新規登録ボタンより機器を登録します。
② RADIUSクライアント登録後、SSL-VPNシングルサインオン設定から、認証スイッチとの認証連携の設定を行います。
③ ダイナミックACL/ダイナミックVLAN等を使用する場合には、アトリビュートを追加します。

◆ RADIUSクライアント新規登録



① RADIUSクライアント名を入力。
② クライアントのIPアドレスを入力します。
（AXシリーズのRADIUSサーバへの送信元となるIPアドレスを指定します。）
③ RADIUS認証用のシークレットキーを入力します。
④ SSL-VPNシングルサインオン利用機器の設定を「汎用設定」とします。
⑤ ステータスが無効になっていないことを確認して登録ボタンをおします。

◆ SSL-VPNシングルサインオン設定



各項目の説明は次ページへ

◆ SSL-VPNシングルサインオン設定項目

① アクセスパスを設定します

本項目は任意の文字列を指定します。本例では/alaxala/としています。
認証スイッチ毎にユニークになるように設定してください。
/alaxala/と設定した認証のアクセスパスは場合以下となります。
「https://SECUREMATRIX GSBサーバ名/インストール時に設定した中間パス/alaxala/」
AXシリーズにWeb認証ページを上記サーバのパスへURLリダイレクトするように設定してください。

（SSLを使用する場合は、エラーとならないように、WebサーバのSSLサーバ証明書とサーバ名称が一致するように注意して構築してください。）

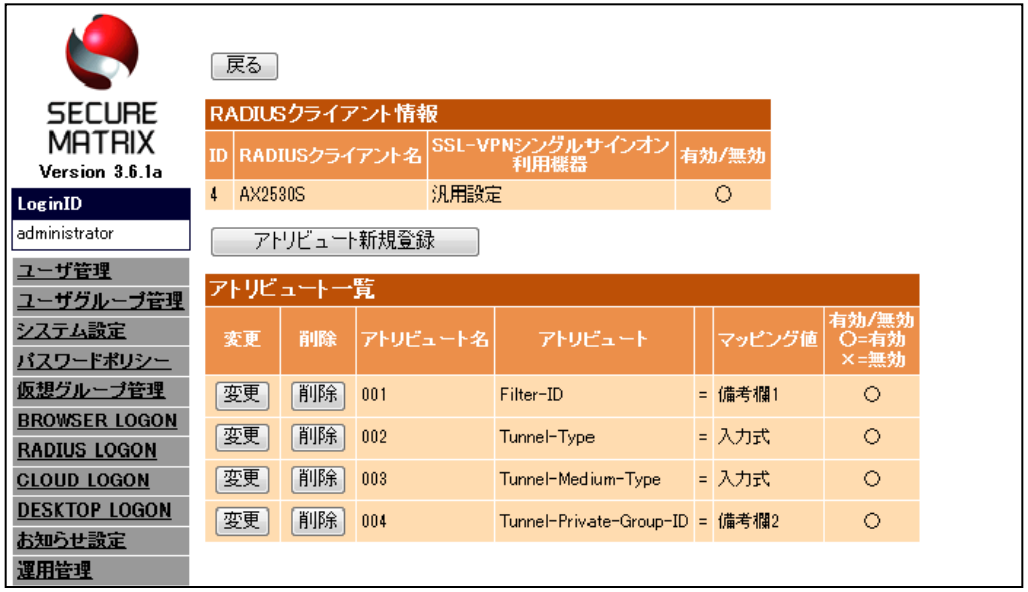
②プロパティ設定を設定します。

ssl.form.action.base = http://1.1.1.1 /cgi-bin/Login.cgi	ー＞認証スイッチのURLは http://認証専用IP/cgi-bin/Login.cgi
ssl.form.username = uid	ー＞uid としてください
ssl.form.password = pwd	ー＞pwd としてください
ssl.form.method = POST	ー＞POSTとしてください
ssl.form.hashEnabled = false	ー＞必ずfalse指定に変更してください

●httpの場合はスイッチのWeb認証専用IPアドレス直接指定してください。
認証スイッチのURLはhttpsも使用可能です、その場合はエラー回避のためスイッチのSSLサーバ証明書と一致するサーバ名で指定します。（別途端末が参照するDNSサーバへ認証専用IPアドレスと、サーバ名の登録などの設定をしてください。）
●ssl.form.hashEnabledは必ずfalse指定としてください。

