

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

© ALAXALA Networks Corporation 2013. All rights reserved.

資料No. NTS-13-R-007

Rev. 0

The
Guaranteed
Network

Alaxala

■ 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/>)

1. SECUREMATRIXとAXシリーズの連携概要
 - 1.1 概要と結果
 - 1.2 SECUREMATRIXの概要
 2. SECUREMATRIXとAXシリーズの連携評価
 - 2.1 評価構成と内容
 - 2.2 評価機器および設定条件
 - 2.3 評価項目と使用機器
 - 2.4 評価結果
 3. SECUREMATRIXとAXシリーズの設定とポイント
 - 3.1 SECUREMATRIXの設定
 - 3.2 AXシリーズの設定ポイント
- 付録 ユーザ認証画面

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. SECUREMATRIXとAXシリーズの連携概要

1.2 SECUREMATRIXの概要

「SECUREMATRIX」はワンタイムパスワードシステムです。

● **パスワードイメージ**

あらかじめ自分の好きなパスワードイメージを登録しておきます。



● **アクセスごとに異なるマトリクス表 ▶ 異なるパスワード**

1回目



パスワード: [OK] [キャンセル]

認証を行います。
パスワードを入力して下さい。

マトリクス認証[®]は、アクセスの度に表示される数字が変わるマトリクス表を使用しています。
たとえば「V」というイメージのパターンを、あらかじめ登録しておきます。

入力するパスワード
74894354 (一度だけ)

2回目



パスワード: [OK] [キャンセル]

認証を行います。
パスワードを入力して下さい。

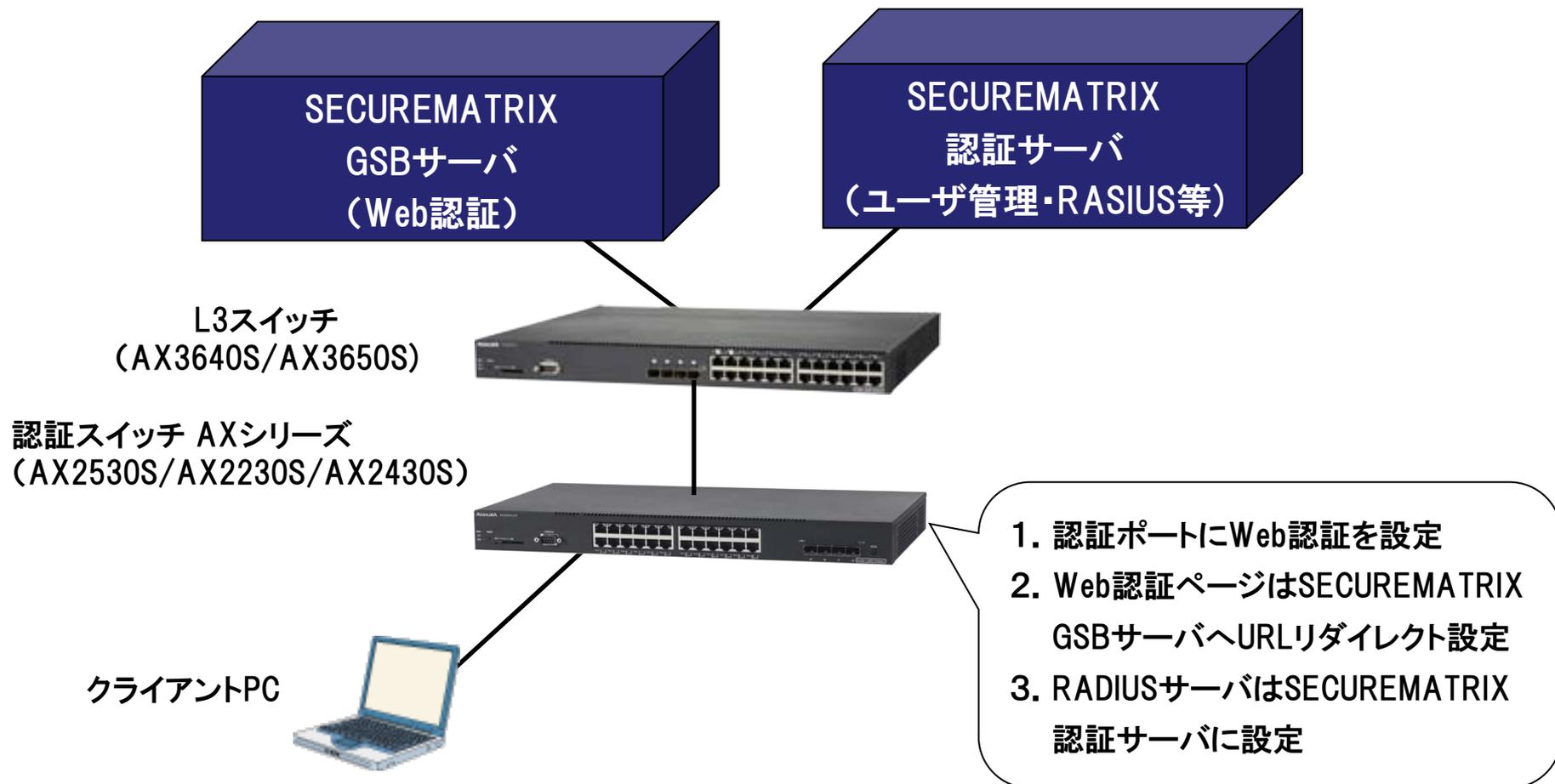
マトリクス認証[®]は、毎回マトリクス表に表示する数字が変わるので、二度と同じパスワードを入力することはありません。

