2024 年 2 月 14 日
OP24-DE-701-01

RADIUS GUARD S V7

簡単スタートアップガイド（vol.1）

SCSK Corporation

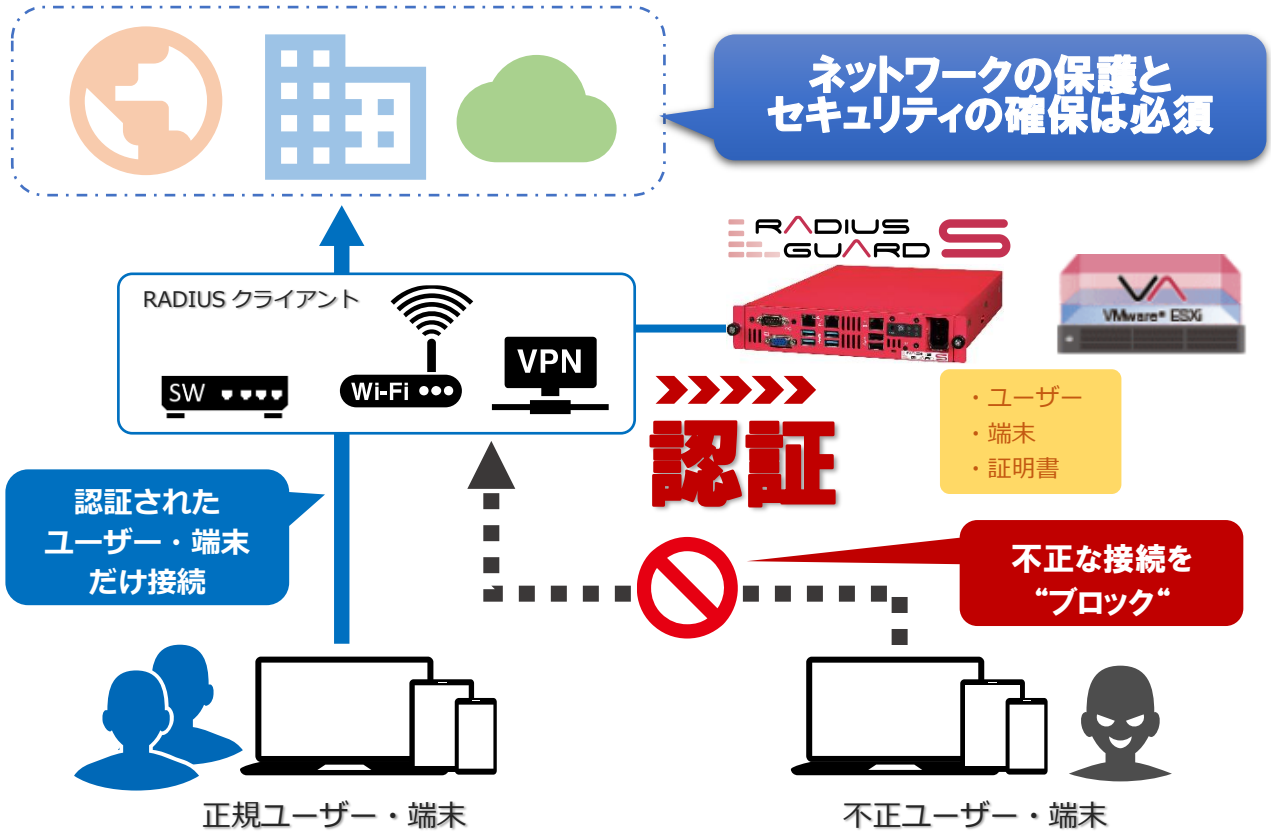
目次

概要

“無線(Wi-Fi)” **“有線(スイッチ)”**

“リモートアクセス(VPN)“

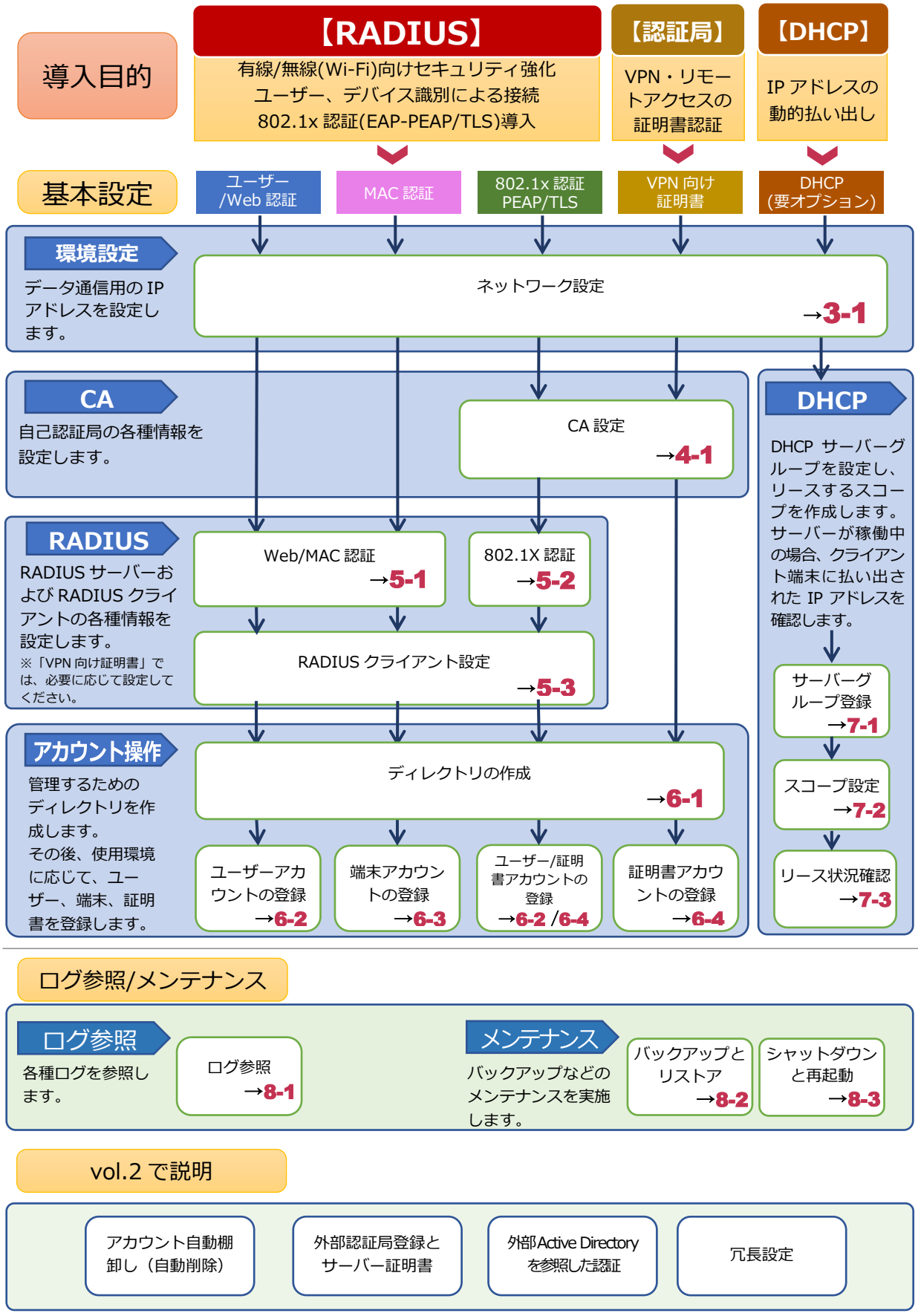
各シーンで不正端末・ユーザーの排除を実現し セキュリティを向上！



・RADIUS GUARD S V7 なら

【RADIUS】	• 様々なメーカーの無線やスイッチと認証環境の構築が可能
【認証局】	• クライアント証明書の発行と管理、配布フローが標準実装
【DHCP】	• 認証とDHCPを1台の筐体で実現
【管理機能】	• 自動棚卸しやワークフローなどの管理負担軽減機能が多数

