

RADIUS GUARD®とAXシリーズによる認証連携 の相互接続情報と設定ポイント

2013年10月10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-019

Rev. 0

The
Guaranteed
Network

AlaxaIA

■ 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。
- RADIUS GUARDは、SCSK株式会社の登録商標です。
- 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>)
- RADIUS GUARDについて
(<http://www.scsk.jp/product/common/radius/>)

1. RADIUS GUARDとAXシリーズの連携概要
 - 1.1 概要と結果
 - 1.2 RADIUS GUARDを利用したWeb認証とMAC認証の利便性向上
2. RADIUS GUARDとAXシリーズの認証連携基本評価
 - 2.1 評価構成
 - 2.2 設定条件
 - 2.3 評価項目と使用機器
 - 2.4 評価結果
3. Web認証端末のMACアドレス自動学習連携評価
 - 3.1 評価構成
 - 3.2 設定条件
 - 3.3 評価項目と使用機器
 - 3.4 評価結果
4. AXシリーズ使用時のRADIUS GUARDの設定ポイント
5. RADIUS GUARD連携時のAXシリーズの設定ポイント
 - 5.1 「RADIUS GUARD」によるWeb認証端末のMACアドレス自動登録機能との連携
 - 5.2 「RADIUS GUARD」のユーザ認証時の利用端末制限機能との連携

1. RADIUS GUARDとAXシリーズの連携概要

1.1 概要と結果

■RADIUS GUARDとAXシリーズの認証連携の特徴

1. RADIUSサーバとしての使用

AXシリーズの全てのネットワーク認証(IEEE802.1X、Web認証、MAC認証)にて、RADIUS GUARDをRADIUSサーバとして使用可能です。

2. WEB認証機能との連携

AXシリーズの認証画面編集機能や、認証前端末の通信許可機能等により、未登録ユーザについてはRADIUS GUARDのアカウント申請画面へ誘導し、RADIUS GUARDの特徴機能であるユーザ自身でのアカウント申請、MACアドレスの申請、ユーザ証明書の発行などの豊富な機能を用いて、システム管理者の負担を軽減させます。

3. MACアドレス自動登録機能との連携

RADIUS GUARDのユーザ認証時MACアドレス自動登録機能を利用する事で、Web認証とMAC認証の連携を図り、ユーザや管理者の入力負担を軽減することができます。

4. 利用端末制限機能との連携

ユーザ認証の際に、ユーザ毎に登録された利用端末のMACアドレスをチェックする機能が利用できるため、不正端末の接続を防止し、よりセキュアな認証ネットワークが簡単に構築できます。