入力するパスワード
41406182 (一度だけ)

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。

2.1 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. SECUREMATRIXとAXシリーズの連携評価

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. SECUREMATRIXとAXシリーズの連携評価

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. SECUREMATRIXとAXシリーズの設定とポイント

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。

ようこそ administrator さん

Copyright© 2002-2013 CSE Co.,Ltd

左側のメニューから管理したい項目をクリックしてください。
※このページに戻りたい場合は、左側のメニューのSECUREMATRIXのロゴマークをクリックしてください。

Version 3.6.1a

LoginID
administrator

ユーザ管理
ユーザグループ管理
システム設定
パスワードポリシー
仮想グループ管理
BROWSER LOGON
RADIUS LOGON
CLOUD LOGON
DESKTOP LOGON
お知らせ設定
運用管理
ライセンス管理
監査
カスタマイズ
バックアップ
ログオフ
EasySetup ^

ライセンス情報	
ライセンスID	alaxE1

登録ユーザ数	
ユーザ数	3
ユーザグループに割り当てられているユーザ数	10
割り当てユーザ数が設定なしとなっているユーザグループの使用ユーザ数	0
監査者数	0
登録できる残りユーザ数	12
合計	25
無効ユーザ数	0

認証有効稼働期日	
SecureMatrixは 後20日 で有効期限切れになります	
正式認証有効稼働終了日	2013/07/16
残日数	20日

ログイン認証に成功しました
次へを押してください

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



Copyright© 2002-2013 CSE Co.,Ltd.

RADIUS LOGON (RADIUS クライアント) 情報の反映について
同一アトリビュートのVPN装置のみ、グループ制御が可能となります。
RADIUSクライアント情報を削除した際は、設定反映のため、認証サーバの再起動が必要になります。

RADIUSクライアント一覧									
変更	削除	ID	RADIUSクライアント名	アトリビュート 設定	SSL-VPNシングルサインオン設定			クライアントのIPアドレス	有効/無効 ○=有効 ×=無効
					利用機器	アクセスパス	設定		
<input type="button" value="変更"/>	<input type="button" value="削除"/>	1	aaaa	<input type="button" value="設定"/>	ブラウザトークンのみ			192.168.0.100	○
<input type="button" value="変更"/>	<input type="button" value="削除"/>	2	bbbb	<input type="button" value="設定"/>	ブラウザトークンのみ			192.168.0.101	○
<input type="button" value="変更"/>	<input type="button" value="削除"/>	3	juniper	<input type="button" value="設定"/>	NetScreen SA ver4	/juniper/	<input type="button" value="設定"/>	192.168.0.200	○
<input type="button" value="変更"/>	<input type="button" value="削除"/>	4	AX2530S	<input type="button" value="設定"/>	汎用設定	/alaxala/	<input type="button" value="設定"/>	172.16.0.12	○
<input type="button" value="変更"/>	<input type="button" value="削除"/>	5	AX2230S	<input type="button" value="設定"/>	汎用設定	/alaxala2/	<input type="button" value="設定"/>	172.16.0.13	○

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。

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ RADIUSクライアント新規登録



Copyright© 2002-2013 CSE Co.,Ltd.

