SonicWall®
Secure Mobile Access 9.0

管理ガイド

SMA 200/400
SRA 1600/4600
SMA 500v Virtual Appliance

SONICWALL®

目次

第 1 部 はじめに

第 2 部 Secure Mobile Access の設定

第 4 部 ユーザとログの設定

第 1 部

はじめに

- このガイドについて
- Secure Mobile Access の概要

1

このガイドについて

この『*SonicWall® Secure Mobile Access 管理ガイド*』では、ネットワーク管理者を対象に、Secure Mobile Access 管理インターフェースを使用した SonicWall SMA/SRA 装置の有効化、設定、管理などを含む Secure Mobile Access (SMA) 技術の概要について説明します。

このガイドを含め、SonicWall の製品やサービスに関するドキュメントについては、「SMA ドキュメント」で最新版の有無を確認してください。

メモ：本書には、一部の国や地域ではリリースされていないプラットフォーム/バージョンに関する記述が含まれている場合があります。

表記上の規約

このガイドの表記上の規約は次のとおりです。

このガイドの表記上の規約

表記	説明
太字	フィールド、ボタン、およびタブの名前を強調します。また、ウィンドウ、ダイアログ ボックス、および画面の名前も強調します。また、ファイル名やインターフェースに入力するテキストや値にも使用されます。
斜体	技術マニュアルのタイトル、文中の特定の語、重要な用語や概念の初出を強調するために使われます。
メニュー項目 > メニュー項目	管理インターフェースで選択する複数のメニュー項目を表します。例えば、「**システム > 状況**」は「**システム**」メニューから「**状況**」ページを選択することを意味します。

2

Secure Mobile Access の概要

このセクションでは、Secure Mobile Access (SMA) の技術、概念、基本ナビゲーション要素、および標準配備ガイドラインの概要を説明します。

トピック:

SMA/SRA のハードウェアとコンポーネントの概要

SMA および SRA 装置は、特にリモート社員やモバイル社員のための単純で安全なクライアント不要のアプリケーション アクセスおよびネットワーク リソース アクセスを実現します。SMA 接続は、大規模なインストール ホストを事前に設定することなく使用できます。ユーザはどこにいても、標準のウェブ ブラウザを通じて、会社のローカル エリア ネットワーク (LAN) 上にある電子メール ファイル、イントラネット サイト、アプリケーション、およびその他のリソースに簡単かつ安全にアクセスできます。

このセクションは、次のサブセクションから構成されています。

SMA のソフトウェア コンポーネント

SMA/SRA 装置は、保護されている内部ネットワークに対し、クライアント不要で ID ベースの保護されたリモート アクセスを提供します。SMA/SRA 装置では、仮想オフィス環境を使用することで、ユーザがプライベート ネットワーク全体または個々のコンポーネント (ファイル共有、ウェブ サーバ、FTP サーバ、リモート デスクトップなどに加え、Citrix や Microsoft のターミナル サーバ上でホストされている個々のアプリケーションまで対応可能) に対して安全なリモート アクセスを行うことができます。

SMA プロトコルはクライアント不要とされていますが、一般的な SMA ポータルは、ポータルから透過的にダウンロードされるウェブ コンポーネント、Java コンポーネント、および ActiveX コンポーネントを組み合わせたものなので、ユーザは VPN クライアント アプリケーションを手動でインストールして設定しなくてもリモート ネットワークに接続できます。さらに SMA では、ユーザが Windows PC、Macintosh PC、Linux PC など多様な機器から接続できます。ActiveX コンポーネントは、ウィンドウズ プラットフォームでのみサポートされます。

管理者は、SMA のウェブベース管理インターフェースを使って、エンド ツー エンドの SMA ソリューションを提供できます。このインターフェースには、SMA ユーザ、アクセス ポリシー、認証方式、ネットワーク リソースに関するユーザ ブックマーク、システム設定などを設定する機能があります。

クライアントは、SMA のウェブベースのカスタマイズ可能なユーザ ポータルを使って、ファイルのアクセス、更新、アップロード、ダウンロードを実行できるだけでなく、デスクトップ マシンにインストールされている (またはアプリケーション サーバ上でホストされている) リモート アプリケーションを使用できます。さらにこのプラットフォームは、安全なウェブベースの FTP アクセス、ネットワーク コンピュータに似たファイル共有用のインターフェース、セキュア シェル バージョン 2 (SSHv2)、Telnet エミュレーション、VNC (仮想ネットワーク コンピューティング) および RDP (リモート デスクトップ プロトコル) のサポート、Citrix ウェブ アクセス、オフロードされたポータル (外部ウェブ サイト) のブックマーク、ウェブおよび HTTPS のプロキシ転送をサポートしています。

SMA ネットワーク拡張クライアント NetExtender は、Windows、Linux、MacOS の各プラットフォーム用スタンドアロン アプリケーションを通じて SMA ウェブ ポータルから利用できます。NetExtender スタンドアロン アプリケーションは、ユーザが仮想オフィス ポータルで「NetExtender」リンクを初めて選択したときに、クライアント システムに自動的にインストールされます。NetExtender を使用すると、エンド ユーザは複雑なソフトウェアのインストールや設定をせずにリモート ネットワークに接続し、リモート ネットワーク上のあらゆる種類のデータに、セキュリティで保護された方法でアクセスできます。NetExtender は、Vista またはそれよりも新しいウィンドウズ システムと Linux クライアントからの IPv6 クライアント接続をサポートしています。

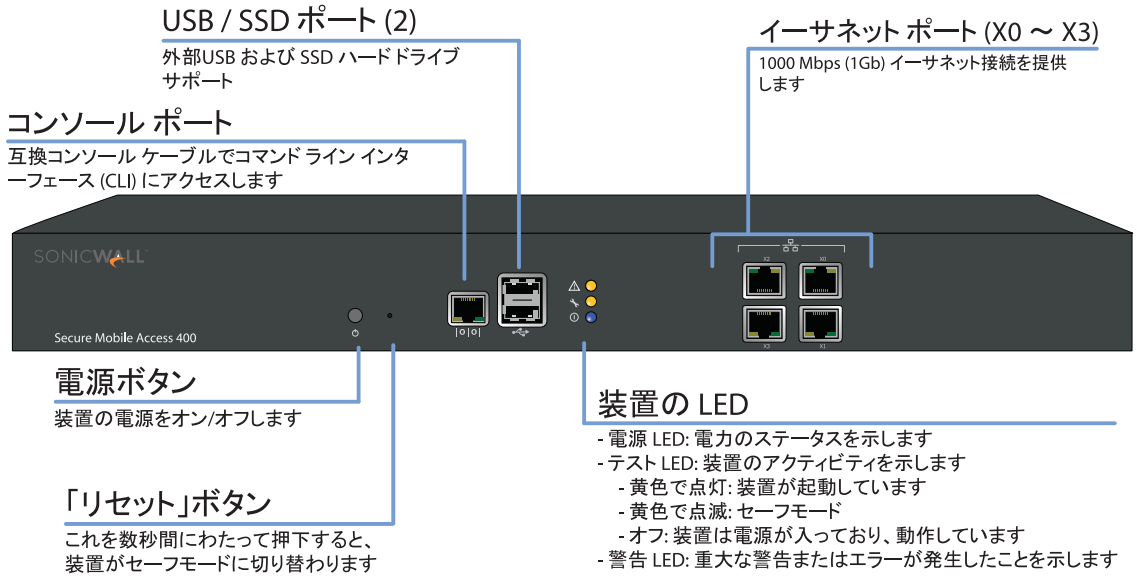
SMA ハードウェア コンポーネント

SMA 装置のハードウェア コンポーネントについては、以下のセクションの説明を参照してください。

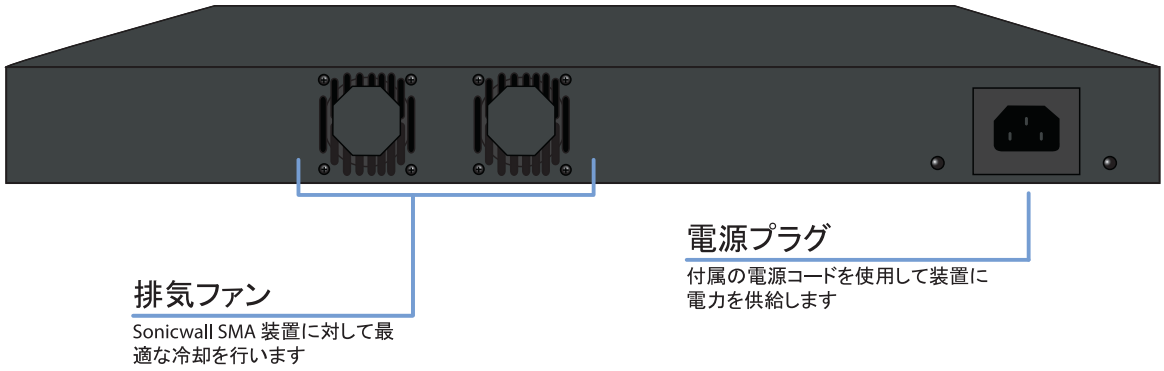
- SMA 400 の前面/背面パネルの概要 (16 ページ)
- SMA 200 の前面/背面パネルの概要 (17 ページ)

SMA 400 の前面/背面パネルの概要

フロント パネル



リア パネル



SMA 400 の前面パネルの機能

フロント パネルの機能	説明
コンソール ポート	RJ-45 ポート。シリアル接続によるコンソール メッセージへのアクセスを提供します (115200 ボー)。コマンド ライン インターフェースへのアクセスを提供します (将来的に使用)。
USB/SSD ポート	外部 USB へのアクセスおよび SSD ハード ドライブのサポートを提供します。
「リセット」ボタン	セーフモードへのアクセスを提供します。
電源 LED	SMA 400 の電源がオンかどうかを示します。

SMA 400 の前面パネルの機能 (続き)

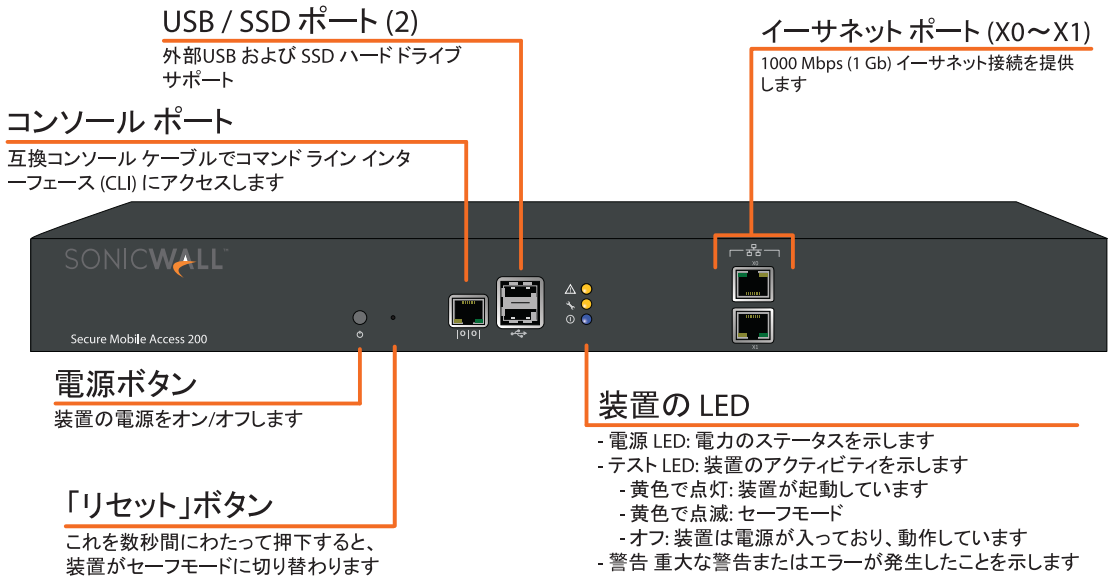
フロント パネルの機能	説明
テスト LED	SMA 400 がテスト モードであることを示します。
警告 LED	重大なエラーまたは障害が発生したことを示します。
X3	X3 インターフェースおよび SMA リソースへのアクセスを提供します。
X2	X2 インターフェースおよび SMA リソースへのアクセスを提供します。
X1	X1 インターフェースおよび SMA リソースへのアクセスを提供します。
X0	既定の管理ポート。SMA 400 とゲートウェイ間の接続を提供します。

SMA 400 の背面パネルの機能

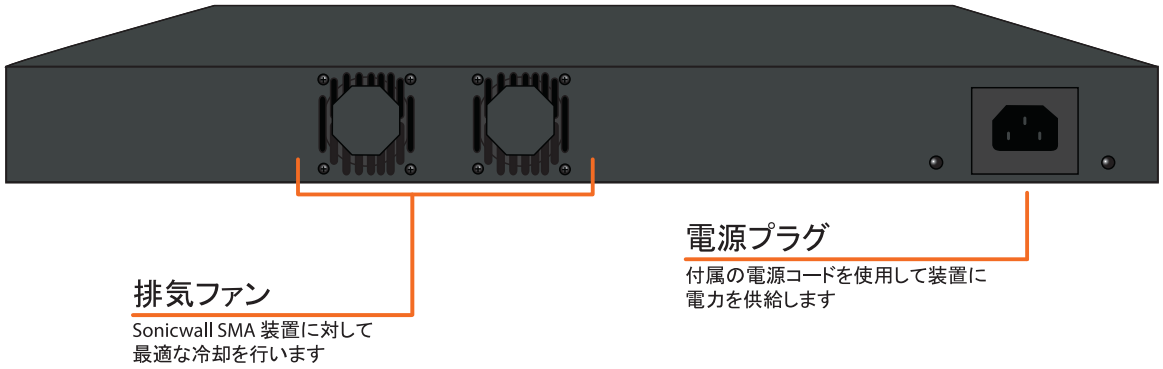
背面パネル機能	説明
排気ファン	SMA 400 装置に対して最適な冷却を行います。
電源プラグ	付属の電源コードを使用して電源と接続します。

SMA 200 の前面/背面パネルの概要

フロント パネル



リア パネル



SMA 200 の前面パネルの機能

フロント パネルの機能	説明
コンソール ポート	RJ-45 ポート。シリアル接続によるコンソール メッセージへのアクセスを提供します (115200 ボー)。コマンド ライン インターフェースへのアクセスを提供します。
USB/SSD ポート	外部 USB へのアクセスおよび SSD ハード ドライブのサポートを提供します。
「リセット」ボタン	セーフモードへのアクセスを提供します。
電源 LED	SMA 200 の電源がオンかどうかを示します。
テスト LED	SMA 200 がテスト モードであることを示します。
警告 LED	重大なエラーまたは障害が発生したことを示します。
X1	X1 インターフェースおよび SMA リソースへのアクセスを提供します。
X0	既定の管理ポート。SMA 200 とゲートウェイ間の接続を提供します。

SMA 200 の背面パネルの機能

背面パネル機能	説明
排気ファン	SMA 200 装置に対して最適な冷却を行います。
電源プラグ	付属の電源コードを使用して電源と接続します。

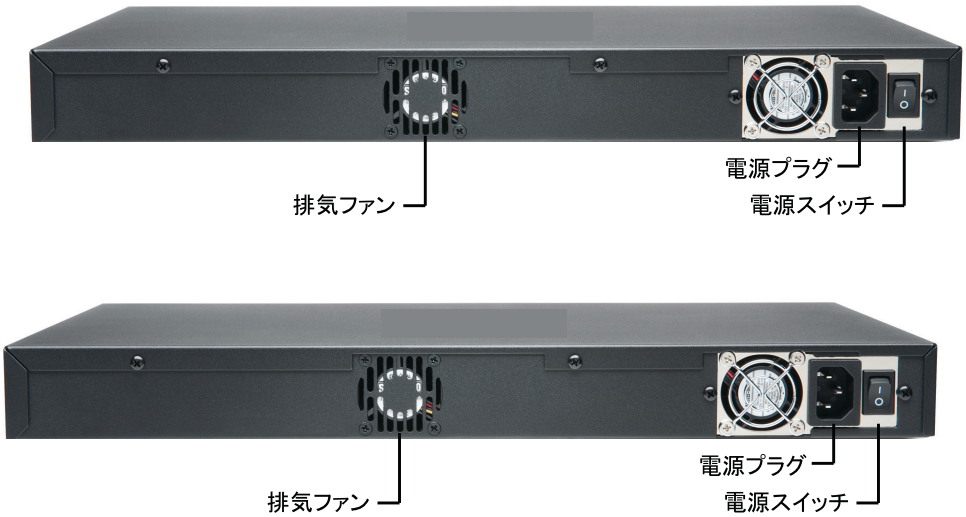
SRA ハードウェア コンポーネント

SRA 装置のハードウェア コンポーネントについては、以下のセクションの説明を参照してください。

- SRA 4600 の前面/背面パネルの概要 (19 ページ)
- SRA 1600 の前面/背面パネルの概要 (20 ページ)

SRA 4600 の前面/背面パネルの概要

SRA 4600 の前面/背面パネル



SRA 4600 の前面パネル機能

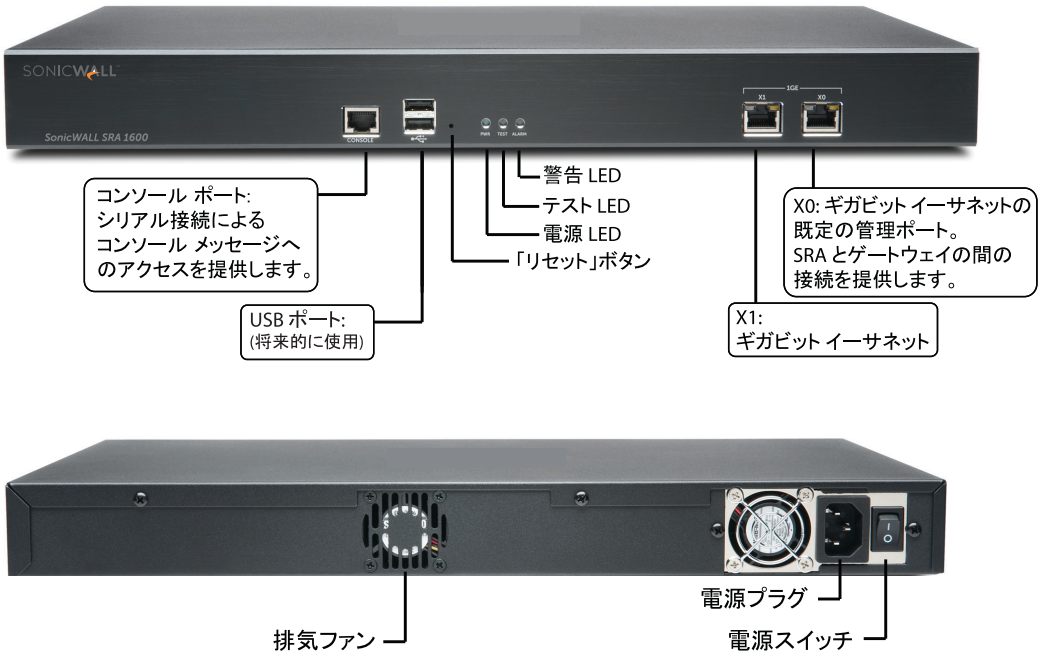
フロント パネルの機能	説明
コンソール ポート	RJ-45 ポート。シリアル接続によるコンソール メッセージへのアクセスを提供します (115200 ボー)。コマンド ライン インターフェースへのアクセスを提供します (将来的に使用)。
USB ポート	USB インターフェースへのアクセスを提供します (将来的に使用)。
「リセット」ボタン	セーフモードへのアクセスを提供します。
電源 LED	SRA 4600 の電源がオンかどうかを示します。
テスト LED	SRA 4600 がテスト モードであることを示します。
警告 LED	重大なエラーまたは障害が発生したことを示します。
X3	X3 インターフェースおよび SRA リソースへのアクセスを提供します。
X2	X2 インターフェースおよび SRA リソースへのアクセスを提供します。
X1	X1 インターフェースおよび SRA リソースへのアクセスを提供します。
X0	既定の管理ポート。SRA 4600 とゲートウェイ間の接続を提供します。

SRA 4600 の背面パネル機能

背面パネル機能	説明
排気ファン	SRA 4600 装置に対して最適な冷却を行います。
電源プラグ	付属の電源コードを使用して電源と接続します。
電源スイッチ	SRA 4600 装置の電源をオンまたはオフにします。

SRA 1600 の前面/背面パネルの概要

SRA 1600 の前面/背面パネル



SRA 1600 の前面パネル機能

フロント パネルの機能	説明
コンソール ポート	RJ-45 ポート。シリアル接続によるコンソール メッセージへのアクセスを提供します (115200 ボー)。コマンド ライン インターフェースへのアクセスを提供します (将来的に使用)。
USB ポート	USB インターフェースへのアクセスを提供します (将来的に使用)。
「リセット」ボタン	セーフモードへのアクセスを提供します。
電源 LED	SRA 1600 の電源がオンかどうかを示します。
テスト LED	SRA 1600 がテスト モードであることを示します。
警告 LED	重大なエラーまたは障害が発生したことを示します。
X1	X1 インターフェースおよび SRA リソースへのアクセスを提供します。
X0	既定の管理ポート。SRA 1600 とゲートウェイ間の接続を提供します。

SRA 1600 の背面パネル機能

背面パネル機能	説明
排気ファン	SRA 1600 装置に対して最適な冷却を行います。
電源プラグ	付属の電源コードを使用して電源と接続します。
電源スイッチ	SRA 1600 装置の電源をオンまたはオフにします。

SMA 500v Virtual Appliance

SMA 500v Virtual Appliance は、SMA ソフトウェアを VMware プラットフォームで実行する仮想マシンです。本ガイドで説明されているすべてのソフトウェア コンポーネントおよび機能は、高可用性機能と SSL オフローダを除き、SMA 500v Virtual Appliance でサポートされています。

SMA を仮想装置として配備すると、共有コンピューティング リソースを利用して、使用率を最適化し、移行を容易にし、資本コストを削減することができます。SMA 500v Virtual Appliance には、次のようなメリットがあります。

- コスト節減:
  - 複数の仮想マシンを 1 台のサーバ上で実行して、ハードウェア コスト、電力消費量、および保守費用を削減することができます。
  - Microsoft Windows サーバが不要なので、Windows ライセンスのコストが必要ありません。
- 運用しやすさ:
  - 仮想環境では、新しいサーバの使用開始、古いサーバの廃止、サーバの起動または停止を容易に行えます。
  - インストールは、ファイルを仮想環境にインポートすることによって行われるので、インストーラを実行する必要がありません。
- セキュリティ:
  - SMA 500v Virtual Appliance は、SMA/SRA ハードウェア装置に付随しているのと同じ、堅牢なオペレーティング システムを提供します。

SMA 500v Virtual Appliance を配備する前に、基本的な VMware 構造の要素を実装する必要があります。SMA 500v Virtual Appliance の配備の詳細については、以下で入手可能な『*SonicWall Inc. SMA500v Virtual Appliance 導入ガイド*』を参照してください。SMA ドキュメント

Secure Mobile Access の概念

このセクションでは、管理者が SMA/SRA 装置およびウェブベースの SMA 管理インターフェースを使用する上で理解しておく必要がある、主要な概念の概要を説明します。

- SNMP の概要 (43 ページ)
- DNS の概要 (43 ページ)
- ネットワーク ルートの概要 (43 ページ)
- NetExtender の概要 (43 ページ)
- 二段階認証の概要 (49 ページ)
- ワンタイム パスワードの概要 (52 ページ)
- エンド ポイント制御の概要 (55 ページ)
- セキュア仮想アシストの概要 (57 ページ)
- ウェブ アプリケーション ファイアウォールの概要 (73 ページ)

キャプチャ ATP 統合の概要

キャプチャ ATP (Capture Advanced Threat Protection) は、さまざまな種類のコンテンツを分析して有害な動作を見つけるクラウドベースのサービスです。Capture Advanced Threat Protection (キャプチャ ATP) を追加すると、ファイアウォールは、ファイルが悪質なものかを識別するため、そのファイルをクラウドに転送します。クラウドでは SonicWall キャプチャ ATP サービスがファイルを分析して、ウイルスなどの有害な要素が含まれるかどうかを確認します。続いてキャプチャ ATP は、結果をファイアウォールに送信します。分析と報告は、ファイルがファイアウォールによって処理されている間にリアルタイムで実行されます。

キャプチャ ATP クラウドに送信されるすべてのファイルは、暗号化された接続を経由します。ファイルの分析は数分で完了し、有害であると判定された場合を除き、削除されます。有害ファイルは、暗号化された HTTPS 接続経由で SonicWall Threats Research チームに送信され、詳細に分析されたのち、脅威に関する情報の充実に活用されます。それ以外の場所にファイルを分析用に転送することはありません。有害ファイルは、脅威に関する情報に活用した後、受信から 30 日以内に削除されます。キャプチャ ATP は、ファイル分析報告 (脅威報告) を作成して、脅威となる動作に関する詳細な情報を提供します。

管理者は、キャプチャ ATP の設定をユーザ レベル、グループ レベル、グローバル レベルで変更できます。

VPN 常時有効

VPN 常時有効 (AOV) は、SMA 9.0 でサポートされています。Windows NetExtender クライアントと連携して動作し、MSI インストーラからインストールされます。VPN 常時有効 は、リモート ユーザに継続的なネットワーク アクセスを提供します。AOV 検出はユーザ ログオン イベントによってトリガーされ、ユーザがコンピュータからログアウトすると終了します。AOV 設定はドメイン、グループ、ユーザに適用され、それらには継承関係があります。AOV モードでは、VPN CLI ツールは VPN を切断したり、プロファイルを編集したりできません。

トピック:

- 安全なネットワークの検出
- AOV 制御
- AOV ログ
- 改竄防御

安全なネットワークの検出

AOV は 安全なネットワークの検出 (SND) をサポートし、SND が検出されたときに VPN 接続を制御するために「**信頼済みネットワークに VPN を接続しない**」設定を提供します。このオプションが有効化されている場合、AOV モードで SND が検出されると VPN が自動的に切断されます。このオプションが無効化されている場合、VPN は接続されたままです。

SND に関して、VPN クライアントに適用される DNS と接尾辞は、システムの DNS および接尾辞のサブセットです。DNS または接尾辞のいずれか 1 つだけが一致する場合、それは最終的な一致として使用されます。VPN 接尾辞が設定されていない場合、少なくとも 1 つの DNS 結果に一致するものがあれば SND が確認されます。

AOV 制御

VPN 状況が「*切断*」の場合、AOV は VPN 接続が回復するまでネットワーク リソースへのユーザ アクセスを遮断できます。これは AOV オプション「**VPN が接続に失敗した場合にネットワークへのアクセスを許可する**」で制御されます。

- 有効 - ユーザはネットワークにアクセスできます。
- 無効 - VPN 接続が復旧するまで、ユーザはネットワークにアクセスできません。

ユーザは、設定された電子メールで受信したチャレンジ コードを入力することにより、AOV を一時的に無効にするよう要求できます。これは、AOV オプション「**ユーザに切断を許可する**」で制御されます。

- 有効 - ユーザは AOV を一時的に無効にでき、クライアント側にある「**ロック解除** 」ボタンをクリックしてロック解除を要求できます。
- 無効 - ユーザは AOV を無効にできず、「**ロック解除** 」も「**切断** 」ボタンも使用できません。

クライアント側で発生した問題を解決するために、SMA 管理者が常時稼働クライアントをリモートから無効にする方法があります。

- 管理者は「**クライアント > 状況**」ページに移動し、VPN セッションを選択し、「**オン**」スイッチをクリックすることで、AOV を一時的に無効にすることができます。
- AOV を無効にすると、障害ポリシーは適用されず、自動接続は確立されません。

VPN セッション制御に関して、クライアント側の NetExtender で自動再接続が有効化されているとき、管理者が手動でユーザ セッションを終了すると、クライアントは再接続を試みません。NetExtender は、VPN の切断を引き起こすネットワーク切断がある場合にのみ再接続を試みます。

AOV ログ

VPN ログ ビューアは、AOV の状況変化に関するログを保存します。ユーザは、状態が変化したことやアクションが遮断されたことをポップアップで通知され、ログに記録されている該当メッセージの履歴を見ることができます。

改竄防御

SMA NEService、インストール ディレクトリ、レジストリを保護するために改竄防御サービスが NetExtender に統合されています。

暗号化の概要

暗号化とは、データを符号化することで、不正なユーザがデータを読み取れないようにする機能です。暗号化は、インターネット経由でプライベートで安全な通信を行うための手段です。

公開鍵暗号化 (PKE) と呼ばれる特殊な暗号化では、公開鍵と秘密鍵を使用してデータを暗号化および復号化します。公開鍵暗号化では、ウェブ サイトなどの当事者が公開鍵と秘密鍵を生成します。保護されているウェブ サーバは、ウェブ サイトにアクセスするユーザに公開鍵を送信します。ユーザのウェブ ブラウザはこの公開鍵を使用して、対応する秘密鍵によって暗号化されたデータを復号化します。さらに、ユーザのウェブ ブラウザはこの公開鍵を使用してデータを透過的に暗号化することができ、このデータは保護されたウェブ サーバの秘密鍵でのみ復号化できます。

公開鍵暗号化により、ユーザはウェブ サイトの身元を SSL 証明書を通じて確認できます。ユーザが SMA/SRA 装置にアクセスした後、装置はユーザに対して、自身の暗号化情報 (公開暗号鍵を含んでいる SSL 証明書など) を送信します。

仮想プライベート ネットワーク (VPN) 用の SSL

セキュア ソケット レイヤ ベースの仮想プライベート ネットワーク (SSL VPN) では、安全な接続を通じて、アプリケーションやプライベートなネットワーク リソースにリモートからアクセスすることができます。SSL VPN を使用すると、モバイル社員、ビジネス パートナー、および顧客を会社のエクストラネットまたはプライベート LAN上にあるファイルやアプリケーションにアクセスさせることができます。

仮想プライベート ネットワーク (VPN) を使用すると、公共のネットワーク インフラストラクチャ上で安全なエンド ツー エンドのプライベート ネットワーク接続を確立することができ、通信費用を節減したり、組織内のユーザとサイトの間にプライベートで安全な接続を実現したりできます。SMA/SRA 装置はセキュア ソケット レイヤ (SSL) VPN の機能を備えており、それを使用するための特別機能ライセンス費用も必要ないため、並列的なリモート アクセス インフラストラクチャを配備するための費用効果の高い代替法となります。

SSL ハンドシェイクの手順

以下の手順は、ウェブベースの Secure Mobile Access 管理インターフェースを使用して、ユーザと SMA/SRA ゲートウェイとの間の SSL セッションを確立するために必要な標準的手順の例を示しています。

1. ユーザが SMA/SRA 装置への接続を試みると、ユーザのウェブ ブラウザは、そのブラウザがサポートしている暗号化の種類に関する情報を装置に送信します。
2. 装置はユーザに対して、自身の暗号化情報 (公開暗号鍵を含んでいる SSL 証明書など) を送信します。
3. ウェブ ブラウザはその SSL 証明書が示す認証局に基づいて、SSL 証明書の正当性を確認します。
4. ウェブ ブラウザはプリマスタ暗号化鍵を生成し、そのプリマスタ鍵を SSL 証明書内の公開鍵で暗号化し、暗号化済みのプリマスタ鍵を SMA/SRA ゲートウェイに送信します。
5. SMA/SRA ゲートウェイはこのプリマスタ鍵を使用してマスタ鍵を作成し、新しいマスタ鍵をユーザのウェブ ブラウザに送信します。
6. ウェブ ブラウザと SMA/SRA ゲートウェイは、このマスタ鍵と互いに同意した暗号化アルゴリズムを使用して、SSL 接続を確立します。この時点で、ユーザと SMA/SRA ゲートウェイは同じ

暗号化鍵を使用してデータの暗号化と復号化を行うようになります。これは対称暗号化と呼ばれます。

7 SSL 接続が確立されると、SMA/SRA ゲートウェイはウェブ ブラウザに SMA/SRA ゲートウェイ ログイン ページを暗号化して送信します。

8 ユーザは自分のユーザ名、パスワード、およびドメイン名を送信します。

9 ユーザのドメイン名を RADIUS サーバ、LDAP サーバ、またはアクティブ ディレクトリ サーバを通じて認証する必要がある場合、SMA/SRA ゲートウェイはユーザの情報を適切な認証サーバに転送します。

10 認証されたユーザは Secure Mobile Access ポータルにアクセスできるようになります。

IPv6 サポートの概要

(Windows、MacOS、Linux でサポート)インターネット プロトコル バージョン 6 (IPv6) は、ネットワーク機器でよく使われるようになっている IPv4 の後継です。IPv6 は、インターネット エンジニアリング タスク フォース (IETF) によって開発された一群の標準とプロトコルから成り、IPv4 よりも大きなアドレス空間ならびに追加的な機能とセキュリティを提供し、IPv4 の設計上の問題を解決します。IPv4 の通信に影響を与えずに IPv6 を使用することができます。

IPv6 はステートフル アドレス設定とステートレス アドレス設定をサポートしています。ステートフル アドレス設定は DHCPv6 サーバで使用されます。ステートレス アドレス設定では、リンク上のホストがそのリンクの IPv6 アドレスで自分自身を自動的に設定します。このアドレスは *リンク ローカル* アドレスと呼ばれます。

IPv6 では、送信元アドレスと送信先アドレスの長さが 128 ビット (16 バイト) です。なお、32 ビットの IPv4 アドレスは、8 ビットずつピリオドで区切られたドット 10 進表記で表現されます。128 ビットの IPv6 アドレスは 16 ビットずつコロンで区切られ、それぞれの 16 ビット ブロックは 4 桁の 16 進数として表現されます。これはコロン 16 進表記と呼ばれます。

IPv6 アドレスの 2008:0AB1:0000:1E2A:0123:0045:EE37:C9B4 は、各 16 ビット ブロックに少なくとも 1 つの数字がある限りにおいて、各ブロック内の先頭のゼロを取り除いて簡略化することができます。先頭のゼロを抑止すると、アドレスの表現は次のようになります。2008:AB1:0:1E2A:123:45:EE37:C9B4

アドレスにゼロの 16 ビット ブロックの連続シーケンスが含まれていれば、そのシーケンスを:: (2 つのコロン) として圧縮できます。例えば、リンク ローカル アドレスの 2008:0:0:0:B67:89:ABCD:1234 は、2008::B67:89:ABCD:1234 に圧縮できます。マルチキャスト アドレスの 2008:0:0:0:0:0:0:2 は、2008::2 に圧縮できます。

IPv6 接頭辞はアドレスの中でサブネット接頭辞のビットを表す部分です。IPv6 サブネット、ルート、およびアドレス範囲の接頭辞は、アドレス/接頭辞長または CIDR 表記で記述されます。例えば、2008:AA::/48 と 2007:BB:0:89AB::/64 は IPv6 アドレス接頭辞です。

Secure Mobile Access は、次の部分で IPv6 をサポートしています。

サービス

- **FTP ブックマーク** - IPv6 アドレスを使って FTP ブックマークを定義します。
- **Telnet ブックマーク** - IPv6 アドレスを使って Telnet ブックマークを定義します。
- **SSHv2 ブックマーク** - IPv6 アドレスを使って SSHv2 ブックマークを定義します。
- **HTTP/HTTPS ブックマークのリバース プロキシ** - IPv6 アドレスを使って HTTP ブックマークまたは HTTPS ブックマークを定義します。

- **Citrix ブックマーク** - IPv6 アドレスを使って Citrix ブックマークを定義します。
- **RDPブックマーク** - IPv6 アドレスを使って RDP ブックマークを定義します。
- **VNC ブックマーク** - IPv6 アドレスを使って VNC ブックマークを定義します。

メモ：ファイル共有 (CIFS) に対しては、IPv6 はサポートされていません。

設定

- **インターフェース設定** - インターフェースの IPv6 アドレスを定義します。**リンク ローカル** アドレスは「インターフェース」ページのツール チップに表示されます。
- **ルート設定** - IPv6 の送信先ネットワークとゲートウェイで静的ルートを定義します。
- **ネットワーク オブジェクト** - IPv6 を使ってネットワーク オブジェクトを定義します。IPv6 アドレスと IPv6 ネットワークを、このネットワーク オブジェクトに結び付けることができます。

NetExtender

クライアントが NetExtender に接続すると、クライアント マシンが IPv6 をサポートしていて、SMA/SRA 装置で IPv6 アドレス プールが設定されていれば、SMA/SRA 装置から IPv6 アドレスを取得できます。NetExtender は、Vista またはそれよりも新しいウィンドウズ システムと Linux クライアントからの IPv6 クライアント接続をサポートしています。

セキュア仮想アシスト

ユーザと技術者は IPv6 アドレスを使用するときにサポートを要求したり提供したりすることができます。

ルール

- **ポリシー ルール** - ユーザまたはグループのポリシー。「**ポリシーの適用先**」ドロップダウン リストには、次の 3 つの IPv6 オプションがあります。
  - IPv6 アドレス
  - IPv6 アドレス範囲

    - すべての IPv6 アドレス
- **ログイン ルール** - アドレス フィールドに IPv6 を使用します。
    - IPv6 を使って**定義済みアドレスからのログイン**を定義
    - 「**送信元アドレス**」ドロップダウン リストの 2 つの IPv6 オプション: **IPv6 アドレス** / **IPv6 ネットワーク**

仮想ホスト

管理者は仮想ホストに IPv6 アドレスを割り当て、このアドレスを使ってその仮想ホストにアクセスすることができます。

アプリケーション オフロード

管理者はアプリケーション オフロード用のアプリケーション サーバに IPv6 アドレスを割り当て、このアドレスを使ってそのサーバにアクセスすることができます。

ポータルの概要

Secure Mobile Access には、仮想オフィスと呼ばれるメカニズムがあります。これは、クライアントが組織の内部リソースに簡単にアクセスできるようにするウェブベースの*ポータル* インターフェースです。NetExtender、仮想アシスト、ファイル共有やその他のネットワーク リソースへのブックマークなどのコンポーネントは、仮想オフィス ポータルを通してユーザに表示されます。ユーザを複数のタイプに分けている組織では、SMA/SRA 装置で複数の個別化したポータルを作成して、それぞれに個別の共有リソース ブックマークを設定することができます。ポータルでは、個々のドメイン証明書やセキュリティ証明書をポータル単位で許可することもできます。ポータルのコンポーネントは、ポータルを追加するときに個別化されます。

ファイル共有

ファイル共有は、CIFS (Common Internet File System) プロトコルまたは SMB (Server Message Block) プロトコルを使用して、Microsoft ファイル共有への安全なウェブ インターフェースをリモート ユーザに提供します。ファイル共有では、Microsoft のネットワーク コンピュータやマイ ネットワークによく似たスタイルのウェブ インターフェースが採用されており、適切な権限を持つユーザがネットワーク共有を参照して、ファイルの名前変更、削除、取得、アップロードを行ったり、ブックマークを作成して後で参照したりすることができます。ファイル共有を設定することで、制限されたサーバ パス アクセスを実現することもできます。

個別ポータル

SMA/SRA 装置では、複数のポータルを作成し、それぞれに個別のタイトル、バナー、ログイン メッセージ、ロゴ、および使用可能なリソースのセットを設定できます。また、個別の仮想ホスト/ドメイン名を設定して、既定ポータルの URL を個別に作成することもできます。ユーザがポータルにログインすると、あらかじめ設定されたポータル固有のリンクとブックマークが表示されます。NetExtender を仮想オフィス ポータルに表示するかどうか、およびユーザがポータルにログインしたときに NetExtender を自動的に起動するかどうかを設定できます。管理者は、「**ポータル設定**」ウィンドウを使って、各ポータルに表示する要素を選択できます。ポータルの設定の詳細については、ポータル > ポータル (148 ページ) を参照してください。

ドメインの概要

Secure Mobile Access 環境のドメインとは、SMA/SRA 装置のサービス下のネットワークにアクセスしようとするユーザを認証するためのメカニズムです。ドメインの種類としては、Secure Mobile Access の内部にある LocalDomain と、外部プラットフォームのマイクロソフト アクティブ ディレクトリ、LDAP、および RADIUS があります。多くの組織では、1 つのドメインを使用するだけで認証機能を十分に実現できますが、大きな組織の場合は、ポータルを通じてアプリケーションにアクセスしようとするユーザの複数のノードやコレクションを扱うために、複数の分散ドメインが必要になることがあります。

アプリケーション オフロードと HTTP (S) ブックマークの概要

SMA/SRA 装置は、イントラネット内のサーバで稼動しているウェブベースのアプリケーションへのアクセスを提供するために、HTTP(S) ブックマークとアプリケーション オフロードを使用します。これは SharePoint 2007、および Microsoft OWA Premium や Domino Web Access 8.0.1、8.5.1、および 8.5.2 といった一般的に使用されるウェブ メール インタフェースの拡張版を含みます。SharePoint 2010 はアプリケーション オフロードでサポートされますが、HTTP(S) ブックマークではサポートされません。SharePoint 2013 はアプリケーション オフロードでサポートされます。プロキシ フレンドリーではないサードパーティのモジュールは、SharePoint でサポートされない場合があります。

アプリケーション オフロードと HTTP(S) ブックマークの両方が HTTP(S) リバース プロキシを使用します。リバース プロキシは、イントラネット外のリモート ユーザとイントラネット内の目標のウェブ サーバの間に配備されるプロキシサーバです。リバース プロキシは、イントラネット外から開始されるパケットをインターセプトして転送します。HTTP(S) リバース プロキシは特に HTTP(S) 要求と応答を途絶します。

アプリケーション オフロードは、内部および公開されているホストのウェブ アプリケーションへの安全なアクセスを提供します。アプリケーション オフロード ホストは、バックエンド ウェブ アプリケーションのプロキシとして機能する仮想ホストを持つ専用のポータルとして作成されます。