基本設定の流れ


導入目的
【RADIUS】
有線/無線(Wi-Fi)向けセキュリティ強化
ユーザー、デバイス識別による接続
802.1x 認証(EAP-PEAP/TLS)導入
【認証局】
VPN・リモートアクセスの証明書認証
【DHCP】
IP アドレスの動的払い出し
基本設定
ユーザー/Web 認証
MAC 認証
802.1x 認証 PEAP/TLS
VPN 向け証明書
DHCP (要オプション)
環境設定
データ通信用の IP アドレスを設定します。
ネットワーク設定 →3-1
CA
自己認証局の各種情報を設定します。
CA 設定 →4-1
DHCP
DHCP サーバーグループを設定し、リースするスコープを作成します。サーバーが稼働中の場合、クライアント端末に払い出された IP アドレスを確認します。
サーバーグループ登録 →7-1
スコープ設定 →7-2
リース状況確認 →7-3
RADIUS
RADIUS サーバーおよび RADIUS クライアントの各種情報を設定します。
※「VPN 向け証明書」では、必要に応じて設定してください。
Web/MAC 認証 →5-1
802.1X 認証 →5-2
RADIUS クライアント設定 →5-3
アカウント操作
管理するためのディレクトリを作成します。
その後、使用環境に応じて、ユーザー、端末、証明書を登録します。
ディレクトリの作成 →6-1
ユーザーアカウントの登録 →6-2
端末アカウントの登録 →6-3
ユーザー/証明書アカウントの登録 →6-2 /6-4
証明書アカウントの登録 →6-4
ログ参照/メンテナンス
ログ参照
各種ログを参照します。
ログ参照 →8-1
メンテナンス
バックアップなどのメンテナンスを実施します。
バックアップとリストア →8-2
シャットダウンと再起動 →8-3
vol.2 で説明
アカウント自動棚卸し（自動削除）
外部認証局登録とサーバー証明書
外部Active Directoryを参照した認証
冗長設定

1 セットアップ

RADIUS GUARD S V7 を設置する場合は、次の通り設置して管理ツールにログインしてください。

1-1 RADIUS GUARD S V7 の簡易構成図

Tips
初期出荷時の IP アドレスは【192.168.0.1/24】に設定されています。初期化を行った場合も同様です。
仮想版の場合は、各手順書を参照のうえ IP アドレスを設定し、到達性を確保した端末より操作ください。

RADIUS GUARD S V7 は、次のように構成されます。セットアップ時はブラウザ操作が可能な設定用端末を用意し、RADIUS GUARD S V7 と通信可能な状態を準備ください。

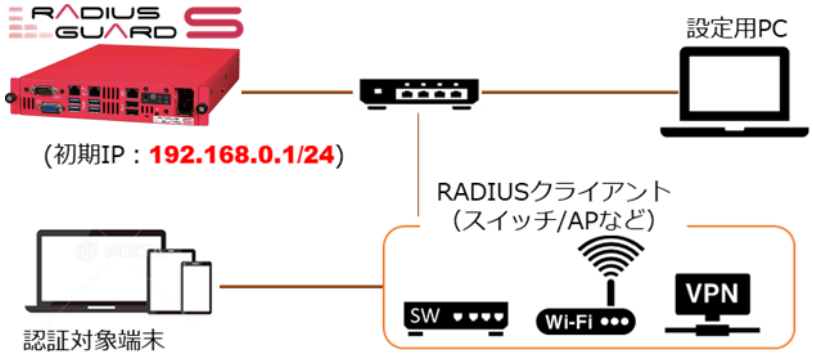
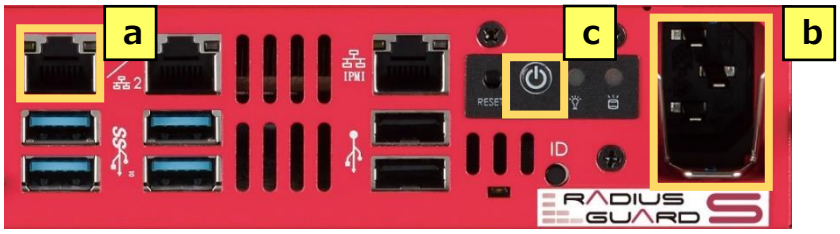


図 1

Tips
電源ケーブルを接続すると、RADIUS GUARD S V7 が自動で起動し、電源ランプが緑色に点灯します。

1-2 電源ケーブルを接続する

はじめに、RADIUS GUARD S V7 の LAN1 ポートと、端末またはスイッチを LAN ケーブルで接続します（a）。次に、電源ケーブルのメス側を RAIDUS GUARD S V7 の電源ケーブル挿入口に接続し（b）、電源ケーブルのオス側をコンセントに接続します。



注意：
ディスクを積んだサーバーアプライアンスのため、電源切断時にはシャットダウン手続きが必要となります。

・8-3：【シャットダウン】
・電源ボタン

のいずれかでシャットダウンを行ってください。

（c）は電源ボタンです。管理端末を接続せずにシャットダウンする場合は電源ボタンを短押し（1 秒以内）します。

管理ツールにログインする

設定用 PC で Web ブラウザを起動し、次の URL にアクセスします。

http://<RADIUS GUARD S V7 の IP アドレス>:8080/manager

ログイン画面が表示されるので、ログイン ID とパスワードを入力し（a）、「ログイン」ボタンをクリックします（b）。はじめてログインする場合、次の初期ログイン ID と初期パスワードを入力してください。

初期ログイン ID：*naadmin*　　初期パスワード：*naadmin*

Tips
ライセンス認証を実施していない場合は、自動的にライセンス認証の画面が表示されます。ライセンスは納品証書もしくは検証用ライセンスとして提供されます。

2 メイン画面の構成

Web MAC 802.1x VPN DHCP

RADIUS GUARD S V7 の管理ツールは、本機の各種設定およびアカウントの管理を行います。また、ログの参照やバックアップなど、メンテナンスも実施できます。

2-1 管理ツール画面の構成

RADIUS GUARD S V7 の管理ツールは、次のような 3 ペインで構成されています。

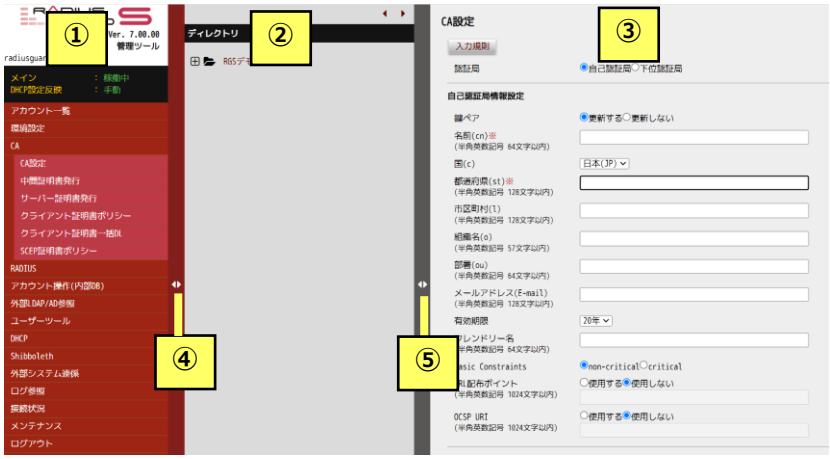
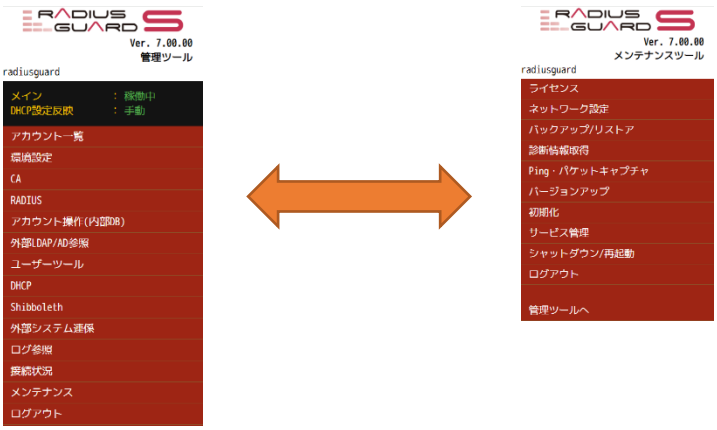