[戻る](#)

RADIUSクライアント情報

基本設定

RADIUSクライアント名	<input type="text" value="AX2530S"/>	RADIUSクライアント名を入力します。 入力できるのは半角64文字または全角32文字以下です。 半角スペース、全角スペースは使用できません。
クライアントのIPアドレス	<input type="text" value="172.16.0.12"/>	クライアントのIPアドレスを入力します。 IPアドレス(IPv4、IPv6)の形式で入力して下さい。
シークレットキー	<input type="text" value="alaxala"/>	シークレットキーを入力します。 入力できるのは半角31文字以下です。 入力可能文字は「0-9」、「a-z」、「A-Z」、「-」です。
SSL-VPNシングルサインオン利用機器	<input type="text" value="汎用設定"/>	使用VPN装置を選択します。
ステータス		
有効/無効	<input type="checkbox"/> 無効にする	このRADIUSクライアント情報を無効にする場合はチェックします。

設定の反映について

新規登録時、またはクライアントのIPアドレスとシークレットキーの値を変更した際は認証サーバの再起動が必要になります。
また、SSL-VPNシングルサインオン利用機器を変更した際は、登録後この画面からSSL-VPNシングルサインオン設定を行う必要があります。

[EasySetup](#) ^

- 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。

Alaxala

© ALAXALA Networks Corporation 2013. All rights reserved.

12

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ SSL-VPNシングルサインオン設定



SECURE MATRIX
Version 3.6.1a

LoginID
administrator

ユーザ管理

ユーザグループ管理

システム設定

パスワードポリシー

仮想グループ管理

BROWSER LOGON

RADIUS LOGON

CLOUD LOGON

DESKTOP LOGON

お知らせ設定

運用管理

ライセンス管理

監査

カスタマイズ

バックアップ

ログオフ

EasySetup >

SSL-VPNシングルサインオン設定		
RADIUSクライアント名	AX2530S	RADIUSクライアント名です。
SSL-VPNシングルサインオン利用機器	汎用設定	SSL-VPNシングルサインオン利用機器です。
アクセス設定		
アクセスパス	<input type="text" value="/alaxala/"/>	SSL-VPNシングルサインオン時のアクセスパスを設定します。 入力できるのは半角32文字以下です。 (「/」もしくは「/~」という形式で入力して下さい)
アクセス可能ユーザグループ	<input type="checkbox"/> 所属しない <input checked="" type="checkbox"/> group1(+0)	SSL-VPNシングルサインオン利用時に実際にアクセスするパスは以下のようになります。 「https://<GSBサーバ>/<インストール時に設定した中間パス>/<アクセスパス>」 このSSL-VPNシングルサインオンに対してアクセスを許可するユーザグループを指定します。 ここでチェックを入れたユーザグループの人が利用可能となります。 全てがチェックされていないときは、全てのユーザグループが利用できます。
プロパティ設定		
<pre>sll.form.action.base = http://1.1.1.1/cgi-bin/Login.cgi sll.form.username = uid sll.form.password = pwd sll.form.method = POST sll.form.hashEnabled = false</pre>		

[sll.form.action.base]
送信先のホストアドレスとパスを記入します。

[sll.form.username]
ユーザ名の入力欄のname値を指定します。

[sll.form.password]
パスワードの入力欄のname値を指定します。

[sll.form.method]
フォームのメソッド値を指定します。
「POST」または「GET」を指定してください。

[sll.form.hashEnabled]
パスワードを暗号化するかどうかを指定します。
「true」または「false」を指定してください。

[sll.redirecturl]
GSBサーバへの初回アクセス時、ご利用のVPN機器へリダイレクトする場合は、このパラメータを記憶してください。
例: アクセスするVPN機器のURLが
[https://universal.securematrix.jp/login/top.html] の場合は、
以下のURLを記入します。
sll.redirecturl =
https://universal.securematrix.jp/login/top.html