HTTP(S) ブックマークと異なり、オフロードされたアプリケーションへのアクセスはリモート ユーザに制限されません。管理者は特定のユーザやグループに対して強力な認証とアクセス ポリシーを強制することができます。例えば、組織では一定のゲスト ユーザは Outlook Web Access (OWA) へのアクセスに二段階認証やクライアント証明書認証が必要なこともありますが、OWA パブリック フォルダへのアクセスは許されません。認証が有効なら、オフロードされたホストにはワンタイム パスワード、二段階認証、クライアント証明書認証、シングル サイン オンといった高度な認証機能を積層することができます。

このオフロードされたアプリケーション ポータルは、適切な Secure Mobile Access ドメインを持つ仮想ホストとして設定しなければなりません。このようなオフロードされたホストに対しては、認証とアクセス ポリシーの強制を無効にすることが可能です。

ウェブ トランザクションは、ログを確認することで集中監視することができます。さらに、ウェブ アプリケーション ファイアウォールによって、クロスサイト スクリプティングや SQL インジェクションなどの予期せぬ侵入から、オフロードされたアプリケーション ホストを保護することができます。

プロキシされたページ内の URL は HTTP ブックマークや HTTPS ブックマークで使われる方法で書き換えられないので、オフロードされたウェブ アプリケーションへのアクセスはシームレスに行われます。

HTTP(S) ブックマークの利点

HTTP(S) ブックマークを使用することによって、ユーザは SharePoint 2007、Microsoft OWA Premium や Domino Web Access 8.0.1、8.5.1、および 8.5.2 ウェブ メール インターフェースの完全機能版にアクセスできます。これらのインターフェースは基本提供されるものより使いやすく、より多くの拡張機能を提供します。

アプリケーション オフロードの利点

ウェブ アプリケーションを Secure Mobile Access の HTTP(S) ブックマークとして設定するのに比べて、オフロードされたウェブ アプリケーションには次の利点があります。

- URL 書き換えが必要ないので、スループットが著しく向上する。
- 元のウェブ アプリケーションの機能がほぼ完全に維持される。それに対し、HTTP(S) ブックマークは最大努力型のソリューションである。
- アプリケーション オフロードは Secure Mobile Access のセキュリティ機能を公開ホストのウェブ サイトに拡張する。

アプリケーション オフロードは次のシナリオのいずれにも使用できます。

- SSL オフローダとして機能し、オフロードされたウェブ アプリケーションに HTTPS サポートを追加する。これには SMA/SRA 装置の SSL アクセラレーションを使用する。
- ウェブ アプリケーション ファイアウォール購読サービスと共に、オフロードされたウェブ アプリケーションに悪質なウェブ攻撃からの継続的な保護を提供する。
- 二段階認証、ワンタイム パスワード、クライアント証明書認証など、強力な認証や積層された認証をオフロードされたウェブ アプリケーションに追加する。
- グローバルなグループまたはユーザをベースにしたアクセス ポリシーを使って、オフロードされたウェブ アプリケーションへのアクセスをきめ細かに制御する。
- HTTP/HTTPS ブックマークで現在サポートされていないウェブ アプリケーションをサポートする。アプリケーション オフロードでは URL 書き換えが必要ないので、スループットに悪影響を与えずに完全なアプリケーション機能を提供できる。
- 仮想ホストとリバース プロキシを使用してウェブ アプリケーションを提供する ActiveSync アプリケーション オフローダ技術を認証する。ActiveSync 認証はシームレスにウェブ アプリケーションを提供するために URL 書き換えを使用しません。1 つの例として、ActiveSync プロトコルは ActiveSync 認証 (33 ページ) で説明されているように、携帯端末の電子メール クライアントが Exchange サーバと同期を取るために使用されます。

サポート対象プラットフォーム

装置プラットフォーム

アプリケーション オフローダと HTTP(S) ブックマークは、Secure Mobile Access 9.0 リリースをサポートするすべての SMA/SRA 装置でサポートされています。

- SMA 400
- SMA 200
- SRA 4600

- SRA 1600
- SMA 500v Virtual Appliance

HTTP バージョン

HTTP(S) ブックマークとアプリケーション オフロード ポータルは HTTP/1.0 および HTTP/1.1 の両方をサポートします。

キャッシング、圧縮、SSL ハードウェア アクセラレーション、HTTP 接続持続性、TCP 接続多重化、およびプロキシに対する転送チャンク エンコードといった、特定のパフォーマンス最適化機能は、使い方に応じて自動的に有効にされます。

アプリケーション

SharePoint 2010 および **SharePoint 2013** はアプリケーション オフロードでサポートされますが、HTTP(S) ブックマークでサポートされません。以下の機能が記載されたブラウザ上で試験され、動作確認されています。

サポートされる SharePoint 機能

SharePoint 機能	ブラウザ
アナウンスメント追加	Internet Explorer 9
アナウンスメント削除	Firefox 16.0 以降
ドキュメント ダウンロード	Chrome 22.0 以降
ドキュメント追加	
ドキュメント削除	
アイテム追加	
アイテム削除	

以下のウェブ アプリケーションは HTTP(S) ブックマークで動作し、かつ、オフロードされたアプリケーションとして動作することが試験され、確認されました。

- マイクロソフト アウトルック ウェブ アクセス 2013

  マイクロソフト アウトルック ウェブ アクセス 2010

  マイクロソフト アウトルック ウェブ アクセス 2007

  メモ: Outlook Web Access は、SMA 400/200、SRA 4600/1600、および SMA 500v Virtual Appliance プラットフォームでサポートされます。

- Windows SharePoint 2013 (アプリケーション オフローダでのみサポート)

  Windows SharePoint 2007 (アプリケーション オフローダを使用してのみサポート)

  Windows SharePoint Services 3.0

  メモ: SharePoint の統合クライアント機能はサポートされません。

- Lotus Domino Web Access 8.0.1

  Lotus Domino Web Access 8.5.1

  Lotus Domino Web Access 8.5.2

  メモ: Domino Web Access は、SMA 400/200、SRA 4600/1600、および SMA 500v Virtual Appliance プラットフォームでサポートされます。

- Novell Groupwise Web Access 7.0
- マイクロソフト Exchange 2010 ActiveSync
- マイクロソフト Exchange 2007 ActiveSync
- マイクロソフト Exchange 2003 ActiveSync

  Exchange ActiveSync は以下でサポートされます。

  - Apple iPhone
  - Apple iPad
  - Android 2.3 (Gingerbread)、4.0.x (ICS)、および 4.1 (Jelly Bean) ベースの電話機

メモ：アプリケーション オフローダでは、ActiveSync に対する認証がサポートされます。ActiveSync は携帯端末の電子メール クライアントが Exchange サーバと同期するために使われるプロトコルです。管理者はオフロードされたポータルを作成して、バックエンド Exchange サーバへのアプリケーション サーバ ホストを設定できます。その後、ユーザはこの新しいホスト名を携帯端末の電子メール クライアントで使用して、SMA/SRA 装置を通してバックエンド Exchange サーバと同期できます。

認証スキーマ

以下の認証スキーマが、アプリケーション オフロードおよび HTTP(S) ブックマークでの使用をサポートします。

- **基本** - ユーザ名とパスワードの形式で資格情報を収集します。
- **フォーム ベースの認証** - 資格情報の収集にウェブ フォームを使います。

ソフトウェア要件

アプリケーション オフロードおよび HTTP(S) ブックマーク機能の完全セットにアクセスするためには、以下のエンドユーザ要件を満たしている必要があります。

- インターネット エクスプローラ 9.0 以降
- Windows 10 および Windows 7

メモ：

- サポートされるユーザの最大数は、アクセスされているアプリケーション数と送信されているアプリケーション トラフィック量によって制限されます。
- 特定のアプリケーション　サポートに関する詳細情報については、それぞれのセクションを参照してください。

ヒント：正しいウェブ ブラウザとオペレーティング システムを使っていてもサポートされるアプリケーションが動作しない場合は、ブラウザ セッション クッキーを削除して、ブラウザのすべてのインスタンスを閉じて再度開き、ブラウザ キャッシュを消去してから、再度試行してください。

サポートされるアプリケーションの配備要件

アプリケーション オフロードと HTTP(S) ブックマークを以下のソフトウェア アプリケーションで使う場合には、これらのインストールと全体的な機能の警告を考慮してください。

- SharePoint

    - SharePoint 2013 および SharePoint 2010 はアプリケーション オフロードでサポートされますが、HTTP(S) ブックマークでサポートされません。
- Outlook Anywhere
    - アプリケーション オフローダのある SMA/SRA。
    - Outlook Anywhere で使用する Microsoft 独自の MS-RPCH プロトコルは、通常の HTTP(S) プロトコルと競合する可能性があります。

アプリケーション オフロードは SharePoint 2013 でアプリケーションが HTTP/HTTPS を利用する場合にのみサポートされます。ウェブ サービスを利用するアプリケーションに対する Secure Mobile Access のサポートは限定的であり、HTTP でラップされた HTTP 以外のプロトコルはサポートしていません。

アプリケーションはハード コードされた自己参照 URL を含めません。これらがある場合は、アプリケーション オフローダ プロキシは URL を書き換える必要があります。ウェブ サイト開発は常に HTML 標準に従うわけではないので、これらの URL を書き換える際にプロキシは最善の変換を行うことしかできません。ホスティング サーバが別の IP またはホスト名に移動するときは常にコンテンツ開発者がウェブ ページを編集する必要があるため、ウェブ サイトの開発時にハード コードされた、自己参照 URL の指定は推奨されません。

例えば、バックエンド アプリケーションが以下のように URL 内にハード コードされた IP アドレスとスキーマを持つ場合、アプリケーション オフローダは URLを書き換える必要があります。

```
<a href="http://1.1.1.1/doAction.cgi?test=foo">
```

これはアプリケーション オフローダ ポータルの「**自己参照 URL の URL 書き換えを有効化する**」設定を有効にすることで実行可能ですが、ウェブ アプリケーションがどのように開発されたかによって、必ずしもすべての URL を書き換えることはできない場合があります(この制限は通常、リバース プロキシ モードを用いる他のベンダと同様です)。

クロス ドメイン シングル サインオン

外部ウェブサイト ブックマークをアプリケーション オフローダ ポータルに対して作成して、ユーザに対して単一ポイントのアクセスを可能にできます。これにより、ユーザはメイン ポータルにログインした後に、アプリケーション オフローダ ポータルに自動的にサイン インすることが可能になります。

クロス ドメイン シングル サインオン (SSO) を使用するには:

1. 最初に 2 つ以上のポータルを、同一の共有ドメイン (仮想ホスト ドメイン名から) を使って、認証を必要とするように作成します。ポータルの 1 つは通常のポータルである必要があります。これらのポータルも同じ SMA/SRA 装置のドメインにあるので、ユーザは同じ資格情報でログインできます。ポータルの追加 (149 ページ) で、ポータルの作成方法を説明しています。
2. ユーザ ブックマークの追加または編集 (409 ページ) で説明しているように、ポータルにログインしてブックマークを作成します。
3. 外部ウェブ サイト (423 ページ) で説明しているように、サービスを「**外部ウェブ サイト**」に設定します。
4. 「**自動的にログインする**」を選択して、このブックマークに対するクロス ドメイン SSO を有効にします。
5. ホストを指定します。このホストは同一の共有ドメイン名のポータルです。
6. ブックマークを保存して開始します。この新しいポータルには、認証情報無しで自動的にログインされます。

この共有ドメイン名は必ずしも一致する必要はなく、サブドメインでも動作します。例えば、1 つのポータルが仮想ホスト ドメイン名 "www.example.com" の通常ポータルで、その共有ドメイン名が "example.com" で、もう 1 つのポータルの仮想ホスト ドメイン名が "intranet.eng.example.com" で共有ドメイン名が ".eng.example.com" の場合です。xyz.eng.example.com へのブックマークが www.example.com ポータル内に作成された場合、".eng.example.com" は ".example.com" のサブドメインなので、クロス ドメイン SSO は動作します。

ActiveSync 認証

アプリケーション オフローダが、ActiveSync に対する認証をサポートするようになりました。アプリケーション オフローダ技術は、ウェブ アプリケーションに仮想ホストとリバース プロキシの使用を提供します。ユーザは今までどおり、バックエンド ウェブ アプリケーションにアクセスする前に SMA/SRA 装置で認証を受ける必要があります。しかし、プロキシはシームレスにウェブ アプリケーションを提供するために URL 書き換えを使用しません。

ActiveSync は携帯端末の電子メール クライアントが Exchange サーバと同期するために使われるプロトコルです。管理者はオフロードされたポータルを作成して、バックエンド Exchange サーバへのアプリケーション サーバ ホストを設定できます。その後、ユーザはこの新しいホスト名を携帯端末の電子メール クライアントで使用して、SMA/SRA 装置を通してバックエンド Exchange サーバと同期できます。

メモ: iOS 6.1.2 より前のバージョンを搭載する iPhone/iPad 上では、カレンダーに繰り返しの招待が含まれる場合、初期アカウント同期が失敗する可能性があります。

メモ: Exchange Server のセキュリティを向上するため、匿名での ActiveSync アクセスは将来サポートされなくなります。

ActiveSync は、「**ポータル > ウェブ アプリケーションをオフロードする > オフロード > セキュリティ設定**」ページで管理します。

ActiveSync 認証を設定するには、「**認証制御を無効にする**」をオフにして、認証に関するフィールドを表示させます。「**ActiveSync 認証を有効にする**」をオンにして、既定のドメイン名を入力します。この既定のドメイン名は、電子メール クライアントの設定内にドメイン名が設定されている場合は使用できません。

ActiveSync ログ エントリ

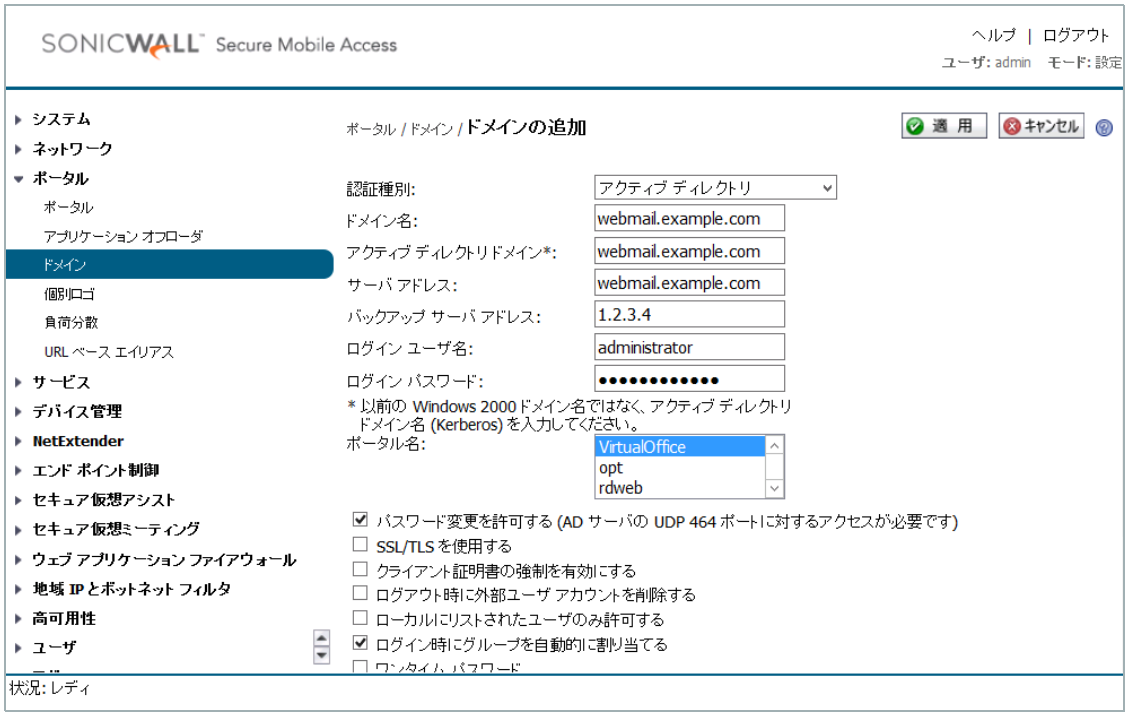
ウェブ アプリケーションがオフロードされている場合は「**ログ > 表示**」ページが更新されます。ほとんどのモバイル システム (iPhone、Android など) で ActiveSync がサポートされています。これらのログ エントリは、クライアントがいつオフロードされたポータルを通して ActiveSync の使用を開始したかを表示します。ActiveSync メッセージは、ActiveSync リクエストに対して、クライアントがアカウントをセットアップしてリクエストがデバイス ID を含んでいない場合を除いて、デバイス ID (ActiveSync: Device ID is...) を表示します。

メモ：Exchange サーバ内のユーザの資格情報は、SMA/SRA 装置内のものと同じである必要があります。装置内のそれぞれのドメインに対して多くの認証種別が利用可能です。ローカル ユーザ データベースを使用している場合は、ユーザ名とパスワードを Exchange サーバ上のものと同じにしてください。幸いなことに、それ以外のアクティブ ディレクトリのような認証種別は、Exchange サーバと SMA/SRA 装置の両方で認証情報を共有できます。しかしながら、認証情報を共有する認証種別を使う認証には時間がかかり、最初の ActiveSync リクエストがタイムアウトすることがあります。認証が成功すると、セッションが構築されて、他のリクエストに再度の認証は不要になります。

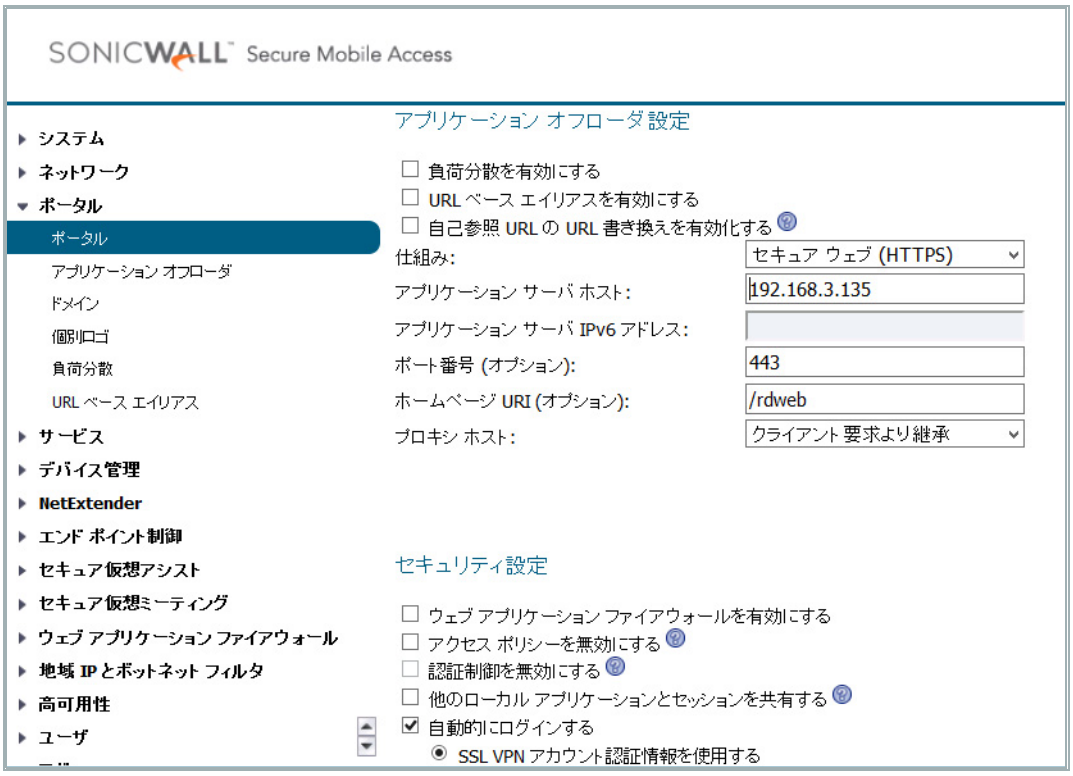
Android デバイスからの電子メールを確認するようにポータルを設定する

下記の例は、Android デバイスを使って電子メールを確認するために ActiveSync を設定する手順を示します。例の中のエントリは、あなたの環境に合わせて書き換えて、また注意深く正しいパスワードを入力してください。これを行わないと、アカウントはブロックされます。

1 「webmail.example.com」という「**ドメイン名**」でドメインを作成します。「**アクティブ ディレクトリ ドメイン**」と「**サーバ アドレス**」に「webmail.example.com」を設定します。「**ポータル名**」を「VirtualOffice」に設定します。



2 Secure Mobile Access 管理インターフェースで、関連セクションまで下にスクロールし、「**sales**」という名前でオフロード ポータルを作成します。



3 「**仕組み**」に「**セキュア ウェブ (HTTPS)**」を設定します。

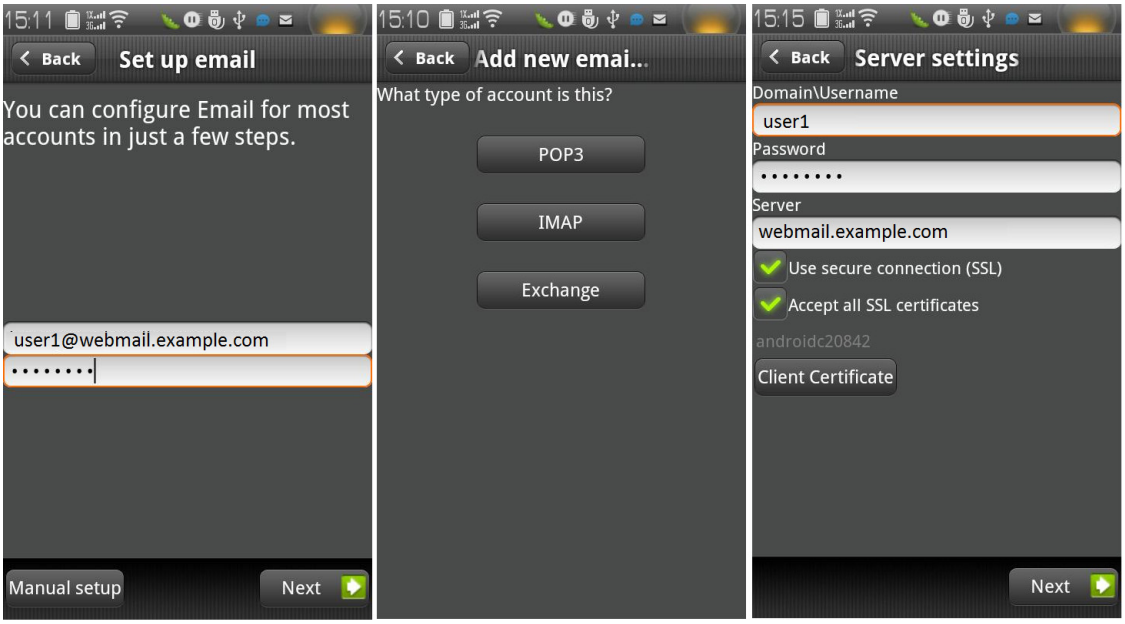
4 Exchange サーバの「**アプリケーション サーバ ホスト**」を設定します (例:*webmail.example.com*)。

5 仮想ホスト名を設定します (例:*webmail.example.com*)。仮想ホスト名は DNS サーバで解決できる必要があります。できない場合は、Android 端末内の hosts ファイルを編集します。

6 「**電子メール クライアント認証を有効にする**」を選択します。「**既定のドメイン名**」は空白のままにするか、「webmail.example.com」と入力します。

7 「**仮想ホスト**」タブを選択します。

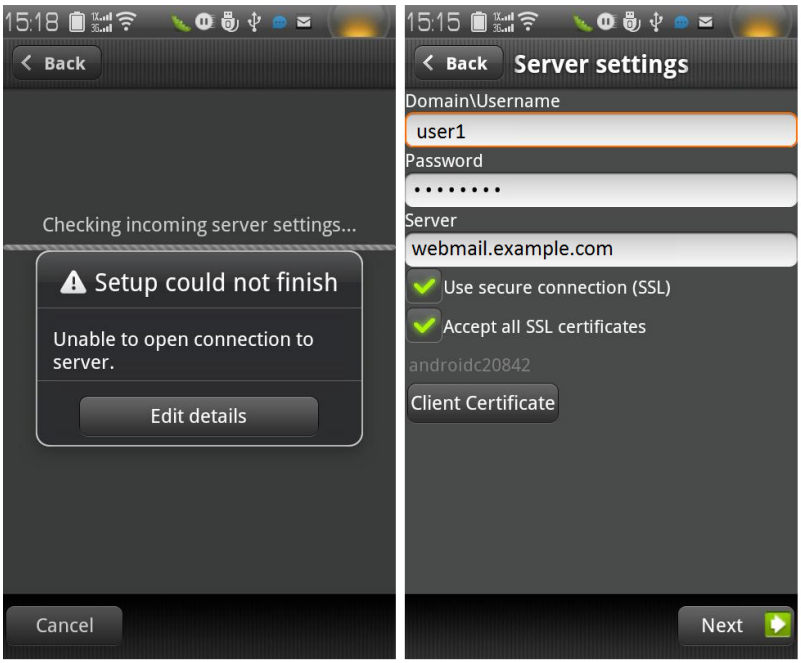
8 Android 端末を起動して、電子メール アプリケーションを開き、電子メール アドレスとパスワードを入力します。「**次へ**」を選択します。



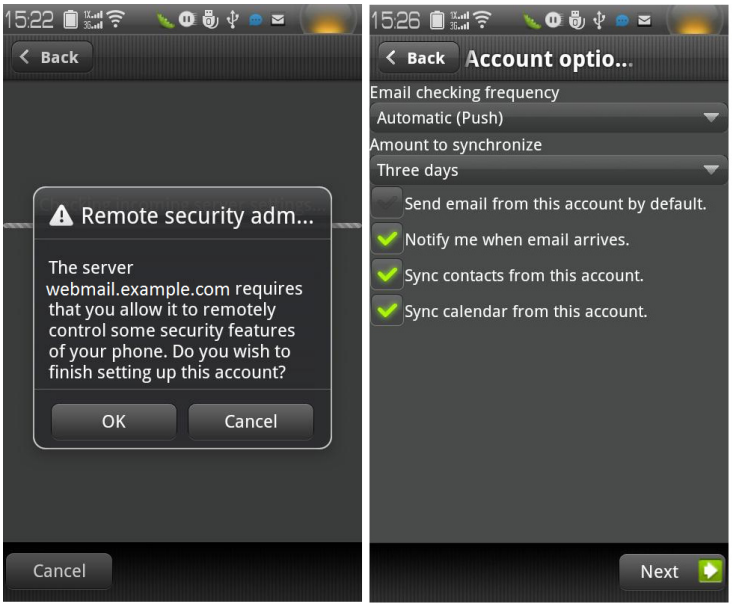
9 「**Exchange**」を選択します。

10 あなたの「**Domain\Username**」、「**Password**」、「**Server**」を入力します。ドメイン名は表示されず、オフロードされたポータルの設定内に指定された既定のドメイン名が使用されます。「**Accept all SSL certificates**」を選択して「**Next**」を選択します。

11 AD 認証がタイムアウトした場合、「**Setup could not finish**」メッセージが表示されます。20 秒くらい待ってから再試行します。Secure Mobile Access のログを見て、ユーザが正しくログインしたかどうか確認することもできます。AD 認証が高速の場合は、この問題はまず発生しません。



12 認証が終了すると、セキュリティ警告が表示されます。「**OK**」を選択して継続し、アカウント設定を編集して「**Next**」を選択します。



13 電子メールの送受信を試行して、ActiveSync エントリが Secure Mobile Access のログに含まれることを確認します。

ネットワーク リソースの概要

ネットワーク リソースとは、SMA/SRA 装置を使用してアクセスできる信頼済みネットワークの、細かいレベルのコンポーネントです。管理者がネットワーク リソースを事前定義してユーザまたはグループにブックマークとして割り当てることもできれば、ユーザが自分用のネットワーク リソースを定義してブックマークを作成することもできます。

以下のセクションでは、SMA/SRA 装置でサポートされる各種のネットワーク リソースについて説明します。

HTTP (ウェブ) およびセキュア HTTPS (ウェブ)

SMA/SRA 装置は、内部ネットワーク、インターネット、またはその装置が到達できるその他の任意のネットワーク セグメント上の HTTP または HTTPS サーバに対するプロキシ アクセスを提供します。リモート ユーザは HTTPS を使用して SMA/SRA 装置と通信し、URL を要求します。SMA/SRA 装置は HTTP 経由でその URL を取得します。URL は必要に応じて変換され、暗号化されてリモート ユーザに返されます。

Secure Mobile Access 管理者は、ユーザが HTTP(S) リバース プロキシ サポートを使って Microsoft OWA Premium、Windows SharePoint 2007、Novell Groupwise Web Access 7.0、または Domino Web Access 8.0.1、8.5.1、および 8.5.2 などのウェブベースのリソースとアプリケーションにアクセスできるように、ウェブ (HTTP) またはセキュア ウェブ (HTTPS) ブックマークを設定できます。リバース プロキシ ブックマークはまた、HTTP 1.1 プロトコルと接続持続性をサポートします。

SMA 400 装置および SRA 4600 装置の HTTPS ブックマークでは、最大 2048 ビットの鍵がサポートされます。

SMA/SRA 装置では、HTTP(S) キャッシュがサポートされています。このキャッシュは、装置がリモート ユーザとローカル ウェブ サーバの間に配備されるプロキシ ウェブ サーバとして機能しているときに使用されます。プロキシは、内部ウェブ サーバが HTTP(S) プロトコルの仕様に基づいてキャッシュ可能と見なす HTTP(S) コンテンツを SMA/SRA 装置上にキャッシュすることができます。それ以降の要求に関しては、ユーザが SMA/SRA 装置で認証されており、アクセス ポリシーによってアクセスが許可されていることが確認された場合に限り、キャッシュされたコンテンツが返されます。ただし、Secure Mobile Access では、バックエンド ウェブ サーバへのトラフィックを、同一ウェブ サーバに対する複数のユーザ セッションで単一の TCP 接続が使用されるように、TCP 接続の多重性を用いて最適化します。キャッシュは主に、JavaScript ファイル、スタイルシート、イメージなどの静的ウェブ コンテンツに使用されます。プロキシは無限の長さの HTML/JavaScript/CSS ドキュメントを解析できます。管理者は、キャッシュの有効と無効の切り替え、キャッシュされたコンテンツのフラッシュ、およびキャッシュの最大サイズの設定を行うことができます。

SMA/SRA 装置がローカル ウェブ サーバから受け取ったコンテンツは、*gzip* を使って圧縮されてから、インターネット経由でリモート クライアントに送信されます。装置から送信されるコンテンツを圧縮することで、帯域幅が節約され、それによってスループットが向上します。しかも、圧縮されたコンテンツのみがキャッシュされるので、必要なメモリのほぼ 40 ～ 50% が節約されます。gzip 圧縮は、SMA/SRA 装置のローカル (クリア テキスト側)、またはリモート クライアントからの HTTPS 要求には利用できないことに注意してください。

Telnet

Telnet クライアントは、リモート ユーザのウェブ ブラウザを介して提供されます。リモート ユーザがアクセス可能な Telnet サーバの IP アドレスを指定すると、SMA/SRA 装置がそのサーバへの接続を確立します。SSL 経由のユーザとサーバの通信は、ネイティブ Telnet を使用してプロキシ接続されます。

SSHv2

SSH クライアントは、リモート ユーザのウェブ ブラウザを介して提供されます。リモート ユーザがアクセス可能な SSH サーバの IP アドレスを指定すると、SMA/SRA 装置がそのサーバへの接続を確立します。SSL 上のユーザとサーバ間の通信は、ネイティブに暗号化された SSH を使用してプロキシが行われます。SSHv2 の暗号化は SSHv1 よりも強力であり、それ以外にも高度な機能を備えていますが、SSHv2 をサポートするサーバにしか接続できません。

FTP (ウェブ)

内部ネットワーク、インターネット、または SMA/SRA 装置が到達できるその他の任意のネットワーク セグメント上の FTP サーバに対するプロキシ アクセスです。リモート ユーザが HTTPS を使用して SMA/SRA 装置と通信し、URL を要求すると、SMA/SRA 装置がその URL を HTTP 経由で取得し、必要に応じて変換し、暗号化してリモート ユーザに返します。FTP は、4 種類の日本語セット、2 種類の中国語セット、および 2 種類の韓国語セットを含めて、25 種類の文字セットをサポートします。クライアントのブラウザとオペレーティング システムは目的の文字セットをサポートする必要があり、場合によっては言語パックが必要です。FTP は、HTML5 と Smart Access の選択もサポートしています。

ファイル共有 (CIFS)

(Windows のみでサポート) ファイル共有は、CIFS (Common Internet File System) プロトコルまたは旧式の SMB (Server Message Block) プロトコルを使用して、Microsoft ファイル共有への安全なウェブ インターフェースをリモート ユーザに提供します。ファイル共有では、Microsoft のネットワーク コンピュータやマイ ネットワークによく似たスタイルのウェブ インターフェースが採用されており、適切な権限を持つユーザがネットワーク共有を参照して、ファイルの名前変更、削除、取得、アップロードを行ったり、ブックマークを作成して後で参照したりすることができます。ファイル共有を設定することで、制限されたサーバ パス アクセスを実現することもできます。

リモート デスクトップ プロトコルと仮想ネットワーク コンピューティング

RDP と VNC は、Windows、Linux、および Mac オペレーティング システムでサポートされます。マイクロソフトの多くのワークステーションやサーバにはリモート アクセスを実現できる RDP サーバの機能が用意されており、ダウンロードしてインストールできる無償の VNC サーバもほとんどのオペレーティング システム用に数多く公開されています。RDP と VNC は、HTML5 と Smart Access の選択もサポートしています。RDP クライアントや VNC クライアントは、許可されたリモート ユーザのウェブ ブラウザを通じて次のような形式で自動的に配信されます。

- **VNC** - VNC はもともと AT&T によって開発されたものですが、今日ではオープン ソース ソフトウェアとして広く使われています。さまざまな VNC サーバがありますが、どの VNC サーバもほとんどのワークステーションやサーバにインストールしてリモート アクセスを実現することができます。これらのサーバに接続するための VNC クライアントは、リモート ユーザのウェブ ブラウザを通じて Java クライアントとして配信されます。

RDP 7 サポート

SMA/SRA 装置は、RDP 7 クライアントとの接続をサポートしており、RDP 7 の機能セットに対応しています。RDP 7 は、以下のオペレーティング システムで利用可能です。

- Windows Server 2016
- Windows Server 2012
- Windows 10
- Windows 7
- Windows Vista SP2
- Windows Vista SP1

RDP 6 サポート

SMA/SRA 装置は、RDP 6.1 および RDP 6 クライアントとの接続をサポートしており、RDP 5 の機能セットに加えて RDP 6 の 4 つの機能に対応しています。

RDP 6.1 は、以下のオペレーティング システムに含まれています。

- Windows 7
- Windows Server 2008
- Windows Vista サービスパック 1 (SP1)

RDP 6.1 は、Windows Server 2008 の以下の機能性を組み入れています。

- Terminal Services RemoteApp
- Terminal Services EasyPrint driver
- シングル サインオン

詳細については、ユーザ ブックマークの追加または編集 (409 ページ) を参照してください。

メモ：RDP 6 および RDP 7 のクライアント システム側には、システム上にクライアント ソフトウェアがインストールされている必要があります。SMA/SRA 装置は mstsc クライアントを供給せず、接続のためにローカルにインストールされているクライアントを使用します。

RDP を使用したアプリケーション プロトコル

(Windows、MacOS、Linux でサポート) アプリケーション プロトコルとは、デスクトップ全体ではなく特定のアプリケーションへのアクセスを提供する RDP セッションのことを指します。これによって、CRM ソフトウェアや財務会計ソフトウェアといった個別のアプリケーションへのアクセスを定義できます。アプリケーションを閉じると、そのセッションも終了します。アプリケーション プロトコルとして以下の RDP 形式を使用できます。

- **RDP ネイティブ** - ネイティブ RDP クライアントを使用してターミナル サーバに接続し、指定のパス (例えば **C:\programfiles\microsoft office\office11\winword.exe**) にあるアプリケーションを自動的に呼び出します。
- **RDP HTML5** - HTML5 ベースの RDP クライアントを使用してターミナル サーバに接続し、指定のパス (例えば **C:\programfiles\wireshark\wireshark.exe**) にあるアプリケーションを自動的に呼び出します。

SSO、ユーザ ポリシー、ブックマークのアプリケーション サポート

下記の表は、シングル サインオン (SSO)、グローバル/グループ/ユーザの各ポリシー、およびブックマーク シングル サインオン制御ポリシーに関するアプリケーション固有サポートのリストです。

アプリケーション サポートの表

アプリケーション	SSO のサポート	グローバル/グループ/ユーザ ポリシー	ブックマーク ポリシー
ターミナル サービス (RDP - ネイティブ)	はい	はい	はい
ターミナル サービス (RDP - HTML5)	はい	はい	はい
仮想ネットワーク コンピューティング (VNC - HTML5)	はい	はい	はい
ファイル転送プロトコル (FTP)	はい	はい	はい
Telnet	はい	はい	はい
Telnet (HTML5)	はい	はい	はい
セキュア シェル (SSH)	はい	はい	はい
ウェブ (HTTP)	はい	はい	はい
セキュア ウェブ (HTTPS)	はい	はい	はい
ファイル共有 (CIFS)	はい	はい	はい
Citrix Portal (Citrix)	いいえ	はい	はい

マイクロソフト アウトルック ウェブ アクセス

Secure Mobile Access は、OWA 2013、2010、2007 のすべてのバージョンのリバース プロキシ アプリケーションをサポートしています。

Microsoft OWA Premium モードは、Microsoft Outlook 用のウェブ クライアントで、Microsoft Outlook のインターフェースをシミュレートし、基本的な OWA よりも多くの機能を提供します。マイクロソフト OWA プレミアムには、スペル チェック、サーバ側のルールの作成と変更、ウェブ ビーコンのブロック、仕事のサポート、自動署名のサポート、アドレス帳の拡張などの機能が備わっています。Secure Mobile Access HTTP(S) リバース プロキシは、Microsoft OWA Premium をサポートします。

アウトルック ウェブ アクセスにアクセスする必要がある複数のアクティブ ディレクトリ グループに対するグループ ベースのアクセス ポリシーの設定を含むユースケースについては、AD グループの一意アクセス ポリシーの作成 (521 ページ) を参照してください。

Windows SharePoint Services

Windows SharePoint 2007、および Windows SharePoint Services 3.0 対応の Secure Mobile Access リバース プロキシ アプリケーション サポートには、以下の機能があります。

- サイト テンプレート
- Wiki サイト
- ブログ
- RSS フィード
- Project Manager
- コンテンツへのモバイル アクセス
- 個人用サイト
- 検索センター

- ドキュメント センター
- 文書翻訳管理
- ウェブ コンテンツ管理
- ワークフロー
- レポート センター

ロータス ドミノ ウェブ アクセス

(Windows、MacOS、Linux でサポート) Domino Web Access 8.0.1、8.5.1、および 8.5.2 対応の SMA/SRA 装置のリバース プロキシ アプリケーション サポートには、以下の機能があります。

Lotus Domino Web Accessサポート される機能

8.5.1 および 8.5.2 の機能	8.0.1 の機能
フル モード:	
電子メール	電子メール
カレンダー	カレンダー
連絡先	連絡先
To Do	To Do
ノートブック	ノートブック
ライト モード:	
電子メール	電子メール
カレンダー	カレンダー
連絡先	
ウルトラ ライト モード:	
受信トレイ	
送信済み	
すべての文書	
1 日表示カレンダー	
連絡先	
ごみ箱	

Citrix ポータル

Citrix は、RDP に似たリモート アクセスのアプリケーション共有サービスです。これにより、ユーザはセキュアな接続を通して、中央のコンピュータにあるファイルやアプリケーションにリモート アクセスすることができます。

ActiveX および Java 版 Citrix Receiver クライアントに加え、以前の XenApp および ICA クライアントがサポートされます。以前のバージョンの Citrix では、Citrix ICA クライアントは、Citrix XenApp プラグインに名称が変更されました。

Secure Mobile Access では、Citrix XenApp Server 7.6、XenApp Server 6.5、XenApp Server 6.0、および XenApp Server 5.0 をサポートします。

また、Secure Mobile Access では、Citrix Receiver for Windows 4.2、4.1、4.0 (オンライン プラグイン 14.2、14.1、14.0)、Java クライアント バージョン 10.1.006 以上をサポートします。

メモ：Citrix が Java の Receiver のサポートを終了したため、SonicWall Inc. は Citrix Java ブックマークの公式サポートを終了しました。SonicWall Inc. は、HTML5 または ActiveX を使用して Citrix ブックマークにアクセスする方法を推奨しています。

SNMP の概要

SMA/SRA 装置は、Simple Network Management Protocol (SNMP) をサポートしています。SNMP は、リモート アクセスに関する統計情報を提供します。SNMP がサポートされたことにより、管理者は標準的なレポート作成ツールを利用できることになり、ネットワークの管理が楽になります。

DNS の概要

管理者は、SMA/SRA 装置で DNS を設定することによって、ホスト名を IP アドレスで解決できるようになります。ウェブベースの Secure Mobile Access 管理インターフェースで、管理者は、ホスト名、DNS サーバ アドレス、および WINS サーバ アドレスを設定できます。