■評価試験結果

AXシリーズのレイヤ2認証機能とRADIUS GUARDが認証連携できることを確認しました。

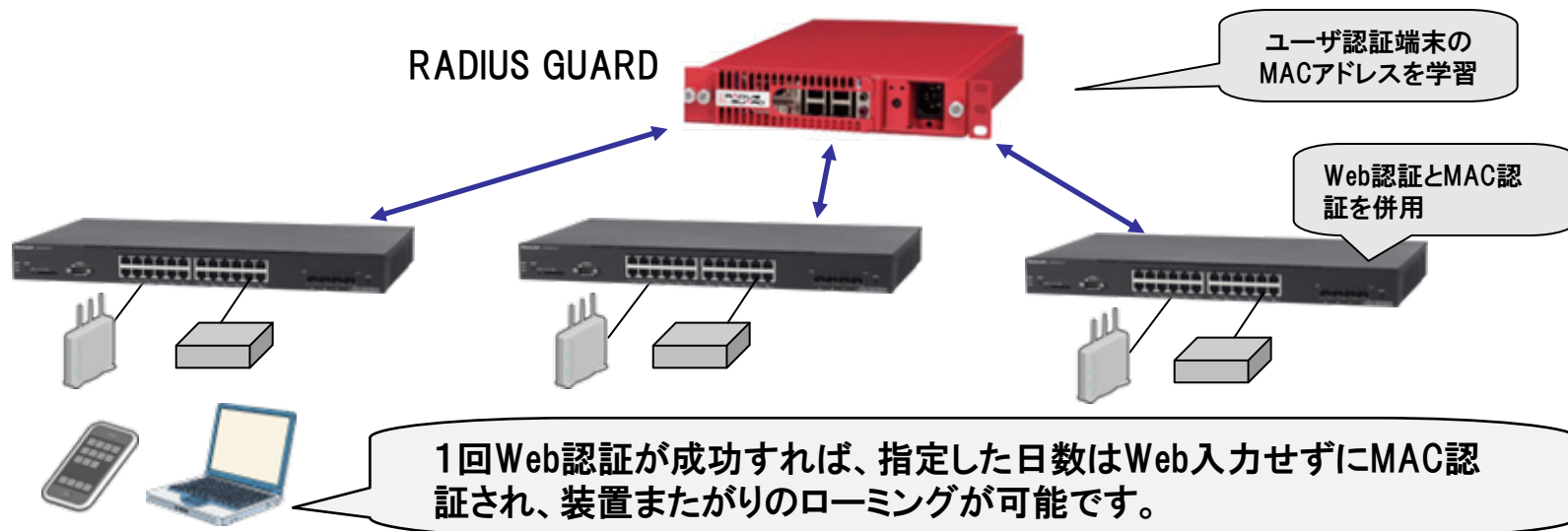
1. RADIUS GUARDとAXシリーズの連携概要

1.2 RADIUS GUARDを利用したWeb認証とMAC認証の利便性向上

RADIUS GUARDの特徴機能である、ユーザ認証時の端末MACアドレス自動登録機能と、AXシリーズのWeb認証/MAC認証を連携することで、ユーザ、管理者双方にメリットのある利便性の高い認証ネットワークシステムを構築することができます。