表 1

	項目名	内容
①	管理メニュー	管理ツールで利用できる機能が、種類別に表示されています。選択すると、右ペインに設定項目が表示されます。
②	ディレクトリ	アカウントを管理するディレクトリがツリー構造で表示されます。ディレクトリを選択すると、そのディレクトリに保存されているアカウントを操作できます。
③	設定画面	管理メニューで選択した設定項目やアカウント情報が表示されます。
④、⑤	各ペインの開閉ボタン	クリックすることで、各ペインの表示と非表示を切り替えます。

2-2 メンテナンスツールへの切り替え

メニューの中には、クリックするとメンテナンスツールに切り替わるものがあります。
メンテナンスツールでは、ネットワーク設定といった本機の基本的な設定や、ライセンス登録、バージョンアップなど、本機のメンテナンスに必要な設定ができます。
メンテナンスツールの「**管理ツールへ**」のリンクをクリックすると、管理メニューに戻ることができます。



3 環境設定

Web MAC 802.1x VPN DHCP

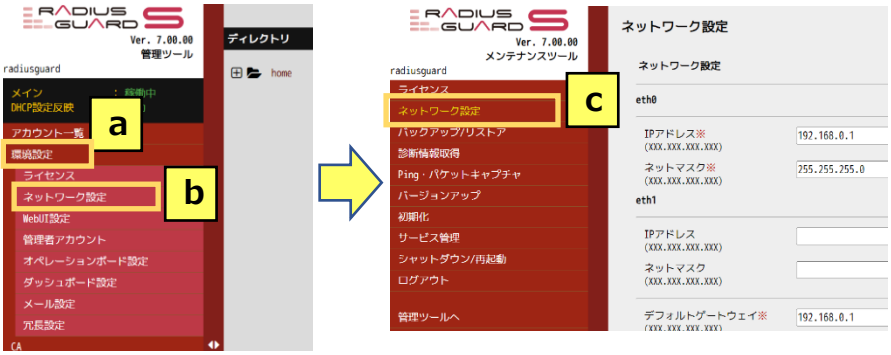
環境設定では、データ通信用の IP アドレス、時刻の設定などのサーバー情報を設定します。

3-1 ネットワーク設定

管理メニューの「**環境設定**」をクリックし (a)、「**ネットワーク設定**」を選択します (b)。メンテナンスツールメニューに切り替わるので、「**ネットワーク設定**」をクリックします (c)。

Tips

メイン 1 台に対し、最大 19 台のレプリカとの同期が可能です。また、DHCP 機能では、プライマリ 1 台に対し、セカンダリ 1 台との冗長構成ができます。
→参照『簡単セットアップガイド（vol.2)』の「4 冗長設定」



「ネットワーク設定」画面が表示されます。この画面で、自機のインターフェースの IP アドレス、サブネットマスク、デフォルトゲートウエイなどの情報を設定し、画面下部の「**登録**」ボタンをクリックすると登録されます。

Tips

RADIUS GUARD S V7 で 2 つのインターフェースに IP アドレスを設定する場合、“eth1”にも同様にアドレスを設定します。
主にバックドア的な管理アクセス等に使用可能となります。

表 2

	項目名	初期値	内容
①	IP アドレス	空欄	サーバーに割り当てる IP アドレス
②	ネットマスク	空欄	サブネットマスク
③	ゲートウェイ	空欄	デフォルトゲートウエイ

その他設定：本画面では次の項目も設定できます

- ホスト名/DNS サーバー/NTP サーバー/Syslog/SNMP/SSH

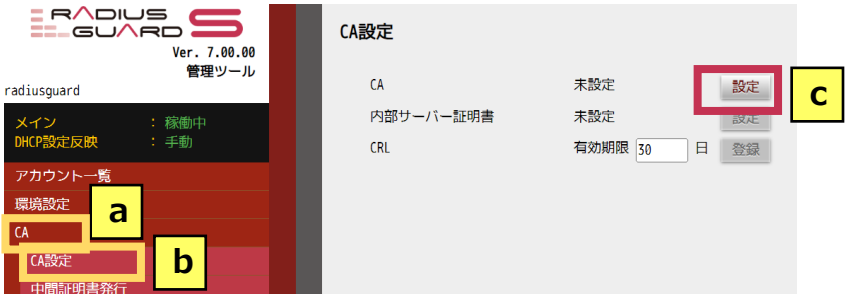
4 CA：認証局

802.1x VPN

証明書の発行や 802.1x 認証（EAP-PEAP/TLS 等）に必要な認証基盤の構築に必要な CA の設定を行い、認証局として構成します。

4-1 CA 設定

管理メニューで「**CA**」をクリックし（a）、「**CA 設定**」を選択します（b）。「CA 設定」画面が表示されるので、「CA」の「**設定**」ボタンをクリックします（c）。



CA を登録する画面が表示されます。認証局の種類、認証局の名称、国名などの情報を設定し、画面下部の「**登録**」ボタンをクリックすると、設定が登録されます。

表 3

	項目名	初期値	内容
①	認証局	自己認証局	「**自己認証局**」を選択
②	名前※	空欄	認証局の名称を入力
③	国	日本	国名を選択
④	都道府県※	空欄	都道府県名を入力
⑤	有効期限	10 年	※推奨 20 年
⑥	CRL 配布ポイント	使用する	**TLS 認証の場合、“使用しない”を選択**
⑦	OCSP URI	使用する	**TLS 認証の場合、“使用しない”を選択**

Tips

CA として設定完了後は、このメニューより、CA 証明書のダウンロードが可能となります。

Tips

1 度設定した認証局情報を変更すると、CA の構成情報が更新され、過去に発行した証明書が利用できなくなるので注意が必要です。

その他設定：本画面では次の項目も設定できます

- 下位認証局設定(CSR 作成、上位/下位 CA 証明書登録)により、既存の CA の配下として動作させることも可能です。

5 RADIUS

Web MAC 802.1x

RADIUS 設定では、接続する認証方式に合わせた設定を行います。複数の認証方式を同時に利用することも可能です。RADIUS 設定を変更した場合、RADIUS サービスの再起動が行われます。

下記のように、各サービスの動作を定義する変更が行われた場合、サービスの再起動をともなった設定反映が必要です（a）。この再起動により接続済みの端末などへの通信断は発生しません。約数秒ほど認証サービスの応答が停止します。

5-1 Web/MAC 認証時の RADIUS 設定

Web MAC

管理メニューで「**RADIUS**」をクリックし（a）、「**RADIUS 設定**」を選択します（b）。Web/MAC 認証の場合、認証サーバー証明書で「使用しない」を選択し、画面下部の「**登録**」ボタンをクリックします。表示されるすべての確認メッセージの「**OK**」ボタンをクリックすると、設定が登録されます。

Tips
主に PAP、CHAP、MS-CHAPv2 等の認証方式を利用する場合、初期設定で動作し、認証動作が可能です。

表 4

	項目名	初期値	内容
①	RADIUS ポート番号	1812	
②	RADIUS Accounting	使用しない	
③	認証サーバー証明書	使用しない	PAP/CHAP 認証では使用しません

その他設定：本画面では次の項目も設定できます

- MAC アドレスの区切り文字、パスワードチェック、ログ設定(拡張)

5-2 802.1X 認証時の RADIUS 設定 802.1x

主に EAP-PEAP や EAP-TLS 認証を行う場合の RADIUS 設定となります。802.1X 認証には証明書の利用が必要なため、RADIUS 設定前に、4:CA 設定を行ってください。