ネットワーク ルートの概要

既定のネットワーク ルートを設定することによって、SMA/SRA 装置は、指定のデフォルト ゲートウェイを経由してリモート IP ネットワークに到達できます。ゲートウェイは、通常、SMA/SRA 装置が接続されるアップストリームのファイアウォールです。既定のルートに加えて、優先パスとして、デフォルト ゲートウェイを使用しない、ホストおよびネットワークへの具体的な静的パスを設定することも可能です。

NetExtender の概要

(Windows、MacOS、Linux でサポート)このセクションでは、NetExtender 機能の概要を説明します。

トピック:

- NetExtender とは (43 ページ)
- メリット (44 ページ)
- NetExtender の概念 (44 ページ)

NetExtender の使用の詳細については、クライアント > 状況 (261 ページ) または『*Secure Mobile Access ユーザガイド*』を参照してください。

NetExtender とは

SonicWall Inc. NetExtender は、Windows および Linux ユーザがリモート ネットワークにセキュアな方法で接続できるようにする、透過的なソフトウェア アプリケーションです。NetExtender により、リモート ユーザはリモート ネットワーク上の任意のアプリケーションを安全に実行できます。ファイルのアップロード/ダウンロード、ネットワーク ドライブのマウント、リソースへのアクセスといっ

た作業がローカル ネットワークにいる感覚で行えます。NetExtender の接続では、ポイント ツー ポイント プロトコル (PPP) 接続を使用します。

NetExtender の機能には、Mac、Apple iPhone、iPad、および iPod Touch 用の SonicWall Inc. Mobile Connect アプリケーションが含まれます。Mobile Connect は SonicWall Inc. セキュリティ装置によって保護されたプライベート ネットワークへの保護されたモバイル接続を可能にします。SonicWall Inc. Mobile Connect のインストールと使用に関する情報は、『*SonicWall Inc. Mobile Connect ユーザー ガイド*』を参照してください。

メリット

NetExtender により、リモート ユーザは保護された内部ネットワークへのフル アクセスが可能になります。その際の操作方法は従来の IPSec VPN クライアントとほとんど同じですが、NetExtender の場合はクライアントを手動でインストールする必要がありません。Windows 用の NetExtender クライアントは、インターネット エクスプローラまたは Firefox の使用時に ActiveX コントロールによって、リモート ユーザの PC に自動的にインストールされます。Linux システムの場合は、サポート対象のブラウザが Java コントロールを使用して、仮想オフィス ポータルから NetExtender を自動的にインストールしてくれます。

NetExtender ウィンドウズ クライアントにはまた、ウィンドウズ **ネットワーク接続** メニューから起動できる個別ダイアラがあります。この個別ダイアラにより、NetExtender はウィンドウズ ドメイン ログインの前に接続することが可能になります。NetExtender ウィンドウズ クライアントは、単一アクティブ接続もサポートし、クライアント側にスループットとデータ圧縮率をリアルタイムで表示します。

インストール後に、NetExtender が自動的に起動して仮想アダプタに接続し、内部ネットワーク上の許可されたホストおよびサブネットに対する SSL ベースの安全なポイント ツー ポイント アクセスを提供します。

NetExtender の概念

以下のセクションでは、NetExtender の概念について詳しく説明します。

- スタンドアロン クライアント (44 ページ)
- Microsoft インストーラによる NetExtender インストール時のサーバおよびドメイン フィールドの事前設定 (45 ページ)
- 複数の範囲とルート (47 ページ)
- NetExtender と外部認証方法 (48 ページ)
- ポイント ツー ポイント サーバの IP アドレス (48 ページ)
- 接続スクリプト (48 ページ)
- 強制トンネル方式 (48 ページ)
- プロキシの設定 (49 ページ)

スタンドアロン クライアント

Secure Mobile Access では、スタンドアロンの NetExtender アプリケーションを提供します。NetExtender は、包括的なリモート アクセスを提供する軽量なアプリケーションです。 ブラウザによってインストールされるため、ユーザが手動でダウンロードしてインストールする必要はありません。ユーザが NetExtender を初めて起動したとき、NetExtender スタンドアロン クライアントがそのユーザの PC に自動的にインストールされます。インストーラはユーザのログイン情報に基づいてプロファイルを作

成します。その後、インストーラのウィンドウが閉じ、NetExtender が自動的に起動します。すでに以前のバージョンの NetExtender がインストールされていた場合は、古いバージョンのアンインストールが行われたうえで新しいバージョンがインストールされます。

NetExtender スタンドアロン クライアントのインストール後、Windows の場合は「**スタート > プログラム**」メニューを使用して NetExtender を起動し、Windows の起動時に NetExtender が起動されるように設定できます。

NetExtender はユーザが Windows ドメインにログインする前に VPN セッションを確立できます。Windows Vista 以降では、ユーザは Windows ログイン画面上で「**ユーザーの切り替え**」を選択して、画面右下隅に現れる青いコンピュータ アイコンを選択してから、NetExtender で接続するように選択できます。

Linux システムでは、インストーラによってデスクトップ ショートカットが `/usr/share/NetExtender` に作成されます。このショートカットは、Gnome や KDE といった環境のショートカット バーにドラッグできます。

NetExtender は以下の SonicWall Inc. 装置と互換性があります。

- SMA 400/200
- SRA 4600/1600
- SMA 500v Virtual Appliance
- NSA、TZ、および SuperMassive 9000 シリーズ (SSL VPN ライセンス搭載)

NetExtender はまた、旧 SRA 1200/4200 および SSL-VPN 2000/4000 装置と下位互換があり、接続可能です。

NetExtender は以下のクライアント プラットフォーム上で公式にサポートされています。

- Fedora 14+
- Ubuntu 11.04+
- OpenSUSE 10.3+
- Windows 10、Windows 7、Windows 2012、Windows Server 2008 R2

NetExtender はその他の Linux ディストリビューション上でも正しく動作することがありますが、それらは SonicWall Inc. によって公式にサポートされていません。

メモ: Mobile Connect アプリケーションが iOS 4.3 以降および Android 4.0 以降で利用可能になりました。

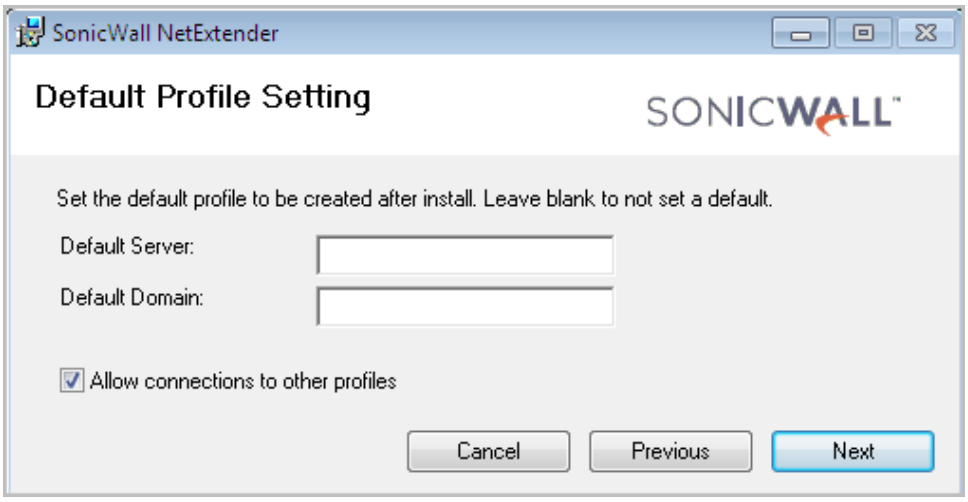
Microsoft インストーラによる NetExtender インストール時のサーバおよびドメイン フィールドの事前設定

Microsoft インストーラ (MSI) による NetExtender のインストールで、デフォルト プロファイル設定をインストール プロセスで使用できるようになりました。デフォルト サーバとデフォルト ドメインに加え、サーバおよびドメイン フィールドの編集を標準ユーザに許可するかどうかを制御するその他のオプションを、事前に設定しておくことができます。これは、インストール プロセスにおいてデフォルトのサーバとドメインを事前に設定しておきたい管理者用の機能です。

Microsoft インストーラによる NetExtender のインストール時に、デフォルトのサーバとドメインを設定するには:

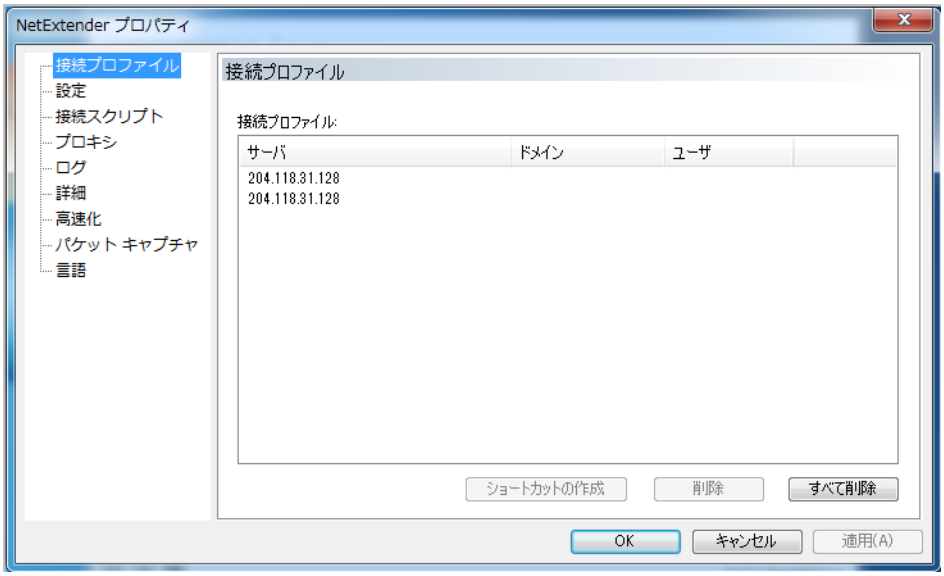
1 「**デフォルト プロファイル設定**」ページで、「**デフォルト サーバ**」のフィールドに IP アドレス、「**デフォルト ドメイン**」のフィールドにドメインを入力します。

メモ：このページが表示されるようにするには、Microsoft Installer を使用する必要があります。



2 ユーザが他のプロファイルに接続できないようにするには、「**他のプロファイルへの接続を許可する**」をオフにします。この設定により、NetExtender のログイン ページで「サーバ」と「ドメイン」のフィールドを編集することはできなくなります。

3 その接続を許可する場合は、このオプションをオンにします。このオプションがオフの場合、ユーザは NetExtender のプロパティ ページでプロファイルを追加または削除することはできません。



複数の範囲とルート

SMA/SRA 装置の NetExtender の複数の範囲とルートのサポートでは、ネットワーク管理者がグループとユーザを簡単にセグメント分割できます。アクセスを制御するファイアウォールのルールを設定する必要はありません。このユーザのセグメント化によって、ネットワークへのアクセスを細かく制御できます。ユーザに対しては必要なリソースへのアクセスを認め、機密性の高いリソースへのアクセスは必要最小限のユーザのみに制限できます。

セグメント分割を必要としないネットワークでは、クライアントのアドレスとルートをグローバルに設定できます。以下のセクションでは、複数の範囲とルートの改良点について説明します。

- IP アドレス ユーザ セグメント分割 (47 ページ)
- クライアント ルート (47 ページ)

IP アドレス ユーザ セグメント分割

管理者は、複数の NetExtender IP アドレス範囲をユーザとグループに設定できます。これらの範囲は、「**ユーザの編集**」ウィンドウおよび「**グループの編集**」ウィンドウの「**NetExtender**」タブを使用して、「**ユーザ > ローカル ユーザ**」ページと「**ユーザ > ローカル グループ**」ページで設定します。

複数の NetExtender IP アドレス範囲をユーザとグループに設定する際には、SMA/SRA 装置の IP アドレスの割り当て方法を理解している必要があります。SMA/SRA 装置では、以下の優先順位で IP アドレスを NetExtender クライアントに割り当てます。

1. ユーザのローカル プロファイルに定義された範囲にある IP アドレス。
2. ユーザが所属するグループ プロファイルに定義された範囲にある IP アドレス。
3. グローバル NetExtender 範囲にある IP アドレス。

個々のユーザに常に同じ IP アドレスを割り当てるには、「**グループの編集**」ウィンドウの「**NetExtender**」タブで、「**クライアント アドレス範囲の開始**」フィールドと「**クライアント アドレス範囲の終了**」フィールドに同じ IP アドレスを入力します。

クライアント ルート

NetExtender クライアント ルートは、さまざまなネットワーク リソースへのアクセスを許可または拒否するために使用されます。クライアント ルートは、ユーザ レベルまたはグループ レベルでも設定

できます。NetExtender クライアント ルートは、「**ユーザの編集**」ウィンドウと「**グループの編集**」ウィンドウでも設定できます。クライアント ルートのセグメント分割は完全なカスタマイズが可能であり、あらゆる組み合わせでユーザ ルート、グループ ルート、およびグローバル ルートを指定できます (例えばグループ ルートのみ、ユーザ ルートのみ、グループ ルートとグローバル ルート、これらのすべてのルートなどの指定が可能です)。このセグメント分割は、「**グローバル クライアント ルートを追加する**」と「**グループ クライアント ルートを追加する**」を使って制御します。

NetExtender と外部認証方法

外部認証サーバを使用するネットワークでは、SMA/SRA 装置にローカル ユーザ名が設定されません。その場合、「**グローバル クライアント ルートを追加する**」および「**グループ クライアント ルートを追加する**」の設定が有効になっていれば、ユーザの認証が正常に完了したときにローカル ユーザ アカウントが作成されます。

ポイント ツー ポイント サーバの IP アドレス

Secure Mobile Access では、PPP サーバの IP アドレスは接続中のすべてのクライアントに対して 192.0.2.1 になります。この IP アドレスは、内部ネットワークに接続中のリモート ユーザと、リモート NetExtender クライアントと通信する内部ネットワーク ホストに接続中のリモート ユーザの両方にとって意識せずに使用できます。PPP サーバの IP アドレスは、NetExtender アドレス プールから独立しているため、グローバル NetExtender アドレス プールのすべての IP アドレスが NetExtender クライアントに使用されます。

接続スクリプト

SMA/SRA 装置は、NetExtender の接続が確立されたときと切断されたときにバッチ ファイル スクリプトを実行する機能を提供しています。これらのスクリプトを使って、ネットワーク ドライブやプリンタのマッピングおよび切断、アプリケーションの起動、ファイルやウェブ サイトの表示などを行うことができます。NetExtender の接続スクリプトでは任意の有効なバッチ ファイル コマンドを使用できます。

強制トンネル方式

強制トンネル方式では、リモート ユーザとやり取りされるすべてのトラフィックが (リモート ユーザのローカル ネットワークへのトラフィックを含め) Secure Mobile Access NetExtender トンネルを経由します。これは、次のルートをリモート クライアントのルート テーブルに追加することで実現されます。

強制トンネル方式: リモート クライアントのルート テーブルに追加されるルート

IP アドレス	サブネット マスク
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender は、接続中のすべてのネットワーク接続のローカル ネットワーク ルートも追加します。これらのルートは既存のどのルートよりも高いメトリックで設定されるため、ローカル ネットワークへのトラフィックが強制的に Secure Mobile Access トンネル経由に切り替わります。例えば、リモート ユーザが 10.0.*.* ネットワークの IP アドレス 10.0.67.64 を使用している場合、ルート 10.0.0.0/255.255.0.0 が追加され、トラフィックが Secure Mobile Access トンネルを経由するようになります。

トンネル オール モードは、グローバル、グループ、ユーザの各レベルで設定できます。

プロキシの設定

SMA/SRA 装置では、プロキシ設定を使用する NetExtender セッションがサポートされます。現在サポートされているのは、HTTPS プロキシのみです。NetExtender をウェブ ポータルから起動する場合、プロキシ アクセスを行うようにブラウザが既に設定されているときは、NetExtenderが自動的にそのプロキシ設定を継承します。プロキシ設定は、NetExtender クライアントでの手動設定も可能です。NetExtender は、Web Proxy Auto Discovery (WPAD) プロトコルに対応したプロキシ サーバ用のプロキシ設定を自動的に検出できます。

NetExtender には、次の 3 つのプロキシ設定オプションが用意されています。

- **設定を自動的に検知する** - この設定を使用するには、プロキシ サーバが、クライアントにプロキシ設定スクリプトを自動的にプッシュできる Web Proxy Auto Discovery Protocol (WPAD) をサポートしている必要があります。
- **自動設定スクリプトを使用する** - プロキシ設定スクリプトの場所がわかっている場合は、このオプションを選択してスクリプトの URL を指定することができます。
- **プロキシ サーバを使用する** - このオプションを選択すると、プロキシ サーバの IP アドレスとポートを指定できます。また、「**プロキシのバイパス**」フィールドに IP アドレスまたはドメインを入力すれば、それらのアドレスに直接接続してプロキシ サーバをバイパスすることができます。必要に応じて、プロキシ サーバ用のユーザ名とパスワードも入力できます。プロキシ サーバがユーザ名とパスワードを要求しているのにそれらを指定していない場合は、最初の接続時に NetExtender のポップアップ ウィンドウが表示され、その入力を求められます。

プロキシ設定を使用して接続する場合、NetExtender は、SMA/SRA サーバに直接接続するのではなく、プロキシ サーバに対して HTTPS 接続を確立します。次に、プロキシ サーバがトラフィックを SMA/SRA サーバに転送します。すべてのトラフィックは、NetExtender とネゴシエートされた証明書を使って SSL によって暗号化されます。 これについては、プロキシ サーバ側は関知していません。プロキシを使用してもしなくても、接続のプロセスに違いはありません。

二段階認証の概要

二段階認証とは、2 つの個別の情報を要求して ID と権限を確立する認証方式です。二段階認証は、1 段階 (ユーザのパスワード) だけを要求する従来のパスワード認証より強力で、厳密です。

SonicWall Inc. が実装している二段階認証は、高度なユーザ認証で業界の先端をゆく RSA および VASCO と提携しています。

二段階認証に対して 2 台の RADIUS サーバが使用可能で、ユーザをウェブ ポータルを通して、または NetExtender やセキュア仮想アシストといった Secure Mobile Access クライアントを使って認証できます。

メモ：SMA/SRA 装置のシングル サイン オン (SSO) は、二段階認証をサポートしていません。

以下のセクションを参照してください。

- 二段階認証のメリット (50 ページ)
- 二段階認証の動作方法 (50 ページ)
- サポートされている二段階認証プロバイダ (50 ページ)

二段階認証のメリット

二段階認証には、以下のメリットがあります。

- 2 つの個別の認証情報を要求することで、セキュリティが大きく強化されます。
- 簡単に破られてしまうような脆弱なユーザ パスワードが招くリスクを軽減できます。
- 簡単で直感的に使用でき、自動化されている強力な認証プロセスを提供することで、管理者がユーザのトレーニングとサポートに費やす時間を最小化できます。

二段階認証の動作方法

二段階認証では、サードパーティの認証サービス、または、2 台の別々の RADIUS 認証サーバを使用する必要があります。

二段階認証では、ユーザは正しい一時パスコードを入力してアクセスを取得する必要があります。パスコードは以下のもので構成されています。

- ユーザの個人識別番号 (PIN)
- 一時トークン コード

2 台の RADIUS サーバを使う場合は、2 番目のステージの PIN またはパスワードを、SMS か電子メールでユーザに送ることができます。NetExtender ログインと仮想アシストの両方が、それの入力のためのエクストラ チャレンジを提供します。

サードパーティの認証サービスを使う場合は、それは 2 つのコンポーネントで構成されています。

- 管理者がユーザ名の設定、トークンの割り当て、および認証関連タスクの管理を行うための認証サーバ。
- 管理者がユーザに与える物理トークン。トークンには、一時トークン コードが表示されます。

ユーザは、自分の RSA トークン カードまたは VASCO トークン カードから一時トークン コードを受け取ります。トークン カードには、毎分、新しい一時トークン コードが表示されます。RSA サーバまたは VASCO サーバがユーザを認証する場合は、トークンコードのタイムスタンプが最新であることを確認します。PIN が正しく、かつ、トークン コードが正しくて最新の場合に、ユーザは認証されます。

ユーザ認証ではこの 2 段階が要求されるため、二元 RADIUS サーバ ソリューション、RSA SecureID ソリューション、および VASCO DIGPASS ソリューションは、従来のパスワード (一段階認証) より強力なセキュリティを実現します。

サポートされている二段階認証プロバイダ

RSA

(Windows、MacOS、Linux でサポート) RSA は、公開鍵暗号化のアルゴリズムです。RSA では、RSA SecurID トークンを使って、RSA 認証マネージャ サーバ経由で認証を行います。RSA はすべてのハードウェア プラットフォームでサポートされず、RADIUS 経由でのみサポートされます。

VASCO

(Windows、MacOS、Linux でサポート) VASCO はユーザ認証製品を提供する企業です。VASCO では、Digipass トークンを使って、VACMAN IdentiKey サーバ経由で認証を行います。VASCO は、すべての SMA/SRA プラットフォームでサポートされています。

VASCO DATA Security は、ワンタイム パスワード技術の使用を通して信頼できる認証を提供します。SMA/SRA とファイアウォール VPN 装置と組み合わせた VASCO IdentiKey は、VASCO IdentiKey 技術を通じて提供される公開市場アプローチを作成します。

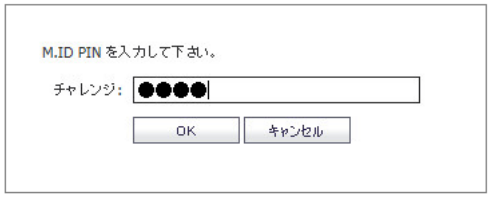
VASCO IdentiKey により、ユーザは簡単で保護されたリモート アクセスを提供する、時間区分で割り当てられるワンタイム パスワードを使用する VASCO DIGIPASS の概念を利用できます。認証要求内のワンタイム パスワードは、VASCO IdentiKey 上で検証されます。検証の後で、RADIUS アクセス受諾メッセージが認証のために SMA/SRA サーバに送信されます。

二段階認証のログイン プロセス

このセクションでは、ウェブ ログインおよび NetExtender を使用する場合の二段階認証ログイン プロンプトの例を提供します。

ウェブ ログインでは、1 番目のステージの資格情報を入力するために「**ユーザ名**」と「**パスワード**」フィールドが使われます。

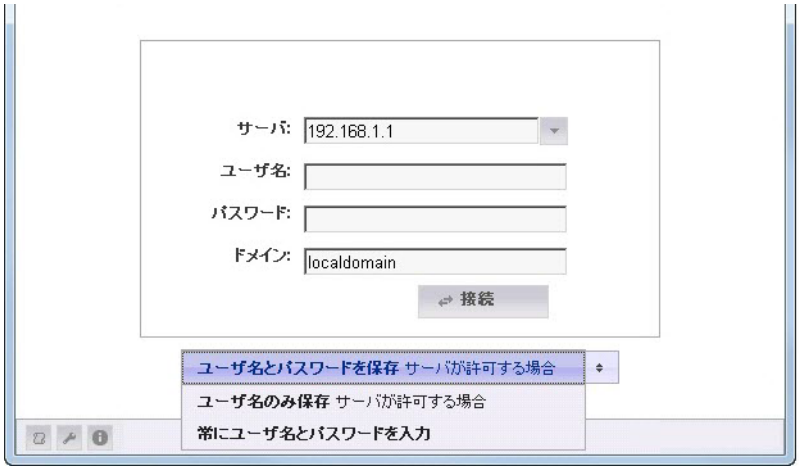
この例では、ユーザにチャレンジ コードを入力するように要求する際のメッセージ "M.ID PIN を入力してください" が RADIUS サーバからの応答メッセージですが、異なる RADIUS サーバでは応答メッセージの形式は異なります。



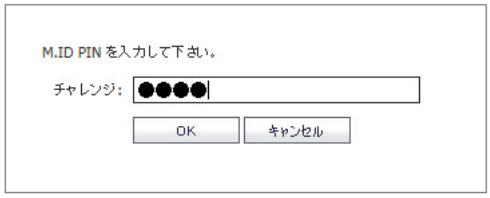
RADIUS サーバによっては、認証を完了するためにユーザにいくつかのチャレンジへの応答を要求することがあります。この例では、M.ID サーバはユーザに 2 つのチャレンジを提示するように要求しています。以下のパスコードは電子メールか携帯電話 (SMS が設定されている場合) を通して受け取ることができます。

NetExtender ウィンドウズ クライアントで二段階認証を使う場合は、クライアントを通したログイン プロセスは、ウェブ ページを通したログインとよく似ています。

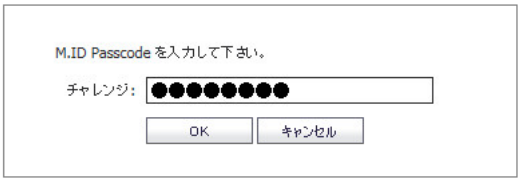
最初に、1 番目のステージの資格情報を入力するために「**ユーザ名**」と「**パスワード**」フィールドが使われます。



引き続き、PIN チャレンジが要求されます。



最後に、パスコード チャレンジが要求されます。



ワンタイム パスワードの概要

(Windows、MacOS、Linux でサポート)このセクションでは、ワンタイム パスワード機能の概要を説明します。このセクションには次の内容が含まれています。

ワンタイム パスワードとは

Secure Mobile Access ワンタイム パスワード機能は、標準のユーザ名とパスワードのログイン セキュリティにもう一段階のセキュリティ階層を追加します。ワンタイム パスワードとは、ランダムに生成される使い捨てのパスワードのことです。Secure Mobile Access ワンタイム パスワード機能は、ワンタイム パスワードを標準のユーザ名とパスワードの資格情報とともに利用する二段階認証方式になっており、Secure Mobile Access ユーザに追加のセキュリティを提供します。

Secure Mobile Access ワンタイム パスワード機能では、ユーザは最初に正しい Secure Mobile Access ログイン資格情報を提示する必要があります。標準ログイン手順を実行した後、Secure Mobile Access はワンタイム パスワードを生成し、ユーザの事前定義された電子メール アドレスに送信します。ユーザは、ワンタイム パスワードの期限内にその電子メール アドレスにログインし、ワンタイム パスワードを取得して、Secure Mobile Access のログイン画面に入力する必要があります。

時刻ベースのワンタイム パスワードとは何ですか？

Secure Mobile Access 時刻ベースのワンタイム パスワード機能は、従来の二段階認証に代わる認証方式です。Secure Mobile Access の時刻ベースのワンタイム パスワード機能は、サードパーティの統合によってサードパーティの認証アプリ経由で安全な時刻ベースのワンタイムパスワードを生成できるようにするマルチファクタ認証方式です。

Secure Mobile Access 時刻ベースのワンタイム パスワード機能では、ユーザが最初に正しい Secure Mobile Access ログイン資格情報を提示する必要があります。標準ログイン手順の実行後、サードパーティの認証アプリがワンタイム パスワードを生成します。ユーザは、ワンタイム パスワードの有効期限が切れる前に、プロンプトに応じて Secure Mobile Access ログイン画面にパスワードを入力する必要があります。

ワンタイム パスワードのメリット

Secure Mobile Access ワンタイム パスワード機能を使うと、単一の静的なパスワードのみを使う場合よりもセキュリティが向上します。ワンタイム パスワードを通常のログイン資格情報と組み合わせて使うことで、事実上、認証の層がもう1段追加されます。ユーザは Secure Mobile Access ワンタイム パスワードのログイン プロセスを実行する前に、Secure Mobile Access の管理者が定義した電子メール アドレスにアクセスする必要があります。個々のワンタイム パスワードは使い捨てで、一定期間を過ぎると無効になります。このため、ログイン要求の成功、キャンセル、失敗、またはタイムアウトが発生するたびに、新しいワンタイム パスワードを生成する必要があります。こうすることで、ワンタイム パスワードが悪用される可能性を減らしています。

ワンタイム パスワード機能の仕組み

Secure Mobile Access の管理者は、ワンタイム パスワード機能をユーザごとまたはドメインごとに有効にすることができます。ワンタイム パスワード機能をユーザごとに有効にするには、Secure Mobile Access 管理インターフェースでユーザ設定を編集する必要があります。また、ワンタイム パスワード機能を有効にする各ユーザの外部電子メール アドレスも入力する必要があります。アクティブ ディレクトリと LDAP のユーザに関しては、ワンタイム パスワード機能をドメインごとに有効にすることができます。

ドメインごとに有効にしたワンタイム パスワード機能は、個別に“有効”または“無効”にしたワンタイム パスワードの設定よりも優先されます。ドメインのワンタイム パスワード機能を有効にしても、手動で入力された電子メール アドレスは無効にならず、ドメイン ポリシーによって自動的に設定された電子メール アドレスや、AD/LDAP の設定よりも優先されます。

Secure Mobile Access ワンタイム パスワード機能を使用するには、Secure Mobile Access 管理インターフェースの「**ログ > 設定**」ページで有効なメール サーバの設定を構成する必要があります。ワンタイム パスワード機能をユーザごとまたはドメインごとに設定し、ユーザのタイムアウト ポリシーを設定します。

ワンタイム パスワードの配信先の電子メール アドレスが外部ドメイン (SMS アドレスや外部ウェブメール アドレスなど) にある場合は、SMA/SRA 装置から外部ドメインへの中継を行うように SMTP サーバを設定する必要があります。

ユーザごとまたはドメインごとの設定でワンタイム パスワード機能が有効になったユーザは、Secure Mobile Access インターフェースで標準のユーザ名とパスワードの資格情報を入力してログイン プロセスを開始します。ログインすると、ユーザの事前定義された電子メール アカウントに一時的なパスワードが送信されたというメッセージが表示されます。ユーザは外部電子メール アカウントにログインし、ワンタイム パスワードを取得して、それを Secure Mobile Access ログイン インターフェースの該当フィールドに入力するか、貼り付ける必要があります。正しいワンタイム パスワードを入力するまでは、ユーザが何を要求してもログイン ページが再表示されます。

ワンタイム パスワードは、ログインが成功すると自動的に削除されます。ユーザが Secure Mobile Access インターフェースで「**キャンセル**」を選択して削除することもできます。また、ユーザがタイムアウト ポリシーの期間内に正しくログインできなかった場合も、パスワードは自動的に削除されます。

時刻ベースのワンタイム パスワード機能を使用するには、管理者が「**ユーザ > ローカル ユーザ > ローカル ユーザの編集 > ログイン ポリシー**」または「**ユーザ > ローカル グループ > ローカル グループの編集 > ログイン ポリシー**」ページでローカル ユーザまたはローカル グループのログイン ポリシーを構成する必要があります。管理者は、ワンタイム パスワード機能を有効化して「モバイル アプリを使用」を選択することにより、タイムワンタイム パスワード機能をユーザごとまたはドメイン単位で構成できます。管理者は、ユーザの電話機と認証アプリをバインドして安全な時刻ベースのワンタイム パスワードを使用するように構成できます。

SMS 対応電話でのワンタイム パスワードの設定

Secure Mobile Access ワンタイム パスワードを SMS 対応電話に電子メールで直接送信するように設定することができます。SMS (ショート メッセージ サービス) を有効にする方法の詳細については、携帯電話サービス会社にお問い合わせください。以下に、主な電話会社の SMS 電子メール フォーマットを示します。

以下に、主な電話会社の SMS 電子メール フォーマットを示します。ここで、4085551212 は 10 桁の電話番号と局番を表します。

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T PCS: 4085551212@text.att.net
- Cingular: 4085551212@mobile.mycingular.com
- T-Mobile: 4085551212@tmomail.net
- Nextel: 4085551212@messaging.nextel.com
- Virgin Mobile: 4085551212@vmobl.com
- Qwest: 4085551212@qwestmp.com

ヒント：SMS 電子メール形式の詳細なリストについては、SMS 電子メール形式の使用 (566 ページ)を参照してください。

メモ：これらの SMS 電子メール フォーマットは参考用です。これらの電子メール フォーマットは変更される可能性があります。SMS を使用する前に、サービス会社から追加的なサービスまたは情報を入手しなければならないこともあります。これらのフォーマットと、SMS のサービス、オプション、機能の詳細については、SMS を提供する会社に直接問い合わせてください。

SMS 電子メール アドレスにワンタイム パスワードを送信するように SMA/SRA 装置を設定するには、ユーザ設定の編集 (391 ページ)で説明している手順に従って操作を行い、「**電子メール アドレス**」フィールドにユーザの SMS アドレスを入力します。

ワンタイム パスワードの設定の確認

個々のユーザ アカウントでワンタイム パスワード機能が有効になっているかどうかを確認するには、そのアカウントの資格情報を使って Secure Mobile Access 仮想オフィス ユーザ インターフェースにログインします。

仮想オフィスに正常にログインできれば、ワンタイム パスワード機能を正しく使用できています。

ワンタイム パスワードを使ってログインできない場合は、以下の点を確認します。

- 電子メールでワンタイム パスワードを取得するように求めるメッセージが表示されずにログインできましたか? そのユーザ アカウントはワンタイム パスワード機能を使うように設定されていません。
- 電子メール アドレスは正しく設定されていますか? ユーザ アカウントの電子メール アドレスが正しく設定されていない場合は、管理インターフェースにログインして電子メール アドレスを修正します。
- ワンタイム パスワードの記載された電子メールを確実に受信しましたか? 電子メールが届いていない場合は、数分待ってから受信ボックスを更新してください。スパム フィルタも確認してください。数分待っても電子メールが届かない場合は、再度ログインして新しいワンタイム パスワードを生成してみてください。
- ワンタイム パスワードを所定のフィールドに正確に入力しましたか?「**ログ > 設定**」ページで設定されているユーザのタイムアウト ポリシーで指定された期間内に、ワンタイム パスワードを再度入力するかコピーして貼り付けてください。
- QR コードをスキャンできますか? 認証アプリをダウンロードしましたか? 認証アプリ (Google Authenticator、Duo Mobile など) をダウンロードしてください。
- 認証アプリをモバイル機器にバインドしましたか? 認証アプリをモバイル機器にバインドできない場合は、管理者にお問い合わせください。
- ワンタイム パスワードの期限が切れていませんか? パスワードが受け入れられない場合は、認証アプリを開き、パスワードが最新か確認します。古いパスワードの期限が切れると、新しいパスワードが表示されます。
- システム クロックが現在の時刻を示していますか? システム クロックが同期していない場合は、クロックをリセットしてください。

エンド ポイント制御の概要

このセクションでは、エンド ポイント制御機能の概要を説明します。このセクションには次の内容が含まれています。

エンド ポイント制御とは

従来の VPN ソリューションでは、あなたのネットワークに社員個人所有のコンピュータ、空港、またはホテルといった信頼していない場所からアクセスすることにより、ネットワーク資源に対する危険が増大します。EPC は、信頼していない環境内の機器など、あらゆるウェブ対応システムからの安全なアクセスを提供します。

エンド ポイント制御のメリット

SMA/SRA 装置がサポートするエンド ポイント制御 (EPC) には、以下のメリットがあります。

- 接続を確立する前にユーザの環境が安全かどうかを確認する
- 機密性の高いデータを保護する
- 信頼していない環境内の機器からアクセスされる際にネットワークに危険が及ばないように守る
- SMA/SRA に参加しているクライアント機器を起源とする脅威からネットワークを保護する

エンド ポイント制御の仕組み

SMA/SRA 装置はエンド ポイント セキュリティ制御を、トンネル セッションが開始される前にホストの健全性確認とセキュリティ防御機構を実行することで提供します。ホストの健全性確認は、クライアント システムを組織のセキュリティ ポリシーに確実に準拠させるのに役立ちます。SonicWall エンド ポイントのセキュリティ制御はアクセス制御としっかり統合されており、Windows クライアント システムを分析した結果に基づいてアクセス制御を適用するようになっています。

エンドポイント制御は、Mobile Connect を用いる Mac iOS および Android モバイル機器でサポートされており、これらの機器に対してデバイス プロファイルの作成が可能です。これによって、クライアント機器を脅威から保護するとともに、SMA/SRA 装置にログインするクライアント機器を起源とする脅威からこれらの機器を保護します。Mobile Connect の詳細については、Mobile Connect の各種ユーザ ガイドを参照してください。

エンド ポイント制御の設定

エンド ポイント制御 (EPC) を設定するには、以下の手順に従います。

1. 様々なグローバル、グループ、またはユーザ属性に基づいてユーザ認証を許可または禁止するデバイス プロファイルを設定します。エンド ポイント制御 > デバイス プロファイル (280 ページ) を参照してください。
2. エンド ポイント制御プロファイルを許可または禁止するグループとユーザを追加して設定します。EPC 設定の編集 (480 ページ) を参照してください。
3. グループ プロファイルを継承するようにユーザを設定します。EPC 設定の編集 (480 ページ) を参照してください。
4. エンド ポイント制御を有効にします。エンド ポイント制御 > 状況 (287 ページ) を参照してください。
5. NetExtender に接続して、エンド ポイント制御のログを監視します。エンド ポイント制御 > ログ (288 ページ) を参照してください。

セキュア仮想アシストの概要

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

(Windows と MacOS でサポート)このセクションでは、セキュア仮想アシスト機能の概要を説明します。このセクションには次の内容が含まれています。

セキュア仮想アシストとは

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

Secure Mobile Access ユーザがリモートの場所から顧客をサポートするために顧客の使用しているコンピュータの制御を取得できる、使いやすいツールがセキュア仮想アシストです。顧客サポートは、昔から費用と時間がかかるビジネス分野でした。セキュア仮想アシストは、簡単に展開できる、使いやすいリモート サポート ソリューションを実現します。

セキュア仮想アシストのメリット

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想アシストには、次のようなメリットがあります。

- **顧客サポートの簡略化と効率化** - サポート スタッフは、セキュア仮想アシストを使って顧客のコンピュータに直接アクセスし、問題のトラブルシュートと解決を行うことができます。顧客が問題やコンピュータの動作について電話で説明する必要はありません。
- **時間とコストの節減** - セキュア仮想アシストを使うことにより、サポート スタッフが顧客を訪問して問題をトラブルシュートする必要はなくなり、サポート要求の平均解決時間が短縮されます。
- **教育用ツール** - トレーナーとサポート スタッフは、セキュア仮想アシストを使ってリモートから顧客にプログラムやツールの使い方を示すことができます。
- **既存の認証システムとのシームレスな統合** - 顧客の身元が本物かどうかを確認することができます。また、SMA/SRA 装置のローカル データベースおよびトークンなしの二段階認証を利用することもできます。
- **安全な接続** - SMA/SRA 装置によるデータの 256 ビット AES SSL 暗号化は、データを保護する安全な環境をもたらし、Sarbanes-Oxley 法や HIPAA 法などの法令の遵守に役立ちます。
- **リモート アクセスに対する卓越した柔軟性** - セキュア仮想アクセス機能を使って、サポート スタッフは SMA/SRA 装置の LAN の外側にある個人のシステムにアクセスできます。

セキュア仮想アシストの仕組み

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

以下のセクションでは、セキュア仮想アシスト機能の動作について説明します。

- 基本的な操作 (58 ページ)
- リモート ファイル転送 (59 ページ)
- チャット機能 (59 ページ)
- 電子メール招待 (59 ページ)
- セキュア仮想アクセス (59 ページ)

基本的な操作

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想アシストは Java を使用して Secure Mobile Access 仮想オフィスから自動的にインストールされる軽量なシン クライアントであり、外部ソフトウェアのインストールは一切必要としません。Java 未対応のコンピュータでは、仮想オフィスからセキュア仮想アシストの実行可能ファイルをダウンロードして、手動でインストールできます。

基本的な画面共有サポートに対しては、セキュア仮想アシストを実行するために管理権限は不要です。クライアントの完全インストールに対しては、管理権限が必要になることもありますが、サービスを使うために完全インストールする必要はありません。

ユーザが顧客としてサービスを要求した際に、Windows 7 または Windows Vista プラットフォームの RDP を介してシステムに接続している間は、セキュア仮想アシストは動作しません。セキュア仮想アシストは顧客のシステムに適切にアクセスするためにサービスとして動作するので、RDP 接続から動作している場合は、正しいアクセス権が設定できません。

セキュア仮想アシスト セッションには 2 つの面、顧客ビューと技術者ビューがあります。ユーザーとは、自分のコンピュータに対するサポートを要求する人のことです。技術者は、アシストを提供する人です。セキュア仮想アシスト セッションは以下の一連の流れから成り立っています。

1. 技術者が、セキュア仮想アシストを Secure Mobile Access 仮想オフィスから起動します。
2. 技術者は、アシストを要求する顧客のアシスト キューを監視します。
3. 顧客が、次のいずれかの方法でアシストを要求します。
    - Secure Mobile Access 仮想オフィスにログインして、セキュア仮想アシストのリンクを選択する
    - 技術者からの電子メール招待を受信して、セキュア仮想アシストを起動するためのリンクを選択する
    - 技術者から示された URL を使用して、セキュア仮想アシストのホーム ページに直接アクセスする
4. 顧客のブラウザにセキュア仮想アシスト アプリケーションがインストールされ、実行されます。
5. 顧客の情報がセキュア仮想アシストのアシスト キューに表示されます。
6. 技術者が顧客の名前を選択して、セキュア仮想アシストのセッションを開始します。
7. 顧客のコンピュータにポップアップの警告ウィンドウが表示され、顧客が許可すると、技術者が顧客のコンピュータを制御できる状態になります。

8 技術者のセキュア仮想アシスト ウィンドウに、顧客のコンピュータの画面全体が表示されます。技術担当者は、ユーザーのコンピュータのマウスおよびキーボードを完全に制御できるようになります。顧客は、技術者が行う操作をすべて観察できます。