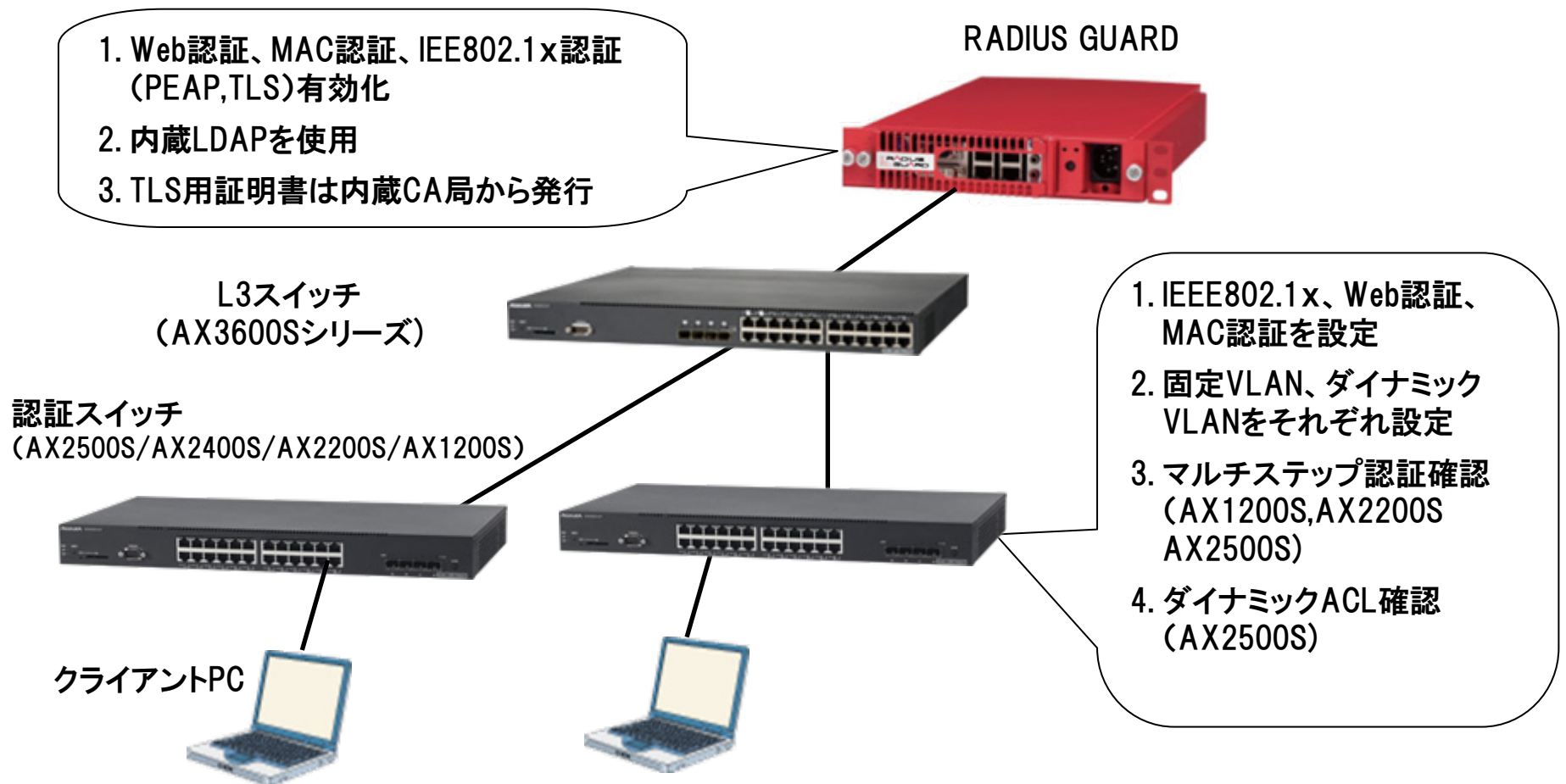
・ Web認証とMAC認証の融合による利便性の向上ポイント

1. 端末がスイッチをまたいでローミングした際にも、即座にMAC認証が実行されるため、Web認証の操作をすることなく通信可能となり、ユーザの利便性を向上することができます。
2. 端末スリープ等でユーザが認証ネットワークからログアウトした際にも、再びユーザが復帰した場合はMAC認証が実施されるため、Web認証でユーザIDを入力する必要がなくなります。
3. MAC認証を主に使用する場合でも、未登録端末については一度だけWEB認証を使用することによりMACアドレスを自動収集するため、管理者が端末登録する必要もなく運用できます。



2. RADIUS GUARDとAXシリーズの連携基本評価

2.1 評価構成



1. 基本的なトリプル認証(固定VLAN、ダイナミックVLAN、ダイナミックACL)連携を評価する。
2. ユーザ認証利用端末の許可(AXシリーズのマルチステップ認証、RADIUS GUARD利用端末指定)連携を評価する。

2. RADIUS GUARDとAXシリーズの連携基本評価

2.2 設定条件

(1)「RADIUS GUARD」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
- ・内蔵LDAPを使用する
- ・認証成功時のアトリビュートを設定を行う(ダイナミックVLAN,ダイナミックACL/QoS)
(共通アトリビュート、ユーザ個別ネットワークプロファイル指定)
- ・ユーザ認証における利用端末制限の設定(RADIUS GUARD独自機能の設定)
- ・AXシリーズマルチステップ認証確認のための端末を登録
(アトリビュート(Filter-ID)にマルチステップ応答するように設定)

(2)認証スイッチ「AXシリーズ」の設定条件

- ・認証ポートは、トリプル認証(Web認証、MAC認証、IEEE802.1x認証)ポートに設定する。
(固定VLAN、ダイナミックVLAN、AX2500SはダイナミックACLを追加で設定)
- ・マルチステップ認証評価用にマルチステップ認証ポートを設定する。
(AX1200S,AX2200S,AX2500S)

2. RADIUS GUARDとAXシリーズの連携基本評価

2.3 評価項目と使用機器

(1) 評価項目

- ◆ RADIUS GUARDでトリプル認証が可能であること
 - ・Web認証の連携ができること
 - ・MAC認証の連携ができること
 - ・IEEE802.1xの認証が出来ること(EAP-PEAP,EAP-TLS)
- ◆ 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/Qos(Filter-ID)の指定が可能であること
- ◆ マルチステップ認証の連携(Filter-IDの指定)が出来ること
- ◆ RADIUS GUARDのユーザ別利用端末制限が連携可能であること

(2) 使用機器・ソフトウェア

- ・ RADIUS GUARD® : Version 5.03.01
- ・ 認証スイッチ
 - AX1240S/AX2230S : Ver2.4A
 - AX2530S : Ver3.5A
 - 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