各項目の説明は次ページへ

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ 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/](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  
ssl.form.username = uid  
ssl.form.password = pwd  
ssl.form.method = POST  
ssl.form.hashEnabled = false
```

→ 認証スイッチのURLは <http://認証専用IP/cgi-bin/Login.cgi>

→ uid としてください

→ pwd としてください

→ POSTとしてください

→ 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。

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ 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。

The screenshot shows the SECURE MATRIX Version 3.6.1a web interface. On the left is a navigation menu with items like 'LoginID', 'ユーザ管理', 'ユーザグループ管理', 'システム設定', 'パスワードポリシー', '仮想グループ管理', 'BROWSER LOGON', 'RADIUS LOGON', 'CLOUD LOGON', 'DESKTOP LOGON', 'お知らせ設定', and '運用管理'. The main content area is titled 'RADIUSクライアント情報' and contains a table with one row: ID 4, RADIUSクライアント名 AX2530S, SSL-VPN:シングルサインオン利用機器 汎用設定, and 有効/無効 status as a radio button. Below this is a button 'アトリビュート新規登録'. Underneath is a table titled 'アトリビュート一覧' with columns for '変更', '削除', 'アトリビュート名', 'アトリビュート', 'マッピング値', and '有効/無効'. It lists four attributes: 001 (Filter-ID), 002 (Tunnel-Type), 003 (Tunnel-Medium-Type), and 004 (Tunnel-Private-Group-ID), all with '有効' status.

RADIUSクライアント情報					
ID	RADIUSクライアント名	SSL-VPN:シングルサインオン 利用機器	有効/無効		
4	AX2530S	汎用設定	<input type="radio"/>		

アトリビュート一覧					
変更	削除	アトリビュート名	アトリビュート	マッピング値	有効/無効 ○=有効 ×=無効
<input type="button" value="変更"/>	<input type="button" value="削除"/>	001	Filter-ID	= 備考欄1	<input type="radio"/>
<input type="button" value="変更"/>	<input type="button" value="削除"/>	002	Tunnel-Type	= 入力式	<input type="radio"/>
<input type="button" value="変更"/>	<input type="button" value="削除"/>	003	Tunnel-Medium-Type	= 入力式	<input type="radio"/>
<input type="button" value="変更"/>	<input type="button" value="削除"/>	004	Tunnel-Private-Group-ID	= 備考欄2	<input type="radio"/>

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

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ 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。

Copyright© 2002-2013 OSE Co.,Ltd.

戻る

SECURE MATRIX
Version 3.6.1a

LoginID
administrator

ユーザ管理
ユーザグループ管理
システム設定
パスワードポリシー
仮想グループ管理
BROWSER LOGON
RADIUS LOGON
CLOUD LOGON
DESKTOP LOGON
お知らせ設定
運用管理
ライセンス管理
監査
カスタマイズ
バックアップ
ログオフ

EasySetup >

アトリビュート設定		
RADIUSクライアント名	AX2530S	RADIUSクライアント名です。
SSL-VPNシングルサインオン利用機器	汎用設定	SSL-VPNシングルサインオン利用機器です。
アトリビュート設定		