9 顧客はいつでもセッションを終了できます。セッションを終了するには、画面右下隅の「**仮想アシストの終了**」を選択します。

10 セッションが終了すると、ユーザーだけがコンピュータを制御できるようになります。

リモート ファイル転送

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

技術者は、セキュア仮想アシストのリモート ファイル転送機能を使って、顧客のコンピュータを相手にファイルの送受信を行えます。ファイル転送プロセスを起動するには、セキュア仮想アシスト ウィンドウの左上隅にある仮想アシスト タスクバーでボタンを選択します。ファイル転送機能は、複数のファイルのアップロードとダウンロードをサポートしています。

チャット機能

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想アシストのチャット機能により、技術者と顧客はインスタント メッセージ形式のチャット機能で会話することができます。技術者または顧客は、セキュア仮想アシスト タスクバーの「**チャット**」を選択してチャットを開始できます。

電子メール招待

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想アシストの技術者側では、セキュア仮想アシスト セッションを開始するための直接 URL リンクが含まれる電子メール招待を顧客に送信できます。技術者は、顧客向けに任意のメッセージを付け加えることもできます。顧客がセキュア仮想アシストへの電子メール リンクを選択すると、招待を送信した技術者のみが顧客にサポートを提供できます。

セキュア仮想アクセス

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想アクセスは、より大きなセキュア仮想アシスト機能の一部で、技術者はこの機能を使用して、個人システムなど SMA/SRA 装置の LAN 外部のシステムにアクセスできます。セキュア仮想アクセス モードのためのクライアントをポータル ページからダウンロードしてインストールすると、その個人システムは Secure Mobile Access 管理インターフェース上で、その技術者の仮想アシスト サポート待ち行列にのみ表示されます。セキュア仮想アクセス モードのためのクライアントをポータル ページからダウンロードしてインストールした後に、その個人システムは SRA 装置の管理インターフェース上で、その技術者のセキュア仮想アシスト サポート待ち行列にのみ表示されます。

セキュア仮想アクセスはポータル毎に有効にする必要があるので、この機能はサポート技術者に対して卓越したリモート アクセスの柔軟性を提供します。

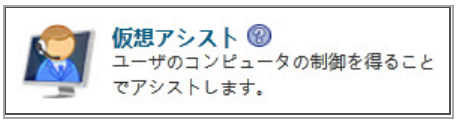
セキュア仮想アシストの技術者セッションの開始

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

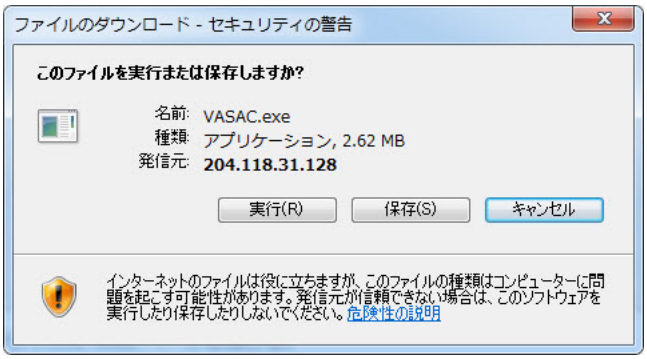
技術者としてセキュア仮想アシスト セッションを起動するには:

1 Secure Mobile Access 仮想オフィスにログインします。Secure Mobile Access の管理インターフェースにログイン済みの場合は、「**仮想オフィス**」を選択します。

2 「**仮想アシスト**」をクリックします。



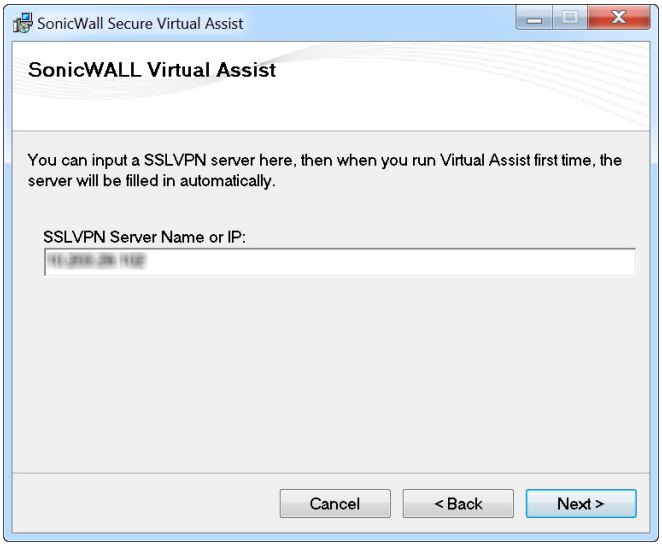
3 仮想アシスト プラグインがインストールされていない場合は、「ファイルのダウンロード」ウィンドウが表示され、セキュア仮想アシストの自動インストールが試行されます。「**実行**」を選択してプログラムを直接起動するか、「**保存**」を選択してインストーラ ファイルをコンピュータに保存した後、手動で起動します。



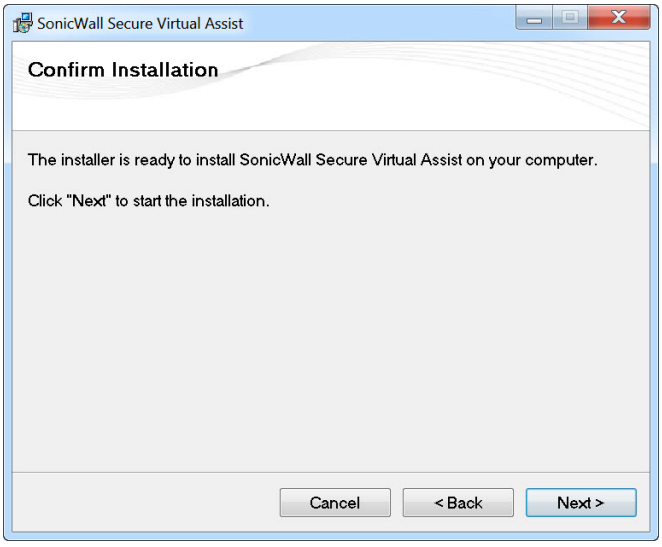
IPv6 経由でダウンロードする場合には、「ファイルのダウンロード」ウィンドウに IPv6 情報が表示されます。

4 ポップアップ ウィザードが開いて、セキュア仮想アシストをスタンドアロン クライアントとしてインストールするかどうかを確認するメッセージが表示されます。「**次へ**」をクリックしてインストールを開始します。

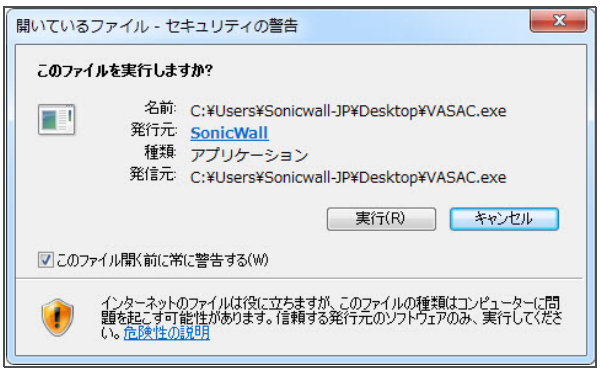
5 表示されるフィールドに「**SSLVPN サーバの名前または IP**」を入力し、「**次へ**」をクリックします。



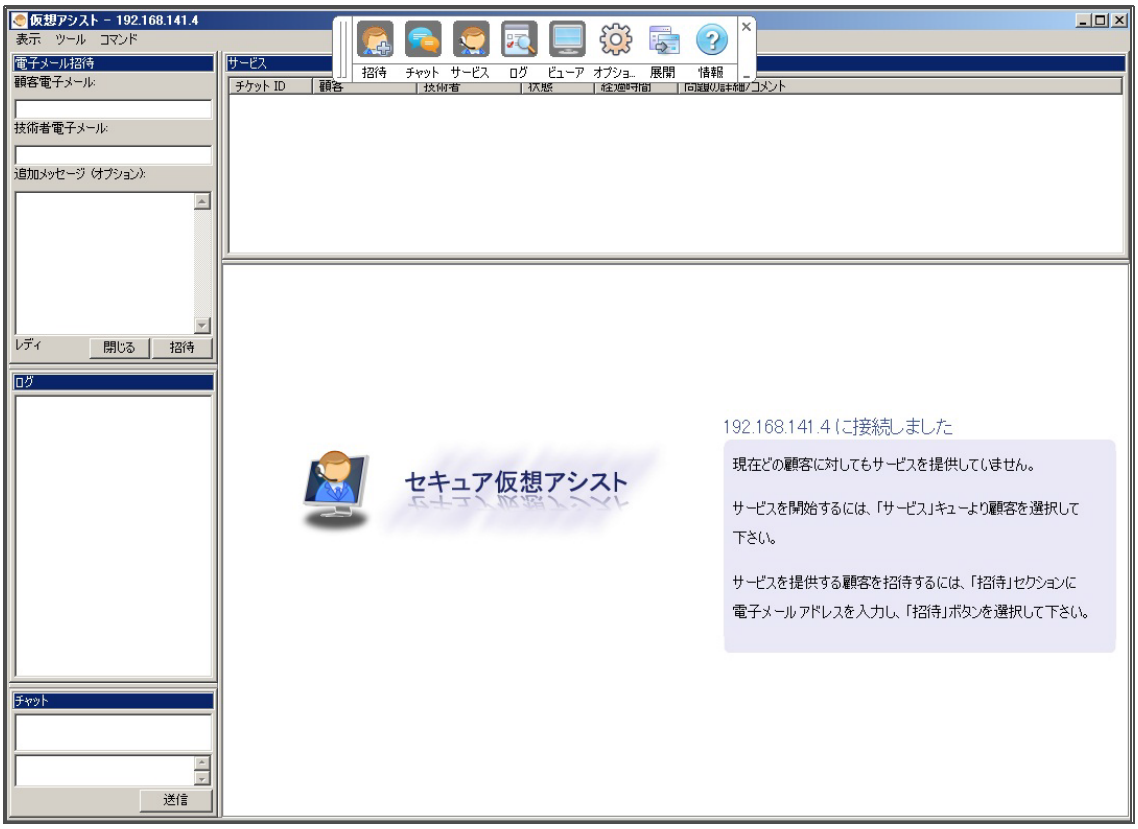
6 確認画面が表示されたら、SonicWall Inc. セキュア仮想アシストをコンピュータにインストールする準備は完了です。「**次へ**」をクリックしてインストールを開始します。



7 セキュア仮想アシストを初めて起動するときに、セキュリティ警告ポップアップ ウィンドウが表示される場合があります。「**このファイルを開く前に常に警告する**」をオフにすると、このウィンドウは次回から表示されません。「**実行**」を選択します。



8 セキュア仮想アシストのスタンドアロン アプリケーションが起動します。



9 これで、顧客をアシストする準備ができました。

セキュア仮想アシストの技術者タスクの実行

メモ：セキュア仮想アシストは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

最初に技術者は、SMA/SRA 装置にログインし、セキュア仮想アシスト アプリケーションを起動します。

メモ：各技術者が同時にアシストできる顧客は 1 人だけです。

技術者はセキュア仮想アシスト アプリケーションを起動した後、顧客をアシストする次のタスクを実行できます。

- ユーザーを電子メールで招待する (62 ページ)
- ユーザーをサポートする (63 ページ)
- セキュア仮想アシスト タスクバーの使用 (63 ページ)
- セキュア仮想アシストの表示の制御 (65 ページ)
- 完全操作の要求 (65 ページ)

ユーザーを電子メールで招待する

電子メールで顧客をセキュア仮想アシスト セッションに招待するには、以下の手順に従います。

1 顧客にセキュア仮想アシストの利用を勧めるには、セキュア仮想アシスト ウィンドウの左側に表示される電子メール招待フォームを使用します。

> **メモ**：招待の電子メールに記述されているリンクを使用してセキュア仮想アシストを起動した顧客にアシストを提供できるのは、その電子メールを送信した技術者のみです。仮想アシストを手動で起動した顧客は、任意の技術者からアシストを受けられます。

2 ユーザーの電子メール アドレスを [**顧客電子メール**] フィールドに入力します。

3 デフォルトの技術担当者の電子メールとは異なる電子メール アドレスにメールが返信されるようにする場合は、その電子メール アドレスを [**技術者電子メール**] に入力します。

4 オプションで、ユーザーへのメッセージを [**追加メッセージ**] に入力します。

5 [**招待**] をクリックします。セキュア仮想アシストを起動するための HTML リンクが含まれる電子メールが顧客に送信されます。

6 アシストを要求している顧客がアシスト キューに表示され、その待ち時間が表示されます。

ユーザーをサポートする

1 顧客がアシスト キューに登録されると、システム トレイのポップアップ ウィンドウによって技術者に通知されます。

2 ユーザーのユーザー名をダブルクリックして、ユーザーのサポートを開始します。

3 この機能は次のような場合に便利です。

技術担当者は、ユーザーのコンピュータのマウスおよびキーボードを完全に制御できるようになります。顧客には、技術者が実行する操作がすべて表示されます。

セキュア仮想アシスト セッションの実行中、顧客は自分のコンピュータからロック アウトされるわけではありません。顧客のコンピュータは技術者と顧客のどちらからも制御できますが、両者が同時に操作を実行しようとすると混乱を招くおそれがあります。

顧客側の画面の下部に、3 つのオプションがある小さなツールバーが表示されます。

セキュア仮想アシスト セッション中に顧客は次のオプションを使用できます。それぞれ対応するボタンを選択すると実行されます。

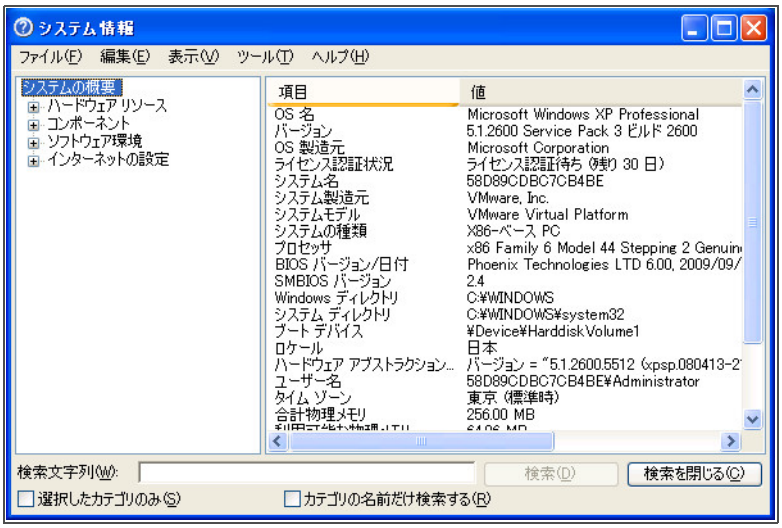
- **状態 [稼動]** - 選択すると**表示のみ** モードに切り替わります。
- **チャット** - 技術者とのチャット ウィンドウを開きます。
- **End Virtual Assist** - セッションを終了します。

セキュア仮想アシスト タスクバーの使用

技術者側のセキュア仮想アシスト ビューには、複数のオプションがあるタスクバーが表示されます。

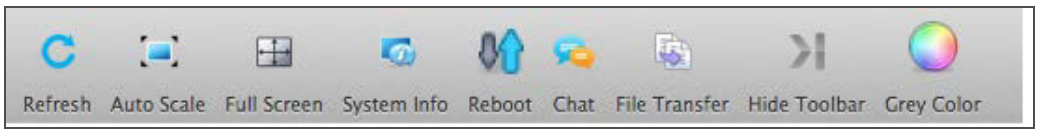
Windows では、タスクバーには以下のボタンがあります。

- **全画面表示** - ウィンドウいっぱいに表示されるように画面サイズを調整します。
- **自動拡大/ 縮小** - ウィンドウに合わせて画面サイズを調整します。
- **拡大** - 設定済みの値の 1 つを選択するか、特定の値を入力して表示をズームします。
- **実際のサイズ** - 100% にズームします。
- **更新** - 顧客のコンピュータ画面を最新の表示に更新します。
- **ファイル転送** - 顧客のコンピュータとの間でファイルを転送するためのウィンドウを開きます。詳細については、セキュア仮想アシストのファイル転送の使用 (66 ページ) を参照してください。
- **チャット** - 顧客と通信するためのチャット ウィンドウを開きます。技術者は、セキュア仮想アシスト アプリケーションの左下ウィンドウの専用チャット ウィンドウを使用することもできます。
- **システム情報** - 顧客のコンピュータに関する詳細な情報を表示します。



- **顧客を再起動** - 顧客のコンピュータを再起動します。完全操作を要求した場合を除き、顧客には再起動が要求されたことが警告され、顧客は再起動を拒否することもできます。
- **表示画面** - 顧客のコンピュータに複数のモニタが設定されている場合に第 2 のモニタに切り替えます。

MacOS では、タスクバーには以下のボタンがあります。



- **更新** - 顧客のコンピュータ画面を最新の表示に更新します。
- **システム情報** - 顧客のコンピュータについて、Windows コンピュータで表示されるような詳細情報を表示します。
- **再起動** - 顧客のコンピュータを再起動します。完全操作を要求した場合を除き、顧客には再起動が要求されたことが警告され、顧客は再起動を拒否することもできます。
- **チャット** - 顧客と通信するためのテキスト チャット ウィンドウを開きます。技術者は、セキュア仮想アシスト アプリケーションの左下ウィンドウの専用チャット ウィンドウを使用することもできます。

- **ファイル転送** - 顧客のコンピュータとの間でファイルを転送するためのウィンドウを開きます。詳細については、セキュア仮想アシストのファイル転送の使用 (66 ページ) を参照してください。
- **ツールバーの非表示** - タスクバーを非表示にします。
- **グレー カラー** - すべてをグレーのモノクロで表示します。

セキュア仮想アシストの表示の制御

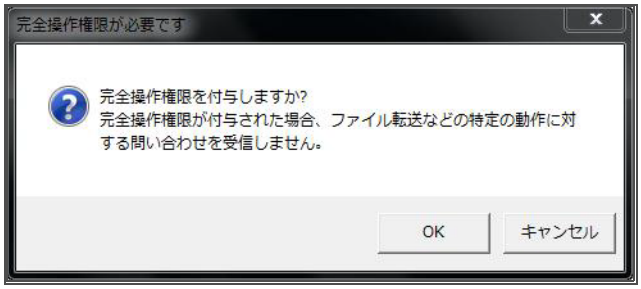
- **全画面表示** - すべてのセキュア仮想アシスト ツールバーを非表示にし、顧客のデスクトップを技術者側の画面全体に表示し、セキュア仮想アシスト タスクバーを左上隅に配置します。

  セキュア仮想アシスト タスクバーが表示されない場合は、マウス ポインタを画面最上部の中央に移動します。タスクバーを右クリックし、「**戻る**」を選択して全画面モードを終了します。
- **自動拡大/縮小** - 表示をセキュア仮想アシスト ウィンドウ全体にズームします。
- **拡大** - 設定済みの値の 1 つを選択するか、特定の値を入力して表示をズームします。
- **実際のサイズ** - 100% にズームします。

ⓘ **メモ**：これらのオプションの多くは、セキュア仮想アシスト アプリケーションの上部にあるドロップダウン メニューを使って設定できます。

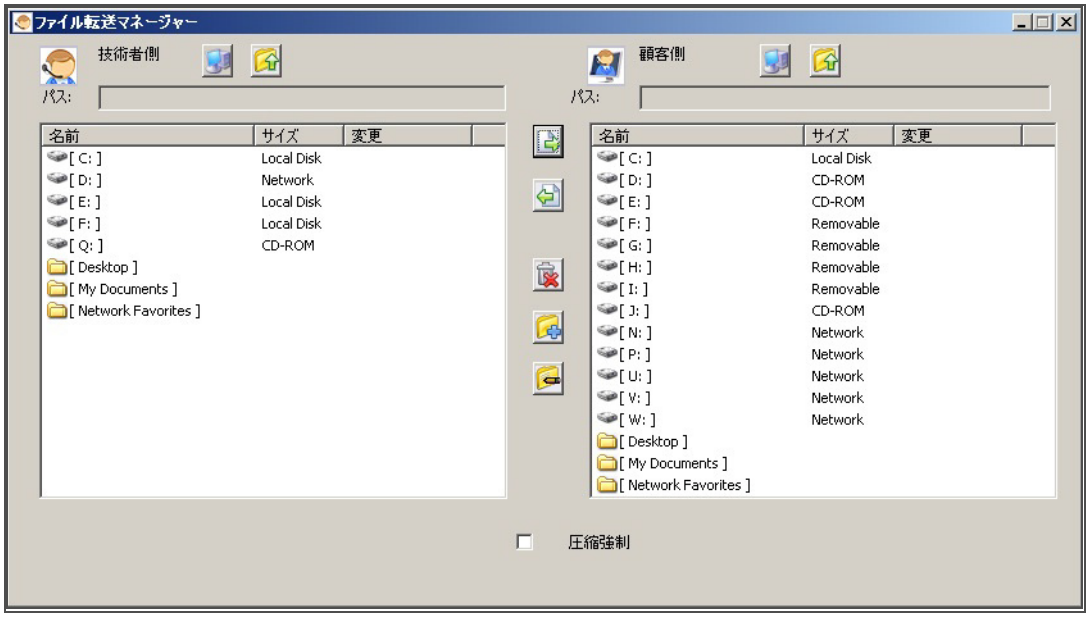
完全操作の要求

技術者は、顧客のデスクトップの完全な制御を要求できます。完全な制御とは、システムの再起動、顧客のコンピュータにあるファイルの削除や上書きを、顧客の同意を得ずに行えることです。「コマンド」メニューの「完全操作の要求」を選択して要求を発行します。この要求は顧客のデスクトップに表示されます。



セキュア仮想アシストのファイル転送の使用

「ファイル転送マネージャ」ウィンドウでは、顧客のコンピュータとの間でファイルを転送できます。左側に技術者のコンピュータのファイル ディレクトリが、右側に顧客のコンピュータのファイル ディレクトリが表示されます。



「ファイル転送マネージャ」ウィンドウは、Windows エクスプローラや FTP プログラムとほぼ同様に機能します。「ファイル転送マネージャ」ウィンドウ内を移動するには、フォルダをダブルクリックし、ファイルを選択します。「ファイル転送マネージャ」ウィンドウには次の機能があります。

- **デスクトップ** - 技術者または顧客のコンピュータのデスクトップに移動します。
- **上へ** - 技術者または顧客のコンピュータの 1 階層上のディレクトリに移動します。
- **ダウンロード** - 選択されている 1 つ以上のファイルを技術者のコンピュータから顧客のコンピュータに転送します。
- **アップロード** - 選択されている 1 つまたは複数のファイルを顧客のコンピュータから技術者のコンピュータに転送します。
- **削除** - 選択されている 1 つ以上のファイルを削除します。

  ⓘ **メモ**：技術者が「**完全操作の要求**」を選択し、顧客がこれを承認した場合を除き、ファイルを削除または上書きしようとすると顧客に警告が送信され、顧客がこの確認に同意しない限り削除や上書きは行われません。

- **新規フォルダ** - 選択されているディレクトリ内に新しいフォルダを作成します。
- **名前の変更** - 選択されているファイルまたはディレクトリの名前を変更します。

ファイルの転送中、「ファイル転送マネージャ」ウィンドウの下部に転送の進捗が表示されます。「**終了**」を選択すると、実行中の転送が中止されます。

ⓘ **メモ**：ファイル転送では、1 つ以上のファイルを転送できます。現時点で、ディレクトリの転送はサポートされていません。複数のファイルを選択するには、**Ctrl** キーを押しながらファイルを選択します。

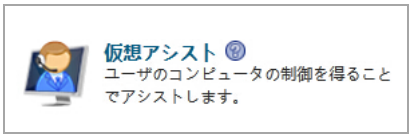
セキュア仮想アクセス用のシステムの有効化

メモ：セキュア仮想アクセスは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

Secure Mobile Access 管理インターフェースの「**ポータル > ポータル**」ページの「仮想アシスト」タブで、セキュア仮想アクセスを有効にすると、システムをセキュア仮想アクセス向けにセットアップするためのリンクがポータル上に表示されます。Secure Mobile Access 管理インターフェースでセキュア仮想アクセスを有効にするには、ポータルごとの仮想アシスト設定の設定 (157 ページ) を参照してください。

次の手順を実行すると、セキュア仮想アクセスをシステムにセットアップできます。

1 セキュア仮想アクセスを設定するシステムからポータルにログインし、「**仮想アクセス**」リンクを選択します。

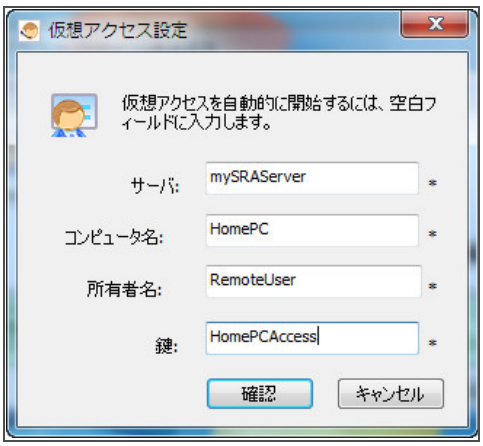


2 VASAC.exe ファイルのインストール ファイルをダウンロードする必要があります。インストール ファイルには VASAC.exe のインストールに必要なパラメータと、セキュア仮想アクセス モードに必要なクライアントが含まれています。このファイルを保存して実行します。

メモ：システムによっては、このダイアログ ボックスからファイルを直接実行できないことがあります。その場合は、ファイルをシステムに保存した後で、アプリケーションを実行します。

3 表示されるフィールドに、システムをセキュア仮想アクセス モードに設定するために必要な情報を入力してから、「**OK**」を選択します。

- **サーバ:** 技術者が、管理インターフェースの外部から仮想オフィスにアクセスするときに使用する装置の名前または IP アドレスを指定します ("https://" は省きます)。
- **ポータル:** 技術者が通常ログインするポータルの名前を指定します。
- **コンピュータ名:** これは、サポートされるのをキューで待機している他のシステムから目的のシステムを区別するための識別子となります。
- **鍵:** これは、技術者がサポート キューを通してシステムにアクセスする前に入力する必要があるパスワードです。



4 インストールが完了すると、VASAC クライアントは、デスクトップ トレイ内に常駐します。

これで、このシステムの識別名が、管理インターフェース内の「**セキュア仮想アシスト > 状況**」ページに表示される技術者のサポート キューに追加されます。システムの一覧をダブルクリックすると、システムへのセキュア仮想アクセスをセットアップする作業で指定したパスワードを入力するように求められます。

セキュア仮想アクセス モードの終了

セキュア仮想アクセス セッションから切断すると、システムはサポート キューに戻ります。技術者は後で再びシステムにアクセスできます。個人システムの側からは、ユーザ/技術者がトレイ オプションのアイコンを使用してアプリケーションをアンインストールしたり、終了したりすることができます。

管理者は、キューからシステムを強制的に削除できます。管理者がシステムをキューから強制的に削除すると、セキュア仮想アクセス システムは今後サポート キューへの接続を試行しなくなり、エラー メッセージが表示されます。

メモ：セキュア仮想アシストをエンド ユーザとして使用する方法およびそのタスクについては、『*Secure Mobile Access ユーザ ガイド*』を参照してください。

セキュア仮想ミーティングの概要

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

(Windows のみでサポート) このセクションでは、セキュア仮想ミーティング機能の概要を説明します。このセクションには次の内容が含まれています。

セキュア仮想ミーティングとは

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想ミーティングは、SMA 400、SRA 4600、および SMA 500v Virtual Appliance 用のウェブベースの管理インターフェースです。セキュア仮想ミーティングでは、複数のユーザがインターネット接続によって実質的に任意の場所から、デスクトップを表示し、ミーティングに対話形式で参加することができます。セキュア仮想ミーティングは、仮想アシストが提供する 1 対 1 のデスクトップ共有に似ていますが、複数のユーザがデスクトップを共有できる点が異なります。

セキュア仮想ミーティングのメリット

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想ミーティングには、次のようなメリットがあります。

- **安全な接続** - SMA/SRA 装置によるデータの 256 ビット AES SSL 暗号化は、データを保護する安全な環境をもたらし、Sarbanes-Oxley 法や HIPAA 法などの法令の遵守に役立ちます。

- **時間とコストの節減** - セキュア仮想ミーティング を使うことにより、顧客サイトを訪問する必要はなくなり、サポート要求に対する平均解決時間が短縮されます。
- **教育用ツール** - トレーナーとサポート スタッフは、セキュア仮想ミーティング を使ってリモートから顧客にプログラムやツールの使い方を示すことができます。
- **複数の機能を提供する構成可能な環境** - すべての仮想ミーティングに適用されるミーティング構成に加えて、特定のミーティング向けにミーティング パラメータを設定できます。
- **ミーティング機能** - ミーティング参加者は、ミーティング参加者による投票、テキスト チャット、デスクトップ共有者の切り替え、ミーティングの制御など、複数の機能を実行できます。

ユーザの役割

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想ミーティングにはいくつかのユーザの役割があります。

- **責任者** (ミーティングのオーナー) - 責任者は、装置上の Secure Mobile Access ユーザである必要があります。責任者は、ミーティングをスケジュール、セットアップ、および制御します。また、責任者には、参加者をアシスタントに昇格する独占的な権限もあります。
- **アシスタント** (責任者指名のアシスタント) - 責任者は、利用可能な参加者の一覧からアシスタントを選択して、アシスタント権限を割り当てます。責任者がミーティングを終了すると、アシスタントは自動的に責任者になります。1 つのミーティングに複数のアシスタントを設定できます。全員が同じ権限セットを持つことも、各自異なる権限セットを持つこともできます。アシスタントは SMA/SRA 装置のユーザである必要はありません。アシスタントには、次の権限を割り当てることができます。
  - ミーティングを開始/終了する
  - ホストを設定する
  - 投票を開始する
  - 「表示のみ」を設定/解除する
  - 参加者を招待する
  - 参加者を追放する
  - ミーティングの予定を変更する
- **ホスト** - ホストは、ミーティングの参加者全員とデスクトップを共有する参加者です。ミーティングが始まると、ホストのデスクトップがすべての参加者に表示されます。責任者は別の参加者を選択することによって、ミーティング中にホストを交代できます。ミーティングの開始時にホストが明示的に設定されていない場合は、責任者がホストになります。同時に 1 人の参加者のみをホストに指名できます。

  ホスト システムを制御できるのはホストのみです。ただし、参加者が制御を要求し、ホストが権限を与える場合を除きます。ホストは、権限を与える参加者をミーティング参加者の一覧から選択することもできます。同時に 1 人の参加者のみが、ホスト システムを制御できます。ある参加者がホスト システムの制御権を持っていても、ホストが画面上でマウス ポインタを動かした時点で、その参加者は制御権を失います。ミーティングの制御権限の状況は、ロビーにいる参加者全員に表示されます。
- **参加者** (ミーティングに参加する認証情報を持つユーザ) - 参加者は、ミーティングに参加する前にミーティング コードを入力する必要があります。ミーティングへの参加に必要なコードは、ミーティングの前に責任者によって決定されます。ミーティングに参加すると、参加者は

共有デスクトップを表示したり、他の参加者とプライベートでチャットしたり、すべての参加者に表示される「チャット」ウィンドウにメッセージを入力したりできます。責任者または必要な権限を持つアシスタントによって選択された参加者は、アシスタントになります。

- **「表示のみ」参加者** (ミーティング機能が制限されるユーザ) - 責任者は、参加者を「表示のみ」参加者に指定できます。「表示のみ」参加者は、権限の割り当てを受けることも、アシスタントやホストになることもできません。

役割は、ミーティング前またはミーティング中に切り替えられます。責任者または必要な権限を持つアシスタントは、ミーティング中に、任意の参加者の役割を変更できます。ホストになりたい参加者は、責任者に権限を要求する必要があります。

セキュア仮想ミーティングの仕組み

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

以下のセクションを参照してください。

- セキュア仮想ミーティングの設定 (70 ページ)
- 責任者タスクの実行 (70 ページ)
- 参加者タスクの実行 (72 ページ)

セキュア仮想ミーティングの設定

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

セキュア仮想ミーティングの設定と管理は、ウェブベースの Secure Mobile Access 管理インターフェースから行います。以下のタスクがあります。

- 状況
- 設定
- ログ
- ライセンスの適用

上記のタスクの詳細については、セキュア仮想ミーティングの概要 (68 ページ) およびセキュア仮想ミーティング機能モジュールの説明に記載されています。

責任者タスクの実行

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

仮想ミーティングの責任者は、次のタスクを実行します。

仮想ミーティングの責任者のタスク

責任者タスク	説明
ログイン	Secure Mobile Access 認証情報を使用して仮想ミーティング クライアントからログインします。
ミーティングのセットアップ	ミーティングの時刻を予定し、ミーティング参加者がミーティングに参加するためのミーティング コードを作成して、ミーティングをセットアップします。
ロビー機能の実行	ミーティング前またはミーティング中に、ロビーの各種ミーティング機能にアクセスします。ロビー機能の実行 (71 ページ) を参照してください。
役割の制御	ミーティング参加者が実行できる操作を制御し、アシスタントを指名してミーティングを促進します。
ミーティングの設定の修正	プロキシをセットアップするか、ログイン プロファイルをミーティングに合わせて変更します。
動作とメッセージのログ	発生した動作のログを確認し、注意を要する警告またはエラー メッセージの詳細を参照します。
ミーティング中の制御メニューの使用	ミーティング中に、利用可能な機能にアクセスします。ミーティング中の制御メニューの使用 (72 ページ) を参照してください。
電子メールの招待状の作成	ミーティング前またはミーティング中に、電子メールでミーティング参加者を招待します。
投票	参加者が参加する投票を作成します。
投票のフィードバックの確認	投票に対して送信されたフィードバックを確認します。
テキスト チャット	全員と、またはミーティング内の特定の個人とチャットします。

ロビー機能の実行

各ボタンを選択することによって、ロビーで次の機能が実行できます。


「**ミーティングの開始**」を選択して、ミーティングを開始します。ミーティングを開始できるのは、責任者とアシスタントのみです。


「**ミーティングの終了**」を選択して、ミーティングを終了します。ミーティングを終了できるのは、責任者とアシスタントのみです。


「**投票**」を選択して、投票ウィンドウを開きます。投票ウィンドウでは、現在のミーティング参加者を対象とした投票の読み込み、編集、開始が可能です。投票を開始できるのは、責任者とアシスタントのみです。


「**招待**」を選択して、参加者に電子メールの招待状を送信します。参加者を招待できるのは、責任者とアシスタントのみです。


「**予定の変更**」を選択して、ミーティングの開始時刻と終了時刻の予定を変更します。ミーティングの予定を変更できるのは、責任者とアシスタントのみです。


「**ホストの要求**」を選択して、自分がホストになってデスクトップを共有したいことをホストに伝えます。ホストになることを要求できるのは、その時点でホストではない参加者のみです。


「**ミーティングから退席**」を選択して、ミーティングを終了し、ミーティング選択ウィンドウに戻ります。ミーティングに参加している誰もがミーティングから退席できます。


「**共有の開始**」を選択して、ミーティング参加者全員でホストのデスクトップを共有します。共有できるのはミーティング中のみです。

 「**共有の停止**」を選択して、ホスト システムのデスクトップの共有を停止します。共有を停止できるのはホストのみで、(「共有の開始」が選択されて) 共有状態にある場合のみです。

 「**制御の要求**」を選択して、自分にキーボード/マウス制御を与えるようにホストに要求します。制御を要求できるのは、ホスト以外の参加者のみです。

ミーティング中の制御メニューの使用

操作メニューは、ミーティング中にホストがデスクトップを共有している場合に、共有デスクトップの上部に表示されます。

 「**招待**」は、責任者または招待権限を持つアシスタントが使用できます。ロビーが開いていない場合は、招待ダイアログが開きます。

 「**投票**」は、責任者または投票権限を持つアシスタントが使用できます。投票ダイアログが開きます。

 「**チャット**」は、参加者全員 (「表示のみ」参加者を含む) が使用できます。ロビーが開いていない場合は、チャット ダイアログが開きます。

 「**ロビー**」は、ミーティング参加者全員 (「表示のみ」参加者を含む) が使用できます。ミーティング中にロビーが非表示になっており、ホストが画面を共有している場合は、ロビー ウィンドウが表示されます。

 「**設定**」を選択すると、ミーティングの設定ウィンドウが開きます。この機能は参加者全員が使用できます。

 「**ビューア**」は、ホスト以外の参加者全員が使用できます。このボタンは、参加者のウィンドウとホストのデスクトップの間で、ウィンドウを切り替えます。

 「**情報**」は、セキュア仮想ミーティング クライアントとバーションを示す「バージョン情報」ダイアログを開きます。「**情報**」は、ミーティング参加者全員 (「表示のみ」参加者を含む) が使用できます。

参加者タスクの実行

メモ：セキュア仮想ミーティングは廃止される予定です。レガシー サポートが必要な場合は、SonicWall カスタマー サポートに設定の手順をお問い合わせください。

参加者は、「表示のみ」参加者または通常の参加者として指定できます。「表示のみ」参加者は、他の参加者と同じようにミーティングに参加し、退場することができますが、実行できる機能はほとんどありません。ただし、「表示のみ」参加者は追放されることがあります。これについては他の通常の参加者と同様です。通常の参加者は次の操作も行えます。

- 投票に回答する
- テキスト チャット

- ホストのキーボード/マウス制御を要求する
- ホストになることを要求し、参加者のデスクトップを共有する
- アシスタントになる
- 「表示のみ」アシスタントになる

ウェブ アプリケーション ファイアウォールの概要

(ウィンドウズのみサポート) このセクションでは、ウェブ アプリケーション ファイアウォール機能の概要を説明します。このセクションには次の内容が含まれています。

- ウェブ アプリケーション ファイアウォールとは (73 ページ)
- ウェブ アプリケーション ファイアウォールの利点 (76 ページ)
- ウェブ アプリケーション ファイアウォールの仕組み (77 ページ)

ウェブ アプリケーション ファイアウォールとは

ウェブ アプリケーション ファイアウォールは購読ベースのソフトウェアです。このソフトウェアは、SMA/SRA 装置で実行され、装置の背後のサーバ上で実行されているウェブ アプリケーションを保護します。また、ウェブ アプリケーション ファイアウォールは、SMA/SRA 装置本体で実行される HTTP(S) ブックマーク、Citrix ブックマーク、オフロードされたウェブ アプリケーション、Secure Mobile Access 管理インターフェースやユーザ ポータルなどのリソースをリアルタイムで保護します。

ウェブ アプリケーション ファイアウォールは、クロスサイト スクリプティング、SQL インジェクション、OS コマンド インジェクションなどさまざまなウェブ攻撃からリアルタイムで防御します。ウェブ アプリケーションに発見される脆弱性のトップ 10 が、OWASP によって追跡されています。OWASP は、ウェブ アプリケーションのセキュリティ強化に専門に取り組むオープン ソース コミュニティの組織です。Secure Mobile Access ウェブ アプリケーション ファイアウォールは、これらの脆弱性トップ 10 からシステムを保護するため、次の対策をとります。

OWASP の脆弱性トップ 10

名前	説明
A1 - クロスサイト スクリプティング (XSS)	XSS によって攻撃されるのは、ユーザから入力されたデータをアプリケーションがウェブ ブラウザに送信するときに、その内容が事前に検証もエンコーディングもされない場合です。攻撃者は、XSS を利用してターゲットのブラウザでスクリプトを実行することにより、ユーザのセッションを乗っ取ったり、ウェブ サイトを改ざんしたり、ワームを侵入させたりすることができます。
A2 - インジェクション フロー	インジェクション フロー、特に SQL インジェクションは、ウェブ アプリケーションに対して一般的に試みられる手口です。インジェクションは、ユーザから提供されたデータが、コマンドまたは問い合わせの一部としてインタプリタに送信される場合に起こります。攻撃者は、悪意のあるデータ トリックにより、インタプリタが意図しないコマンドを実行したり、データを変更したりするように仕向けます。

OWASP の脆弱性トップ 10 (続き)

名前	説明
A3 - 悪意のあるファイルの実行	RFI (Remote File Inclusion) に脆弱なコードは、攻撃者が用意した悪意のあるコードやデータを取り込んでしまい、サーバ全体の侵害など、破壊的な攻撃を招きます。"悪意のあるファイルの実行" 攻撃は、PHP、XML、またはユーザからファイル名またはファイルを受け取るすべてのフレームワークで起こり得ます。
A4 - 危険な直接的オブジェクト参照	直接的オブジェクト参照は、開発者がファイル、ディレクトリ、データベース レコード、キーなどの内部実装オブジェクトを URL またはフォーム パラメータとして公開した場合に起こります。攻撃者は、これらの参照を操作して、承認を得ずに他のオブジェクトにアクセスできます。
A5 - クロスサイトリクエストフォージェリ (CSRF)	CSRF 攻撃は、ユーザがログオン中のブラウザに対して、認証済みの要求を脆弱性のあるウェブ アプリケーションに送信することを強制し、そのウェブ アプリケーションを通じて、攻撃者の利益になる不正な操作をブラウザに実行させることを指します。CSRF を利用すると、攻撃対象のウェブ アプリケーションが持つ機能を自由に悪用できます。
A6 - 情報の漏洩および脆弱なエラー処理	アプリケーション側のさまざまな問題により、アプリケーションの設定や内部処理に関する情報が予期せずに漏洩したり、プライバシーが侵害されることがあります。この脆弱性は、機密データを盗むための手段となったり、さらに深刻な攻撃の足がかりとなったりします。
A7 - 不適切な認証およびセッション管理	アカウント資格情報やセッション トークンが適切に保護されないことがあります。パスワード、キー、または認証トークンを不正に入手し、他人に成りすますことができます。
A8 - 安全でない暗号での保存	ウェブ アプリケーションでは、データや資格情報を保護するために暗号機能が適切に使用されることはめったにありません。十分に保護されていないデータを不正に入手し、成りすましや、クレジットカード詐欺などの他の犯罪に悪用できます。
A9 - 安全でない通信	秘匿すべき通信を保護するためにネットワーク トラフィックを暗号化する必要がある場合でも、それを怠るアプリケーションがよく見られます。
A10 - URL アクセスの制限の欠陥	未認証のユーザに対してリンクまたは URL を表示しないだけで重要な機能を保護できると考えて設計されたアプリケーションがよく見られます。この脆弱性を悪用すると、このような URL に直接アクセスすることにより、不正に操作を実行できます。