2.4 評価結果

以下に、RADIUS GUARDとAXシリーズの認証連携評価の結果を示します。

RADIUS GUARD : Version 5.03.01

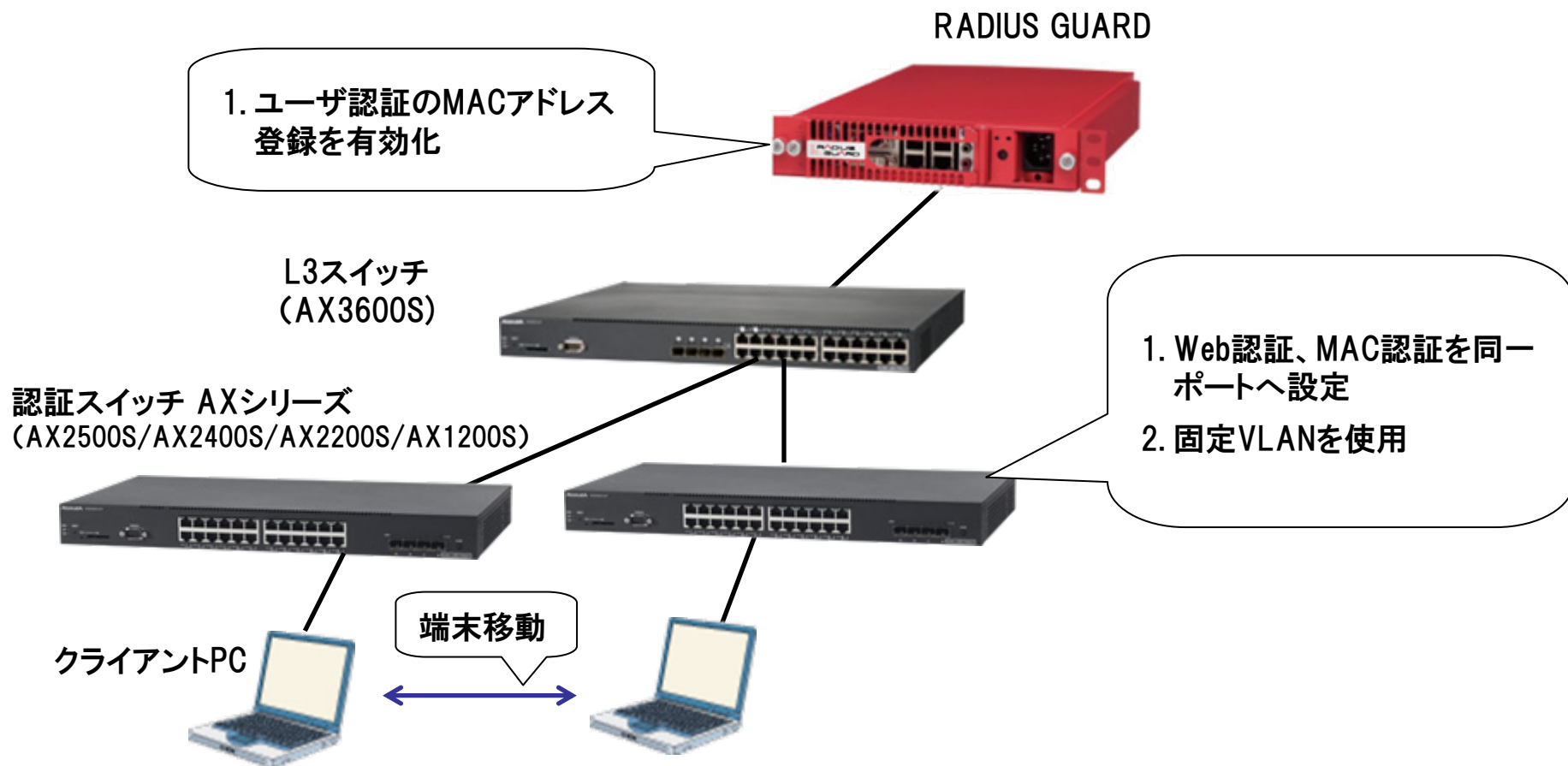
対象機器	機器バージョン	Web認証	MAC認証	IEEE802.1x (PEAP,TLS)	アトリビュート配布			利用端末制限
					VLAN	マルチステップ	ダイナミックACL/QoS	
AX2400S	11.7F	○	○	○	○	—	—	○
AX3600S	11.11A	○	○	○	○	—	—	○
AX1200S	2.4A	○	○	○	○	○	—	○
AX2200S	2.4A	○	○	○	○	○	—	○
AX2500S	3.5A	○	○	○	○	○	○	○