EAP-PEAP　＝　ユーザー認証
EAP-TLS　＝　証明書認証

となります。

Tips
Windows や iOS にクライアント証明書をインストールする方法などの代表的な設定例は別途ガイドとして公開しておりますので参照ください。

管理メニューで「**RADIUS**」をクリックし（a)、「**RADIUS 設定**」を選択します（b)。802.1X 認証の場合、認証サーバー証明書で「**内部サーバー証明**」を選択し、認証局の情報を設定します。設定完了後、画面下部の「**登録**」ボタンをクリックし、表示されるすべての確認メッセージの「**OK**」ボタンをクリックすると、設定が登録されます。

Tips
自 CA からサーバー証明書を取得する場合は、“内部サーバー証明書”、外部の CA からサーバー証明書を取得する場合は“外部サーバー証明書”となりますが、外部サーバー証明書を利用する場合、先にメニューの【RADIUS】-【外部認証局】より、CSR を作成し、外部サーバー証明書を登録してください。登録後に選択が可能となります。

スタートアップガイド Vol2 参照

表 5

	項目名	初期値	内容
①	RADIUS ポート番号	1812	
②	RADIUS Accounting	使用しない	
③	認証サーバー証明書	使用しない	「**内部サーバー証明書**」を選択
④	認証局	すべてチェックなし	「**内部認証局**」を選択
⑤	IEEE802.1X 認証	すべてチェックなし	「**EAP-TLS**」「**PEAP**」を選択

その他設定：本画面では次の項目も設定できます

- 他の認証局で発行された証明書を利用するための外部認証局の追加、認証時の詳細動作、ログ出力のカスタマイズなどが可能となります。

5-3 RADIUS クライアント設定 Web MAC 802.1x

802.1X 認証、または Web/MAC 認証の RADIUS 設定ができたら、RADIUS クライアントを登録します。

管理メニューで「**RADIUS クライアント**」をクリックします（a)。「**RADIUS クライアント**」タブを選択し（b)、「**新規登録**」ボタンをクリックします（c)。

「RADIUS クライアント登録」画面が表示されます。RADIUS クライアントのクライアント ID、IP アドレス、シークレットキーなどの情報を設定し、画面下部の「**登録**」ボタンをクリックします。表示される確認メッセージの「**OK**」ボタンをクリックすると、設定が登録されます。

Tips

RADIUS クライアントの登録は“登録用サンプルファイル”を利用して CSV ファイルによる一括登録も可能です。

表 6

	項目名	初期値	内容
①	クライアント ID	空欄	任意名称。「**radius_client**」を入力
②	IP アドレス	空欄	RADIUS クライアントの IP アドレス
③	シークレットキー	空欄	RADIUS クライアントと共通のキー設定

Tips

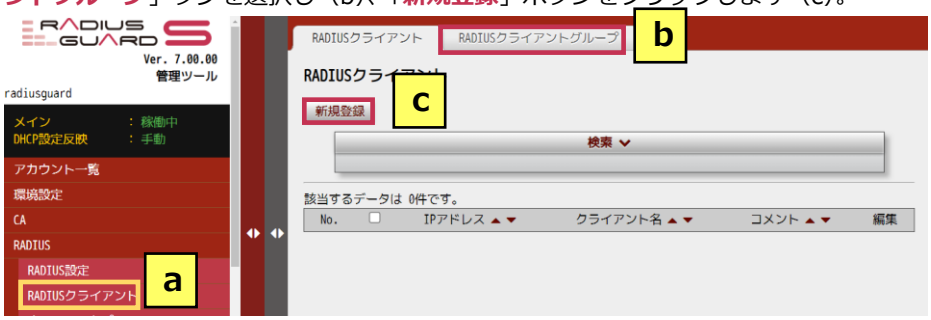
RADIUS クライアント時の IP アドレスは、ホスト指定もしくは、サブネット指定が可能です。

RADIUS クライアントの登録が完了すると、「**設定が変更されています**」というメッセージが表示されるので、「**RADIUS 設定反映**」ボタンをクリックし（a)、表示されるメッセージの「**OK**」ボタンをクリックします。管理メニューの「**RADIUS クライアント**」をクリックすると（b)、登録した RADIUS クライアントが表示されます（c)。

5-4 RADIUS クライアントグループ設定 Web MAC 802.1x

複数の RADIUS クライアントをグループ化します。グループ化することで、グループごとに設定を変更できます。

管理メニューで「**RADIUS クライアント**」をクリックします（a)。「**RADIUS クライアントグループ**」タブを選択し（b)、「**新規登録**」ボタンをクリックします（c)。



「RADIUS クライアントグループ登録」画面が表示されます。RADIUS クライアントグループの名称、グループに登録する RADIUS クライアントなどの情報を設定し、画面下部の「**登録**」ボタンをクリックします。表示される確認メッセージの「**OK**」ボタンをクリックすると、設定が登録されます。

表 7

	項目名	初期値	内容
①	名称	空欄	RADISU クライアントグループの名称
②	RADIUS クライアント	空欄	グループに登録する RADIUS クライアントを左側のリストボックスで選択、「»」ボタンをクリックして右側のリストボックスに移動

6 アカウント

Web MAC 802.1x VPN

各アカウントを追加する場合、まずアカウントを保存するためのディレクトリを作成し、その中に必要な種類のアカウントを登録します。登録可能なアカウント数の上限はライセンス数となります。

Tips
ここで作成するディレクトリは、様々なポリシーや動作の基準となる入れ物となります。
このため、ディレクトリの作成は運用ポリシー単位等で作成することが推奨されます。

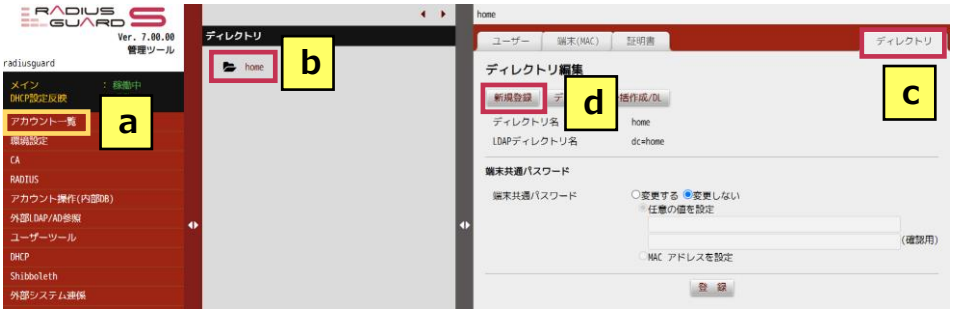
例：
VPN 用証明用
本社無線（某 SSID 用）
　等

6-1 ディレクトリの作成

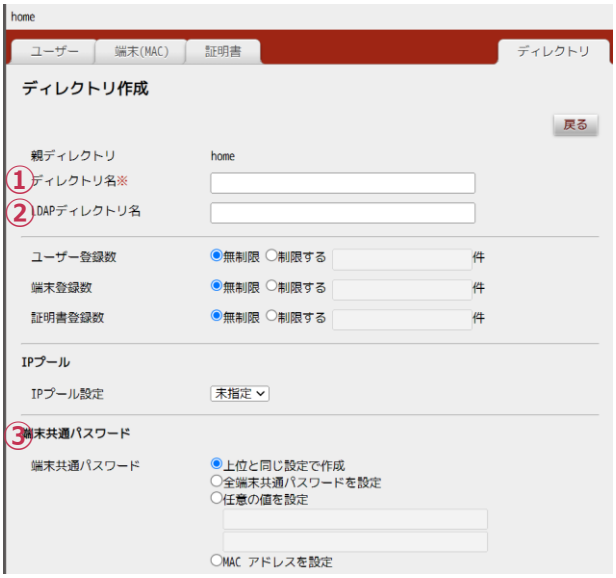
Web MAC 802.1x VPN

ディレクトリは、親ディレクトリとして「**home**」が用意されています。この配下にアカウントを管理するためのディレクトリを作成します。
はじめてディレクトリを作成するときは、管理メニューで「**アカウント一覧**」をクリックし（a）、ディレクトリツリー内の「**home**」をクリックします（b）。「**ディレクトリ**」タブをクリックし（c）、「**新規登録**」ボタンをクリックします（d）。