Slowloris 防御

前記のリストにあるトップ 10 脅威に加えて、ウェブ アプリケーション ファイアウォールは Slowloris HTTP DoS 攻撃に対する保護を行います。これは、ウェブ アプリケーション ファイアウォールがすべてのバックエンド ウェブ サーバをこの攻撃から保護することを意味します。Apache を含む多くのウェブ サーバは、Slowloris に対して弱点があります。Slowloris は特に、スレッド化プロセスを使い、許可されるスレッド数を制限するウェブ サーバに対して影響を与えます。

これは、他の接続が閉じてソケットが開いたときにソケットを消費して、徐々にすべてのソケットを拘束します。Slowloris は異なるホスト ヘッダを送信可能で、GET、HEAD、そして POST 要求を送信可能です。不完全な要求の文字列は、TCP ではなく HTTP を使うということを除いて、Slowloris を SYN フラッドに匹敵するものにします。対象のウェブ サーバのみが影響を受ける一方、同サーバ上の他の

サービスやポートは利用可能のままです。攻撃が中断された際、ウェブ サーバは 5 秒程度で通常の状態に戻ることができるので、Slowloris は他の攻撃が開始される間の短時間のダウンタイムや混乱を引き起こすために効果的です。攻撃が中断された際、ウェブ サーバは 5 秒程度で通常の状態に戻ることができるので、Slowloris は他の攻撃が開始される間の短時間のダウンタイムや混乱を引き起こすために効果的です。攻撃が停止されるかセッションが閉じられると、ウェブ サーバは数百の 400 エラーを表示する場合があります。

ウェブ アプリケーション ファイアウォールが OWASP トップ10 および Slowloris 種別の攻撃にどのように対抗するかは、ウェブ アプリケーション ファイアウォールの仕組み (77 ページ) を参照してください。

オフロードされたウェブ アプリケーション防御

ウェブ アプリケーション ファイアウォールは、オフロードされたウェブ アプリケーションを保護することもできます。オフロードされたウェブ アプリケーションは、SMA/SRA 装置の背後のサーバで実行されるウェブ アプリケーションにシームレスにアクセスできる専用ポータルとして作成されます。このポータルは仮想ホストとして設定します。このようなオフロードされたホストに対しては、認証とアクセス ポリシーの強制を無効にすることが可能です。SonicWall Inc.認証を有効にする場合、このポータルに適切なドメインを関連付ける必要があり、オフロードされたホストには、ワンタイム パスワード、二段階認証、シングル サイン オンといった SonicWall の高度な認証機能すべてが適用されます。

アプリケーション プロファイリング

アプリケーション プロファイリング (フェーズ 1) により、管理者は入力の信頼されるセットに基づいて自動化された方法でユーザ定義ルールを生成できます。これは、どの入力がアプリケーションによって受諾しうるかのプロファイルを展開するので、ウェブ アプリケーションにセキュリティを提供する非常に効果的な手法です。その他すべてが拒否され、肯定的セキュリティ拡張が提供されます。これは否定的セキュリティ モデルを採用する一般的なシグネチャに比べて、誤検知が少なくなります。管理者が準備環境に機器を学習モードで配備すると、SMA/SRA 装置は信頼されたユーザによってアクセスされた各 URL に対する正しい入力を学習します。学習プロセス中または後のどのタイミングでも、"学習した" プロファイルに基づいてユーザ定義ルールを生成できます。

ユーザ定義ルールに対する速度制限

ユーザ定義ルールまたは連鎖ルールに一致している速度を監視できます。これは辞書攻撃やブルートフォース攻撃を遮断するために、きわめて有用です。連鎖ルールに対する動作は、連鎖ルールが設定された回数と同じだけ一致した場合にのみ起動されます。

Cookie 改竄防御

Cookie 改竄防御は Payment Card Industry Data Security Standard (PCI DSS) セクション 6.6 要件内で重要な項目で、バックエンド ウェブ サーバによって Cookie セットに対して厳格なセキュリティを提供するウェブ アプリケーション ファイアウォール評価基準の部分です。暗号化およびメッセージ ダイジェストといった様々なテクニックが Cookie 改竄を防ぐために使われます。詳細については、Cookie 改竄防御の設定 (316 ページ) を参照してください。

クレジット カードおよび社会保障番号 (SSN) 保護

クレジット カードおよび社会保障番号 (SSN) 保護は、クレジット カード番号や社会保障番号といった取り扱いに慎重を要する情報がウェブ ページ内に漏洩しないように保護する、データ損失保護技術です。そういった漏洩が検知されると、管理者はこれらの番号を部分的または全体的に隠す、設定可能なエラー ページを表示する、または単にイベントをログ記録する選択ができます。詳細については、情報暴露防御の設定 (319 ページ) を参照してください。

ウェブ サイト隠蔽

ウェブ サイト隠蔽は、ウェブ サーバの配備情報を推測することと、その弱点を突くことを防ぎます。詳細については、ウェブ サイト隠蔽の設定 (318 ページ) を参照してください。

WAF 監視用 PDF レポートおよび PCI DSS 6.5 と 6.6 準拠

ウェブ アプリケーション ファイアウォール監視、および、PCI DSS 6.5 と 6.6 準拠に対して PDF レポートが提供されます。「**ウェブ アプリケーション ファイアウォール > 状況**」ページ上でレポートを生成できます。レポート内に記載されるデータを生成するためのタイムラインは、「**ウェブ アプリケーション ファイアウォール > 監視**」ページで設定可能です。

ウェブ アプリケーション ファイアウォールの利点

ウェブ アプリケーション ファイアウォールは安全です。金融サービス、医療、アプリケーション サービス プロバイダ、電子商取引など、さまざまな分野で使用できます。Secure Mobile Access は SSL 暗号化を用いてウェブ アプリケーション ファイアウォールとクライアントの間でデータを暗号化します。Secure Mobile Access は OWASP の暗号化ストレージに関する要件も満たしており、必要に応じてキーとパスワードを暗号化します。

ウェブ アプリケーション ファイアウォールを導入した企業は、安全性の高いアプリケーションの作成に必要な開発コストを削減できるだけでなく、サインアップしてウェブ アプリケーション ファイアウォールのシグネチャの更新を行うことで、新しく見つかった脆弱性への対処をすべてのウェブ アプリケーションについて行うための膨大な作業時間を省くことができます。

オフロード アプリケーションのポータルや HTTP(S) ブックマークからアクセスされるリソースは、手法の不備やプログラミング エラーなどさまざまな理由で攻撃を受けやすくなります。ウェブ アプリケーション ファイアウォールは、SMA/SRA 装置の背後のウェブ アプリケーションをリアルタイムに保護することによって、このような脆弱性に対するハッカーの攻撃を効果的に防ぎます。

ウェブ アプリケーション ファイアウォールを SMA/SRA 装置に配備すると、セキュリティを必要とするウェブ アプリケーションが内部ユーザとリモート ユーザに公開されることになる場合でも、ネットワーク管理者はアプリケーション オフロードを使用できます。アプリケーション オフロードでは URL 書き換えを回避できるので、プロキシのパフォーマンスと機能性が向上します。

ウェブ アプリケーション ファイアウォールを SMA/SRA 装置に統合することにはさまざまな利点があります。第 1 に、ID ベースのポリシー制御がウェブ アプリケーション ファイアウォールの中核であり、Secure Mobile Access テクノロジを使って容易にこれが実現可能になります。第 2 に、既存のハードウェア ベースの SSL オフロードにより、待ち時間が短くなります。最も重要なのは、ウェブ アプリケーションを実行する SMA/SRA 装置をこうした攻撃から保護する必要があるということです。

中小企業が仕入先との提携、在庫管理、オンライン販売、顧客アカウント管理にホスト サービスを採用する場合も、大企業と同じような厳しい順守要件に直面します。SMA/SRA 装置のウェブ アプリケーション ファイアウォールは、便利で費用効果の高いソリューションを提供します。

ウェブ アプリケーション ファイアウォールは、Secure Mobile Access 管理インターフェースで容易に設定できます。管理者は、グローバルにも、攻撃危険度ごとにも、シグネチャごとにも設定できます。個別の設定または除外項目を指定した後は、ウェブ アプリケーション ファイアウォールを無効にしてもそれらの設定は維持されるので、保守作業やテストを行ってから容易にまた有効に戻すことができます。

ウェブ アプリケーション ファイアウォールの仕組み

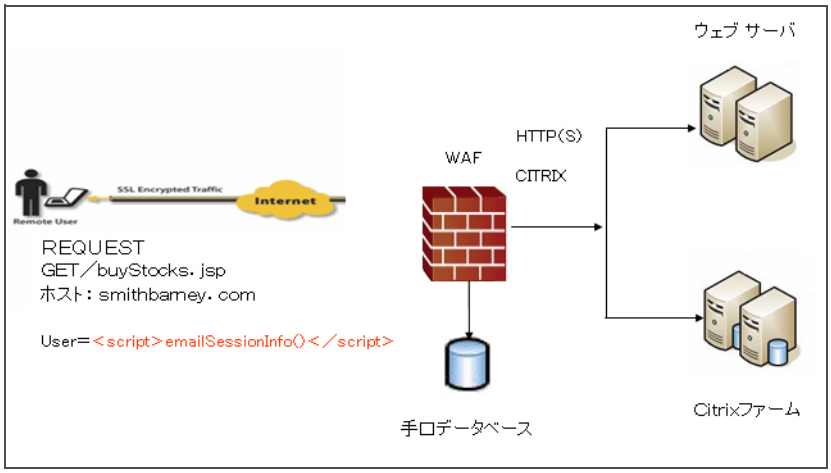
ウェブ アプリケーション ファイアウォール機能を使用するには、管理者はまずこのソフトウェアのライセンスを取得するか、無料トライアルを開始する必要があります。次に、Secure Mobile Access 管理インターフェースの「**ウェブ アプリケーション ファイアウォール > 設定**」ページで、ウェブ アプリケーション ファイアウォールを有効にする必要があります。検出されたインターネット経由の攻撃をログ記録または遮断するようウェブ アプリケーション ファイアウォールを設定できます。

次の各セクションでは、Slowloris または、OWASP のトップ 10 に挙げられるような攻撃を阻止するためのウェブ アプリケーション ファイアウォールと SMA/SRA 装置の仕組み、ウェブ アプリケーション ファイアウォールが情報暴露に対して保護する仕組みと、その他の機能が動作する仕組みについて説明します。

シグネチャに基づいて攻撃を阻止する方法

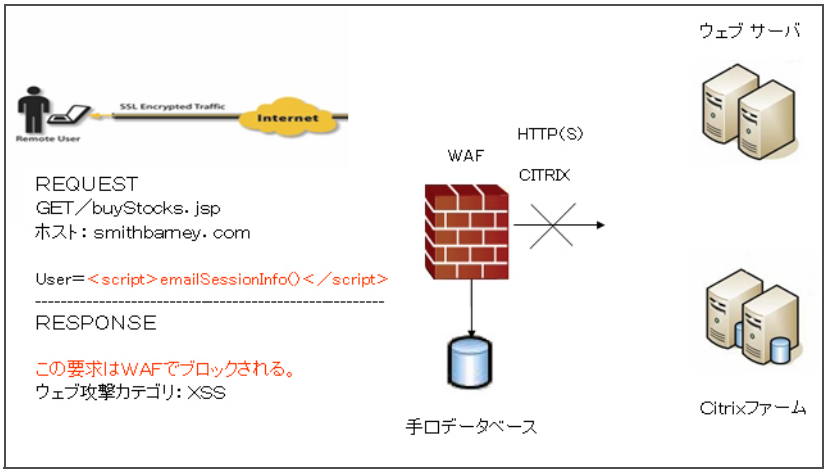
クロスサイト スクリプティング、インジェクション フロー、悪意のあるファイルの実行、危険な直接的オブジェクト参照の脆弱性について、ウェブ アプリケーション ファイアウォール機能では、ウェブ アプリケーション攻撃の既知のシグネチャのブラック リストが使用されます。SonicWall Inc. シグネチャ データベース サーバから定期的に新しいシグネチャ情報更新をダウンロードすることによって、新しい攻撃からの保護に対応します。

シグネチャを使用して攻撃を阻止する方法



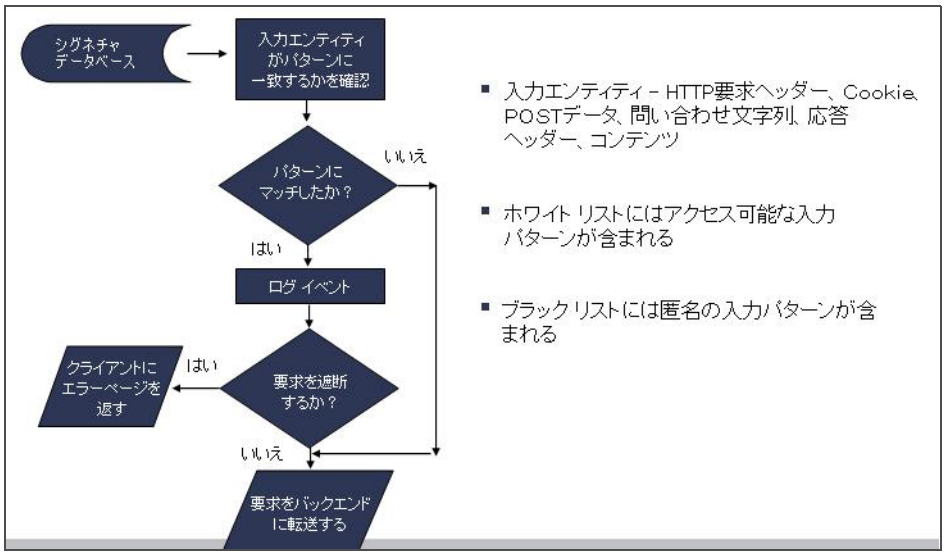
インターネットからの入力があると、ウェブ アプリケーション ファイアウォールは、HTTP/HTTPS 要求ヘッダー、Cookie、POST データ、問い合わせ文字列、応答ヘッダー、コンテンツを検出します。この入力は、シグネチャのブラック リストとホワイト リストの両方と照合されます。いずれかのシグネチャとパターンが一致すると、設定に応じて、そのイベントが記録され、その入力が遮断されます。遮断された場合は、クライアントにエラー ページが返され、リソースへのアクセスは拒否されます。遮断された場合は、クライアントにエラー ページが返され、リソースへのアクセスは拒否されます。脅威の詳細は、エラー ページの URL には示されません。検出のみを設定していた場合は、攻撃は記録されますが、クライアントはリソースにアクセスできます。どのシグネチャとも一致しなかった場合は、要求はウェブ サーバに転送されて処理されます。

どのシグネチャとも一致しなかった場合はどうなるか



ウェブ アプリケーション ファイアウォールのプロセスの概要を以下のフローチャートに示します。

ウェブ アプリケーション ファイアウォール プロセス



要求が遮断された場合、以下のエラー ページがクライアントに返されます。

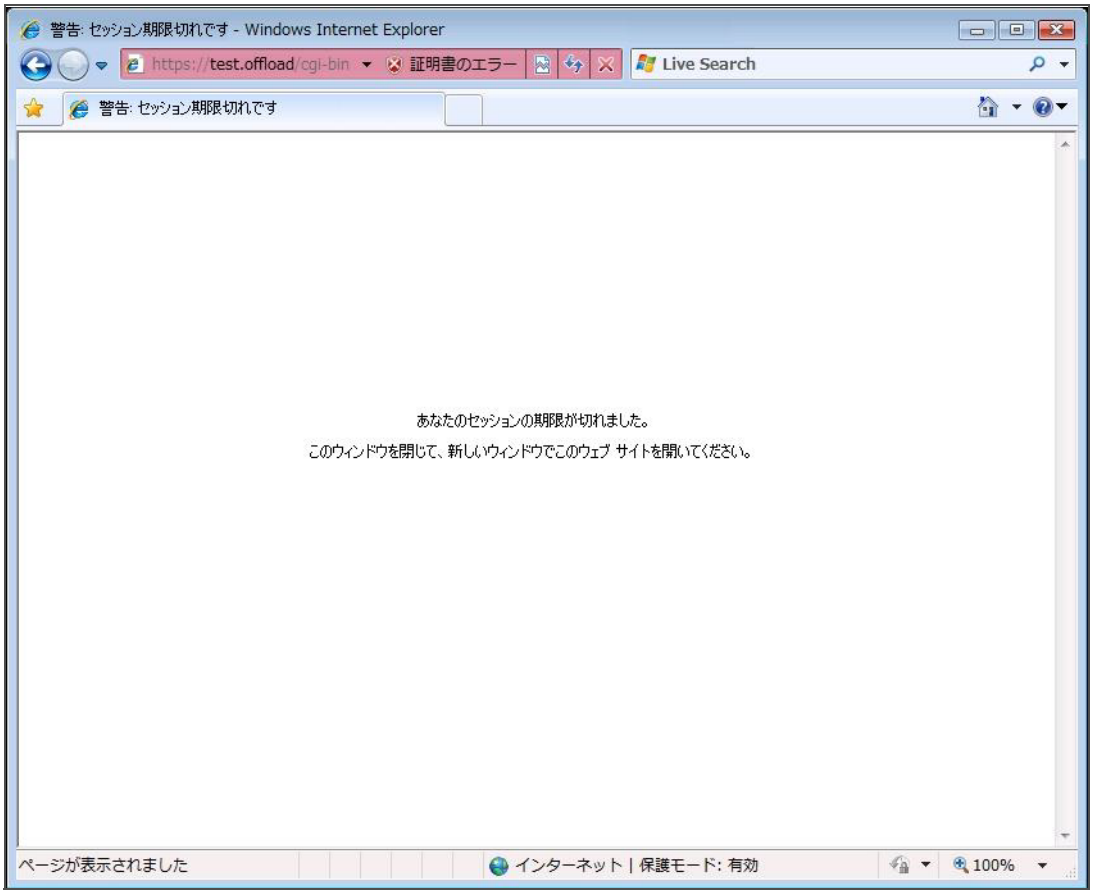
このページは、Secure Mobile Access 管理インターフェースの「**ウェブ アプリケーション ファイアウォール > 設定**」でカスタマイズできます。管理者によっては、このページの HTML コンテンツをカスタマイズしたいという場合があります。セキュリティ上の理由から、ユーザにわかりやすいページを表示しないようにしたい場合もあります。その場合、404 (Not found) や 403 (Access Denied) などの HTTP エラー コードを表示するという方法もあります。

クロスサイトリクエストフォージェリを阻止する方法

CSRF 攻撃は、シグネチャを照合する方法では検出されません。この脆弱性を使ってユーザに成りすましたハッカーは、ユーザ セッションの Cookie を盗まなくても、アプリケーションに不正にアクセスできます。被害にあったユーザは攻撃対象のウェブ サイトで認証されますが、同じブラウザ プロセスのコンテキスト内に別のサイトから悪意のあるウェブ ページが知らない間に読み込まれます。これは、同じブラウザ ウィンドウの新しいタブにページを読み込む、などの方法で行われます。この悪意のあるページから密かに要求が攻撃対象のウェブ サーバに送信されると、ブラウザ メモリ内のセッション Cookie がこの要求の一部として使われ、要求は認証されたものとして扱われます。ウェブ サーバは、ユーザがサイトで行った操作の結果として要求が送信されたと見なし、要求元のウェブ ページに応答します。通常、ハッカーはこの脆弱性を最大限に利用するために、データの更新など、アクションを伴う要求を攻撃実行に使用します。

CSRF 攻撃を阻止するには、ブラウザ セッション内の各 HTTP 要求に、ユーザ セッションに基づくトークンを添付する必要があります。ウェブ アプリケーション ファイアウォールでは、各要求にこのトークンを添付するために、HTTP (S) ブックマークのリバース プロキシ機能による URL の書き換えと似た方法で、ウェブ ページ内のすべての URL を書き換えます。CSRF 保護を有効にすると、この措置がアプリケーション オフローダについても実行されます。

ポータルで認証が強制されている場合は、ユーザはポータルのログイン ページにリダイレクトされます。



情報の暴露を阻止する方法

ウェブ アプリケーション ファイアウォールでは、情報の暴露と脆弱なエラー処理を狙う攻撃を阻止するために、機密情報や取り扱いに注意を要する情報が含まれるテキストを設定して、ウェブ サイトからウェブ アプリケーション ファイアウォールを通してそのようなテキストにアクセスできないようにすることができます。このようなテキストは、「**ウェブ アプリケーション ファイアウォール > 設定**」ページで入力します。

個別テキストのパターン一致を検出する機能に加え、情報の暴露に関するシグネチャもこのタイプの攻撃を阻止するために使用できます。

ウェブ アプリケーション ファイアウォールは、HTML ウェブ ページ内でのクレジット カードまたは社会保障番号 (SSN) の不慮の暴露に対して保護します。

ⓘ **メモ**：クレジット カードまたは SSN の暴露に対しては、テキストまたは HTML ページのみで、最初の 512 キロバイトのみ検査されます。

ウェブ アプリケーション ファイアウォールは様々な形式でクレジットカードと SSN 番号を特定できます。例えば、XXX XX XXXX か XXX-XX-XXXX のような SSN を特定できます。ウェブ アプリケーション ファイアウォールは、クレジット カードや SSN 仕様に従わない形式を除外することで、誤検知を排除するように試みます。例えば、クレジットカードは、n 桁の数がクレジットカード番号であるかどうかを決定するために Luhn アルゴリズムに従います。

管理者はユーザの身元を明らかにできる桁を、検出 (ログ)する、防御する、または単にマスクするといった、適切な動作を設定できます。文字の隠蔽 (マスキング) は全体または一部に適用でき、次の文字を隠蔽文字として使用できます: #、*、-、x、X、.、!、$、?。このマスクされた番号は、送り状に印刷されたクレジット カード番号の外観と同様になります。

不適切な認証への攻撃を阻止する方法

不適切な認証およびセッション管理への攻撃に対抗するために、ウェブ アプリケーション ファイアウォールは、強力なセッション管理を提供することでウェブ サイトの必要な認証レベルを強化することが求められます。Secure Mobile Access は既に強力な認証機能を備えており、ワンタイム パスワード、二段階認証、シングル サインオン、クライアント証明書認証に対応することができます。

セッション管理については、ユーザ ポータルが起動するときやユーザがアプリケーション オフロード ポータルにログインするときに、ウェブ アプリケーション ファイアウォールはセッション ログアウトのダイアログ ボックスをポップアップ表示します。この機能は、ウェブ アプリケーション ファイアウォールがライセンスされると既定で有効になります。無効にするには、「**ウェブ アプリケーション ファイアウォール > 設定**」ページを使用します。

安全でない保存と通信への攻撃を阻止する方法

安全でない暗号での保存および安全ではない通信の脆弱性を狙う攻撃を阻止するために、必要に応じてキーとパスワードを暗号化し、さらに SSL 暗号化を使ってウェブ アプリケーション ファイアウォールとクライアント間のデータを暗号化します。また、Secure Mobile Access ではバックエンド ウェブ サーバで HTTPS もサポートされます。

URL アクセスの制限の欠陥への攻撃を阻止する方法

Secure Mobile Accessは、ホスト、サブネット、プロトコル、URL パス、およびポートに基づいてウェブ サイトへのアクセスを許可または拒否するアクセス ポリシーをサポートしています。このポリシーは、グローバルに設定することも、ユーザやグループ単位で設定することもできます。

Slowloris 攻撃を阻止する方法

Slowloris 攻撃は SMA/SRA セキュリティ装置のような、HTTP 要求を制限、バッファ、またはプロキシするアップストリームの機器がある場合には阻止できます。ウェブ アプリケーション ファイアウォールは、速度制限を使って Slowloris HTTP DoS 攻撃を阻止します。

利用可能な PCI 準拠レポートの種別

PCI レポートでは、Payment Card Industry Data Security Standard (PCI DSS) 6.5 (バージョン 2.0) and PCI DSS 6.6 (バージョン 1.2) がカバーされています。管理者は、これらの PCI 要求を満たすようにウェブ アプリケーション ファイアウォールを構成できます。

「**ウェブ アプリケーション ファイアウォール > 状況**」ページから PCI レポート ファイルの生成とダウンロードが可能です。

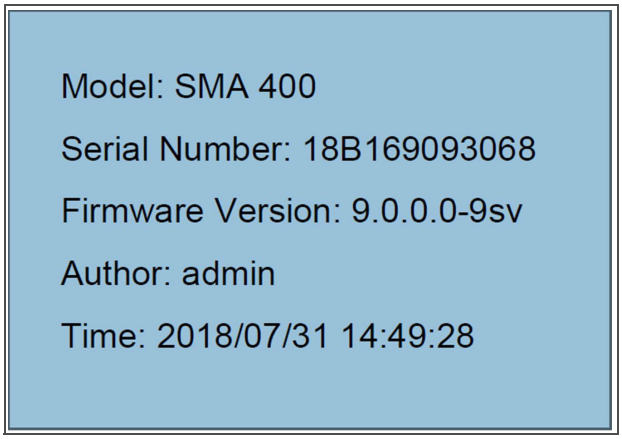
メモ : これは公式な PCI 準拠レポートではありません。自己評価のためだけに使用してください。

レポートの表紙には、以下の情報が表示されます。

- 装置のモデル、シリアル番号、ファームウェア バージョン

- レポートの著者として、レポートをダウンロードした人のユーザ名
- レポートが生成された日時

以下に例を示します。



PCI 準拠レポート内に、それぞれの PCI 要件の状況を表示するための 2 つの表が動的に生成されます。表の形式は次の例のとおりです。

PCI DSS 6.5 準拠レポート (PCI DSS バージョン 2.0)

PCI DSS 6.5 要件	状況	コメント
1. インジェクションの不具合 (特に SQL インジェクション)。OS コマンド インジェクション、LDAP および Xpath のインジェクションの不具合、その他のインジェクションの不具合も考慮する。	適合	

1 列目は、PCI 要件を説明します。

2 列目は、現在のウェブ アプリケーション ファイアウォール設定下での、それぞれの PCI 要件の状況を示します。この列に対して可能な値は 4 つあり、色で区別されています。

- 適合 (緑)
- 一部適合 (オレンジ)
- 不適合 (赤)
- 判断不能 (黒)

3 列目は、コメントと状況評価を説明する詳細を提供します。状況が「適合」の場合はコメントは提供されません。

Cookie 改竄防御の動作

SMA/SRA 装置は、重要なサーバ側 Cookie を改竄から保護します。

Cookie には 2 種類あります。

- **サーバ側 Cookie** - これらの Cookie はバックエンド ウェブ サーバによって生成されます。これらは重要で保護される必要があります。これらは Path、Domain、Secure、および HttpOnly のような、オプションの属性を持ちます。
- **クライアント側 Cookies** - これらの Cookie はユーザのブラウザ内のクライアント側スクリプトによって生成されます。これらは安全ではなく、容易に改竄可能です。

この機能は、「**ウェブ アプリケーション ファイアウォール > 設定**」ページにあります。

このページには以下のオプションがあります。

ポータル - すべてのアプリケーション オフロード ポータルのリストです。各ポータルには独自の設定があります。「**グローバル**」は、すべてのポータルに対する既定の設定です。

改竄防御モード - 3 つのモードが利用可能です。

- **防御** - すべての改竄された Cookie を除去して、それらをログします。
- **検知のみ** - 改竄された Cookie をログだけします。
- **グローバルを継承** - このポータルでグローバル設定を使います。

サーバ Cookies の暗号化 - 名前と値の暗号化を別々に選択します。これは Cookie 名または値を読めなくするので、クライアント側スクリプトの振舞いに影響します。これらのオプションによって、サーバ側 Cookie のみが暗号化されます

Cookie 属性 - 有効の場合、*HttpOnly* および *Secure* 属性がサーバ側 Cookie に追加されます。

HttpOnly 属性は、クライアント側スクリプトが Cookie にアクセスすることを防ぎます。これはクロスサイト スクリプティングやセッション ハイジャックといった攻撃を軽減するときに重要です。*Secure* 属性は、Cookie が HTTPS 接続のみで送信されることを確かにします。両方協力して、サーバ側 Cookie に対して強固なレイヤのセキュリティを追加します。

メモ：既定では、Secure 属性は Cookie 改竄防御が無効になっていたとしても、常に HTTP 接続に付加されます。この振舞いは設定可能なオプションで、無効にできます。

クライアント Cookie - クライアント Cookie は、既定で許可されています。厳しいモードでは、クライアント Cookie は許可されません。無効の場合、クライアント側 Cookie はバックエンド システムに送信されることが許可されません。このオプションはサーバ側 Cookie には影響しません。

除外リスト - 除外リストが有効で Cookie を含む場合、その Cookie は通常通り通過されて、保護されません。サーバ側 Cookie とクライアント側 Cookie を除外することができます。

除外リストの項目は大文字と小文字が区別されます。形式は "CookieName@CookiePath" です。同じ名前で異なるパスを持つ Cookie は、異なる Cookie として扱われます。"CookiePath" はすべてのパスを表すために、空白のままにできます。

グローバルのインポート - アプリケーション オフロード ポータルが、グローバル除外リストをインポートできます。

アプリケーション プロファイリングの動作

管理者は、アプリケーション プロファイリングを「**ウェブ アプリケーション ファイアウォール > ルール**」ページで設定できます。アプリケーション プロファイリングは、それぞれのポータルで独立して実行され、複数のアプリケーションを同時にプロファイルできます。

ポータルを選択した後で、プロファイルしたいアプリケーションのコンテンツ種別を選択できます。「**HTML/XML**」、「**JavaScript**」、「**CSS**」、または画像、HTML、CSS といったすべてのコンテンツ種別を含む「**すべて** 」を選択できます。HTML/XML コンテンツは一般的により取り扱いに慎重を要するウェブ トランザクションをカバーするため、セキュリティの観点から最重要です。このコンテンツ種別は既定で選択されています。

次に、「**プロファイリングの開始**」を選択して (このときボタンが「**プロファイリングの停止**」に変わります)、SMA/SRA 装置を学習モードにします。プロファイリングは、信頼されたユーザが適切な方法でアプリケーションを使用している間に完了するべきです。Secure Mobile Access は入力を記録してそれらを URL プロファイルとして保存します。URL プロファイルは、「**ウェブ アプリケーション ファイアウォール > ルール**」ページの「アプリケーション プロファイリング」セクションにツリー構造でリストされます。

ハイパーリンクとして表示されている URL のみが、バックエンド サーバ上でアクセス可能な URL です。ハイパーリンクを選択して、URL に対する “学習済み” の値が適切でない場合に編集できます。その後、編集された URL プロファイルを使うルールを生成できます。

SMA/SRA 装置は以下の HTTP パラメータを学習します。

- レスポンス ステータス コード

- ポスト データ長 - ポスト データ長は、Content-Length ヘッダ内の値を学習することによって見積もられます。最大値はこの値より大きくもっとも近い 2 のべき乗に設定されます。これはバックエンド アプリケーションによって割り当てられたメモリ量に対応できる値です。例えば、Content Length 65 に対しては、65 より大きい次の 2 のべき乗は 128 です。これは URL プロファイル内で設定される制限です。管理者がこれを的確でないと判断する場合は、この値を適切に編集できます。
- 要求パラメータ - これらは特定の URL が受諾できるパラメータのリストです。

適切な量の入力が学習されてから、「**プロファイリングの停止**」を選択して、学習された入力からルールを生成するための準備を完了します。生成された連鎖ルールに対する既定の動作として、以下の 1 つを設定できます:

- **無効** - 生成されたルールは、アクティブではなく無効になります。
- **検知のみ** - 生成されたルールを起動するコンテンツは、検知されてログ記録されます。
- **防御** - 生成されたルールを起動するコンテンツは、遮断されてログ記録されます。

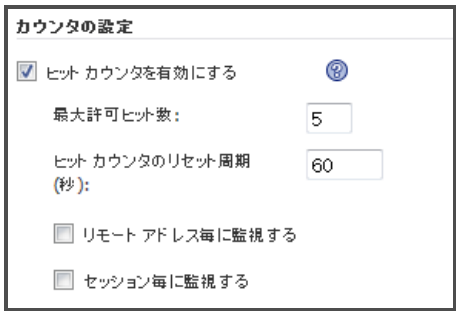
これまでに連鎖ルールが既に URL プロファイルから生成されている場合は、「**URL プロファイルに対する既存の連鎖ルールを上書きする**」がオンになっている場合にのみ連鎖ルールは上書きされます。「**ルールの生成**」を選択すると、URL プロファイルからルールが生成されます。URL プロファイルが編集された場合は、それらの変更は組み入れられます。

ユーザ定義ルールに対する速度制限の動作

「**ウェブ アプリケーション ファイアウォール > ルール**」ページから連鎖ルールを追加または編集する際に、管理者は速度制限を設定できます。連鎖ルールに対して速度制限が有効な場合、その連鎖ルールに対する動作は、設定期間内の一致数が設定されたしきい値を超えたときにだけ開始されます。

この種別の防御は、ブルート フォースや辞書攻撃を防ぐために有用です。Secure Mobile Access 管理インターフェース内で管理者が参考として使える連鎖ルール ID が 15002 の連鎖ルール例が利用可能です。

「**新規連鎖ルール**」または「**連鎖ルールの編集**」画面の「**ヒット カウンタを有効にする**」をオンにすると、関連するフィールドが表示されます。



連鎖ルールが一致すると、ウェブ アプリケーション ファイアウォールは連鎖ルールが何回一致したかを内部カウンタに監視させ続けます。「**最大許可ヒット数**」フィールドは、連鎖ルールの動作が始動するまでに発生しなくてはならない一致回数を含みます。連鎖ルールが「**ヒット カウンタのリセット周期**」フィールドに設定された秒数の間一致しない場合、このカウンタは 0 にリセットされます。

速度制限はリモート IP アドレス毎、または、ユーザ セッション毎、またはその両方に対して強制できます。「**リモート アドレス毎に監視する**」は、攻撃者のリモート IP アドレスに基づいた速度制限を有効にします。

「**セッション毎に監視する**」は、攻撃者のブラウザ セッションに基づいた速度制限を有効にします。この方式は各ブラウザ セッションに対して Cookie を設定します。攻撃者が各攻撃に対して新し

いユーザ セッションを開始する場合は、ユーザ セッションによる追跡はリモート IP による追跡ほど効果的ではありません。

「**リモート アドレス毎に監視する**」オプションでは、SMA/SRA 装置が確認したものと同じリモート アドレスを使います。攻撃が、NAT が設定されている 1 台のファイアウォールの背後にある複数のクライアントを使う場合は、異なるクライアントが実質的には同じ送信元 IP アドレスを持つパケットを送信し、一緒に数えられます。

管理インターフェースのナビゲート

次のセクションでは、Secure Mobile Access 管理インターフェースのナビゲート方法について説明します。

ブラウザの要件

次のセクションでは、Secure Mobile Access 管理インターフェースのブラウザ要件について説明します。

トピック:

管理者のブラウザ要件

ウェブベースの Secure Mobile Access 管理インターフェースおよびユーザ ポータルである**仮想オフィス**は、以下のウェブ ブラウザとオペレーティング システムでサポートされています。

Secure Mobile Access 管理者のブラウザ要件

ブラウザ	オペレーティング システム	
Internet Explorer 9	• Windows 7	
Internet Explorer 10	• Windows 10	
Internet Explorer 11	• Windows 10	
Mozilla Firefox (最新バージョン)	• Windows Vista • Windows 10 • Windows 7	• Linux • MacOS X
Google Chrome	• Windows Vista • Windows 10 • Windows 7	• Linux • MacOS X

ウェブベースの Secure Mobile Access 管理インターフェースを使用して SMA/SRA 装置を設定する場合、管理者は、Java、JavaScript、ActiveX、Cookie、ポップアップ、TLS 1.0、TLS 1.1、および TLS 1.2 対応のウェブ ブラウザを使用する必要があります。Java は、Secure Mobile Access 仮想オフィスの各種機能でのみ必要であり、Secure Mobile Access 管理インターフェースには必要ありません。

エンド ユーザのブラウザ要件

以下に、NetExtender や各種のアプリケーション プロキシ要素など、さまざまな Secure Mobile Access プロトコルをサポートするウェブ ブラウザとオペレーティング システムのリストを示します。Windows、Windows Vista、Windows 7、Linux、および MacOS に関するブラウザの最低バージョン要件を示します。

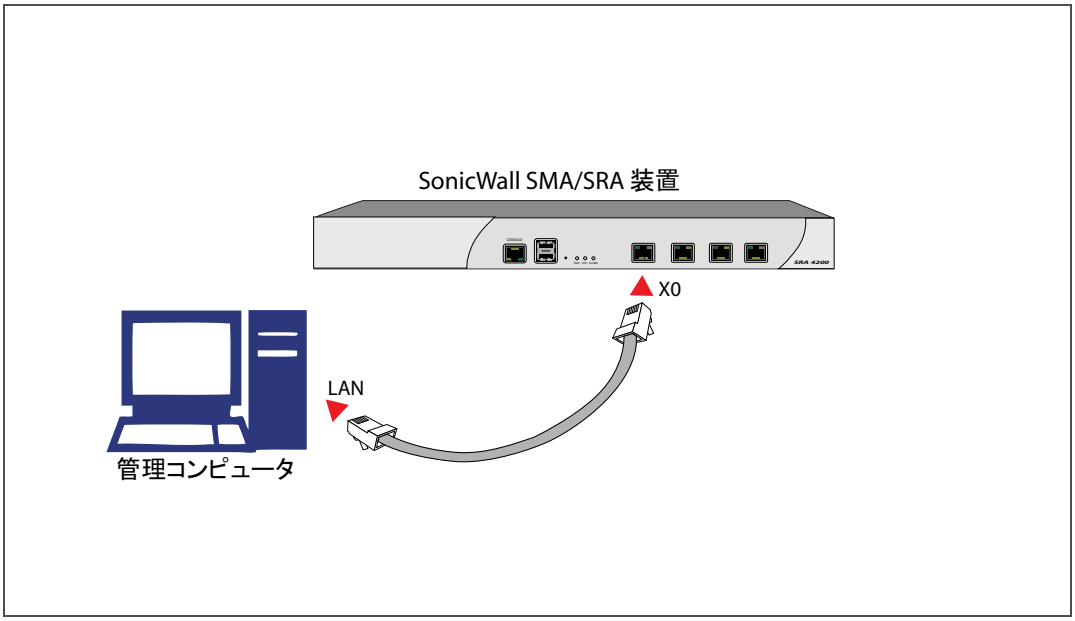
以下の表に、Secure Mobile Access エンド ユーザ インターフェースの具体的なブラウザ要件を示します。

ブラウザ	オペレーティング システム	
Internet Explorer 11	• Windows 10	
Mozilla Firefox (最新バージョン)	• Windows Vista • Windows 10 • Windows 7	• Linux • MacOS X
Google Chrome (最新バージョン)	• Windows Vista • Windows 10 • Windows 7	• Linux • MacOS X
Apple Safari (最新バージョン)	• MacOS X	

管理インターフェースの概要

ここでは、SMA/SRA 装置のウェブベースの Secure Mobile Access 管理インターフェースに接続するための基本セットアップ タスクの概要を説明します。管理セッションの確立と基本セットアップ タスクの詳細については、ご使用のプラットフォームの導入ガイドを参照してください。SonicWall SMA/SRA 装置のウェブベースの Secure Mobile Access 管理インターフェースにアクセスするには、以下の手順に従います。

1 SMA/SRA 装置の **X0** ポートにカテゴリ 6 のケーブルの片端を接続します。SMA/SRA 装置の管理に使用しているコンピュータにケーブルのもう一方の端を接続します。



2 SMA/SRA 装置の管理に使用するコンピュータの静的 IP アドレスが、**192.168.200.20** など、**192.168.200.x/24** サブネットに入るように設定します。コンピュータの静的 IP アドレスのセットアップについては、ご使用のモデルに対応する導入ガイドを参照してください。

> **メモ**：ウェブベースの Secure Mobile Access 管理インターフェースを使用して SMA/SRA 装置を設定する場合は、Internet Explorer 9 以上、Firefox 16.0 以上、Chrome 22.0 以上など、Java と HTTP のアップロードをサポートしているウェブ ブラウザの使用をお勧めします。Secure Mobile Access アプリケーションの全スイートを利用するためには、JavaScript、Java、Cookie、SSL、および ActiveX をサポートしている IE 9 以上を使用する必要があります。

3 ウェブ ブラウザを開き、「**場所**」または「**アドレス**」フィールドに **https://192.168.200.1** (既定の LAN 管理 IP アドレス) を入力します。

4 セキュリティ警告が表示される場合があります。「**はい**」を選択して続行します。

5 「**Secure Mobile Access 管理インターフェース**」が表示され、ユーザ名とパスワードの入力を求められます。「**ユーザ名**」フィールドに「**admin**」を入力し、「**パスワード**」フィールドに「**password**」を入力し、「**ドメイン**」ドロップダウン リストから「**LocalDomain**」を選択して、「**ログイン**」をクリックします。

> **メモ**：Secure Mobile Access の自動ロックアウト機能を使用すると、ログイン試行の回数と期間を制御できます。自動ロックアウト機能の設定の詳細については、ログイン セキュリティの設定 (121 ページ) を参照してください。