○ : 連携OK

— : 機能未サポート

3. Web認証端末のMACアドレス登録連携評価

3.1 評価構成



RADIUS GUARDのユーザ認証時の端末MACアドレス登録機能との連携をテスト

3. Web認証端末のMACアドレス登録連携評価

3.2 設定条件

(1)「RADIUS GUARD」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
- ・内臓LDAPを使用する
- ・ユーザ認証設定で、MACアドレス自動登録機能を有効化する

(2)認証スイッチ「AXシリーズ」の設定条件

- ・認証ポートは、Web認証とMAC認証併用設定する
- ・認証ポートは固定VLANとする

3. Web認証端末のMACアドレス登録連携評価

3.3 評価項目と使用機器

(1) 評価項目

- ◆ Web認証後、RADIUS GUARDにMAC認証用のアカウントが自動的に登録されること。
- ◆ Web認証した装置から、別の装置に端末を移動させた後、MAC認証にて通信許可ができること。
- ◆ RADIUS GUARDに自動的に登録された端末アカウント(MACアドレス)に有効期限が設定されていること。

(2) 使用機器・ソフトウェア

- ・ RADIUS GUARD® : Version 5.03.01
- ・ 認証スイッチ
 - AX1240S/AX2230S : Ver2.4A
 - AX2530S : Ver3.5A
 - 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

3. Web認証端末のMACアドレス登録連携評価

3.4 評価結果

以下に、RADIUS GUARDとAXシリーズの認証連携評価の結果を示します。

RADIUS GUARD : Version 5.03.01

対象機器	機器バージョン	Web認証	移動後のMAC認証
AX2400S	11.7F	○	○
AX3600S	11.11A	○	○
AX1200S	2.4A	○	○
AX2200S	2.4A	○	○
AX2500S	3.5A	○	○

○ : 連携OK

— : 機能未サポート

4. AXシリーズ使用時のRADIUS GUARDの設定ポイント

◆ RADIUSクライアントの登録

Radiusクライアント一覧

▼Radiusクライアント新規登録 ▼リストのダウンロード

該当するデータは3件あります。
1 / 1 ページ

No.	全て	IPアドレス ▲▼	クライアント名 ▲▼	コメント ▲▼	編集
1	<input type="checkbox"/>	192.168.0.251	AX3640S		✕
2	<input type="checkbox"/>	192.168.0.252	AX2530S		✕
3	<input type="checkbox"/>	192.168.0.253	AX1240S		✕

削除

① Radius設定->Radiusクライアント->Radiusクライアント新規登録ボタンより機器を登録します。

4. AXシリーズ使用時のRADIUS GUARDの設定ポイント

◆ RADIUSクライアント新規登録

- ▼ 基本設定
- ▼ CA設定
- ▼ Radius設定
 - 認証設定
 - Radiusクライアント**
 - Radiusクライアントグループ
 - ネットワーク属性
 - ネットワークプロファイル
 - VSA設定
 - Radiusプロキシ設定
- ▼ LDAP設定
 - 端末共通パスワード
- ▼ ディレクトリ管理
 - ▼ ユーザー/端末
 - ユーザー/端末検索
 - ユーザー/端末一覧
 - 共通利用端末
 - 端末利用状況

Radiusクライアント新規登録
戻る

ファイルから一括登録する

[登録用ファイルサンプル](#)

1行目を無視する

クライアントID※ <small>(半角英数記号 32文字以内)</small>	<input type="text"/>
クライアント名称 <small>(80文字以内)</small>	<input type="text"/>
クライアントIPアドレス※ <small>XXXXXXXXXXXX</small>	<input type="text"/>
シークレットキー※ <small>(半角英数記号 30文字以内)</small>	<input type="text"/> <input type="text"/> (確認用)
コメント <small>(100文字以内)</small>	<input type="text"/>