◆ アトリビュートの設定

ダイナミックACL、ダイナミックVLANを使用する場合は、RADIUSクライアント毎にアトリビュートの登録が必要です。



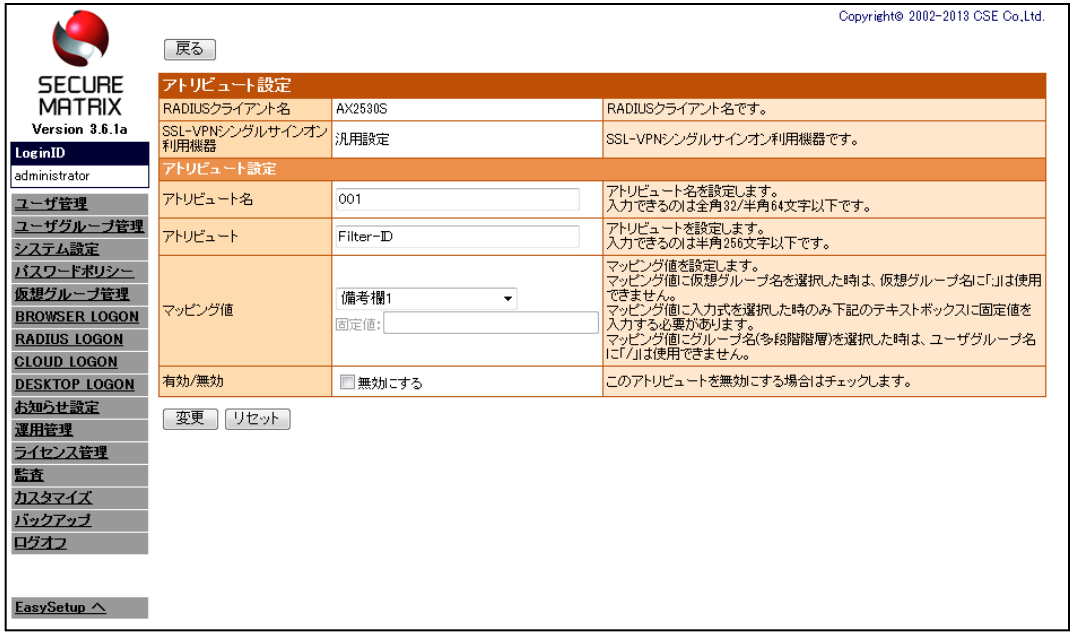
上記設定画面は設定済みの画面の一覧を表示しています。

新規の場合は、「アトリビュート新規登録」から追加してください。
・ダイナミックACLを使用する場合は、Filter-IDを設定しアトリビュートを登録（例：アトリビュート名 001）
・ダイナミックVLANを使用する場合は、3種類のアトリビュートを登録（例：アトリビュート名 002～004）

各アトリビュートの詳細な設定画面は次ページへ

◆ アトリビュートの設定(ダイナミックACL)