ログインに成功すると、既定では「**システム > 状況**」ページが表示されます。

メモ：ログイン後の既定のページが仮想オフィス ユーザ ポータルになっている場合は、ユーザ権限しかないドメインが選択されています。管理は、LocalDomain 認証ドメインからのみ実行できます。管理者としてログインするには、「**ログイン**」画面の「**ドメイン**」ドロップダウン リストから「**LocalDomain**」を選択してください。

ブラウザ ウィンドウの左側にある「**システム**」、「**ネットワーク**」、「**ポータル**」、「**NetExtender**」、「**セキュア仮想アシスト**」、「**ウェブ アプリケーション ファイアウォール**」、「**ユーザ**」、「**ログ**」の各メニュー ヘッダーで、管理設定を構成します。メニュー ヘッダーの 1 つを選択すると、その下にサブ メニュー オプションが表示されます。サブ メニュー リンクを選択すると、対応する管理ページが表示されます。

ナビゲーション メニューの「**仮想オフィス**」オプションを選択すると別のブラウザ ウィンドウが開き、ユーザ ポータルの仮想オフィスのログイン ページが表示されます。

管理インターフェースの右上隅にある「**ヘルプ**」を選択すると別のブラウザ ウィンドウが開き、Secure Mobile Access ヘルプが表示されます。

管理インターフェースの右上隅にある「**ログアウト**」を選択すると、管理セッションが終了し、ブラウザ ウィンドウが閉じます。

管理インターフェースのナビゲート

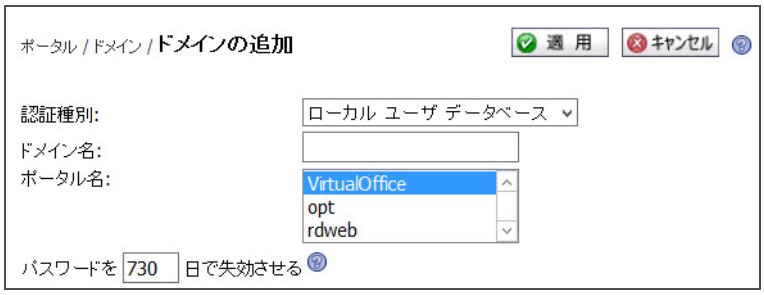
ウェブベースの Secure Mobile Access 管理インターフェースで、管理者は SMA/SRA 装置を設定できます。Secure Mobile Access 管理インターフェースには、トップ レベルの読み取り専用ウィンドウと設定ウィンドウがあります。

- **ウィンドウ** - 読み取り専用の形式で情報を表示します。
- **設定ウィンドウ** - オブジェクトに影響を及ぼす値の追加および変更を管理者が行うことができます。IP アドレス、名前、認証タイプなどがその例です。

次の図は、ウェブベースの Secure Mobile Access 管理インターフェースのサンプル ウィンドウを示しています。標準的な Secure Mobile Access インターフェース ウィンドウの各種要素に注意してください。

「システム > 状況」ページ

設定ウィンドウのサンプル



Secure Mobile Access 管理インターフェースの各要素の詳細については、以下のセクションを参照してください。

- 状況バー (90 ページ)
- 変更の適用 (90 ページ)
- テーブルのナビゲート (91 ページ)
- 再起動 (91 ページ)
- 管理インターフェースの共通アイコン (91 ページ)
- 管理インターフェースのツール チップ (92 ページ)
- ヘルプの表示 (92 ページ)
- ログアウト (92 ページ)

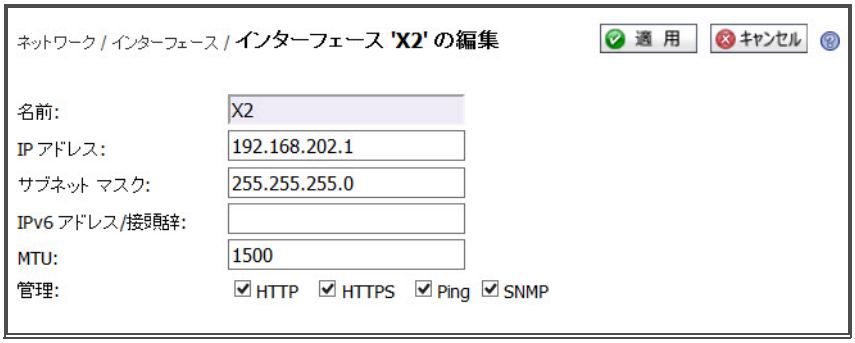
状況バー

管理インターフェース ウィンドウ下部の「**状況**」バーに、Secure Mobile Access 管理インターフェースで実行されるアクションの状況が表示されます。

変更の適用

ページ上で行った設定の変更を保存するには、メイン ウィンドウの右上隅にある「**適用**」を選択します。

設定が Secure Mobile Access 管理インターフェース内の 2 次ウィンドウにある場合は、ウィンドウの右上隅の「**適用**」が利用可能なままです。



テーブルのナビゲート

テーブル上部にある各ナビゲーション ボタンを使用すると、多数のエントリが含まれるテーブル内のナビゲーションが容易になります。たとえば、「**ログ > 表示**」ページには、さまざまなナビゲーション ボタンがあります。

ログ > 表示

ログ > 表示ページのナビゲーション ボタン

ナビゲーション ボタン	説明
検索	「検索」フィールドで指定した内容を含むログ エントリを検索できます。ドロップダウン リストの選択項目で指定したログ エントリの要素が検索対象になります。ドロップダウン リストの選択項目は、「**ログ > 表示**」テーブルの列見出しで示されるログ エントリの要素に対応しています。ログ エントリの時間、優先順位、送信元、送信先、ユーザ、メッセージの各要素を検索対象にすることができます。
除外	ドロップダウン リストで指定したタイプ以外のすべてのログ エントリを表示できます。
リセット	ログ エントリのリストを既定の順序にリセットします。
エクスポート	ログをエクスポートできます。
ログの消去	ログ エントリを消去できます。

再起動

「**システム > 再起動**」ページには、SMA/SRA 装置を再起動するための「**再起動**」ボタンがあります。

メモ：再起動には約 2 分を要し、すべてのユーザが切断されます。

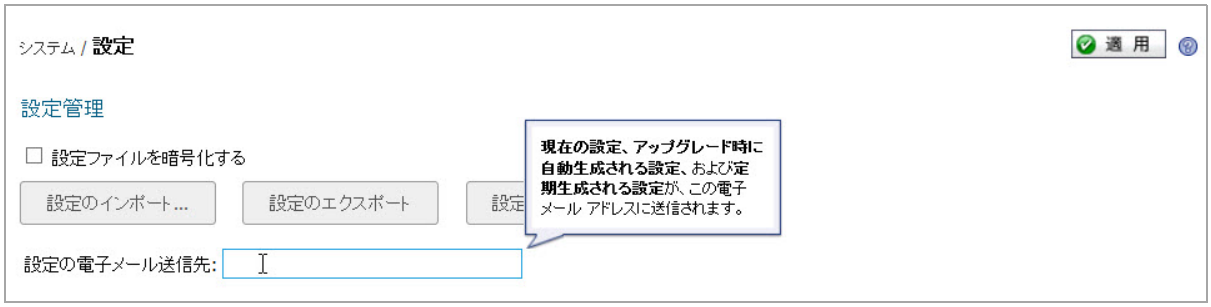
管理インターフェースの共通アイコン

次のアイコンは、Secure Mobile Access 管理インターフェース全体で使用されます。

- 設定 アイコンを選択すると、設定を編集するためのウィンドウが表示されます。
- 削除 アイコンを選択すると、テーブル エントリが削除されます。
- コメント アイコンにポインタを合わせると、「**コメント**」フィールド エントリのテキストが表示されます。

管理インターフェースのツール チップ

Secure Mobile Access 管理インターフェースの多くのページでは、チェックボックス、テキスト フィールド、またはラジオ ボタンの上にマウス カーソルを移動すると、設定情報を示すツール チップが表示されます。フィールドによっては、関連する要件を述べるツールチップを提供する、疑問符 ⓘ アイコンを持つものがあります。



ヘルプの表示

Secure Mobile Access 管理インターフェースの右上隅にある「**ヘルプ**」を選択すると別のウェブ ブラウザが開き、メインの Secure Mobile Access ヘルプが表示されます。

SMA/SRA 装置には、状況に応じたオンライン ヘルプも用意されており、管理インターフェースで各ページの右上隅の疑問符 ⓘ ボタンを選択すると表示されます。疑問符ボタンを選択すると新しいブラウザ ウィンドウが開き、管理ページまたは機能に応じたヘルプが表示されます。

ⓘ **メモ：**SMA/SRA 装置のオンライン ヘルプにアクセスするには、インターネットとの接続が確立されている必要があります。

ログアウト

管理インターフェースの右上隅の「**ログアウト**」を選択すると、管理セッションが終了します。

「**ログアウト**」を選択すると、Secure Mobile Access 管理インターフェースからログアウトし、ウェブ ブラウザが閉じます。

ナビゲーション バー

Secure Mobile Access ナビゲーション バーは、Secure Mobile Access 管理インターフェースの左側にあり、メニュー ヘッダーの階層で構成されています。メニュー ヘッダーを展開すると、関連する管理機能がサブメニュー項目として表示され、最初のサブメニュー項目のページが自動的に表示されます。例えば、「**システム**」ヘッダーを選択すると、「**システム > 状況**」ページが表示されます。ナビゲーション メニューのヘッダーは、「**システム**」、「**ネットワーク**」、「**ポータル**」、「**サービス**」、「**NetExtender**」、「**エンド ポイント制御**」、「**セキュア仮想アシスト**」、「**セキュア仮想ミーティング**」、「**ウェブ アプリケーション ファイアウォール**」、「**高可用性**」、「**ユーザ**」、「**ログ**」、および「**仮想オフィス**」で構成されています。

配備のガイドライン

このセクションでは、SMA/SRA 装置の配備のガイドラインについて説明します。このセクションは、次のサブセクションから構成されています。

サポートするユーザ接続数

装置ごとにサポートされる同時トンネルの最大数と推奨数を次の表に示します。

装置ごとにサポートされる同時トンネル

装置モデルサポートされる最大同時	トンネル数	推奨同時トンネル数
SMA 400	250	125
SMA 200	50	50
SRA 4600	500	100
SRA 1600	50	25
SMA 500v Virtual Appliance	50	50

使用するアプリケーションの複雑さや大きなファイルの共有などは、パフォーマンスに影響を与える要因になります。

リソース タイプのサポート

以下の表は、アクセスできるアプリケーションまたはリソースのタイプを SMA/SRA 装置への接続方法別に示しています。

サポートされるアプリケーションとリソースのタイプ

アクセス メカニズム	アクセス タイプ
標準のウェブ ブラウザ	• FTP およびウィンドウズ ネットワーク ファイル共有のサポートを備えたファイルおよびファイル システム • ウェブベースのアプリケーション • マイクロソフト アウトルック ウェブ アクセスおよびその他のウェブ対応アプリケーション • HTTP および HTTPS のイントラネット

NetExtender	• 以下のようなあらゆる TCP/IP ベースのアプリケーション
	  • ユーザのラップトップ上のネイティブ クライアントを通じた電子メール アクセス (Microsoft Outlook、Lotus Notes など)
	  • 商用アプリケーションおよび自作アプリケーション
	• ネットワーク管理者によって許可された柔軟なネットワーク アクセス

他の SonicWall Inc. 製品との統合

SMA/SRA 装置をその他の SonicWall Inc. 製品と統合すると、SonicWall Inc. NSA、SuperMassive (9000 シリーズ)、TZ シリーズ製品ラインを補完できます。着信 HTTPS トラフィックは、SonicWall Inc. ファイアウォール装置によって SMA/SRA 装置へとリダイレクトされます。このトラフィックは SMA/SRA 装置で復号化されてファイアウォールに返され、そこで内部ネットワーク リソースに到達するための道筋が検討されます。

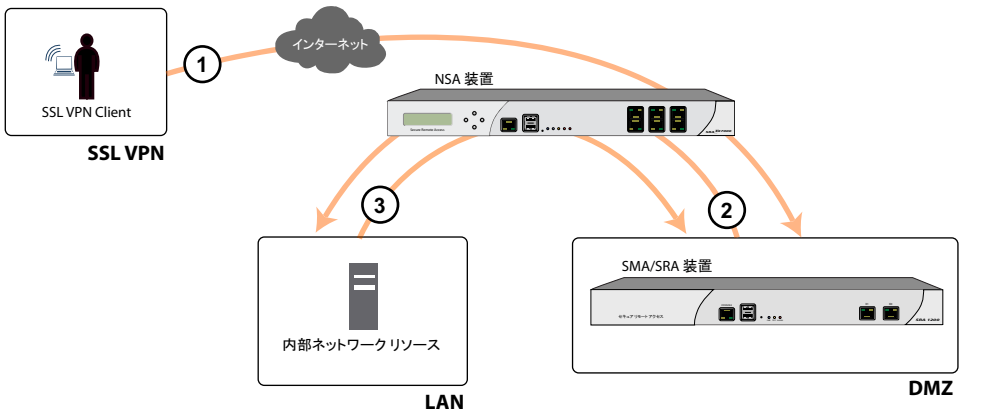
一般的な配備

通常、SMA/SRA 装置は、付随するゲートウェイ装置、例えば NSA 4600 などの SonicWall Inc. ネットワーク セキュリティ装置の DMZ または Opt インターフェースを介した One-Arm モードで直列に接続されて配備されます。

この方法で配備を行うと新たなセキュリティ制御レイヤが追加されます。また、SonicWall Inc. の統合脅威管理 (UTM) の各種サービス (ゲートウェイ アンチウイルス、アンチスパイウェア、コンテンツ フィルタリング、侵入防御など) を利用して着信と発信の全トラフィックをスキャンできるようになります。SonicWall Inc. は、Two-Arm モードよりも One-Arm モードの配備を推奨しています。配備が簡単であり、UTM GAV/IPS と併用して Clean VPN 技術を利用できるからです。

次の図に示すように、One-Arm モードでは、SMA/SRA 装置のプライマリ インターフェース (X0) は、ゲートウェイ機器の使用可能なセグメントに接続されます。暗号化されたユーザ セッションが、ゲートウェイを通じて SMA/SRA 装置に渡されます (ステップ 1)。SMA/SRA 装置がセッションを復号化し、要求されたリソースを判別します。その後、この Secure Mobile Access セッション トラフィックがゲートウェイ装置を通過して (ステップ 2)、内部ネットワーク リソースに到達します。ゲートウェイを通過する際に、侵入防御、ゲートウェイ アンチウィルス、アンチスパイウェア調査などのセキュリティ サービスを適切に設定されたゲートウェイ装置によって適用することができます。その後、内部ネットワーク リソースは要求されたコンテンツをゲートウェイ経由で SMA/SRA 装置に返します (ステップ 3)。そこでコンテンツが復号化され、クライアントに返されます。

初期接続のイベントの流れ



1. X0 インターフェースはゲートウェイの使用可能なセグメントに接続されます。暗号化されたセッションが SMA/SRA 装置に渡されます。
2. SMA/SRA トラフィックがゲートウェイを通過して内部ネットワーク リソースに到達します。
3. 内部ネットワーク リソースはゲートウェイ経由で SMA/SRA 装置にコンテンツを返します。

SMA/SRA 装置とサードパーティ ゲートウェイの連携の設定については、SMA/SRA 装置をサードパーティ ゲートウェイ用に設定する (502 ページ) を参照してください。

Two Arm 配備

SMA/SRA 装置は、1 つの外部 (DMZ または WAN 側) インターフェースと 1 つの内部 (LAN) インターフェースを使う Two Arm 配備シナリオもサポートします。しかしながら、Two Arm モードには配備の前に考慮する必要があるルーティングの問題があります。SMA/SRA 装置はインターフェースを横断してパケットをルートしません (それを妨げる IP テーブル ルールがあり、その結果ルータやデフォルト ゲートウェイとして使用できないため)。Two Arm モードの SMA/SRA 装置の内部インターフェースに接続した別のどのような機器も、異なるゲートウェイを通してインターネットや他のネットワーク リソース (DNS、NTP 等) にアクセスする必要があります。

内部ルータに加えてインターネット ルータがある場合は、内部リソースにアクセスする手段として内部ルータを使うように Two Arm 配備を使うことができます。

サンプル シナリオ: A 社には内部ネットワーク上にリソースと多くのサブネットがあり、すでに強固なルーティング システムが機能しています。SMA/SRA 装置の Two Arm 配備を用いて、社内ネットワーク上の内部リソースへ向かうクライアント要求を、内部ルータに届けることが可能です。

第 2 部

Secure Mobile Access の設定

- システムの設定
- ネットワーク設定
- ポータルの設定

3

システムの設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**システム**」ページで行う、SMA/SRA 装置の登録、日付と時刻の設定、システム設定、システム管理、およびシステム証明書の構成などの設定タスクについて説明します。

トピック:

システム > 状況

このセクションでは、「**システム > 状況**」ページの概要と、このページで実行できる設定タスクについて説明します。

「システム > 状況」の概要

「**システム > 状況**」ページには、SMA/SRA 装置の現在のシステム状況に加え、SMA/SRA 装置および SonicWall Inc. セキュリティ サービス ライセンスを管理するために役立つリンクが用意されています。このセクションでは、「**システム > 状況**」ページの表示内容と、このページでの設定タスクの実行方法について説明します。

「システム > 状況」ページ

以下のセクションでは、「**システム > 状況**」ページの各領域の概要を説明します。

- システム メッセージ (98 ページ)
- システム情報 (98 ページ)
- 最近の警告 (99 ページ)
- ライセンスと登録 (99 ページ)
- ネットワーク インターフェース (99 ページ)

システム メッセージ

「システム メッセージ」セクションには、システム設定の変更など、最近のイベントおよび重要なシステム メッセージが表示されます。たとえば、発信用の SMTP サーバが設定されていない場合は、「発信用の SMTP サーバ アドレスが指定されていないため、ログ メッセージとワンタイム パスワードを送信できません。」というメッセージが表示されます。

システム情報

「システム情報」セクションには、特定の SMA/SRA 装置の詳細情報が表示されます。このセクションには、以下の情報が表示されます。

システム情報

フィールド	説明
モデル	SMA/SRA 装置のタイプ
シリアル番号	SMA/SRA 装置のシリアル番号または MAC アドレス
認証コード	<https://www.MySonicWall.com> の登録データベースで SMA/SRA 装置を認証する場合に使用する英数字コード

システム情報 (続き)

フィールド	説明
ファームウェア バージョン	SMA/SRA 装置にロードされているファームウェア バージョン
ROM バージョン	ROM バージョン。ROM コードは装置の低レベル機能を制御する
CPU (使用率)	SMA/SRA 装置プロセッサのタイプと直前の 5 分間の CPU 平均使用率
搭載メモリ	装置上の RAM とフラッシュ メモリの容量
システム時刻	現在の日付と時刻
稼働時間	最後に再起動したときから現時点まで SMA/SRA 装置がアクティブであった日数、時間数、分数、および秒数
使用中のユーザ	SMA/SRA 装置の Secure Mobile Access 管理インターフェースに現在ログインしているユーザの数

最近の警告

「最新の警告」セクションには、最近の侵入イベント、変則的なシステムの動作やエラーに関するテキストが表示されます。最新の警告には、イベントの日時、イベントを発生したユーザのホスト、およびイベントに関する簡単な説明が表示されます。

このセクションには、システム イベントやシステム エラーに関連するメッセージが表示されます。このセクションの右上隅にある矢印ボタンを選択すると、「**ログ > 表示**」ページが表示されます。

最新の警告セクションのフィールドは、以下のとおりです。

- 「**日付/時間**」- メッセージが生成された日時
- 「**ユーザ**」- メッセージを生成したユーザの名前
- 「**メッセージ**」- エラーを表すメッセージ

ライセンスと登録

「ライセンスと登録」セクションには、SMA/SRA 装置のユーザ ライセンスの許可および登録状況が表示されます。Analyzer、ViewPoint、セキュア仮想アシスト、臨時追加ライセンス、およびウェブ アプリケーション ファイアウォールのライセンスの状況もここに表示されます。

MySonicWall に装置を登録する方法、およびこのセクションの下部にあるフィールドに登録コードを手動で入力する方法については、システム状況を使用した SMA/SRA 装置の登録 (100 ページ) を参照してください。

「**システム > ライセンス**」ページから MySonicWall に装置を登録する方法、および装置と SonicWall Inc. サーバの間で登録状況とライセンス状況を自動的に同期する方法については、「システム > ライセンス」を使用した SMA/SRA 装置の登録 (104 ページ) を参照してください。

ネットワーク インターフェース

「ネットワーク インターフェース」セクションには、SMA/SRA 装置のインターフェースのリストが名前順に表示されます。「ネットワーク インターフェース」タブには、インターフェースごとに、設定されている IP アドレスと現在のリンク状況が表示されます。

ネットワーク インターフェース セクションに関連する設定タスクの詳細については、ネットワーク インターフェースの設定 (102 ページ) を参照してください。

システム状況を使用した SMA/SRA 装置の登録

MySonicWall で登録を行って、SMA/SRA 装置を最大限に活用します。登録は以下のセクションに示す手順に従って行います。

ご登録の前に

SMA/SRA 装置を登録する前に、装置の時間、DNS、およびデフォルト ルートが正しく設定されていることを確認します。通常これらの設定は、SMA/SRA 装置の初期セットアップ プロセスで行います。時間の設定を確認するには、「**システム > 時間**」ページにナビゲートします。DNS の設定を確認するには、「**ネットワーク > DNS**」ページにナビゲートします。デフォルト ルートを確認または設定するには、「**ネットワーク > ルート**」ページにナビゲートします。時間と DNS の設定の詳細については、時刻を設定する (110 ページ)、DNS の設定 (139 ページ)、およびSMA/SRA 装置の既定ルートの設定 (141 ページ) を参照してください。

メモ：SonicWall SMA/SRA 装置を登録するには、MySonicWall アカウントが必要です。

「システム > ライセンス」からの MySonicWall アカウント作成

1 「**システム > ライセンス**」ページで、「**サービスの購読、アップグレード、及び更新**」を選択します。「ライセンス管理」ページが表示されます。

2 MySonicWall アカウントを持っていない、または、ユーザ名やパスワードを忘れた場合は、ページ下部の **https://www.MySonicWall.com** リンクを選択します。「**MySonicWall のログイン**」ページが表示されます。

以下のいずれかを実行します。

- ユーザ名を忘れた場合は、「**ユーザ名を忘れてしまった方は**」リンクを選択します。
- パスワードを忘れた場合は、「**パスワードを忘れてしまった方は**」リンクを選択します。
- MySonicWall アカウントを持っていない場合は、「**ユーザ登録されていない方は**」リンクを選択します。

3 画面の指示にしたがって MySonicWall アカウントを有効化します。

MySonicWall を使った登録

SMA/SRA 装置を登録する方法には次の 2 つがあります。

- MySonicWall アカウントにブラウザから直接ログインするか、または「**システム > 状況**」ページで「**SonicWall Inc.**」リンクを選択して、MySonicWall にアクセスします。次に、装置のシリアル番号やその他の情報を入力し、得られた登録コードを「**システム > 状況**」ページのフィールドに入力します。この手動登録の手順については、このセクションで説明します。
- 「**システム > ライセンス**」ページのリンクを使用して MySonicWall にアクセスし、シリアル番号やその他の情報を MySonicWall に入力します。処理が完了すると、MySonicWall で有効化されたライセンスに装置が自動的に同期されたことが「**システム > ライセンス**」ページに表示されます。この手順については、「システム > ライセンス」を使用した SMA/SRA 装置の登録 (104 ページ) を参照してください。

SMA/SRA 装置を登録するには:

1 Secure Mobile Access 管理インターフェースにログインしていない場合は、ユーザ名 ***admin*** と、SMA/SRA 装置の初期セットアップの過程で設定した管理者パスワード (既定では *password*) を使用してログインします。管理者パスワードの設定方法の詳細については、ご使用の装置モデルの導入ガイドを参照してください。

2 Secure Mobile Access 管理インターフェースに「**システム > 状況**」ページが自動的に表示されない場合は、左ナビゲーション メニューで、「**システム**」を選択し、「**状況**」を選択します。

3 「**ライセンスと登録**」ボックスに表示される「**シリアル番号**」と「**認証コード**」をメモします。

4 次のいずれかの操作を行って、MySonicWall のウェブ ページにアクセスします。

- 「**ライセンスと登録**」セクションの「**SonicWall Inc.**」リンクを選択します。
- ウェブ ブラウザの「アドレス」フィールドに〈http://www.MySonicWall.com〉と入力します。

「**MySonicWall のログイン**」ページが表示されます。

5 MySonicWall アカウントのユーザ名とパスワードを入力します。

ⓘ **メモ**：MySonicWall に未登録の場合は、アカウントを作成してから SonicWall 製品を登録してください。ページの下部にある「**今すぐ登録**」リンクを選択して、無料の MySonicWall アカウントを作成します。

6 左側のナビゲーション バーで、「**製品**」を開きます。

7 「**シリアル番号**」フィールドと「**認証コード**」フィールドに適切な値を入力します。

8 「**ニックネーム**」フィールドに、SMA/SRA 装置のニックネームを入力します。

9 この装置が属する製品グループがある場合は、「**製品グループ**」ドロップダウン リストから選択します。

10 「**登録**」をクリックします。

11 MySonicWall サーバで登録手続きが終了すると、装置が登録されたことを示すメッセージと共に登録コードが表示されます。「**続ける**」を選択します。

12 Secure Mobile Access 管理インターフェースの「**システム > 状況**」ページで、「**ライセンスと登録**」セクションの下部のフィールドに登録コードを入力し、「**更新**」を選択します。

ネットワーク インターフェースの設定

SMA/SRA 装置の IP 設定およびインターフェース設定は、「**システム > 状況**」ページの「ネットワーク インターフェース」セクションの隅にある青色の矢印を選択して指定できます。このリンクによって「**ネットワーク > インターフェース**」ページにリダイレクトされます。このページは、ナビゲーション バーからも表示できます。SMA/SRA 装置の管理者は、「**ネットワーク > インターフェース**」ページから、プライマリ (X0) インターフェースの IP アドレスを設定できます。また、必要に応じて、追加インターフェースを設定することもできます。

SMA/SRA 装置のポートが同じネットワーク上のファイアウォールまたはターゲット機器と通信する場合は、インターフェースに IP アドレスとサブネット マスクを割り当てる必要があります。

インターフェースの設定方法の詳細については、ネットワーク > インターフェース (135 ページ) を参照してください。

システム > ライセンス

このセクションでは、「**システム > ライセンス**」ページの概要と、このページで実行できる設定タスクについて説明します。以下のセクションを参照してください。

- 「システム > ライセンス」の概要 (102 ページ)
- 「システム > ライセンス」を使用した SMA/SRA 装置の登録 (104 ページ)
- ライセンスの有効化またはアップグレード (105 ページ)

「システム > ライセンス」の概要

ライセンスをアップグレードするサービスおよび関連機能は、SMA/SRA 装置で動作するライセンス マネージャによって提供されます。ライセンス マネージャは SonicWall Inc. ライセンス サーバと定期的に (1 時間おきに) 通信を行い、ライセンスが有効かどうかを確認します。管理者がライセンス マネージャでライセンスを直接購入したり、無料トライアルを有効にして購入前の製品を試用したりすることもできます。

メモ：ライセンス マネージャを動作させるためには、装置の初期登録が必要です。

「**システム > ライセンス**」ページには、SonicWall Inc. セキュリティ サービス ライセンスの有効化、アップグレード、及び更新のためのリンクがあります。Secure Mobile Access 管理インターフェースのこのページから、SMA/SRA 装置用の SonicWall Inc. セキュリティ サービス ライセンスをすべて管理できます。

「システム > ライセンス」ページ

セキュリティ サービスの概要

「**セキュリティ サービスの概要**」テーブルには、ノード/ユーザ ライセンス数、および SMA/SRA 装置で使用可能および有効化されたセキュリティ サービスが表示されます。

「**セキュリティ サービス**」列には、セキュリティ装置で利用できるすべての SonicWall Inc. セキュリティ サービスおよびアップグレードが表示されます。「**状況**」列は、セキュリティ サービスが有効であるか (「購読済」)、今後有効にできるか (「未購読」、「臨時追加ライセンス」、「無効」)、すでに有効でなくなっているか (「失効済」) を示しています。ViewPoint、セキュア仮想アシスト、臨時追加ライセンス、ステートフル高可用性機能 (SMA 400、SRA 4600 のみ)、およびウェブ アプリケーション ファイアウォールは、アップグレードとして別個にライセンスされます。

「**ノード**」列には、ライセンスで許可されたノード (IP アドレスを持ち、装置に接続されているコンピュータまたはその他の機器) またはユーザの数が表示されます。この数は、SMA/SRA 装置に同時接続できる最大数を示します。

「**失効期日**」列には、期限付きでライセンスされたサービスの失効期日が表示されます。臨時追加ライセンスに対しては、この失効期日列は、失効するまでの臨時追加ライセンスがアクティブな日数を表示します。この日数は連続的でないことがあります。

「**セキュリティ サービスの概要**」テーブルに示される情報は、SMA/SRA 装置が 1 時間おきに SonicWall Inc. ライセンス サーバと自動で同期するときに更新されます。また、「**同期**」を選択して直ちに同期することもできます。

メモ: 同期の後でライセンスが更新されない場合、SMA/SRA 装置の再起動が必要な場合があります。DNS が正しく設定されていることと、装置から sonicwall.com ドメインに到達できることが必要です。

セキュリティ サービスのオンライン管理

「**システム > ライセンス**」ページから MySonicWall に直接ログインできます。それには、「**サービスの購読、アップグレード、及び更新**」リンクを選択します。このリンクを選択することで、装置の登

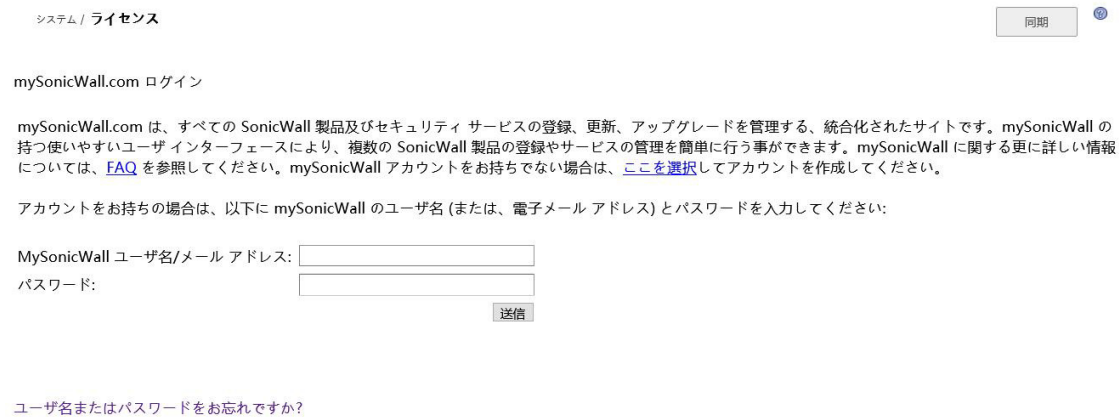
録、サービスのアップグレードや更新のための追加ライセンスの購入、無料トライアルの有効化を行うことができます。

「システム > ライセンス」を使用した SMA/SRA 装置の登録

新しい SMA/SRA 装置の場合、または以前のリリースからファームウェアをアップグレードした場合は、「**システム > ライセンス**」ページから装置を登録できます。

「システム > ライセンス」ページから装置を登録するには、次の操作を行います。

1 「**システム > ライセンス**」ページにログインします。「**サービスの購読、アップグレード、及び更新**」を選択します。MySonicWall のユーザ名とパスワードをフィールドに入力し、「**送信**」を選択します。



2 「ライセンス管理」ページが表示されます。

3 既存のライセンスの「**開始**」、「**アップグレード**」、または「**更新**」を選択します。

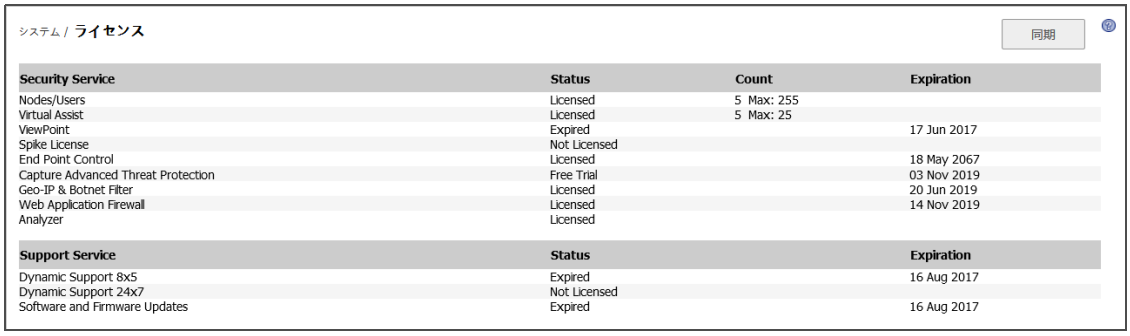
4 ライセンス キーを入力欄に入力します。

5 「**適用**」を選択します。

6 表示が変わり、SMA/SRA 装置が登録されたことが通知されます。

7 「**続ける**」を選択します。

8 「ライセンス管理」ページに最新のライセンス情報が表示されます。



Security Service	Status	Count	Expiration
Nodes/Users	Licensed	5 Max: 255	
Virtual Assist	Licensed	5 Max: 25	
ViewPoint	Expired		17 Jun 2017
Spike License	Not Licensed		
End Point Control	Licensed		18 May 2067
Capture Advanced Threat Protection	Free Trial		03 Nov 2019
Geo-IP & Botnet Filter	Licensed		20 Jun 2019
Web Application Firewall	Licensed		14 Nov 2019
Analyzer	Licensed		

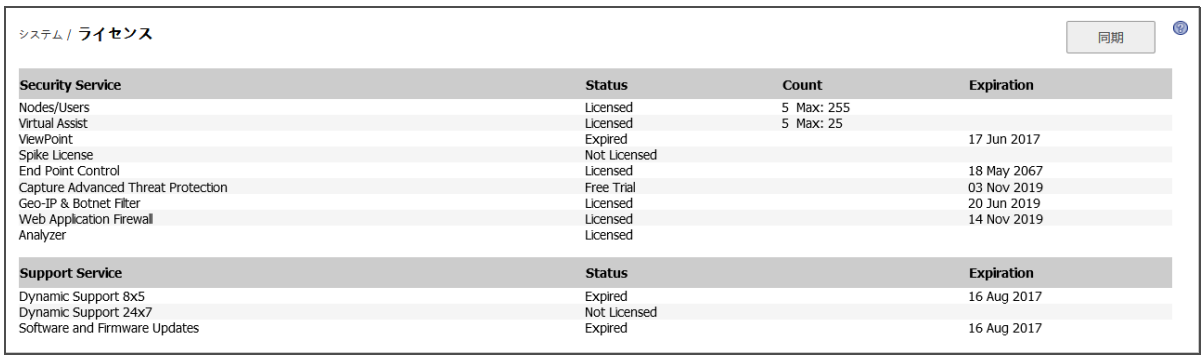
Support Service	Status	Expiration
Dynamic Support 8x5	Expired	16 Aug 2017
Dynamic Support 24x7	Not Licensed	
Software and Firmware Updates	Expired	16 Aug 2017

メモ：ネットワーク環境によっては、登録後に SMA/SRA 装置をオフラインにすることが必要な場合があり、SonicWall Inc. ライセンス サーバに接続できなくなります。このモードでも装置には有効なライセンスが適用されますが、期限付きのライセンスは無効となる場合があります。

ライセンスの有効化またはアップグレード

SMA/SRA 装置を登録した後で、「**システム > ライセンス**」ページから、セキュア仮想アシスト (セキュア仮想ミーティングを含む)、Analyzer/ViewPoint、エンド ポイント制御、臨時追加ライセンス、およびウェブ アプリケーション ファイアウォールのライセンスを有効化できます。セキュア仮想アシスト、Analyzer/ViewPoint、およびウェブ アプリケーション ファイアウォールには、無料トライアルも提供されています。また、このページからライセンスをアップグレードすることもできます。たとえば、装置のライセンスが、仮想アシストの単一の技術者向けの場合、複数の技術者向けのライセンスにアップグレードできます。

有効化またはアップグレードの前に、MySonicWall または再販業者から購読ライセンスを購入する必要があります。購読ライセンスを購入すると、「ライセンス マネージャ」ページに入力する有効化キーが発行されます。



メモ：「**システム > ライセンス**」ページに表示されるサービスは、装置によって異なります。

装置のライセンスまたは無料トライアルを有効化またはアップグレードするには、次の操作を行います。

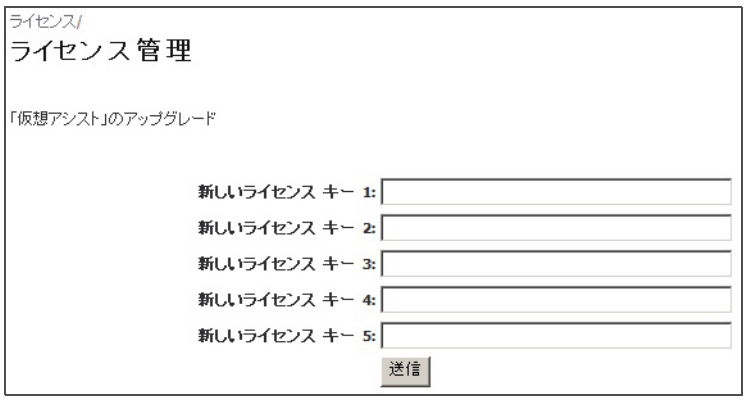
1 「**システム > ライセンス**」ページで、「**サービスの購読、アップグレード、及び更新**」を選択します。「ライセンス管理」ページが表示されます。

2 MySonicWall のユーザ名とパスワードをフィールドに入力し、「**送信**」を選択します。表示が変更され、ライセンスの状況が示されます。サービスには、「**試用**」リンク、「**購読**」リンク、または「**アップグレード**」リンクが表示されます。

3 無料トライアルを有効化するには、目的のサービスの横の「**試用**」を選択します。このページでは、サービスのセットアップの手順が示されることと、試用中または試用後にいつでも SonicWall Inc. 製品の購読を申し込めることが説明されています。「**次へ**」を選択してセットアップ手順に従います。

4 MySonicWall または販売代理店で以前に購入した新しいライセンスを有効化するには、「セキュリティ サービスのオンライン管理」**セクションで「サービスの購読、アップグレード、及び更新」をクリックします。**「**有効化キーを入力してください**」フィールドにライセンスの有効化キーを入力し、「**送信**」を選択します。

5 既に購入済みの新しいライセンスを使って既存のライセンスをアップグレードするには、目的のサービスの横の「**アップグレード**」を選択します。「**新しいライセンス キー**」フィールドに 1 つまたは複数の有効化キーを入力または貼り付けて、「**送信**」を選択します。



6 有効化またはアップグレードの手順を完了した後で「**同期**」を選択して、SonicWall Inc. ライセンス サーバと同期して装置のライセンス状況を更新します。装置を再起動した場合もライセンス状況が更新されます。

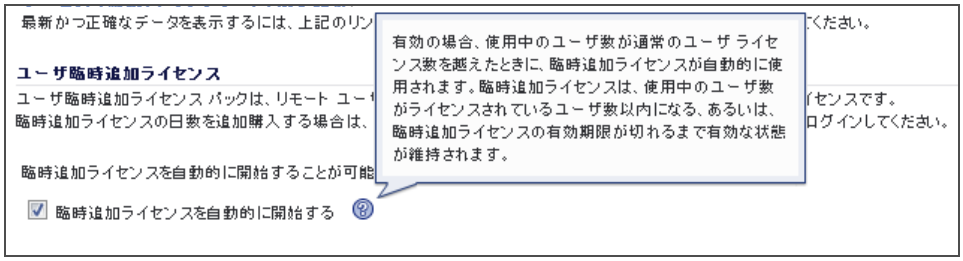
臨時追加ライセンスの使用

臨時追加ライセンスにより、厳しい気象状況やリモートの関係者に対する仕事上のイベントの期間のような、突然リモート アクセスの必要数の増加が生じた場合に、一時的に装置または SMA 500v 仮想装置がサポートできるリモート ユーザ数を増やすことができます。個別にライセンスされるこの機能は、予定された、または予定していないイベントの間、リモート アクセス トラフィックの増加に対応する手助けをします。

臨時追加ライセンスを購入すると、与えられたユーザ数と日数有効です。(これは臨時追加ライセンスが有効化された際にサポートされるユーザの総数であり、基本ライセンス数に追加された数ではありません)。必要に応じてライセンスの使用を一時停止して再開できます。

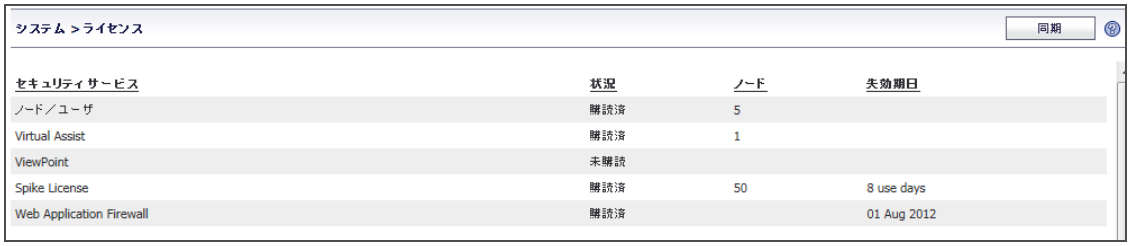
装置に 2 つ以上の臨時追加ライセンスをアップロードできますが、同時に 1 つしか有効にできません。