Tips
ディレクトリは CSV ファイルによる一括作成も可能です。詳しくは「6-5-1 ディレクトリの一括作成」を参照してください。



「ディレクトリ作成」画面が表示されます。ここで、作成するディレクトリ名や端末共通パスワードの情報を設定し、画面下部の「**登録**」ボタンをクリックします。表示される確認メッセージの「**OK**」ボタンをクリックすると、ディレクトリが作成されます。



Tips
“端末共通パスワード”は MAC 認証時に認証問い合わせのパスワード項目の内容を設定します。RADIUS クライアントの仕様と合わせて設定します。

表 8

	項目名	初期値	内容
①	ディレクトリ名	空欄	「任意のディレクトリ名」を入力
②	LDAP ディレクトリ名	空欄	ディレクトリ名のアルファベット表記を推奨
③	端末共通パスワード	空欄	MAC 認証利用時のパスワードを設定

6-2 ユーザーアカウントの登録 Web 802.1x

主にユーザーID/パスワードの形式で認証問い合わせが行われる Web 認証、EAP-PEAP 認証などの場合に利用するユーザーアカウントを登録します。

登録したいディレクトリ名を選択後、登録画面を表示させるため、「**ユーザー**」タブをクリックし（a)、「**新規登録**」ボタンをクリックします（b)。

「アカウント登録」画面が表示されます。ここでは、ユーザーID などの各種情報と接続に必要なパスワードを設定します。画面下部の「**登録**」ボタンをクリックし、表示される確認メッセージの「**OK**」ボタンをクリックすると、選択しているディレクトリにユーザーアカウントが登録されます。

表 9

	項目名	初期値	内容
①	ユーザーID	空欄/必須	登録する「**ユーザーID**」を入力
②	パスワード	空欄/必須	登録する「**パスワード**」を入力

その他設定：アカウント管理の便利な機能

RADIUS GUARD S は各アカウントの管理業務を軽減する多数の機能を実装しています。

・定期インポート機能・・・指定サーバー上の一括登録ファイルを定期取得
・自動削除機能・・・最終認証日時からの経過時間でアカウントを自動で無効・削除
・ディレクトリ管理者・・・ディレクトリ内のアカウント改廃が可能な管理者設定

Tips

ユーザーアカウントは CSV ファイルによる一括登録も可能です。
→参照「6-5-2 ユーザーアカウント、端末アカウント、証明書アカウントの一括登録」

Tips

アカウント登録時の各項目は任意にカスタマイズすることが可能です。必要な項目を追加したり削除したりすることができます。

6-3 端末アカウントの登録 MAC

Tips
MAC認証では、問い合わせ元となる RADIUS クライアント側と問い合わせ時のフォーマットを合わせる必要があります。

MAC アドレスによる問い合わせが行われる MAC 認証で利用する端末アカウントとして MAC アドレスを登録します。
まず、登録画面を表示させるため、「**端末(MAC)**」タブをクリックし（a)、「**新規登録**」ボタンをクリックします（b)。

Tips
端末アカウントは CSV ファイルによる一括登録も可能です。
→参照「6-5-2 ユーザーアカウント、端末アカウント、証明書アカウントの一括登録」

Tips
MACアドレスの入力で、ハイフンやコロンの入れ忘れなどでは自動補正、明らかな入力ミスには入力ミスの内容を表示する「入力サポート」機能が利用できます。

「アカウント登録」画面が表示されます。ここでは、端末の MAC アドレスを設定します。
画面下部の「**登録**」ボタンをクリックし、表示される確認メッセージの「**OK**」ボタンをクリックすると、選択しているディレクトリに端末アカウントが登録されます。

表 10

	項目名	初期値	内容
①	MAC アドレス	空欄	使用する端末の「**MAC アドレス**」を入力

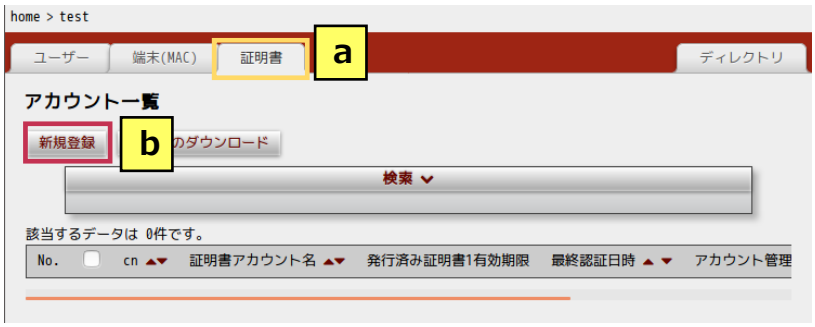
Tips
RADIUS クライアントが複数ベンダーの場合や、区切り文字入りで問い合わせされる場合、【RADIUS 設定】において、区切り文字除去や、パスワードを無視する動作を指定可能です。

MAC 認証時の注意について：
MAC 認証をご利用の場合、認証問い合わせ元となる RADIUS クライアント側で問い合わせ時のフォーマットを確認し、12 桁の区切り文字のない【aabbccddeeff】形式を選択してください。パスワードに設定される情報が【MAC アドレス】/【任意文字列】のいずれかを確認し、ディレクトリ登録時に設定する端末共通パスワードに設定します。

6-4 証明書アカウントの登録

802.1x VPN

クライアント証明書の発行が可能な証明書アカウントを登録します。主に TLS 認証や、VPN でのデバイス認証などに利用可能なクライアント証明書が発行可能です。
まず、登録画面を表示させるため、「**証明書**」タブをクリックし（a)、「**新規登録**」ボタンをクリックします（b)。

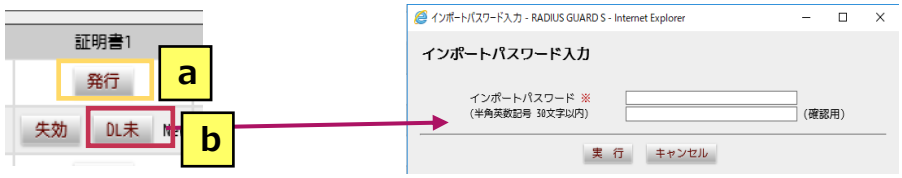


「アカウント登録」画面が表示されます。ここでは、証明書に関する情報や証明書アカウントを設定します。画面下部の「**登録**」ボタンをクリックし、表示される確認メッセージの「**OK**」ボタンをクリックすると、選択しているディレクトリに証明書アカウントが登録されます。

表 11

	項目名	初期値	内容
①	cn	空欄	証明書に設定する「**CN 名**」を入力

一覧ページに、追加された証明書アカウントが表示されます。「発行」ボタンをクリックする（a）か、処理を選択し証明書を発行後、クライアント証明書として発行することが可能となります。「DL 未」ボタンをクリックする(b)と、インポートに使用するパスワード入力が要求されます。



Tips

証明書アカウントは CSV ファイルによる一括登録も可能です。
→参照「6-5-2 ユーザーアカウント、端末アカウント、証明書アカウントの一括登録」

Tips

証明書アカウントを作成し、発行可能なクライアント証明書は PKCS#12 形式でダウンロード可能となります。
利用端末には、ダウンロードした管理者が配布する他に、ユーザーツール機能を利用し、ブラウザからのダウンロード配布を行うことも可能です。