ダイナミックACLではアトリビュート「Filter-ID」を使用します。



・アトリビュート名は任意です。本例では「 001 」としています。

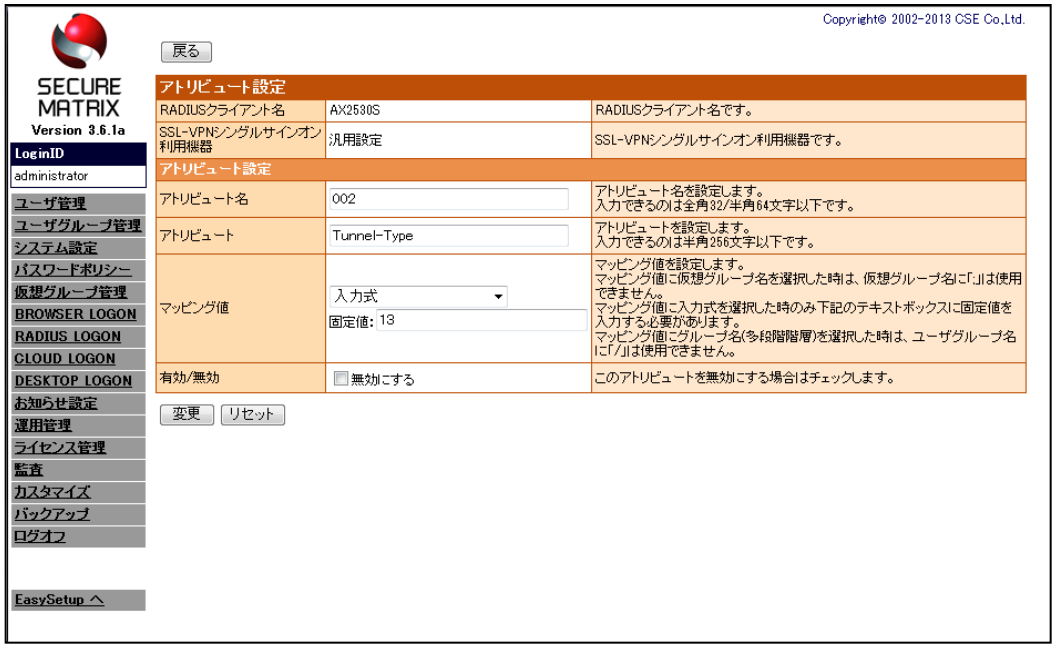
・アトリビュートは 「 Filter-ID 」 を設定してください。

・マッピング値は 本例では「 備考欄1 」 とし、ユーザ情報の 備考欄1 と対応付けました。

※ユーザ情報の備考欄1の方には、実際のFilter-IDに設定する情報を設定します。
AXシリーズのダイナミックACLでは、Filter-IDには ユーザの所属するクラス番号を指定します。
例えばクラス3の場合、Filter-IDの文字列に 「 /Class=3 」 と設定します。
(詳細はAXシリーズ製品マニュアル、AXシリーズ認証ソリューションガイドを参照してください。)

◆ アトリビュートの設定(ダイナミックVLAN)（1）

ダイナミックVLANの設定では3種類のアトリビュートの設定が必要です。
アトリビュート名002～004を設定してください。下図は1番目の設定です。

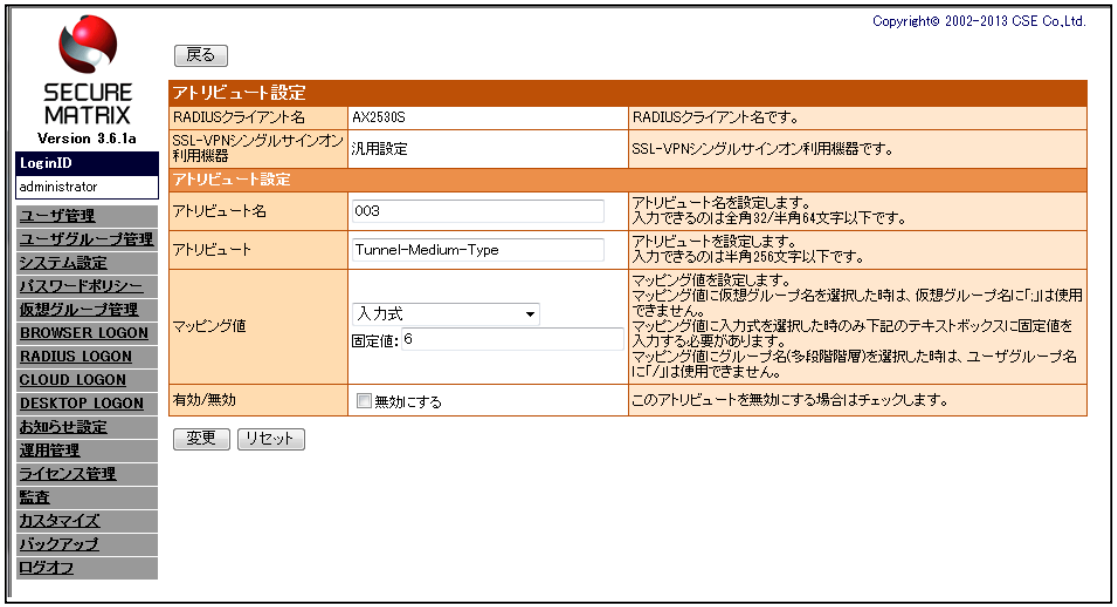


・アトリビュート名は任意です。本例では「 002 」としています。
・アトリビュートは 「 Tunnel-Type 」を設定してください。
・マッピング値は 「 入力式 」として固定値 「 13 」を設定してください。