ユーザの接続数に応じて自動的にライセンスを有効および無効にするオプションが利用可能です。これを有効にするには、「**臨時追加ライセンスを自動的に開始する**」をオンにします。このオプションが有効の場合は、接続ユーザ数が通常ユーザ ライセンス数を超過すると、臨時追加ライセンスが自動的に有効化されます。この臨時追加ライセンスは、ユーザ数が通常ライセンス数まで減るか、臨時追加ライセンスが失効するまで有効であり続けます。

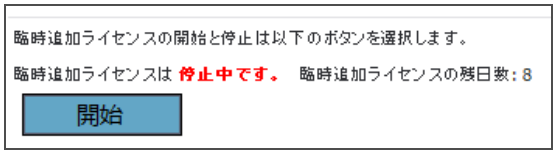


臨時追加ライセンスを開始または停止するには:

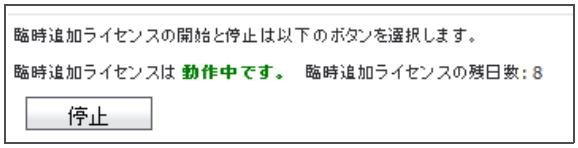
1 ライセンスの有効化またはアップグレード (105 ページ) で説明されているように、MySonicWall から臨時追加ライセンスを購入して、それを装置にインポートします。ライセンシングの後で、状況が「*購読済*」に変わり、臨時追加ライセンスでサポートされる合計ユーザ数と利用可能な残り日数が「**システム > ライセンス**」ページに表示されます。



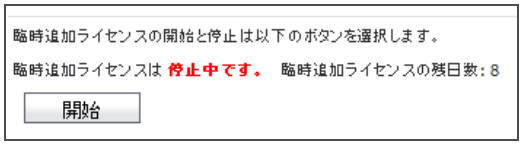
2 ページを再表示すると、臨時追加ライセンスは「*停止中*」として「**システム > ライセンス**」ページにリストされます。



3 より多くのユーザに対応する必要があるときに、「**開始**」を選択します。状況が *動作中* に変わります。



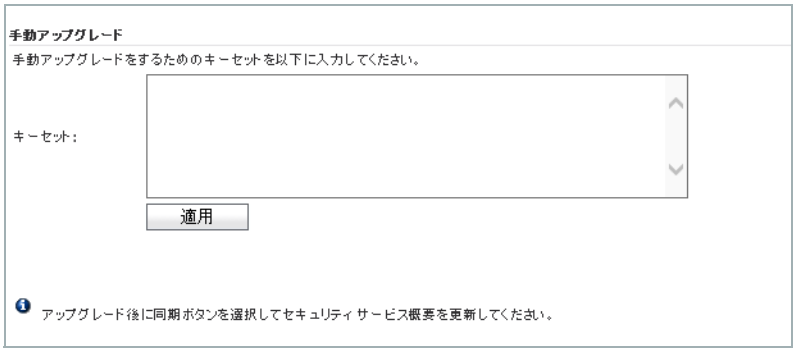
4 動作中の臨時追加ライセンスを停止するには、「**停止**」を選択します。状況が *停止中* に戻り、残り日数が更新されます。



> **メモ**: 臨時追加ライセンスを動作させて停止させるといつでも、たとえ 24 時間経過していなくても有効な残り日数は 1 日ずつ減ります。複数日動作させたままの場合は、24 時間毎に 1 日引かれます。

手動でアップグレード

セキュリティ サービスを手動でアップグレードするには、「**システム > ライセンス**」ページの「手動でアップグレード」セクションまで下方向にスクロールします。アップグレードするサービスのキーセットが必要です。フィールドに**キーセット**を入力し、「**適用**」を選択します。ページ上部の「**同期**」を選択して、「セキュリティ サービスの概要」を更新します。「セキュリティ サービスの概要」に、アップグレードしたライセンスが表示されるはずです。



システム > 時間

このセクションでは、「**システム > 時間**」ページの概要と、このページで実行できる設定タスクについて説明します。

「システム > 時間」の概要

管理者は、「**システム > 時間**」ページで、SMA/SRA 装置のシステム時間、日付、タイムゾーンの設定、および SMA/SRA 装置と NTP サーバとの同期を制御できます。

「システム > 時間」ページ

システム時間

システム時間セクションでは、時間 (hh:mm:ss)、日付 (mm:dd:yyyy)、およびタイムゾーンを設定できます。また、NTP (ネットワーク タイム プロトコル) サーバとの自動同期を選択したり、ローカル時間ではなく UTC (協定世界時) をログに表示することもできます。

NTP の設定

NTP の設定セクションでは、更新間隔 (秒単位)、NTP サーバ、および 2 つの追加の (オプション) NTP サーバを設定できます。

時刻を設定する

時間と日付を設定するには、「**システム > 時間**」ページにナビゲートします。時刻と日付の設定は、ログ イベントのタイムスタンプやその他の内部の目的に使用されます。最適なパフォーマンスと適切な登録を実現するには、システム時間を正確に設定することが不可欠です。

メモ：最適なパフォーマンスを得るためには、SMA/SRA 装置の時刻と日付を正確に設定する必要があります。

時刻と日付を設定するには:

1. 「**タイムゾーン**」ドロップダウン リストで、タイムゾーンを選択します。
2. 現在の時刻が 24 時間形式で「**時刻 (hh:mm:ss)**」フィールドに表示され、現在の日付が「**日付 (mm:dd:yyyy)**」フィールドに表示されます。
3. または、現在の時刻を「**時刻 (hh:mm:ss)**」フィールドに手動で入力したり、現在の日付を「**日付 (mm:dd:yyyy)**」フィールドに入力することもできます。

   メモ：「**NTP を使用して自動的に時刻を調整する**」の横にあるチェックボックスがオンになっている場合は、時刻と日付を手動で入力できません。時刻と日付を手動で入力するには、このチェックボックスをオフにしてください。
4. 「**適用**」を選択して設定を更新します。

ネットワーク タイム プロトコルの有効化

ネットワーク タイム プロトコル (NTP) を有効にしている場合は、NTP の時刻設定が手動の時刻設定より優先されます。NTP の時刻設定は、NTP サーバと、「**タイムゾーン**」ドロップダウン リストで選択したタイムゾーンによって決まります。

ネットワーク タイム プロトコル (NTP) を使って装置の時刻と日付を設定するには:

1. 「**システム > 時間**」ページにナビゲートします。
2. 「**NTP を使用して自動的に時刻を調整する**」をオンにします。
3. NTP の設定セクションの「**間隔の更新**」フィールドに、時刻設定を NTP サーバと同期する間隔を秒単位で入力します。間隔を定義しないと、既定の更新間隔である 3600 秒が自動的に選択されます。
4. 「**NTP サーバ 1**」フィールドに、NTP サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
5. 冗長性を提供する場合は、「**NTP サーバ 2 (オプション)**」フィールドと「**NTP サーバ 3 (オプション)**」フィールドに、バックアップ用 NTP サーバのアドレスを入力します。
6. 「**適用**」を選択して設定を更新します。

システム > 設定

このセクションでは、「**システム > 設定**」ページの概要と、このページで実行できる設定タスクについて説明します。

- 「システム > 設定」の概要 (111 ページ)

- 設定ファイルの管理 (112 ページ)
- ファームウェアの管理 (115 ページ)

「システム > 設定」の概要

「**システム** > **設定**」ページでは、SMA/SRA 装置の設定のインポートとエクスポートができます。ファームウェアのアップグレード後や設定の生成後に外部の FTP サーバに設定内容を自動送信するには、次のオプションを使用できます。SMA には装置の設定を定期的にバックアップする機能が既にありましたが、これらのオプションはバックアップの新しい手段となるものです。

物理装置上では、「**システム** > **設定**」ページは新しいファームウェアをアップロードする方法と、現在のファームウェア、新たにアップロードされたファームウェア、またはバックアップされたファームウェアのどれかを起動する方法が提供されます。

システム > 設定 ページ - 物理装置

FTP サーバを「**システム** > **管理**」ページで設定して、新しい設定が外部 FTP サーバに自動的に送信されるようにします。外部 FTP/TFTP サーバの設定 (123 ページ) を参照してください。

SMA 500v Virtual Appliance 上では、「**システム** > **設定**」ページで設定管理は可能ですが、SMA 500v Virtual Appliance はそれ自身がソフトウェア イメージであるため、ファームウェア管理は提供されません。

設定

「設定」ページには、設定をインポートおよびエクスポートするボタンに加えて、設定を電子メールで送信するボタンがあります。また、管理者は設定ファイルを暗号化することができます。新しいファームウェアが使用可能になったときに通知するオプションもあります。

ファームウェアの管理

「ファームウェアの管理」セクションでは、SMA/SRA 装置で動作するファームウェアを制御できます。このセクションにはさまざまなボタンがあります。新しいファームウェアのアップロード、現在のファームウェアのバックアップ作成、管理用コンピュータへの既存のファームウェアのダウンロード、現在のファームウェアまたは最近アップロードしたファームウェアでの装置の再起動、工場出荷時の設定での装置の再起動などのボタンです。

Phone Home の設定

SONAR 拡張製品分析は、「Phone Home (制御元への通信)」とも呼ばれ、MSW バックエンド サーバを使用してユーザの装置から Phone Home データを収集します。収集されるデータは 2 つの部分に分かれます。1 つは、静的ライセンスと、設定済みの数を示す設定データです。もう 1 つは、使用数を示す実行時データです。このデータとそれに続く分析に基づいて、このデータを正確に追跡し、効果的に改良または廃止することができます。

Phone Home の設定を有効または無効にするには、「**システム > 設定**」ページで Phone Home 設定にアクセスし、「**製品分析用の Phone Home を有効にする**」オプションをオンまたはオフにします。

設定ファイルの管理

SMA/SRA 装置では、SMA/SRA の構成設定を保持するファイルを保存およびインポートすることができます。これらのファイルの保存およびアップロードには、Secure Mobile Access 管理インターフェースの「**システム > 設定**」ページを使用します。

以下ではこれらの方法について説明します。

設定ファイルの暗号化

セキュリティのために、「**システム > 設定**」ページで設定ファイルを暗号化することができます。ただし、設定ファイルを暗号化すると、トラブルシューティングの目的で編集したり確認したりできなくなります。

設定ファイルを暗号化するには、「**システム > 設定**」ページの「**設定ファイルを暗号化する**」をオンにします。

設定ファイルのインポート

以前にバックアップ設定ファイルにエクスポートした設定をインポートできます。

設定ファイルをインポートするには:

1 「**システム > 設定**」ページに移動します。

2 設定のバックアップ ファイルをインポートするには、「**設定のインポート**」を選択します。「**設定のインポート**」ダイアログ ボックスが表示されます。

> **メモ**：一部のプラットフォームは機能に相違点があるため、SMA 200 から SMA 400 (およびその逆) または SRA 1600 から SRA 4600 (およびその逆) への設定のインポートは完全にはサポートされていません。また、異なるプラットフォームへの仮想マシン設定のインポートも完全にはサポートされていません。これらのプラットフォーム間で設定をインポートする場合は、設定が正しくインポートされたかどうかを必ず確認してください。

3 「**Browse**」を選択して、インポートしたい (設定が含まれている) ファイルが置かれている場所にナビゲートします。既定のファイル名は **sslvpnSettings-serialnumber.zip** ですが、どのような名前でも構いません。

4 「**アップロード**」をクリックします。Secure Mobile Access によってファイルから設定がインポートされ、その設定が装置に適用されます。

> **メモ**：システムを再設定する準備が整っていることを確認します。ファイルをインポートすると、直ちに既存の設定が上書きされます。

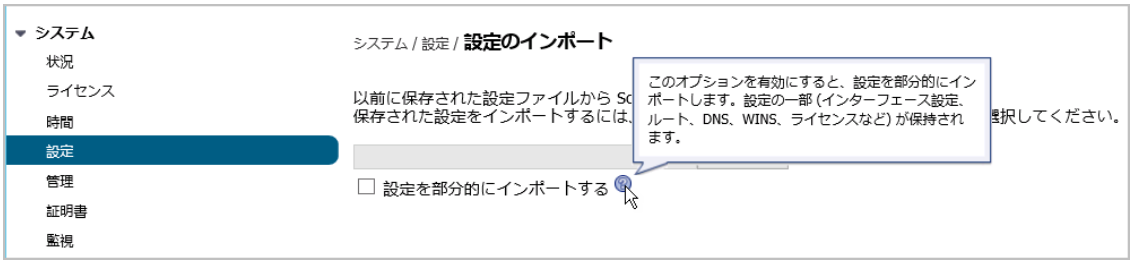
5 ファイルのインポートが終了したら、装置を再起動して変更を永続化します。

設定の部分的なインポート

この機能により、インターフェース設定、ルート設定、DNS 設定、WINS 設定、ライセンスなどを、他の設定を変更することなく部分的にインポートすることができます。

設定を部分的にインポートするには:

1 「**システム > 設定 > 設定のインポート**」に移動します。「**設定のインポート**」ページが表示されます。



2 アップロードする設定ファイルを選択して、「**設定を部分的にインポートする**」を選択します。

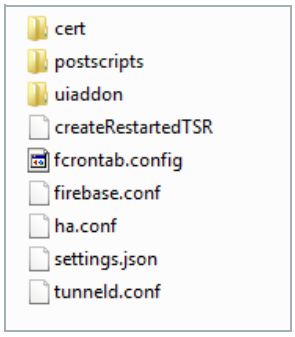
3 「**適用**」を選択します。

バックアップ設定ファイルのエクスポート

バックアップ設定ファイルをエクスポートすると、設定情報のコピーをローカル コンピュータに保存できます。設定情報をバックアップ ファイルに保存またはエクスポートし、必要に応じてこの保

存した設定ファイルを後でインポートすることができます。バックアップ ファイルは既定では **sslvpnSettings-serialnumber.zip** という名前で、下図に示される内容を含みます。

Zip ファイルのバックアップ設定のディレクトリ構造



バックアップ ディレクトリ構造には以下の要素が含まれています。

- **ca** フォルダ (非表示) ― 認証局から提供された CA 証明書が含まれます。
- **cert** フォルダ ― 既定のキー/証明書ペアを格納する **default** フォルダが含まれます。また、「**システム > 証明書**」ページで指定された証明書署名リクエスト (CSR) から生成されたキー/証明書ペアがある場合、それも含まれます。
- **uiaddon** フォルダ ― 各ポータル用のフォルダが含まれます。各フォルダには、ポータル ログイン メッセージ、ポータル ホーム ページ メッセージ、およびポータルの既定のロゴまたは個別ロゴ (アップロードされている場合) が含まれます。既定ポータルは「**VirtualOffice**」です。
- **firebase.conf** ファイル ― ネットワーク、DNS、およびログの設定が含まれます。
- **settings.json** ファイル ― ユーザ、グループ、ドメイン、およびポータルの設定が含まれます。
- **fcrontab.config** ファイル – TSR の定期生成が有効である場合のみ生成されます。

バックアップ設定ファイルをエクスポートするには:

1. 「**システム > 設定**」ページに移動します。
2. 設定のバックアップ ファイルを保存するには、「**設定のエクスポート**」を選択します。使っているブラウザから、設定ファイルを開くかどうかを尋ねるポップアップ ウィンドウが表示されます。
3. ファイルの「**保存**」のオプションを選択します。
4. 設定ファイルを保存する場所を選択します。既定のファイル名は **sslvpnSettings-serialnumber.zip** ですが、変更できます。
5. 「**保存**」を選択して設定ファイルを保存します。

設定の電子メール送信

システムをバックアップするもう 1 つの方法として、現在の設定、アップグレード時に自動生成された設定、および定期生成された設定を電子メール アドレスに送信できます。「**設定の電子メール送信先**」フィールドに電子メール アドレスを指定します。次に「**電子メール設定**」をクリックします。

ファームウェアがアップグレードされるたびに、電子メール設定を自動送信することもできます。「ファームウェアのアップグレード時に設定を電子メールで自動送信する」チェックボックスをオンにします。「**メール サーバ**」と「**メール送信元アドレス**」の値を自動電子メール配信用に設定する必要があります。詳細については、ログ > 設定 (485 ページ) を参照してください。

定期バックアップの有効化

「設定の定期バックアップを有効にする」をオンにして、現在の設定の定期バックアップを設定できます。バックアップを定期生成する頻度を指定します。バックアップの実行を「1 日ごと」、「1 週間ごと」、「2 週間ごと」、または「1 ヶ月ごと」に指定できます。

新しい設定の電子メール送信

「生成時に新しい設定をメールで自動送信する」をオンにして、最新の設定が生成されたらメールで送信することができます。

ファームウェアの管理

管理者は、**「システム > 設定」**のファームウェアの管理セクションで、新しいファームウェアが使用可能になった時に通知するオプションを指定できます。新しいファームウェアのアップロード、バックアップの作成などのファームウェア イメージに関する設定オプションが含まれます。

以下ではこれらの方法について説明します。

- ファームウェア通知の設定 (115 ページ)
- バックアップの作成 (115 ページ)
- ファームウェアのダウンロード (115 ページ)
- ファームウェア イメージの起動 (116 ページ)
- 新しいファームウェアのアップロード (116 ページ)

ファームウェア通知の設定

新しいファームウェア ビルドが使用可能になった時に電子メールで管理者に通知が送られるように設定できます。

新しいファームウェアが使用可能になった時に通知を受けるには、**「新しいファームウェアが利用可能になった時に通知する」**をオンにします。

バックアップの作成

現在のファームウェアおよび設定のシステム バックアップを作成するには、**「バックアップの作成」**を選択します。バックアップには、約 2 分かかります。バックアップが完了すると、画面の下部の**「状況」**に「システム バックアップに成功しました」というメッセージが表示されます。

ファームウェアのダウンロード

ファームウェアをダウンロードするには、ダウンロードするファームウェア イメージ バージョンの横にあるダウンロード アイコン  を選択します。

ファームウェア イメージの起動

「**システム > 設定**」ページの「ファームウェアの管理」テーブルに表示されるファームウェア イメージを使用して装置を起動 (再起動) することができます。現在の設定を保持するか、工場出荷時の設定に戻すかを選択できます。

ファームウェア イメージを起動するには:

1 SMA/SRA 装置で起動するファームウェア イメージ バージョンの行にある起動アイコン を選択します。

2 工場出荷時の設定でイメージを再起動するには、「**工場出荷時の設定で起動**」をオンにします。このオプションがオフになっている場合、現在の設定が保持されます。

3 「このファームウェアで起動しますか?」というポップアップ メッセージが表示されます。「**OK**」を選択します。

新しいファームウェアのアップロード

新しいファームウェアをアップロードするには:

1 MySonicWall にログインします。

2 最新の Secure Mobile Access ファームウェア バージョンをダウンロードします。

3 Secure Mobile Access 管理インターフェースで、「**システム > 設定**」ページを開きます。

4 「ファームウェアの管理」セクションの「**ファームウェアのアップロード**」を選択します。

5 「**参照**」を選択します。

6 ダウンロードした Secure Mobile Access ファームウェアを選択します。ファイルの拡張子は.sigです。

7 「**開く**」を選択します。

8 「**適用**」を選択します。ファームウェアがアップロードされて書き込まれるまで待ちます。

9 「**システム > 設定**」ページのファームウェア テーブルにアップロードされたファームウェアが表示されます。「**アップロードされたファームウェア**」行の起動アイコンを選択して、既存の設定で新しいファームウェアを起動します。

言語設定の管理

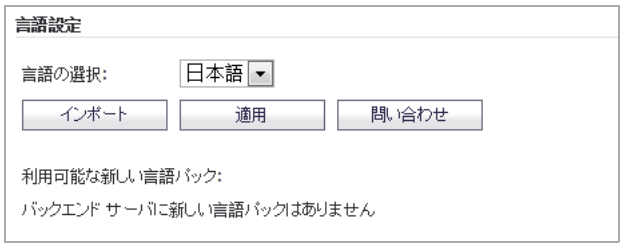
SMA/SRA 装置を使用して、新しい言語パックをインポートし、ファームウェアに適用することができます。言語パックは、バックエンド サーバに格納されます。Secure Mobile Access ファームウェアは、既存または新しい言語パックに対する更新がないか、1 時間ごとにバックエンド サーバを確認するようスケジュールされます。

以下ではこれらの方法について説明します。

- 言語パックのダウンロード (117 ページ)
- 言語パックのインポート (117 ページ)
- 言語の選択 (117 ページ)
- 新しい言語の問い合わせ (117 ページ)

言語パックのダウンロード

「言語設定」セクションには、利用可能な最新の言語パックが表示されます。MySonicWall にログインして言語パックをローカル システムにダウンロードするか、ダウンロードする言語のリンクを選択して MySonicWall に自動的にリダイレクトします。



言語パックのインポート

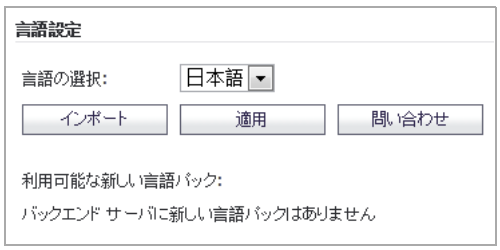
MySonicWall から新しい言語パックをダウンロードしたら、Secure Mobile Access ファームウェアにインポートできます。「**インポート**」を選択します。「**ファイルの選択**」を選択して、インポートする言語ファイルを選択します。「**開く**」を選択します。

言語の選択

「**言語の選択**」ドロップダウン メニューには、SMA/SRA 装置のバックエンド サーバにダウンロード済みの利用可能な言語が表示されます。既定の言語は英語です。ドロップダウン メニューから言語を選択し、「**適用**」を選択します。この処理には数分かかることがあります。

新しい言語の問い合わせ

バックエンド サーバ上で利用可能な言語パックを手動で問い合わせるには、「**問い合わせ**」を選択します。利用可能な新しい言語パックがある場合は、「利用可能な新しい言語パック」の下に表示されます。



システム > 管理

このセクションでは、「**システム > 管理**」ページの概要と、このページで実行できる設定タスクについて説明します。

- ウェブ管理設定の構成 (122 ページ)
- SNMP の設定 (122 ページ)
- GMS 管理を有効にする (123 ページ)
- 外部 FTP/TFTP サーバの設定 (123 ページ)

「システム > 管理」の概要

このセクションでは、「**システム > 管理**」ページの設定タスクに関する情報と実行手順を説明します。「**システム > 管理**」ページでは、ログイン セキュリティ、ウェブ管理設定、SNMP 設定、および GMS　設定を構成できます。

以下のセクションを参照してください。

- ログイン セキュリティ (120 ページ)
- HTTP DoS 設定 (120 ページ)
- グローバル SSL/TLS 設定 (120 ページ)
- キャパシティ マトリックス (121 ページ)
- ウェブ管理設定 (121 ページ)
- SNMP 設定 (121 ページ)
- GMS の設定 (121 ページ)

「システム > 管理」ページ


システム / 管理
ログイン セキュリティ
管理者/ユーザのロックアウトを有効にする
1 分間でのログイン最高試行回数:
5
ロックアウト時間 (分):
5
HTTP DoS 設定
IP 毎最大同時 TCP 接続数:
20
グローバル SSL/TLS 設定
前方秘匿性を強制する
TLS カスタマイズ バージョン:
TLSv1.2
TLSv1.1
TLSv1
暗号スイート:
中間の互換性
プロキシ接続のバックエンド SSL サーバ証明書を確認
キャパシティ マトリックス
SMA キャパシティ マトリックス レポート:
ダウンロード
ウェブ管理設定
既定のテーブル サイズ:
100
ストリーミング更新間隔:
10
SNMP 設定
SNMP の有効化:
無効にする
システム名:
システムの連絡先:
システムの場所:
資産番号:
MIB ファイルのダウンロード
すべての MIB ファイル (.zip)
SONICWALL-SMI.MIB
SNWL-COMMON-MIB.MIB
SNWL-SSLVPN-MIB.MIB
GMS 設定
GMS 管理を有効にする
GMS ホスト名または IP アドレス:
GMS Syslog サーバ ポート:
514
ハートビート間隔 (秒):
60
ハートビート状況メッセージのみ送信する
この SMA 装置をリモート管理するには、GMS 4.0 以降が必要です。
外部 FTP/TFTP サーバ
FTP/TFTP サーバ:
FTP/TFTP ポート:
FTP/TFTP ユーザ名:
FTP/TFTP パスワード:
適用

ログイン セキュリティ

「ログイン セキュリティ」セクションでは、設定されている 1分あたりの最大ログイン試行回数の後に行われる、一定時間 (分単位) の管理者/ユーザのロックアウトを設定できます。

HTTP DoS 設定

「HTTP DoS 設定」セクションでは、クライアントが Secure Mobile Access ウェブ サーバで開くことのできる TCP 最大同時接続数 (20 ～ 100、既定値は 20) を設定します。

グローバル SSL/TLS 設定

「グローバル SSL/TLS 設定」セクションを使用して、管理者は「**システム > 管理**」ページからセキュア ソケット レイヤ (SSL) と Transport Layer Security (TLS) の設定をグローバルに行うことができます。

以下の設定を行います。

- **前方秘匿性を強制する** - このオプションを有効にすると、秘密鍵が盗まれるようなことがあった場合でも、現在の情報の機密性を守ることができます。前方秘匿性をサポートしないブラウザは、SMA/SRA 装置に接続できない可能性があります。また、クライアント ブラウザがサポートする暗号化によっては、この機能のパフォーマンスが低下する可能性もあります。
- **TLS カスタマイズ バージョン** - セキュリティ上の特別な理由からウェブ サーバでサポートされる TLS のバージョンを指定します。このバージョンの TLS は、クライアントとウェブ サーバの間の通信に使用されます。 TLS バージョンを指定するには、「**TLS カスタマイズ バージョン**」スクロール メニューから以下のいずれかのオプションを選択します。
    - TLSv1.2
    - TLSv1.1
    - TLSv1
- **暗号スイート** -「暗号スイート」ドロップダウン メニューから以下のいずれかのオプションを選択して暗号スイートを指定します。
    - **最新 (Modern) 互換性** - より高いレベルのセキュリティを提供します。以前のクライアントと互換性がない可能性があります。最も古い互換クライアントは Firefox 27、Chrome 30、IE 11 (以上 Windows 7)、 Edge、Opera 17、Safari 9、Android 5.0、Java 8 です。
    - **中間 (Intermediate) 互換性 (推奨)** - 幅広いクライアントをサポートしますが、従来のクライアント (主に WinXP) と互換性がありません。最も古い互換クライアントは Firefox 1、Chrome 1、IE 7、Opera 5、Safari 1、Windows XP IE8、Android 2.3、Java 7 です。
    - **古い (Old) 下位互換性 (非推奨)** - Windows XP/IE6 までの過去のすべてのクライアントをサポートします。最も古い互換クライアントは Windows XP、IE6、Java 6 です。
    - **ユーザ定義暗号スイート** - カスタマイズ可能なセキュリティ レベルを提供します。「**ユーザ定義暗号スイート**」を選択し、テキスト フィールドにユーザ定義暗号リストを入力します。
- **プロキシ接続のバックエンド SSL サーバ証明書を確認** - このオプションを有効にすると、バックエンド SSL/TLS サーバ証明書が信頼できなければ、接続が破棄されます。確認の深度は 10 です。このオプションを有効にすると、警告レベルのログ メッセージも生成されます。

キャパシティ マトリックス

Secure Mobile Access キャパシティ マトリックス レポートは、ダウンロード可能な .PDF ファイルで、特定の SMA/SRA 装置モデルで利用できる各種接続、インターフェース、ポータル、ドメイン、グループ、ユーザなどの総数を表示できます。このレポートをローカル システムにダウンロードするには、「**ダウンロード**」を選択します。

ウェブ管理設定

「ウェブ管理設定」セクションでは、Secure Mobile Access 管理インターフェース内の、ページ分けされるテーブルの既定のページ サイズと、動的に更新されるテーブルのストリーミング更新間隔を設定できます。

ページ分けされるテーブルで、既定のページ サイズによって影響を受けるものは次のとおりです。

- セキュア**仮想アシスト > ログ**
- ウェブ アプリケーション **ファイアウォール > ログ**
- **ログ > 表示**

「既定のテーブル サイズ」フィールドの最小値は 10 (行) で、既定値は 100 で、最大値は 99,999 です。

自動的に更新されるテーブルで、ストリーミング更新間隔設定によって影響を受けるものは次のとおりです。

- **システム > 監視**
- **ネットワーク > インターフェース**
- **NetExtender > 状況**
- **ユーザ > 状況**

「ストリーミング更新間隔」フィールドの最小値は 1 (秒) で、既定値は 10、最大値は 99,999 です。

SNMP 設定

SNMP 設定セクションでは、管理者は SNMP を有効にして、装置に対する SNMP 設定を指定できます。ダウンロードされた MIB のリストがフィールドの右側に表示されます。MIB は MySonicWall からダウンロードできます。

GMS の設定

GMS の設定セクションでは、GMS 管理を有効にでき、GMS ホスト名または IP アドレス、GMS Syslog サーバ ポート、ハートビート間隔 (秒単位) を指定できます。

ログイン セキュリティの設定

SMA/SRA 装置のログイン セキュリティは、ユーザ ポータルへの不正なログイン試行から保護する自動ロックアウト機能を備えています。自動ロックアウト機能を有効にするには、以下の手順に従います。

1 「**システム > 管理**」にナビゲートします。

2 「**管理者/ユーザのロックアウトを有効にする**」をオンにします。

3 ユーザをロックアウトするまでに許可するログイン試行の最大数を「**1 分間でのログイン最高試行回数**」フィールドに入力します。既定値は 5 回です。最大数は 99 回です。

4 ログインの最高試行回数を超えたユーザをロックアウトする時間を分単位で「**ロックアウト時間 (分)**」フィールドに入力します。既定値は 5 分です。最大数は 9999 分です。

5 「**適用**」を選択して変更を保存します。

HTTP DoS 設定の構成

HTTP DoS 設定では、IP アドレスごとの TCP 最大同時接続数を設定します。最大同時接続数を変更するには、以下の手順に従います。

1 「**システム > 管理**」にナビゲートします。

2 「**IP 毎最大同時 TCP 接続数**」フィールドに、クライアントが Secure Mobile Access ウェブ サーバで開くことのできる最大同時 TCP 接続数を入力します。既定値は 20 で、最大値は 100 です。

ウェブ管理設定の構成

「ウェブ管理設定」セクションでは、Secure Mobile Access 管理インターフェース内の、ページ分けされるテーブルの既定のページ サイズと、動的に更新されるテーブルのストリーミング更新間隔を設定できます。

テーブルのページ サイズとストリーミング更新間隔を設定するには:

1 「**既定のテーブル サイズ**」フィールドに、Secure Mobile Access 管理インターフェース内のページ分けされるテーブルのページあたりの行数を入力します。既定値は 100、最小値は 10、最大値は 99,999 です。

2 「**ストリーミング更新間隔**」フィールドに、Secure Mobile Access 管理インターフェース内の動的に更新されるテーブルの更新間隔の秒数を入力します。既定値は 10、最小値は 1、最大値は 99,999 です。

3 「**適用**」を選択して変更を保存します。

SNMP の設定

SNMP 設定のフィールドを構成するには、以下の手順に従います。

1 「**システム > 管理**」にナビゲートします。

2 「**SNMP を有効にする**」を選択します。

3 システムの名前 (FQDN) を「**システム名**」フィールドに入力します。

4 システムの連絡先の電子メール アドレスを「**システムの連絡先**」フィールドに入力します。

5 システムの都市や他の識別場所を「**システムの場所**」フィールドに入力します。

6 システムの資産番号を「**資産番号**」フィールドに入力します。この資産番号は管理者により定義されます。

7 パブリック コミュニティ名を「**Get コミュニティ名**」フィールドに入力します。この名前は SNMP GET 要求内で使われます。

8 「**適用**」を選択して変更を保存します。

GMS 管理を有効にする

SonicWall Inc. グローバル管理システム (GMS) は、複数のサイト間 VPN のグローバル管理を一元的に行うなど、何千台もの SonicWall Inc. インターネット セキュリティ装置を設定および管理できるウェブベースのアプリケーションです。

SMA/SRA 装置の GMS 管理を有効にするには、以下の手順に従います。

1 「**システム > 管理**」にナビゲートします。

2 「**GMS 管理を有効にする**」をオンにします。

3 GMS サーバのホスト名または IP アドレスを「**GMS ホスト名または IP アドレス**」フィールドに入力します。

4 GMS サーバのポート番号を「**GMS Syslog サーバ ポート**」フィールドに入力します。GMS サーバとの通信で使用する既定のポートは 514 です。

5 GMS サーバへのハートビートの送信間隔を「**ハートビート間隔 (秒)**」フィールドに入力します。最大ハートビートは 86,400 秒 (24 時間) です。

6 「**適用**」を選択して変更を保存します。

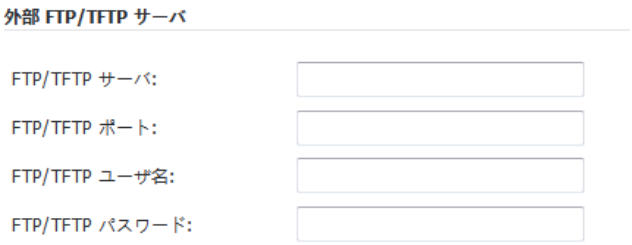
外部 FTP/TFTP サーバ

「外部 FTP/TFTP サーバ」セクションでは、設定と診断データをバックアップするために外部 FTP サーバを設定できます。

外部 FTP/TFTP サーバの設定

「外部 FTP/TFTP サーバ」フィールドを設定するには:

1 「**システム > 管理 | 外部 FTP/TFTP サーバ**」に移動します。



2 FTP/TFTP サーバのアドレス、ポート、ユーザ名、およびパスワードを各フィールドに入力します。

3 「**適用**」を選択して変更を保存します。

システム > 証明書

このセクションでは、「**システム > 証明書**」ページの概要と、このページで実行できる設定タスクについて説明します。

「システム > 証明書」の概要

管理者は、「**システム > 証明書**」ページで、サーバ証明書や追加の CA (認証局) 証明書をインポートできます。

「システム > 証明書」ページ

以下のセクションを参照してください。

- サーバ証明書 (124 ページ)
- 追加の CA 証明書 (125 ページ)

サーバ証明書

サーバ証明書セクションでは、サーバ証明書のインポートと設定、および CSR (証明書署名リクエスト) の生成を行うことができます。

サーバ証明書は、SMA/SRA 装置の身元確認に使用します。ユーザがログイン ページにアクセスすると、装置からユーザのブラウザに対してサーバ証明書が提示されます。各サーバ証明書には、その証明書が属するサーバの名前が示されています。

証明書には、自己署名証明書が必ず 1 つあります (自己署名とは、実際の CA ではなく SMA/SRA 装置によって生成されたという意味です)。また、管理者が複数の証明書をインポートしている場合もあります。管理者が複数のポータルを設定している場合、各ポータルに別個の証明書を関連付けていることがあります。例えば、ブラウザで **virtualassist.test.sonicwall.com** を指せば、**sslvpn.test.sonicwall.com** にもアクセスされます。これらのポータル名それぞれに対し、別個の証明書を持たせることができます。このようにすると、「このサーバは abc ですが、証明書は xyz のものです。続行しますか?」といった証明書の不一致の警告がブラウザから表示されないようにするうえで役立ちます。

CSR とは、証明書署名リクエストのことです。CA から証明書を取得するための準備では、証明書の詳細を記した CSR をまず作成します。そして、その CSR を CA に送り、所定の料金を支払うと、有効な署名が付いた証明書が CA から返送されます。

追加の CA 証明書

「追加の CA 証明書」セクションでは、ローカル ネットワーク内部または外部の認証局サーバから追加の CA 証明書をインポートできます。証明書は、鎖状の証明書とともに、例えば発行した CA が中間 (鎖状) 署名証明書を使っている場合に使用できるように、PEM 暗号化形式になっています。

インポートした追加の証明書が有効になるのは、SMA/SRA 装置を再起動した後です。

証明書の管理

SMA/SRA 装置には、事前インストール済みの SSL 機能対応自己署名 X509 証明書が添付されています。自己署名証明書の機能はすべて、有名な認証局 (CA) から発行される証明書と同じですが、信頼できるルート ストアにインポートするまでセキュリティ警告「信頼できないルート CA 証明書です」が発行されます。このインポート手順を実行するには、認証後にポータルで「**証明書のインポート**」を選択します。

自己署名証明書の使用に代わるもう 1 つの方法は、証明書署名リクエスト (CSR) を生成し、有名な CA に提出して有効な証明書を発行してもらうことです。有名な CA には、RapidSSL (www.rapidssl.com)、Verisign 〈www.verisign.com〉、Thawte 〈www.thawte.com〉などがあります。

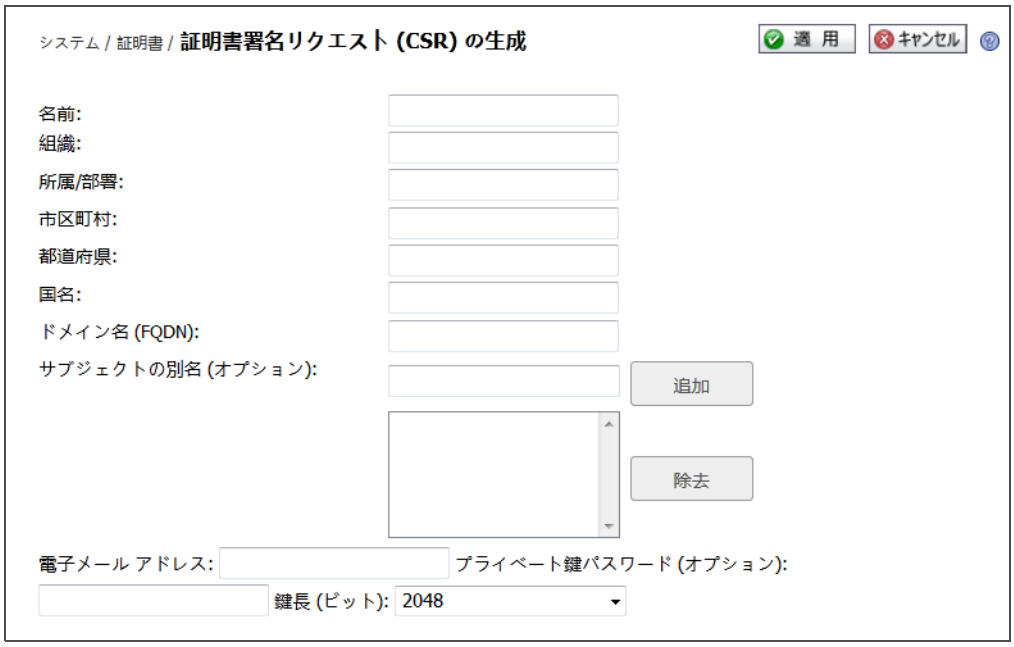
証明書署名リクエストの生成

RapidSSL、Verisign、Thawte などの知名度のある CA から有効な証明書を取得するには、SMA/SRA 装置用に証明書署名リクエスト (CSR) を生成する必要があります。

証明書署名リクエストを生成するには:

1 「**システム > 証明書**」ページに移動します。

2 「**CSR の生成**」を選択して CSR と証明書鍵を生成します。「**証明書署名リクエスト (CSR) の生成**」ダイアログ ボックスが表示されます。



3 ダイアログ ボックスのフィールドに値を入力し、「**適用**」を選択します。

> **メモ**：サブジェクトの別名 (SAN)/統合コミュニケーション証明書 (UCC) をリクエストに含めることができます。

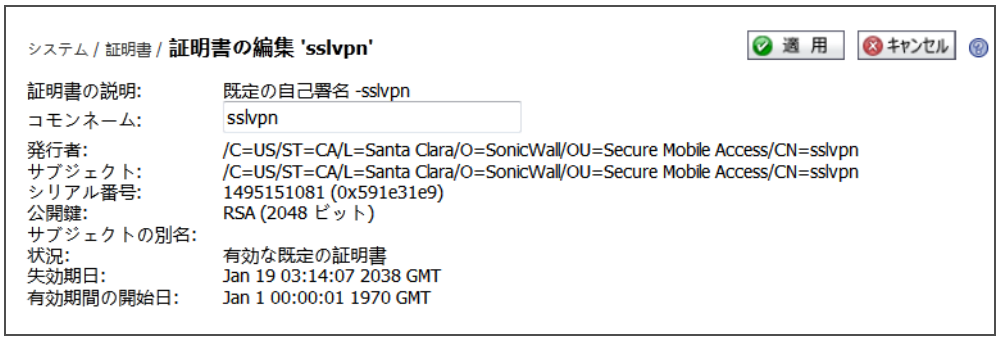
4 すべての情報が正しく入力されると、**csr.zip** ファイルが作成されます。この .zip ファイルをディスクに保存します。この zip ファイル内にある server.csr ファイルの内容を CA に提出する必要があります。

証明書と発行者情報の表示と編集

現在ロードされている SSL 証明書は、「**システム > 証明書**」の現在の証明書テーブルにリストされます。

証明書と発行者情報を表示して証明書のコモンネームを編集するには:

1 証明書に対応する設定アイコンを選択します。「**証明書の編集**」ウィンドウが開き、発行者情報や証明書のサブジェクト情報が表示されます。



2 「**証明書の編集**」ウィンドウでは、発行者情報や証明書のサブジェクト情報を確認することができます。

3 自己署名証明書の「**コモンネーム**」フィールドにウェブ サーバのホスト名または IP アドレスを入力します。

4 「**適用**」を選択して変更を適用します。

期限切れの証明書や不正な証明書を削除することもできます。証明書を削除するには、「**システム > 証明書**」ページで、目的の証明書の行の「**削除**」を選択します。