Tips

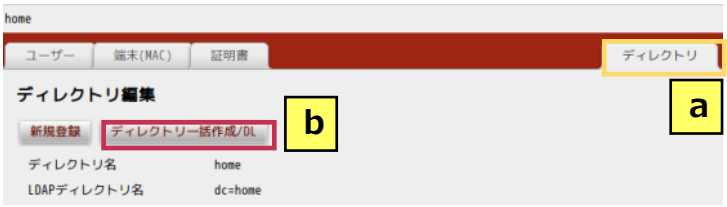
「アカウント一覧」画面で証明書のチェックボックスにチェックを付け、「操作」で PEM 形式または DER 形式を選択することで、それぞれの形式の証明書をダウンロードできます。

6-5 CSV による一括登録

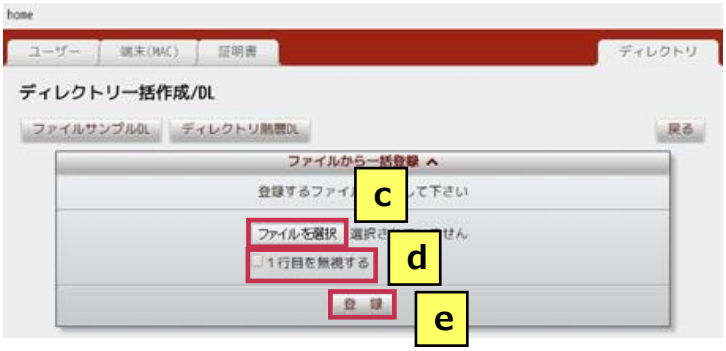
ディレクトリ、ユーザーアカウント、端末アカウント、証明書アカウントは、それぞれ指定フォーマットのテキストファイルで一括登録できます。

6-5-1 ディレクトリの一括作成

「**ディレクトリ**」タブをクリックし（a)、「ディレクトリ編集」画面で「**ディレクトリー括作成/DL**」ボタンをクリックします（b)。



「ディレクトリー括作成/DL」画面が表示されます。「**ファイルを選択**」ボタンをクリックし（c)、指定フォーマットのテキストファイルを選択します。テキストファイルに項目名行（ヘッダー）を含めている場合は、「**1 行目を無視する**」にチェックを付けます（d)。「**登録**」ボタンをクリックすると（e)、テキストファイルの内容が登録されます。



6-5-2 ユーザーアカウント、端末アカウント、証明書アカウントの一括登録

登録するディレクトリ名を選択後、「**ユーザー**」「**端末**」「**証明書**」のそれぞれのタブをクリックし（a)、「**新規登録**」ボタンをクリックします（b)。本操作は各アカウント種別で共通の手順となります。

「アカウント登録」画面が表示されます。
「**登録用サンプルファイル ダウンロード**」ボタンをクリックし（c)、ダウンロードした登録用サンプルファイルを編集します。

「**一括登録**」ボタンをクリックし（d)、「一括登録」画面を表示します。
「**ファイルを選択**」ボタンをクリックし（e)、編集した登録用サンプルファイルを選択します。編集した登録用サンプルファイルに項目名行（ヘッダー）を含めている場合は、「**1行目を無視する**」にチェックを付けます（f)。「**登録**」ボタンをクリックすると（g)、編集した登録用サンプルファイルの内容が登録されます。

Tips
登録済みのユーザーID、MACアドレス、cn を上書きする場合は、「存在するアカウント情報を上書きする」にチェックを付けます。

7 DHCP

DHCP

RADIUS GUARD S V7 を DHCP サーバーとして動作させることができます。本設定を実施するには事前に DHCP オプション（別途有償ライセンス）が必要となります。RADIUS GUARD S V7 は認証サービスと併用して、最大 5 万 IP アドレスまで払い出し可能な DHCP サーバーとして動作させることが可能です。

最大 5 万 IP アドレスの払出には、払い出し処理が瞬間最大 500 件リクエスト/秒以下となる環境が条件です。リース時間は 6 時間以上を推奨します。

7-1 サーバーグループ登録

Tips
RADIUS GUARD S は最大 10 セットまで、統合管理対象として配下に納めることが可能です。

DHCP サーバーとして動作させるには、はじめに RADIUS GUARD S V7 を DHCP サーバーグループに登録します。
管理メニューで「**DHCP**」→「**サーバーグループ**」の順にクリックし、「**サーバーグループ登録**」ボタンをクリックします。
「サーバーグループ登録」画面が表示されるので、DHCP サーバーの情報を設定します。
画面下部の「**登録**」ボタンをクリックすると、設定されます。

表 12

	項目名	初期値	内容
①	グループ名	空欄	任意のサーバーグループの名前を入力
②	プライマリサーバー番号	01	
③	プライマリIP アドレス	空欄	「**自機の eth0 の IP アドレス**」を設定

Tips
冗長構成を構築する場合、もう 1 台の RADIUS GUARD S を指定します。先に【冗長設定】を行う必要があります。
→参照『簡単セットアップガイド（vol.2)』の「4 冗長設定」

7-2 スコープ設定

払い出しを行うセグメントをスコープとして設定します。
管理メニューで「**DHCP**」→「**スコープ設定**」の順にクリックし、「**新規登録**」ボタンをクリックします。
「スコープ設定登録」画面が表示されます。画面上部の各設定項目で、グループ名やネットワークアドレスなど、スコープに関する情報を設定します。

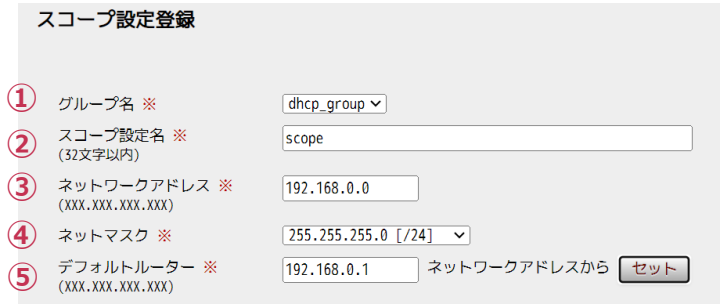


表 13

	項目名	初期値	内容
①	グループ名	先頭に登録されたグループ名	7-1 で設定したグループ名を選択
②	スコープ設定名	空欄	任意のスコープ設定名を入力
③	ネットワークアドレス	空欄	払い出すネットワークアドレスを入力
④	ネットマスク	255.255.255.0 [/24]	サブネットマスクを選択
⑤	デフォルトルーター	空欄	デフォルトルートアドレスを設定

Tips
払い出し時に設定するオプション項目は標準で用意されている以外に、【オプション定義】から個別で追加することが可能です。

画面下部に移動し、払い出す IP アドレスの範囲、除外する IP アドレスの範囲を設定します。「払出」または「除外」を選択し、IP アドレスの範囲を入力したら、「**セット**」ボタンをクリックします。

表 14

	項目名	初期値	内容
①	「払出」「除外」	払出	払出または除外を選択
②	IP アドレス	空欄	払出また除外する IP アドレスの範囲を入力
③	「セット」	-	設定した内容を保存

スコープ設定の登録が完了すると、「**設定が変更されています**」というメッセージが表示されるので、「**DHCP 設定反映**」ボタンをクリックし(a)、表示されるメッセージの「**OK**」ボタンをクリックします。