アトリビュート名	001	アトリビュート名を設定します。 入力できるのは全角32/半角64文字以下です。
アトリビュート	Filter-ID	アトリビュートを設定します。 入力できるのは半角256文字以下です。
マッピング値	備考欄1	マッピング値を設定します。 マッピング値に仮想グループ名を選択した時は、仮想グループ名に「/」は使用できません。 マッピング値に入力式を選択した時のみ下記のテキストボックスに固定値を入力する必要があります。 マッピング値にグループ名(多段階階層)を選択した時は、ユーザグループ名に「/」は使用できません。
有効/無効	<input type="checkbox"/> 無効にする	このアトリビュートを無効にする場合はチェックします。

変更 リセット

- ・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。)

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ 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。

Copyright© 2002-2013 CSE Co.,Ltd.

戻る

SECURE MATRIX
Version 3.6.1a

LoginID
administrator

ユーザ管理
ユーザグループ管理
システム設定
パスワードポリシー
仮想グループ管理
BROWSER LOGON
RADIUS LOGON
CLOUD LOGON
DESKTOP LOGON
お知らせ設定
運用管理
ライセンス管理
監査
カスタマイズ
バックアップ
ログオフ

EasySetup ^

アトリビュート設定		
RADIUSクライアント名	AX2530S	RADIUSクライアント名です。
SSL-VPNシングルサインオン利用機器	汎用設定	SSL-VPNシングルサインオン利用機器です。
アトリビュート設定		
アトリビュート名	002	アトリビュート名を設定します。 入力できるのは全角32/半角64文字以下です。
アトリビュート	Tunnel-Type	アトリビュートを設定します。 入力できるのは半角256文字以下です。
マッピング値	入力式 固定値: 13	マッピング値を設定します。 マッピング値に仮想グループ名を選択した時は、仮想グループ名に「J」は使用できません。 マッピング値に入力式を選択した時のみ下記のテキストボックスに固定値を入力する必要があります。 マッピング値にグループ名(多段階階層)を選択した時は、ユーザグループ名に「J」は使用できません。
有効/無効	<input type="checkbox"/> 無効にする	このアトリビュートを無効にする場合はチェックします。

変更 リセット

- ・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

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ 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。


Copyright© 2002-2013 GSE Co.Ltd.

SECURE MATRIX
Version 3.6.1a

LoginID
administrator

ユーザ管理

ユーザグループ管理

システム設定

パスワードポリシー

仮想グループ管理

BROWSER LOGON

RADIUS LOGON

CLOUD LOGON

DESKTOP LOGON

お知らせ設定

運用管理

ライセンス管理

監査

カスタマイズ

バックアップ

ログオフ

戻る

アトリビュート設定		
RADIUSクライアント名	AX2580S	RADIUSクライアント名です。
SSL-VPNシングルサインオン利用機器	汎用設定	SSL-VPNシングルサインオン利用機器です。
アトリビュート設定		
アトリビュート名	<input type="text" value="003"/>	アトリビュート名を設定します。 入力できるのは全角32/半角64文字以下です。
アトリビュート	<input type="text" value="Tunnel-Medium-Type"/>	アトリビュートを設定します。 入力できるのは半角256文字以下です。
マッピング値	<input type="text" value="入力式"/> 固定値: <input type="text" value="6"/>	マッピング値を設定します。 マッピング値に仮想グループ名を選択した時は、仮想グループ名に「/」は使用できません。 マッピング値に入力式を選択した時のみ下記のテキストボックスに固定値を入力する必要があります。 マッピング値にグループ名(多段階階層)を選択した時は、ユーザグループ名に「/」は使用できません。
有効/無効	<input type="checkbox"/> 無効にする	このアトリビュートを無効にする場合はチェックします。

変更 リセット

- ・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

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ 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。


Copyright © 2002-2013 CSE Co., Ltd.

SECURE MATRIX
Version 3.6.1a

LoginID
administrator

ユーザ管理

ユーザグループ管理