次ページにつづく

◆ アトリビュートの設定(ダイナミックVLAN)（2）

ダイナミックVLANの設定では3種類のアトリビュートの設定が必要です。下図は2番目の設定です。

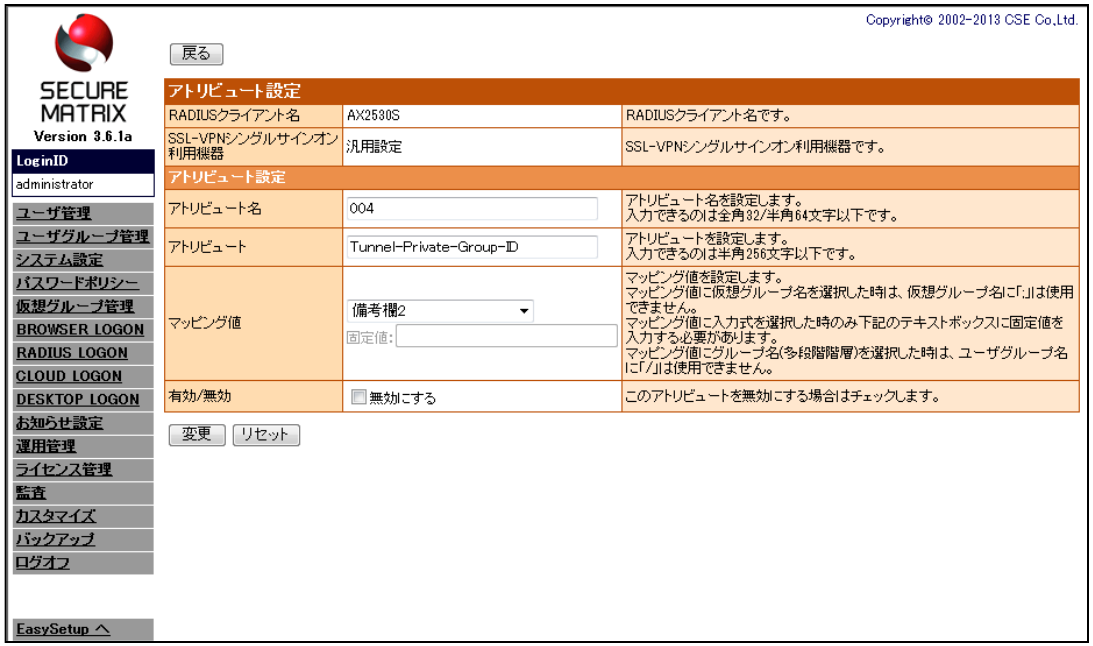


・アトリビュート名は任意です。本例では「 003 」としています。
・アトリビュートは 「 Tunnel-Medium-Type 」を設定してください。
・マッピング値は 「 入力式 」として固定値 「 6 」を設定してください。