Tips
「DHCP 設定反映」をクリックすることで DHCP の設定情報を反映し、DHCP サーバーの再起動を行います。

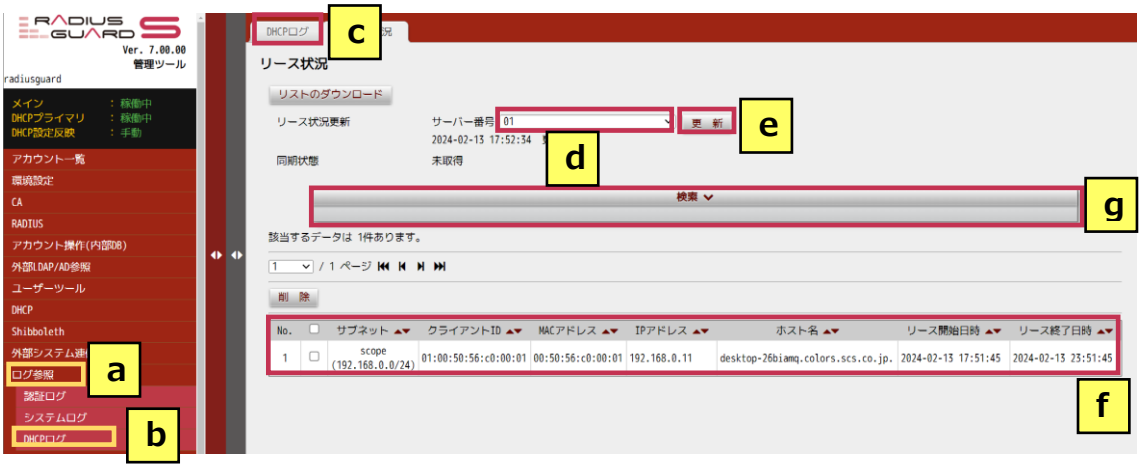
管理メニューの「**DHCP プライマリ**」が「**稼働中**」になっていることを確認し（b)、追加されたスコープが一覧に表示されていることを確認します（C)。

その他設定：本画面では次の項目も設定できます

- スコープ設定では、登録済みの MAC アドレスにしか払い出さない【端末登録】を行うことでスコープ毎に払い出し条件を指定することが可能です。

7-3 リース状況確認

IP アドレスのリース状況を確認するには、管理メニューの「**ログ参照**」をクリックし(a)、「**DHCP ログ**」を選択します（b)。
「**リース状況**」タブをクリックすると（c)、「リース状況」画面が表示されます。
「**サーバー番号**」で確認するサーバー番号を選択し（d)、「**更新**」ボタンをクリックすると（e)、払い出された IP アドレスが表示されます（f)。検索条件を指定して検索することも可能です。(g)



7-4 端末(MAC アドレス)登録

Tips
常に同じ IP アドレスを払い出す動作や、「端末の払出条件」の設定により、登録済み MAC アドレスにのみ払い出すフィルタ的な動作が可能となります。

RADIUS GUARD S V7 を DHCP サーバーとして利用するとき、端末(MAC アドレスを)登録し、「**スコープ設定**」→「**端末の払出条件**」と合わせて設定することで下記の運用が可能となります。

・登録済みの MAC アドレスにしか IP アドレスを払い出さない
・指定した IP アドレスを払い出す

特定の端末に IP アドレスを払い出すため、MAC アドレスを登録します。
管理メニューで「**DHCP**」→「**登録端末一覧**」の順にクリックし、「**新規登録**」ボタンをクリックします。
「登録端末登録」画面が表示されます。画面上部の各設定項目で、グループ名やスコープ名など、登録端末に関する情報を設定します。

	項目名	初期値	内容
①	サーバーグループ名	空欄	7-1 で作成したサーバーグループを選択
②	スコープ名	空欄	7-2 で作成したスコープを選択
③	MAC アドレス	空欄	任意の MAC アドレスを設定
④	IP アドレス	指定しない	登録端末へ払い出す固定 IP アドレスを設定

登録端末の設定後、スコープ設定後と同様に「**DHCP 設定反映**」の操作を行います。

Tips

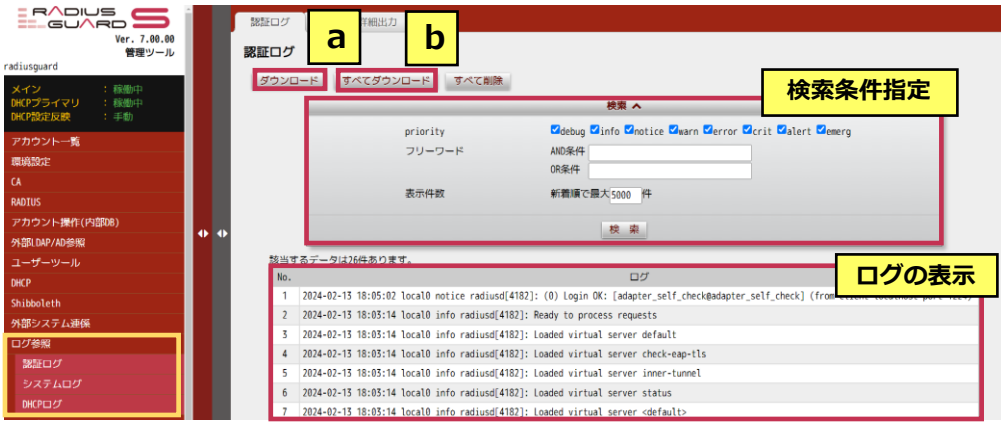
④で選択されているスコープ設定に「固定 IP 自動割当」の範囲が設定されている場合に「IP アドレス取得」ボタンをクリックすると、未使用の IP アドレスが取得され、テキストボックスに表示されます。

8 ログ参照/メンテナンス

8-1 ログ参照

Tips
機器内部に保持可能なログはそれぞれ 1 ヶ月分もしくは 500 万件までとなります。遡ったログの保存が必要な場合、Syslog サーバーへの転送を行ってください。

RADIUS GUARD S V7 では、管理メニューの「**認証ログ**」「**システムログ**」「**DHCP ログ**」のいずれかを開くと、各種ログを参照できます。
ログをダウンロードする場合、表示されているログだけをダウンロードする場合は「**ダウンロード**」を選択し (a)、すべてのログをダウンロードするには「**すべてダウンロード**」をクリックします（b)。



8-2 バックアップとリストア

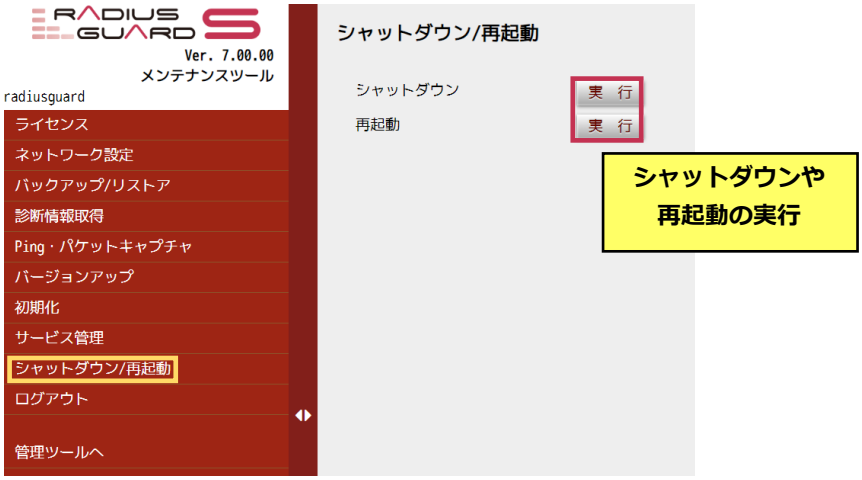
Tips
バックアップファイルには、
・設定情報
・アカウント情報
・ライセンス情報
が含まれます。ファームウェアは含まれず、同一バージョンにおいてリストアが可能となります。
ハードウェア版/VA 版で相互にバックアップファイルは利用可能です。

RADIUS GUARD S V7 では、メンテナンスツールの「**バックアップ/リストア**」をクリックすると、RADIUS GUARD S V7 で設定している内容のバックアップ、バックアップしたデータのリストアを実施できます。

稼働中の RADIUS GUARD S V7 は 1 日 1 回、自動バックアップ（毎日 0:30）が行われ、7 世代までバックアップファイルが自動生成されております。保存先は外部 USB メモリ、ローカルディスクと外部サーバーへのアップロードが可能です。

8-3 シャットダウンと再起動

RADIUS GUARD S V7 をシャットダウンや再起動する場合、メンテナンスツールの「**シャットダウン/再起動**」を開いて実行します。シャットダウンと再起動を実行するボタンが用意されているので、目的のボタンをクリックします。