システム設定

パスワードポリシー

仮想グループ管理

BROWSER LOGON

RADIUS LOGON

CLOUD LOGON

DESKTOP LOGON

お知らせ設定

運用管理

ライセンス管理

監査

カスタマイズ

バックアップ

ログオフ

EasySetup ^

アトリビュート設定		
RADIUSクライアント名	AX2530S	RADIUSクライアント名です。
SSL-VPNシングルサインオン利用機器	汎用設定	SSL-VPNシングルサインオン利用機器です。
アトリビュート設定		
アトリビュート名	<input type="text" value="004"/>	アトリビュート名を設定します。 入力できるのは全角32/半角64文字以下です。
アトリビュート	<input type="text" value="Tunnel-Private-Group-ID"/>	アトリビュートを設定します。 入力できるのは半角256文字以下です。
マッピング値	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;">備考欄2</div> <div style="border: 1px solid black; padding: 2px;">▼</div> </div> <div style="margin-top: 5px;">固定値: <input style="width: 100px;" type="text"/></div>	マッピング値を設定します。 マッピング値に仮想グループ名を選択した時は、仮想グループ名に「/」は使用できません。 マッピング値に入力式を選択した時のみ下記のテキストボックスに固定値を入力する必要があります。 マッピング値にグループ名(多段階階層)を選択した時は、ユーザグループ名に「/」は使用できません。
有効/無効	<input type="checkbox"/> 無効にする	このアトリビュートを無効にする場合はチェックします。

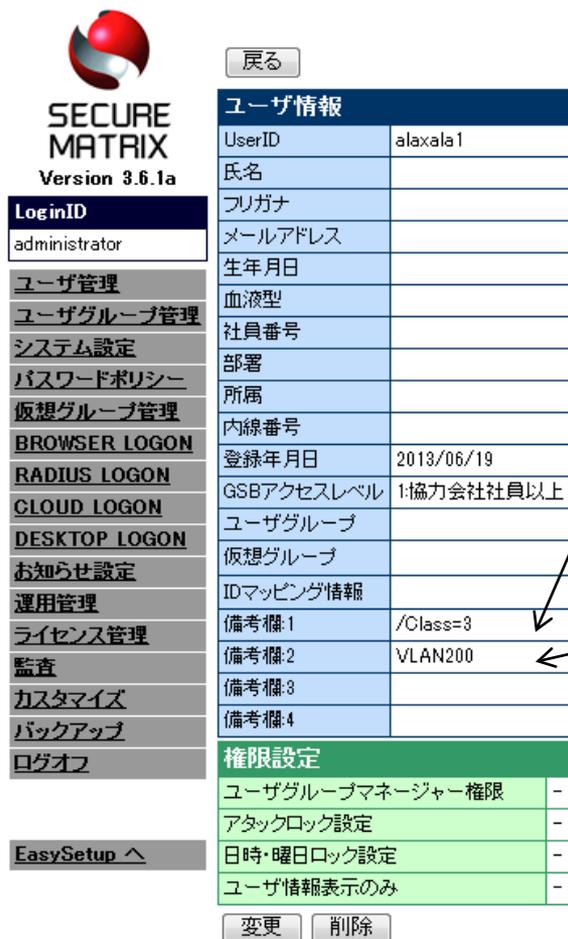
- ・アトリビュート名は任意です。本例では「 004 」としています。
- ・アトリビュートは「 **Tunnel-Private-Group-ID** 」を設定してください。
- ・マッピング値は 本例では「 備考欄2 」とし、ユーザ情報の 備考欄2 と対応付けました。

※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。

3. SECUREMATRIXとAXシリーズの設定とポイント

◆ ユーザ登録情報(アトリビュートの設定)



SECURE MATRIX Version 3.6.1a

LoginID: administrator

ユーザ管理

ユーザグループ管理

システム設定

パスワードポリシー

仮想グループ管理

BROWSER LOGON

RADIUS LOGON

CLOUD LOGON

DESKTOP LOGON

お知らせ設定

運用管理

ライセンス管理

監査

カスタマイズ

バックアップ

ログオフ

EasySetup ^

戻る

ユーザ情報	
UserID	alaxala1
氏名	
フリガナ	
メールアドレス	
生年月日	
血液型	
社員番号	
部署	
所属	
内線番号	
登録年月日	2013/06/19
GSBアクセスレベル	1:協力会社社員以上
ユーザグループ	
仮想グループ	
IDマッピング情報	
備考欄1	/Class=3
備考欄2	VLAN200
備考欄3	
備考欄4	

権限設定

ユーザグループマネージャー権限	-
アタックロック設定	-
日時・曜日ロック設定	-
ユーザ情報表示のみ	-

変更 削除

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. SECUREMATRIXとAXシリーズの設定とポイント

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。

4. 付録

◆ ユーザ認証画面

1. ログインID入力

SECUREMATRIX®

ログインID:

ログインIDを入力して下さい。

Copyright© 2002-2012 CSE Co.,Ltd.

2. パスワード入力

SECUREMATRIX®

3	4	3	1	1	2	3	3	1	2	3	2	4	7	5	7
0	5	0	7	8	3	1	4	2	5	8	4	4	2	4	2
7	3	3	4	0	5	5	6	9	8	2	1	5	0	2	4
9	6	6	9	9	0	2	6	7	2	0	9	5	1	9	6

パスワード:

認証を行います。
パスワードを入力して下さい。

Copyright© 2002-2012 CSE Co.,Ltd.

3. 認証結果表示

SECUREMATRIX®

ログイン認証に成功しました
次へを押してください

最終ログイン日時(日本時間): 2013-07-05 14:39:07
alaxala1 さんの認証が完了しました。連携機器にログインします。

Copyright© 2002-2012 CSE Co.,Ltd.

4. 認証スイッチのログイン結果表示

Login success

Login_Time --- 2013/07/05 14:39:37 JST
Logout_Time --- 2013/07/05 15:39:37 JST

LOGOUT

Please push the following button.

The Guaranteed Network

いちばん近くで、もっと先へ。