※は必須項目です。
 クライアントIDに使用可能な記号は % _ @ + * / : & \$ # ! { } () [] ? ^ ` | ~ ; < > = " ' , ¥ の32種類です。
 シークレットキーに使用可能な記号は % _ @ + * / : & の10種類です。
登録した情報を反映させるにはRadius設定反映操作が必要です。

- ① RADIUSクライアントID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. AXシリーズ使用時のRADIUS GUARDの設定ポイント

◆ アトリビュートの指定

VLAN ID (半角数字 8文字以内)	<input type="text"/>
Access-Defender-Class (半角数字 8文字以内)	<input type="text"/>
Filter-Id (半角英数記号 32文字以内)	<input type="text" value="/Class=3"/>
Callback-Number (半角英数記号 32文字以内)	<input type="text"/>
Tunnel-Type (半角英数記号 256文字以内)	<input type="text" value="13"/>
Tunnel-Medium-Type (半角英数記号 256文字以内)	<input type="text" value="6"/>
Tunnel-Private-Group-Id (半角英数記号 256文字以内)	<input type="text" value="200"/>
NAS-Identifier (1行1属性 最大256行) (1行は半角英数記号 256文字以内)	<input type="text"/>

- ← ダイナミックACL/QoS
所属クラス3の指定例
- ← 固定値13
- ← 固定値6
- ← VLAN200の指定例

認証成功時にスイッチに配布するダイナミックVLANおよびダイナミックACL/QoSの指定例です。

(アラクサラ AXシリーズ共通)

上記画面は、共通アトリビュート、ネットワークプロファイルで指定するネットワーク属性画面の関係するアトリビュートを切り出した例となります。(ディレクトリやユーザ単位の指定方法などは、RADIUS GUARDのマニュアルを参照してください。)

VLAN番号200 および ダイナミックACLでユーザの所属Class番号 3 を指定した例となります。

- ・ダイナミックACL/QoSではFilter-IDにユーザの所属するクラス番号(1~63)を指定します (/Class=クラス番号)
- ・ダイナミックVLANでは、Tunnel-Typeに 13、Tunnel-Medium-Typeに 6、の固定値とTunnel-Private-Group-IdにVLANを指定します。(VLAN200を指定する場合は、200、VLAN200またはAX側の設定したVLAN名称を文字列で指定してください)

4. AXシリーズ使用時のRADIUS GUARDの設定ポイント

◆ 認証ユーザ端末のMACアドレス自動登録

Account > 移動中
DHCPプライマリ: 稼働中

- ▼ 基本設定
- ▼ CA設定
- ▼ Radius設定
- ▼ LDAP設定
- ▼ MACアドレス収集
- ユーザー認証設定
- ▼ ユーザー機能ツール管理
- ▼ 外部サーバー連携
- ▼ DHCP
- ▼ メンテナンス
- ログ参照

ユーザー認証設定

MACアドレス登録	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
登録ディレクトリ*	<input type="button" value="選択"/> home > ALAXALA1 > MACAUTO
有効期限	<input type="radio"/> 無期限 <input checked="" type="radio"/> 認証日からの経過日数 <input type="text" value="1"/> 日後 <input type="radio"/> ユーザーアカウントの有効期限
登録対象 (半角英数記号256文字以内)	<input style="width: 100%;" type="text"/>

*は必須項目です。
「半角英数記号」で使用可能な記号は % _ @ + - * / : & \$ # ! { } () [] ? ` ^ | < > = ' , * の32種類です。

RADIUS GUARDのMACアドレス自動登録機能により、ユーザ認証(Web認証)した端末のMACアドレスを自動的に端末アカウントとして学習することが可能です。この機能によって、Web認証後の端末を次回からMAC認証として扱うことにより、再度のユーザID入力を省略させ、利便性を向上することができます。