Tips

機器を停止する場合、本体の電源ボタンを押すか、このメニューからシャットダウン処理を行ってください。

9 仕様

製品仕様 / 機能一覧（アプライアンス版、仮想アプライアンス版共に、製品機能は共通です。）

RADIUS GUARD S V7 製品仕様

	機能名	機能説明
機能一覧	管理可能アカウント数	200 / 500 / 2,500 / 5,000 / 10,000 / 50,000 / 200,000 （同一筐体のまま、最大 200,000 アカウントまで拡張可能）
	RADIUS クライアント登録数	最大 10,000 エントリ （ネットワークアドレスによる登録可）
	ユーザー/端末/証明書アカウント管理機能	ユーザー/端末/証明書アカウントを管理する機能（作成、編集、一括インポート/エクスポート/証明書ダウンロード、MAC アドレス自動取得、ユーザー/端末/証明書アカウント自動削除、パスワード有効切れフォロー通知メール）
	認証機能（RADIUS）	認証クライアント（無線 AP 等）からの認証要求に対して、認証結果を応答する機能（ネットワーク属性管理、RADIUS プロキシ、外部参照含む）802.1x・Web・MAC 認証に対応（PAP/CHAP/MS-CHAPv1/MS-CHAPv2/EAP-MD5/EAP-MSCHAPv2/EAP-TLS/EAP-TTLS/PEAP）
	自己認証局機能（CA）	証明書を管理する機能（CA 証明書ダウンロード、自己サーバー証明書発行、外部サーバー証明書発行、外部認証局証明書インポート、証明書発行/失効ログ出力、失効リスト公開、下位認証局）
	ユーザーツール	ユーザー/端末/証明書アカウント登録申請・編集・削除ワークフロー、証明更新、端末情報自動収集、ゲスト ID 自動発行、パスワード期限切れ通知、パスワード自動生成
	冗長化機能	ユーザー/端末/証明書アカウント情報や認証機能を冗長化し、可用性を向上させる機能
	外部 LDAP/AD 参照機能 ※1	外部の LDAP や Active Directory®のアカウント情報を参照して認証する機能
	内部 LDAP 登録連係機能 ※2	外部のサーバーから LDAP プロトコルで内部アカウントの情報を改廃する機能（LDAP バインド）
	WebAPI 機能 ※2	外部システムから WebAPI でアカウント情報の取得や改廃、クライアント証明書の取得を行う機能
	AD 登録連係機能 ※3	内部アカウントを Active Directory®へ登録する機能
	DHCP サーバー機能 ※4	DHCP サーバーの設定と IP アドレス払い出しを管理する機能（IP アドレス払い出し、サブネット管理、端末管理、DHCP オプション管理、DHCP 冗長化）
	DHCP 最大 IP 払い出し数	最大 50,000 IP アドレス
	DHCP 統合管理機能	最大 10 セットまで可能
	ブロックリスト機能	syslog サーバー（弊社推奨品 ※5）で受信したセキュリティログを参照し、不正通信を行なった端末のアカウントをブラックリストに自動的に登録して、認証処理において拒否を行なうセキュリティ強化機能
	SAML/Shibboleth SP 機能 ※6	RADIUS GUARD S V7 を Shibboleth 認証のスイッチ認証 SP として使用する機能。ユーザーツールのログインを Shibboleth 認証に対応する機能
	UPKI クライアント証明書配付機能 ※7	国立情報学研究所（NII）「UPKI 電子証明書発行サービス」発行のクライアント証明書を、RADIUS GUARD S V7 に取り込み、利用者ごとのダウンロードが実施可能となる機能

※1 200 および 500 ライセンスは外部 LDAP/AD 参照オプションが必要（2500 ライセンス以上はバンドル）
※2 内部 LDAP 登録連係オプションが必要 ※3 アドバンスト連係オプションが必要 ※4 DHCP オプションが必要
※5 推奨製品 エイチ・シー・ネットワークス製 Log@Adapter+（2019 年 11 月時点）
※6 Shibboleth SP オプションが必要 ※7 UPKI クライアント証明書配付オプションが必要

RADIUS GUARD S V7 VA （仮想アプライアンス版）動作環境 ※2024/2 時点 Ver7.00 の場合

VA 版動作環境※	仮想環境	VMware ESXi 6.5～（リリースバージョンによる） Nutanix, Inc.提供のAHV＋Prism Central環境 Microsoft Hyper-V 環境
	CPU	仮想 CPU を RADIUS GUARD S V7 に 4 個割り当て可能
	RAM	4GB
	HDD	60GB

RADIUS GUARD S V7 機器仕様

項　　目	詳　　細
外形寸法 （W x D x H）	200 x 350 x 42.4mm（突起物含まず）
電源仕様	100～240V（50/60Hz） 付属する電源ケーブルは、国内 AC100 V 仕様
最大消費電力	114W
重量	2.8ｋg（付属物含まず）
インターフェース	10/100/1000 BASE-T x 2
付属品	電源コード(プラグ側：NEMA 5-15P、コネクタ側：IEC60320-C13) 2m×1 外部 USB メモリ×1 、1 台設置用ラックマウント金具
EMI 規格	VCCI Class A
	※記載の情報は、RADIUS GUARD S V7 単体の情報です。

RADIUS GUARD S V7 冗長構成

「RADIUS GUARD S」本体を 2 台並べて、1U サイズにラックマウントすることが可能です。（要 2 台用ラックマウントキット）

RADIUS GUARD S V7 動作実績について

製品 Web サイトにて、連携実績情報を公開中。“scsk radius”と検索ください。RADIUS GUARD S V7 は RADIUS サーバーとして動作します。このため、RADIUS 準拠製品とであれば、参照動作が可能となります。また、一部の機器の連携設定ガイドも公開しております。

RADIUS GUARD S

お問い合わせ・資料請求　SCSK SCSK株式会社

TOP | ラインナップ・保守 | 製品仕様 | 連携製品情報 | 取扱店一覧 | 導入事例 | FAQ | トレーニング | ダウンロード

TOP > 連携製品情報

連携製品情報

RADIUS GUARDシリーズと認証連携可能な製品について、弊社では随時検証を行っております。連携実績のある主な製品について情報を掲載しております。 記載のない製品との連携実績や、最新の連携実績、詳細につきましては、弊社までお問い合わせください。動作検証のためのお貸出、技術支援も実施させて いただいております。お気軽にご相談ください。

RADIUS GUARDシリーズ 主な認証連携 検証済み製品一覧

無線LAN製品

メーカー名	確認済み製品名
ICOM	APシリーズ
アライドテレシス	NWS APシリーズ TQシリーズ
アリスタネットワークス	Cognitive Wi-Fiシリーズ
アルカテルルーセント	OmniAccessWLANシリーズ
エアロハイブネットワークス	Aerohiveシリーズ
HPE	Arubaシリーズ MSMシリーズ
NEC	QXシリーズ
NECプラットフォームズ	NAシリーズ
キーエンス	BTシリーズ　※BT-1000シリーズのEAP認証も確認済み
シスコシステムズ	Meraki(MR)シリーズ Aironetシリーズ ワイヤレスコントローラシリーズ
ジュニパーネットワークス	Mistシリーズ
D-link	DWLシリーズ

SCSK 株式会社
ネットワークセキュリティ事業本部 セキュリティプロダクト第二部
〒135-8110 東京都江東区豊洲 3-2-20 豊洲フロント
TEL：03-5859-3037
E-mail：rg-info@scsk.jp
製品 URL：https://www.scsk.jp/sp/radius/

- 記載の内容は 2024 年 2 月現在、ファームウェアバージョン　Ver7.00 のものです。

RADIUS GUARD S V7
簡単スタートアップガイド（vol.1）

2024 年 2 月 第 1 版

SCSK 株式会社
東京都江東区豊洲 3-2-20
豊洲フロント