次ページにつづく

◆ アトリビュートの設定(ダイナミックVLAN)（3）

ダイナミックVLANの設定では3種類のアトリビュートの設定が必要です。下図は3番目の設定です。



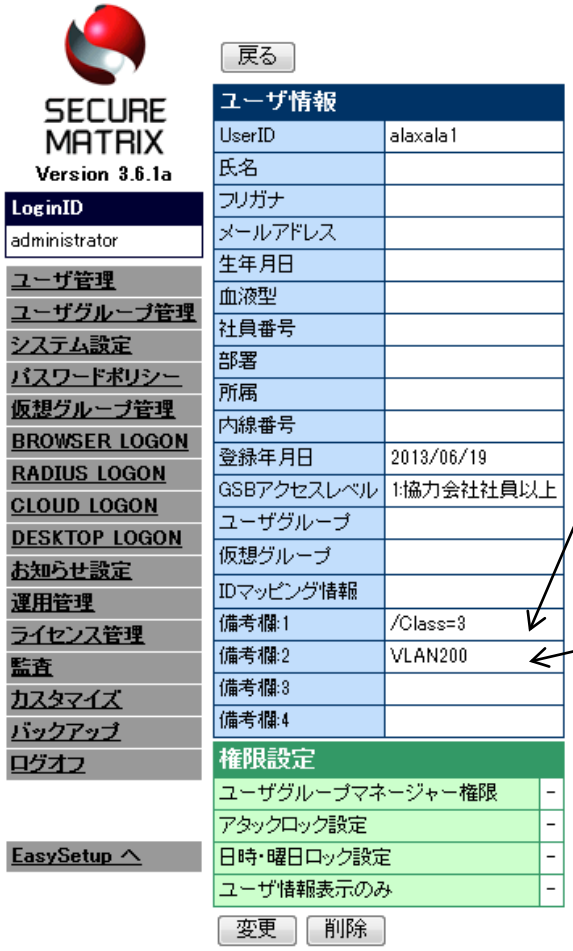
・アトリビュート名は任意です。本例では「 004 」としています。

・アトリビュートは 「 Tunnel-Private-Group-ID 」を設定してください。

・マッピング値は 本例では 「 備考欄2 」とし、ユーザ情報の 備考欄2 と対応付けました。

※ユーザ情報の備考欄2の方には、実際に設定するVLANの情報を設定します。
VLANの情報は、例えばVLAN200にユーザを所属させたい場合は、VLAN番号「 200 」または「 VLAN200 」を指定します。また、AXシリーズ認証スイッチのコンフィグレーションでVLAN名称を設定することで、VLAN名称を指定することもできます。

◆ ユーザ登録情報(アトリビュートの設定)



ダイナミックACL

RADIUSクライアントのアトリビュート登録で、本例では、備考欄1をダイナミックACL(Filter-ID)にマッピングしているため、ユーザ情報の備考欄1にはAXシリーズのダイナミックACLに使用する クラス番号を指定します。

設定値フォーマット

/Class=クラス番号

ダイナミックVLAN指定

RADIUSクライアントのアトリビュート登録で、本例では、備考欄2をダイナミックVLAN(Tunnel-Private-Group-ID)とマッピングしているため、ユーザ情報の備考欄2にVLANの指定を行います

設定値フォーマット

VLAN200を割り当てる場合、

200 または VLAN200

またはVLAN名称で指定したい場合、

VLAN名称

(AXシリーズ認証スイッチのコンフィグレーションでVLAN名称として任意に設定した文字列)。

3.2 AXシリーズの設定ポイント

AXシリーズとSECUREMATRIXを連携する場合にはWeb認証を行います。下記に連携のポイントを示します。

Web認証の設定方法は「AXシリーズ認証ソリューションガイド」および「AXシリーズのマニュアル」を参照してください。

◆ポイント1：クライアントPCを接続する認証ポートは、Web認証ポートに設定する。

（固定VLAN、ダイナミックVLAN、ダイナミックACLいずれも連携可能）

◆ポイント2：Web認証のRADIUSサーバを「SECUREMATRIX認証サーバ」とする。

◆ポイント3：認証ページを「SECUREMATRIX GSBサーバ」へリダイレクトするよう設定する。

リダイレクト先の指定は、AX2500Sではコンフィグにて設定し、
AX2500S以外の機種は「認証画面入替え機能」を使用する。

リダイレクト先のURLは、SECUREMATRIXのRADIUSクライアント登録の
SSL-VPNシングルサインオン設定のところで設定した認証のアクセスパス。

なお、AXの設定方法は「認証ソリューションガイド」の5章を参照してください。

◆ポイント4：認証専用アクセスリストに「SECUREMATRIX GSBサーバ」への通信を許可する。

GSBサーバのIPアドレスを許可するように指定してください。

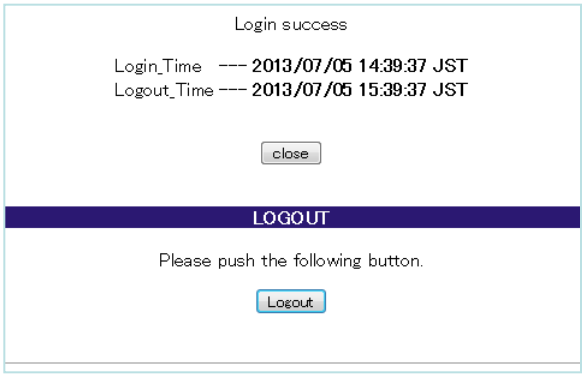
◆ ユーザ認証画面

1. ログインID入力

2. パスワード入力

3. 認証結果表示

4. 認証スイッチのログイン結果表示



The Guaranteed Network

いちばん近くで、もっと先へ。