本機能を有効化するには、「MACアドレス収集->ユーザ認証設定」で「使用する」を選択し、登録ディレクトリを設定してください。

有効期限は本例では1日としています。1日を設定した場合当日0時まで学習したMACアドレス認証が有効となります。

4. AXシリーズ使用時のRADIUS GUARDの設定ポイント

◆ ユーザ認証と利用端末の制限の設定

WebUI接続設定

ライセンス

管理ツール表示設定

ユーザー機能ツール表示設定

管理者設定

管理者アカウント管理

▼ CA設定

▼ Radius設定

▼ LDAP設定

端末共通パスワード

▼ ディレクトリ管理

ディレクトリ作成

ディレクトリ情報編集

ディレクトリ削除

ディレクトリ一括作成

共通アトリビュート

▼ ユーザー/端末

ユーザー/端末検索

ユーザー/端末一覧

共通利用端末

端末利用状況

最終認証日時

アカウント一括変更

自動削除設定

アカウント一括削除

MKへのユーザー登録 戻る

ファイルから一括登録する

[登録用ファイルサンプル](#)

1行目を無視する 存在するユーザー情報を上書きする

個別に登録する

ユーザーID※ <small>(半角英数記号 64文字以内)</small>	<input type="text"/>
名前※ <small>(255文字以内)</small>	姓 <input type="text"/> 名 <input type="text"/>
所属※ <small>(255文字以内)</small>	<input type="text"/>
メールアドレス <small>(半角英数記号 255文字以内)</small>	<input type="text"/>
パスワード※ <small>(半角英数記号 30文字以内)</small>	<input type="password"/> <input type="password"/> <small>(確認用)</small>
ネットワークプロファイル	<input type="text"/>
利用開始日時	2013年 8月 28日 14時
アカウント有効期限※	<input checked="" type="radio"/> 無期限 <input type="radio"/> 期限あり <input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日 <input type="text"/> 時
ネットワーク利用	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
利用端末 <small>(1行/端末)</small>	<input type="checkbox"/> 共通利用端末を利用する <input type="text"/>

※は必須項目です。
「半角英数記号」で使用可能な記号は%_@+-*/:&\$#!{ } () [] ? ^ ` | ~ ; < > = ' , * の32種類です。
 (ユーザーIDは _ - の3種類、
 メールアドレスは%_@+-*/:&\$#!{ } ? ^ ` | ~ ; ' の21種類)

ユーザ登録情報に利用端末を指定すると指定されたMACアドレス以外では認証許可されません
 設定詳細は次ページで説明します。

4. AXシリーズ使用時のRADIUS GUARDの設定ポイント

◆ 利用端末の制限の設定例

利用端末 (1行1端末)	<input type="checkbox"/> 共通利用端末を利用する <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">001122334455 001122667788</div>
-----------------	---

ユーザ認証が実行可能な利用端末を制限する場合、ユーザ情報画面の利用端末欄にMACアドレスを登録することで、ユーザと利用端末を関連付けすることが出来ます。本指定により、ユーザ認証とその利用者の端末を制限することが可能です。

共通利用端末にチェックを入れた場合には、共通利用端末に登録された端末を利用可能とします。

利用端末欄が空欄のユーザはユーザ認証のみで認証許可となります。

注意事項

利用端末の設定欄は初期値では表示されません、「管理ツール表示設定」から表示するように設定してください。利用端末の設定欄は任意と、必須の選択も可能です。

ユーザ認証のMACアドレス登録とは併用できません、ユーザ認証のMACアドレス登録はMAC認証のアカウントとして登録されます。

◆ AXシリーズの設定ポイント

AXシリーズの認証設定に関しては、「認証ソリューションガイド」および「装置マニュアル」を参照してください。ここでは「RADIUS GUARD」の特徴機能である「ユーザ認証時のMACアドレス登録機能」と「ユーザ認証における利用端末制限」の連携のための設定ポイントを紹介します。

5.1 「RADIUS GUARD」によるWeb認証端末のMACアドレス自動登録機能との連携

- ◆ 認証ポートには、Web認証とMAC認証が同時に動作するように設定してください。
- ◆ 認証ポートは固定VLAN認証としてください。

5.2 「RADIUS GUARD」のユーザ認証時の利用端末制限機能との連携

- ◆ 認証ポートには、Web認証またはIEEE802.1Xを設定してください。
- ◆ 認証ポートは固定VLAN,ダイナミックVLAN,ダイナミックACL/QoSどれでも連携可能です。
(ダイナミックACL/QoSはAX2500Sのみサポートしています)

※ AXシリーズではネットワーク認証時のRADIUSパケットの属性のCalling-Station-Idにて認証端末のMACアドレスを通知します。

The Guaranteed Network

いちばん近くで、もっと先へ。