メモ：現在アクティブな証明書は削除できません。証明書を削除するには、別の SSL 証明書をアップロードして有効にします。次に、「**システム > 証明書**」ページから、アクティブでない証明書を削除します。

証明書のインポート

証明書をインポートする場合は、秘密鍵と証明書が含まれる**PKCS #12** (.p12 または.pfx) ファイルをアップロードするか、PEM 形式の秘密鍵ファイル"server.key"と PEM 形式の証明書ファイル"**server.crt**"が含まれる .zip ファイルをアップロードしてください。この .zip ファイルはディレクトリを持たないフラットなファイル構造で、**server.key** ファイルと **server.crt** ファイルだけを含まなければなりません。

証明書をインポートするには:

1 「**システム** > **証明書**」ページにナビゲートします。

2 「**証明書のインポート**」を選択します。「証明書のインポート」ダイアログ ボックスが表示されます。

3 「**参照**」を選択します。

4 サーバ証明書を指定します。PKCS#12 ファイルからアップロードする場合は、.p12 または .pfx ファイルをローカル ディスクまたはネットワーク ドライブ上で探し、選択します。秘密鍵と証明書が含まれる zip ファイルをアップロードする場合は、.zip ファイルをローカル ディスクまたはネットワーク ドライブ上で探し、選択します。どのようなファイル名でも受け入れられますが、拡張子は ".zip" でなければなりません。この zip ファイルには、証明書ファイル**server.crt**と証明書鍵ファイル**server.key**が入っています。鍵と証明書は zip のルートに位置する必要があります。この位置にない場合、ファイルはアップロードされません。

5 「**アップロード**」をクリックします。

証明書のアップロードが終了すると、その証明書は「**システム > 証明書**」ページの証明書リストに表示されます。

メモ：秘密鍵がパスワードを要求する場合があります。

CA 証明書の追加

例えば発行元認証局が中間 (連鎖) 署名証明書を使用する場合に、連鎖証明書で使用される認証局証明書を追加でインポートできます。CA 証明書ファイルをインポートするには、**PEM エンコード**、**DER エンコード**、または **PKCS#7** (.p7b) ファイルをアップロードします。

追加の証明書を PEM 形式で追加するには:

1 「**システム > 証明書**」ページに移動します。

2 「追加の CA 証明書」セクションの「**CA 証明書のインポート**」を選択します。「証明書のインポート」ダイアログ ボックスが表示されます。

3 「**参照**」を選択します。

4 ローカル ディスクまたはネットワーク ドライブ上で、PEM エンコード、DER エンコード、または PKCS#7 の CA 証明書ファイルを探し、選択します。どのようなファイル名でも受け入れられます。

5 「**アップロード**」をクリックします。

証明書のアップロードが終了すると、その CA 証明書は「**システム > 証明書**」ページの「追加の CA 証明書」リストに表示されます。

6 この新しい CA 証明書をウェブ サーバのアクティブ CA 証明書リストに追加するには、ウェブ サーバを再起動する必要があります。SMA/SRA 装置を再起動することでウェブ サーバを再起動します。

システム > 監視

このセクションでは、「**システム > 監視**」ページの概要と、このページで実行できる設定タスクについて説明します。

「システム > 監視」の概要

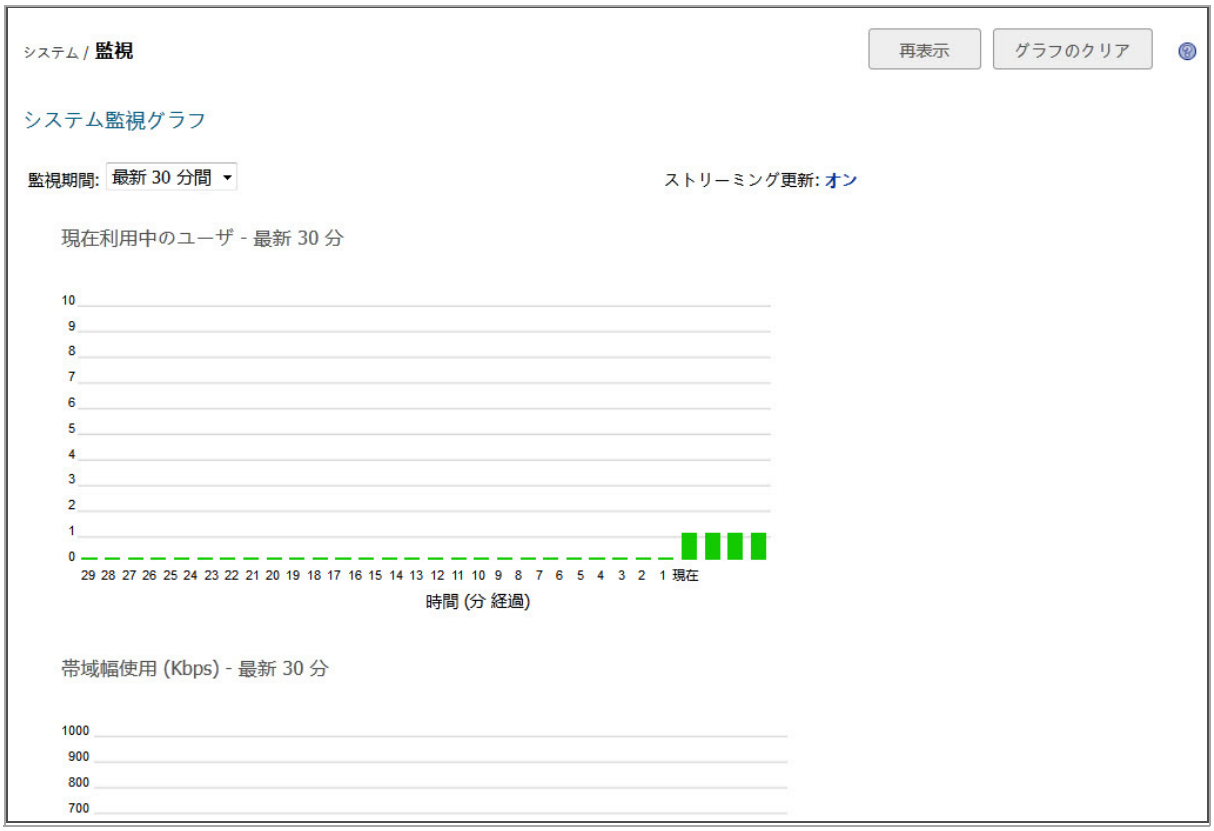
SMA/SRA 装置には、装置の使用状況と処理能力データを表示できる、設定可能な監視ツールが用意されています。「**システム > 監視**」ページでは、次の 4 種類の監視グラフを表示できます。

- 現在利用中のユーザ
- 帯域幅使用
- CPU 使用率 (%)
- メモリ使用率 (%)

管理者は監視期間を、最新の 30 秒、30 分、24 時間、30 日の中から設定できます。たとえば、「**最新 24 時間**」は直近の 24 時間を表します。

次の図に「**システム > 監視**」ページを示します。

「システム > 監視」ページ



監視グラフ

次の 4 種類の監視グラフは、最新の 1 時間から 1 ヶ月の範囲で、対応するデータを表示するように設定できます。

監視グラフのタイプ

グラフ	説明
現在利用中のユーザ	秒、分、時間、または日の単位で測定した、同時に装置にログインしているユーザの数。この数値は、2、3、5 などの整数で表される
帯域幅使用 (Kbps)	秒、分、時間、または日の単位で測定した、装置が送受信する 1 秒あたりのデータ量 (Kbps) を示す
CPU 使用率 (%)	秒、分、時間、または日の単位で測定した、使用中の装置プロセッサにおける処理能力使用量。この数値は、CPU の全処理能力に対するパーセントで表される
メモリ使用率 (%)	秒、分、時間、または日の単位で測定した、装置で使用された利用可能メモリの容量。この数値は、利用可能メモリの全容量に対するパーセントで表される

監視期間の設定

監視期間を設定するには、「**システム > 監視**」ページの「**監視期間**」ドロップダウン リストから次のオプションのいずれかを選択します。

- 最新 30 秒間

- 最新 30 分間
- 最新 24 時間
- 最新 30 日間

モニタの再表示

モニタを再表示するには、「**システム > 監視**」ページの右上隅にある「**再表示**」を選択します。

システム > 診断

このセクションでは、「**システム > 診断**」ページの概要と、このページで実行できる設定タスクについて説明します。

「システム > 診断」の概要

「**システム > 診断**」ページでは、管理者がテクニカル サポート レポートをダウンロードまたはメール送信し、基本的なネットワーク診断を実行できます。

「システム > 診断」ページ

TSR を再起動後や生成後に外部の FTP サーバに自動送信するには、次のオプションを使用できます。FTP サーバを「**システム > 管理**」ページで設定して、TSR が外部 FTP サーバに自動的に送信されるようにします。詳細については、外部 FTP/TFTP サーバの設定 (123 ページ) を参照してください。

テクニカル サポート レポートのダウンロードと生成

テクニカル サポート レポートのダウンロードでは、SonicWall Inc. テクニカル サポートがシステムの動作を分析するうえで役立つシステム情報や設定が記録されます。テクニカル サポート レポートに対し、以下のオプションが提供されています。

- **現在のレポートのダウンロード** - このボタンを選択すると、ダウンロードの実行を確認するポップアップ ウィンドウが表示されます。「**保存**」を選択してレポートを保存します。テクニカル サポート レポートは .zip ファイルとして保存されます。このファイルには、グラフ、イベント ログ、および SMA/SRA 装置に関する他のテクニカル情報が入っています。
- **現在のレポートを電子メールで送信** - テクニカルサポートレポートを「**レポートの電子メール送信先**」フィールドで指定した電子メール アドレスに送信します。
- **再起動時にテクニカル サポートレポートを生成する** - チェックボックスをオンにすると、このオプションが有効になります。このオプションを有効にすると、SMA/SRA 装置は再起動するたびに新しい TSR を生成します。装置で生成された最新のレポートがドロップダウン リストに表示されます。ファイル名の前に “Restarted_TSR_” という接頭辞が付加されます。
  - **ダウンロード** - 最新の再起動テクニカル サポート レポートをローカル システムにダウンロードします。
  - **削除** - 最新の再起動テクニカル サポート レポートを削除します。
  - **電子メール** - 最新の再起動テクニカル サポート レポートを、「**ログ** > **設定**」ページの「**メール サーバ**」フィールドで指定した宛先にメール送信します。
  - **新しいレポートの生成時に電子メールで自動的に送信する** - 最新の再起動テクニカル サポート レポートの自動メール送信を有効にします。メールを自動送信するには、「**ログ** > **設定**」ページの「**メール サーバ**」と「**メール送信元アドレス**」のフィールドを設定しておく必要があります。
- **テクニカルサポートレポートの定期生成を有効にする** - テクニカル サポート レポートの定期生成を有効にします。これを有効にすると、**1 時間ごと**、または **1 日ごと**にレポートを生成できます。保存される TSR は最大 12 件で、合計ファイル サイズは 50 MB を超えてはいけないことに注意してください。テクニカル サポート レポートの定期生成は主に、SonicWall Inc. 技術者が必要に応じて診断やトラブルシューティングのために使用します。

  メモ：TSR の定期生成は、既定では無効になっています。先に **<SSLVPN>/cgi-bin/diag** ページで、この機能を有効にしておく必要があります。

  - **ダウンロード** - 最新の定期生成テクニカル サポート レポートをローカル システムにダウンロードします。
  - **削除** - 最新の定期生成テクニカル サポート レポートを削除します。
  - **電子メール** - 最新の定期生成テクニカル サポート レポートを、「**ログ** > **設定**」ページの「**メール サーバ**」フィールドで指定した宛先にメール送信します。
  - **新しいレポートの生成時に電子メールで自動的に送信する** - 最新の定期生成テクニカル サポート レポートの自動メール送信を有効にします。メールを自動送信するには、「**ログ** > **設定**」ページの「**メール サーバ**」と「**メール送信元アドレス**」のフィールドを設定しておく必要があります。

診断テストの実行

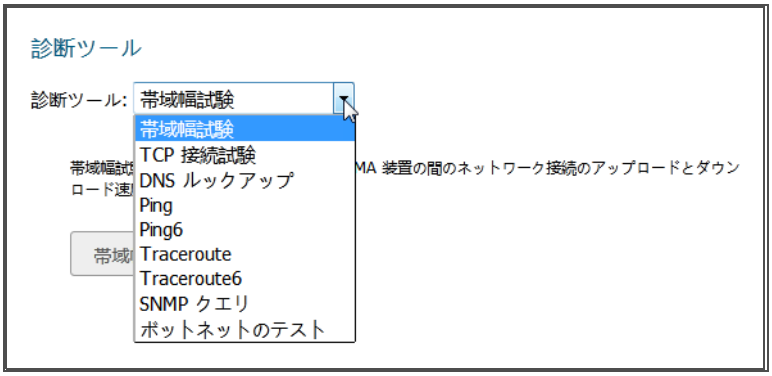
管理者は診断ツールを使用して、特定の IP アドレスまたはウェブ サイトに対して Ping、TCP 接続試験、DNS ルックアップ、または Traceroute を実行することにより、SMA/SRA の接続をテストできます。また、SMA/SRA 装置とローカル コンピュータ間の帯域幅試験を実行したり、SNMP クエリを実行して装置に関する情報を表示したりすることもできます。

「**システム > 診断**」ページで、SMA/SRA 装置の標準ネットワーク診断テストを実行できます。

診断テストを実行するには :

1 「**システム > 診断**」ページにナビゲートします。

2 「**診断ツール**」ドロップダウン リストで、「**帯域幅試験**」、「**TCP 接続試験**」、「**DNS ルックアップ**」、「**Ping**」、「**Ping6**」、「**Traceroute**」、「**Traceroute6**」、「**SNMP クエリ**」、または「**ボットネットのテスト**」を選択します。



次の表に、診断ツールとその機能の説明を示します。

診断ツールとその機能

診断ツール	機能
帯域幅試験	コンピュータと SMA/SRA 装置の間のネットワーク接続のアップロード速度とダウンロード速度を測定します。
TCP 接続試験	ポートの接続性をテストします。ポートは、ホスト名または IP アドレスの後にコロンに続いてポート番号を付加することによって指定します (例えば、10.9.9.19:83 または www.myhost.com:83 など)。ポートを指定しない場合は、ポート 80 がテストされます。
DNS ルックアップ	DNS 名から IP アドレス、またはその逆の変換を行います。
Ping	ホストまたは IP アドレスへの接続をテストします。
Ping6	IPv6 アドレスまたはドメインへの接続をテストします。Ping6 は、IPv6 アドレスと IPv6 ネットワークで使用するためのものです。
Traceroute	ホストまたは IP アドレスへの接続に必要なルートとホップ数を検出します。
Traceroute6	IPv6 アドレスまたはドメインへの接続に必要なルートとホップ数を検出します。Traceroute6 は、IPv6 アドレスと IPv6 ネットワークで使用するためのものです。

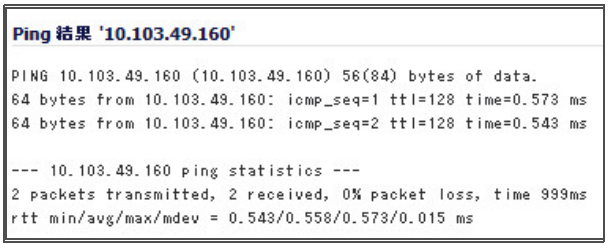
診断ツールとその機能 (続き)

診断ツール	機能
SNMP クエリ	選択された MIB から SNMP 情報を検索します。クエリを実行する前に、SNMP を有効にする必要があります (「**システム > 管理**」ページ)。「**SNMP MIB**」ドロップダウン リストで、値を表示する MIB を選択します。「SNWL-SSLVPN-MIB」は、Secure Mobile Access 固有の MIB で、装置の統計とライセンス情報を表示します。「SNWL-COMMON-MIB」は、すべての SonicWall Inc. 製品に共通のファイルで、製品名、シリアル、ファームウェア、ROM バージョン、資産番号 (ユーザ定義) を表示します。その他には、「SNMPv2-MIB」などの標準 SNMP MIB や「すべての SNMP MIB-2」があり、「すべての MIB」を選択することもできます。
ボットネットのテスト	IP アドレスがボットネット IP アドレスであるかどうかを識別します。

3 ホストや IP アドレスなどの追加情報を求められた場合は、その情報を入力します。

4 「**実行**」を選択します。

結果がページの下部に表示されます。



システム > 再起動

このセクションでは、「**システム > 再起動**」ページの概要と、このページで実行できる設定タスクについて説明します。

- 「システム > 再起動」の概要 (133 ページ)
- SMA/SRA 装置の再起動 (133 ページ)

「システム > 再起動」の概要

「**システム > 再起動**」ページでは、SMA/SRA 装置を再起動できます。

再起動には 1 から 2 分程度かかり、現在のユーザ接続がすべて切断されることを示す警告が表示されます。

SMA/SRA 装置の再起動

SMA/SRA 装置を再起動するには、以下の手順を実行します。

1 「**システム > 再起動**」にナビゲートします。

2 「**再起動**」を選択します。

3 確認のダイアログ ボックスで「**OK**」を選択します。

メモ：再起動には約 2 分を要し、すべてのユーザが切断されます。

システム > 情報

「**システム** > **情報**」ページには、SMA/SRA 装置を使用するためのエンド ユーザ使用許諾契約が表示されます。SonicWall Inc. の著作権情報を確認するには、「**ダウンロード**」を選択します。エンド ユーザ使用許諾契約の詳細は、https://www.sonicwall.com/ja-jp/legal/ を参照してください。

4

ネットワーク設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**ネットワーク**」ページと、このページで行う設定タスクについて説明します。SMA/SRA 装置のネットワーク タスクとして、ネットワーク インターフェース、DNS 設定、ルート、ホスト解決の設定などがあります。

トピック:

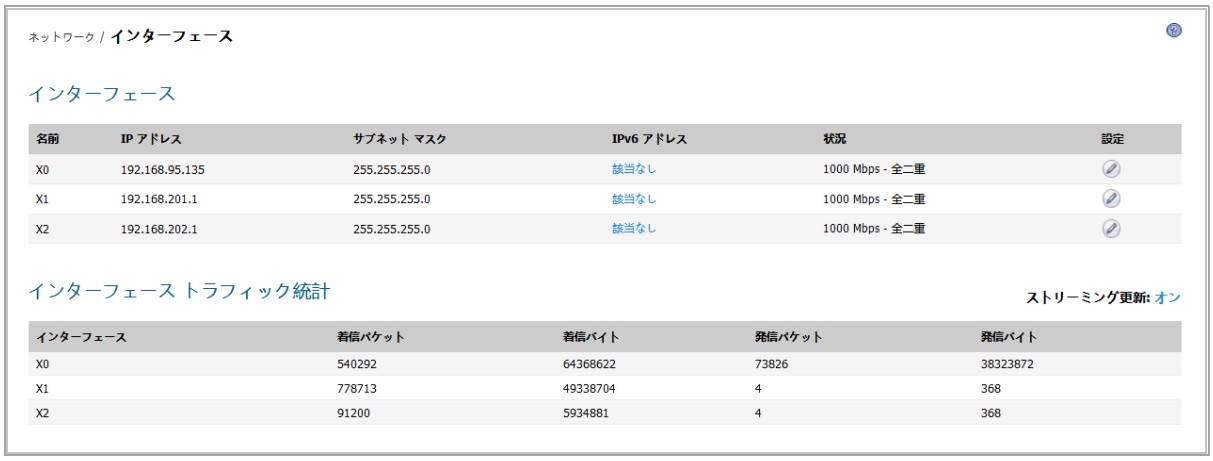
ネットワーク > インターフェース

このセクションでは、「**ネットワーク > インターフェース**」ページの概要と、このページで行う設定タスクについて説明します。

「ネットワーク > インターフェース」の概要

「**ネットワーク > インターフェース**」ページでは、IP アドレスとサブネット マスクを設定し、SMA/SRA 装置の物理ネットワーク インターフェース ポートの接続速度を表示できます。

「ネットワーク > インターフェース」ページ



ネットワーク インターフェースの設定

管理者は「**ネットワーク > インターフェース**」ページで、SMA/SRA 装置の X0、X1、X2、X3、そして利用可能な場合 X4、および X5 インターフェースの IP アドレス、サブネット マスク、速度、および管理設定を表示、設定できます。SMA/SRA 装置のポートが同じネットワーク上のファイアウォールまたはターゲット機器と通信する場合は、インターフェースに IP アドレスとサブネット マスクを割り当てる必要があります。

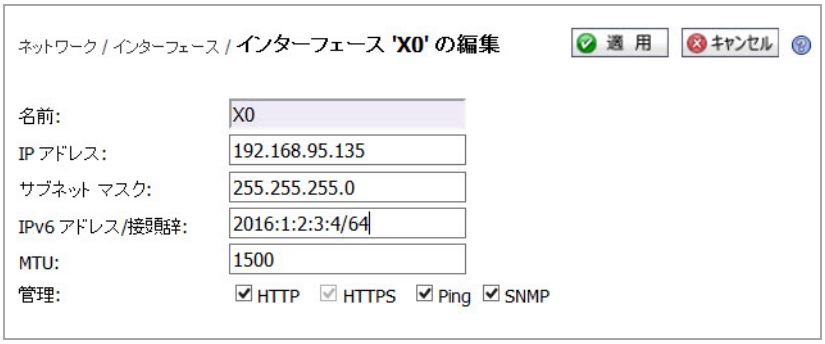
メモ：Secure Mobile Access 管理インターフェースの IP アドレスが変更されると、Secure Mobile Access サービスは自動的に再起動されます。これによって既存のユーザ セッションはすべて切断されるので、SMA/SRA 装置を引き続き使用するには再接続する必要があります。

SMA/SRA 装置のインターフェース用にこれらの設定を構成するには:

1 「**ネットワーク > インターフェース**」ページにナビゲートして、設定するインターフェースの横にある設定アイコンを選択します。

2 SMA/SRA 装置の「**インターフェースの編集**」ダイアログ ボックスで、未使用の静的 IP アドレスを「**IP アドレス**」フィールドに入力します。この IP アドレスは、SMA/SRA 装置の接続先ローカル サブネット内のアドレスでなければなりません。

3 対応するフィールドに**サブネット マスク**を入力します。



4 グローバル スコープに対する IPv6 アドレスを「IPv6**アドレス / 接頭辞**」フィールドに入力します。このフィールドを空にしても、IPv6 利用可能な機器はリンク ローカル アドレスを使用して自

動的に接続できます。スコープは「**ネットワーク > インターフェース**」ページのツールチップ内に表示されます。

5 「**速度**」ドロップダウン　リストでは「**自動ネゴシエーション**」が既定で選択され、SMA/SRA 機器は接続されているスイッチや他のネットワーキング機器との間で速度と通信方式を自動的にネゴシエートします。通常、イーサネット接続は自動的にネゴシエートされます。特定のリンク速度と通信方式を強制的に指定する場合は、以下のいずれかのオプションを選択します。

- 1000Mbps - 全二重
- 100Mbps - 全二重
- 100 Mbps - 半二重
- 10 Mbps - 全二重
- 10 Mbps - 半二重

メモ：特定のリンク速度と通信方式を選択した場合は、接続されているネットワーキング機器から SonicWall Inc. セキュリティ装置への接続の速度と通信方式も強制的に変更する必要があります。

6 「**管理**」オプションでは、このインターフェースを介した SMA/SRA 装置のリモート管理を有効にするには、サポートされている管理プロトコルを選択します。「**HTTP**」、「**HTTPS**」、「**Ping**」から 1 つ以上を選択できます。

7 「**適用**」を選択します。

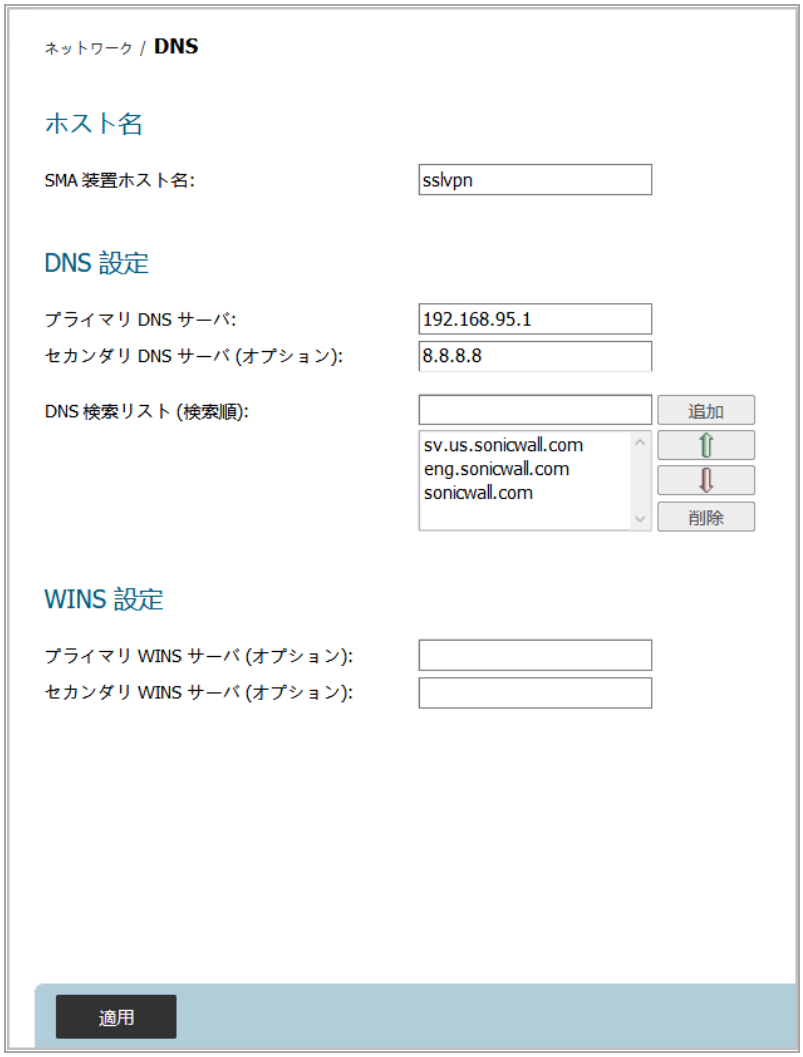
ネットワーク > DNS

このセクションでは、「**ネットワーク > DNS**」ページの概要と、このページで行う設定タスクについて説明します。

「ネットワーク > DNS」の概要

管理者は、「**ネットワーク > DNS**」ページで SMA/SRA 装置のホスト名、DNS 設定、および WINS 設定を設定できます。

「ネットワーク > DNS」ページホスト名



「ホスト名」セクションでは、SMA/SRA ゲートウェイのホスト名を指定できます。

DNS 設定

「DNS 設定」セクションでは、「**プライマリ DNS サーバ**」、「**セカンダリ DNS サーバ (オプション)**」、および「**DNS ドメイン**」(オプション) を指定できます。プライマリ DNS サーバは必ず指定します。

Apple iPhone、iPad、その他の iOS 機器からの SonicWall Inc. Mobile Connect を使った接続をサポートする SMA/SRA 装置に対しては、「**DNS ドメイン**」は必須フィールドです。この DNS ドメインは、iPhone/iPad の VPN インターフェース上に、機器が装置との接続を確立した後で設定されます。モバイル機器のユーザがある URL にアクセスする際に、iOS はこのドメインが VPN インターフェースのドメインと一致しているかどうかを判断し、一致している場合は VPN インターフェースの DNS サーバを使ってホスト名検索を解決します。そうでない場合は、組織のイントラネット内のホストを解決できない Wi-Fi または 3G/4G の DNS サーバが使われます。

WINS 設定

「WINS (Windows Internet Name Service) 設定」セクションでは、プライマリ WINS サーバおよびセカンダリ WINS サーバ (両方ともオプション) を指定できます。

ホスト名の構成

ホスト名を設定するには:

1 「**ネットワーク > DNS**」ページにナビゲートします。

2 「ホスト名」領域の「**SMA 装置 ホスト名**」フィールドに、SMA/SRA 装置のホスト名を入力します。

3 「**適用**」を選択します。

DNS の設定

SMA/SRA 装置で、対応する IP アドレスからホスト名と URL 名を解決するには、ドメイン ネーム サーバ (DNS) が必要です。これによって SMA/SRA 装置は、完全修飾ドメイン名 (FQDN) を使ってホストやサイトに接続できるようになります。

DNS サーバを設定するには:

1 「**ネットワーク > DNS**」ページにナビゲートします。

2 「DNS 設定」領域の「**プライマリ DNS サーバ**」フィールドに、プライマリ DNS サーバのアドレスを入力します。

3 オプションのセカンダリ DNS サーバ アドレスを「**セカンダリ DNS サーバ (オプション)**」フィールドに入力できます。

4 オプションで「**DNS 検索リスト**」フィールドを使ってドメイン名のプールを作成します。

   a 「**DNS 検索リスト**」にドメイン接尾辞を入力して「**追加**」を選択します。ホスト名をホスト解決で使用される完全修飾ドメイン名 (FQDN) にするために、接尾辞はホスト名に付加されます。

   b DNS 接尾辞を削除するには、リストからドメイン接尾辞を選択して「**削除**」を選択します。

   c 上矢印と下矢印を使って、ホスト名を解決するために使用される DNS ドメイン接尾辞を並べ替えます。

   例えば、ホスト名が SonicPRS で、検索リストに DNS 接尾辞 usa.n.sonicwall.com と rsc.sonicwall.com が追加されているとします。1 番目の接尾辞が SonicPRS に付加され、名前解決で使用される FQDN (SonicPRS.usa.n.sonicwall.com) が作成されます。この名前が解決されなかった場合は、検索リスト内の 2 番目の接尾辞が使われます (SonicPRS.rsc.sonicwall.com) 。この処理は名前が解決されるか、すべての接尾辞が試行されるまで継続されます。

5 「**適用**」を選択します。

6 新しい DNS 設定を反映するために、装置を再起動します。

WINS 設定の構成

WINS 設定はオプションです。SMA/SRA 装置は、NetBIOS クライアントと WINS (Windows Internet Naming Service) クライアントの両方として機能し、ローカル ネットワークのホスト名と、対応する IP アドレスを認識することができます。

WINS 設定を行うには:

1 「**ネットワーク > DNS**」ページにナビゲートします。

2 「WINS 設定」領域の「**プライマリ WINS サーバ (オプション)**」フィールドに、プライマリ WINS のアドレスを入力します。

3 「WINS 設定」領域の「**セカンダリ WINS サーバ (オプション)**」フィールドに、セカンダリ WINS のアドレスを入力します。

4 「**適用**」を選択します。

ネットワーク > ルート

ネットワーク > ルート このセクションでは、「**ネットワーク > ルート**」ページの概要と、このページで行う設定タスクについて説明します。

「ネットワーク > ルート」の概要

「**ネットワーク > ルート**」ページでは、デフォルト ゲートウェイとインターフェースの割り当て、および静的ルートの追加と設定を行うことができます。既定ルートや静的ルートの詳細については、ご使用の装置モデルの導入ガイドを参照してください。

「ネットワーク > ルート」ページ

デフォルト ルート

「デフォルト ルート」セクションでは、デフォルト IPv4 ゲートウェイとインターフェース、かつ/またはデフォルト Ipv6 ゲートウェイとインターフェースを設定して、既定のネットワーク ルートを定義できます。既定のネットワーク ルートはインターネット アクセスに必須です。

静的ルート

「静的ルート」セクションでは、送信先ネットワーク、サブネット マスク、オプションのデフォルト ゲートウェイ、およびインターフェースを指定することによって、静的ルートを追加および設定できます。

SMA/SRA 装置の既定ルートの設定

リモート ネットワークと通信できるように、SMA/SRA 装置のデフォルト ゲートウェイを設定する必要があります。リモート ネットワークとは、装置独自のネットワークとは異なる任意の IP サブネットです。一般に、デフォルト ゲートウェイは、SMA/SRA 装置の接続先のファイアウォール インターフェースの LAN IP アドレスになります。これがこの装置の既定ルートです。

既定ルートを設定するには:

1. 「**ネットワーク > ルート**」ページに移動します。
2. 「**デフォルト IPv4 ゲートウェイ**」フィールドに、SMA/SRA 装置がネットワークに接続するときに経由するファイアウォールやその他のゲートウェイ機器の IP アドレスを入力します。このアドレスが装置の既定ルートとして機能します。
3. 「**インターフェース**」ドロップダウン リストから、ネットワークへの IPv4 接続インターフェースの役割を果たすインターフェースを選択します。一般に、このインターフェースは X0 になります。
4. 「**デフォルト IPv6 ゲートウェイ**」フィールドに、SMA/SRA 装置がネットワークに接続するときに経由するファイアウォールやその他のゲートウェイ機器の IPv6 アドレスを入力します。このアドレスが装置の既定 IPv6 ルートとして機能します。
5. 「**インターフェース**」ドロップダウン リストから、ネットワークへの IPv6 接続インターフェースの役割を果たすインターフェースを選択します。
6. 「**適用**」を選択します。

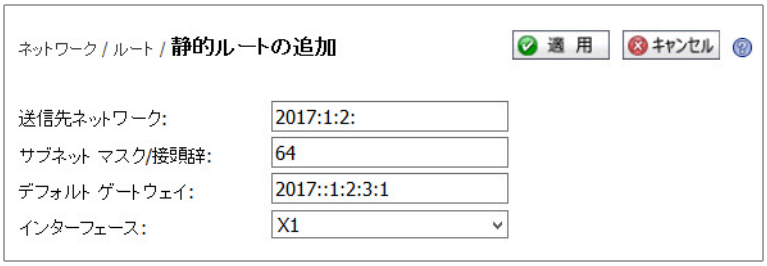
装置の静的ルートの設定

ネットワークのトポロジーに基づき、デフォルト ゲートウェイを通って特定のサブネットにアクセスするよりも、特定のサブネットへの静的ルートを設定することが必要になる、またはそのほうが好ましい場合があります。既定ルートは機器のデフォルト ゲートウェイですが、SMA/SRA 装置が他のネットワークにもアクセスできるようにする必要がある場合は、静的ルートを追加することができます。ルーティングや静的ルートの詳細については、標準的な Linuxの参考書を参照してください。

装置の明示的な宛先への静的ルートを設定するには、以下の手順を実行します。

1 「**ネットワーク > ルート**」ページにナビゲートして、「**静的ルートの追加**」を選択します。

2 「**静的ルートの追加**」ダイアログ ボックスで、「**送信先ネットワーク**」フィールドに、静的ルートの送信先となるサブネットまたはホストを入力します (たとえば、**192.168.220.0** は 192.168.220.X/24 サブネットへのルートを提供します)。IPv6 サブネットの入力もできます (たとえば、**2017:1:2::**)。



3 「**サブネット マスク/接頭辞**」フィールドに、サブネットマスク値または接頭辞に使用するビット数を入力します。

4 「**デフォルト ゲートウェイ**」フィールドに、装置をネットワークに接続するゲートウェイ機器の IP アドレスを入力します。IPv6 アドレスの入力もできます。

5 「**インターフェース**」ドロップダウン リストで、装置を希望の宛先ネットワークに接続するインターフェースを選択します。

6 「**適用**」を選択します。

ネットワーク > ホスト解決

ネットワーク > ホスト解決このセクションでは、「**ネットワーク > ホスト解決**」ページの概要と、このページで行う設定タスクについて説明します。

「ネットワーク > ホスト解決」の概要

管理者は、「**ネットワーク > ホスト解決**」ページを使ってホスト名を設定できます。

「ネットワーク > ホスト解決」ページ

ホスト名設定

「ホスト名設定」セクションでは、IP アドレス、ホスト名 (ホストまたは FQDN)、およびオプションのエイリアスを指定することによって、ホスト名を追加および設定できます。

ホスト解決の設定

「ホスト解決」ページで、ネットワーク管理者は、ホスト名または完全修飾ドメイン名 (FQDN) を IP アドレスに設定つまりマップすることができます。

メモ：ホスト解決エントリは、SMA/SRA 装置自体で自動的に作成されます。削除しないでください。

SMA/SRA 装置は、NetBIOS クライアントと WINS (Windows Internet Name Service) クライアントの両方として機能し、ローカル ネットワークのホスト名と、対応する IP アドレスを認識することができます。

ホスト名を IP アドレスに解決するには:

1. 「**ネットワーク > ホスト解決**」ページにナビゲートします。「**ネットワーク > ホスト解決**」ページが表示されます。
2. 「**ホスト名の追加**」を選択します。
3. 「**ホスト名の追加**」ウィンドウの「**IP アドレス**」フィールドに、ホスト名にマップする IP アドレスを入力します。
4. 「**ホスト名**」フィールドに、指定した IP アドレスにマップするホスト名を入力します。
5. 必要に応じて、「**エイリアス**」フィールドに、ホスト名のエイリアスである文字列を入力します。
6. 「**追加**」を選択します。これで、「**ホスト解決**」ページに、新しいホスト名が表示されます。
7. オプションで、「**ネットワーク > ホスト解決**」ページの「**自動的に追加されたホストの設定**」をオンにできます。このオプションを選択すると、IPv6 のような自動的に追加されたホスト エントリの編集や削除が可能になります。ホストの設定ミスにより期待しない結果になることがあるため、このオプションは推奨されません。

ネットワーク > ネットワーク オブジェクト

このセクションでは、「**ネットワーク > ネットワーク オブジェクト**」ページの概要と、このページで行う設定タスクについて説明します。

「ネットワーク > ネットワーク オブジェクト」の概要

「**ネットワーク > ネットワーク オブジェクト**」ページでは、オブジェクトと呼ばれるネットワーク リソースを追加および設定することができます。便宜上、サービスとそのサービスにマップされている IP アドレスの両方を含むエンティティを作成することができます。このエンティティをネットワーク オブジェクトといいます。これを使えば、ポリシーを適用するときにサービスを明示的な宛先 (ネットワーク オブジェクト) に指定することが簡単になります。サービスと IP アドレスの両方を指定する必要はありません。

IPv6 オブジェクト種別とアドレスを使用することで、IPv6 ネットワーク オブジェクトが作成できます。

「ネットワーク > ネットワーク オブジェクト」ページ

ネットワーク オブジェクトを設定するには、名前を指定し、以下のいずれかのサービスを選択します。

- ウェブ (HTTP)
- セキュア ウェブ (HTTPS)
- NetExtender & Mobile Connect
- ターミナル サービス (RDP)
- 仮想ネットワーク コンピューティング (VNC)
- ファイル転送プロトコル (FTP)
- Telnet、セキュア シェル バージョン 1 (SSHv1) 、セキュア シェル バージョン 2 (SSHv2)
- ファイル共有 (CIFS)
- Citrix Portal (ウェブ アクセス)

どのサービスについてもポートやポート範囲を使用できるため、ネットワーク オブジェクトにポート範囲(たとえば、80-443) やポート番号 (たとえば、80) を設定できます。この機能を使用すると、

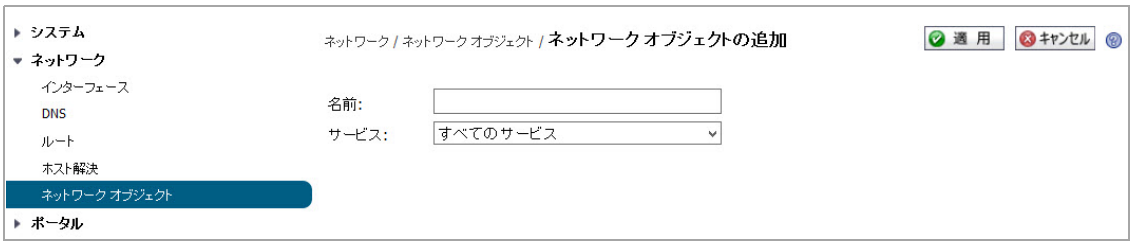
ポートベースのポリシーを作成できます。たとえば、すべて遮断するポリシーを作成し、ウェブサーバのポート 80 で HTTP トラフィックのみを受信することができます。

ネットワーク オブジェクトの追加

ネットワーク オブジェクトを追加するには:

1 「**ネットワーク > ネットワーク オブジェクト**」ページにナビゲートします。

2 「**ネットワーク オブジェクトの追加**」を選択します。「**ネットワーク オブジェクトの追加**」画面が表示されます。



3 「**名前**」フィールドに、作成するネットワーク オブジェクトの名前にする文字列を入力します。

> **メモ**：既存のネットワーク オブジェクトを編集するには、編集するオブジェクトの横にある「**設定**」を選択します。既存のネットワーク オブジェクトと同じ名前で新しいネットワーク オブジェクトを作成しても、既存のネットワーク オブジェクトが置き換えられることや変更されることはありません。

4 「**サービス**」リストを選択し、サービスのタイプを選択します。選択できるサービスは、ウェブ (HTTP)、セキュア ウェブ (HTTPS)、NetExtender、ターミナル サービス (RDP)、仮想ネットワーク コンピューティング (HTML5)、ファイル転送プロトコル、Telnet、Telnet (HTML5)、セキュア シェル バージョン 1 (SSHv1) 、セキュア シェル バージョン 2 (SSHv2) 、ファイル共有 (CIFS)、Citrix Portal です。

5 「**適用**」を選択します。「**ネットワーク オブジェクトの編集**」画面が表示され、ネットワーク オブジェクトの名前とそれに関連付けられたサービスが示されます。ネットワーク オブジェクトにマップさせるアドレスを追加することでオブジェクトを完成するには、ネットワーク オブジェクトの編集 (145 ページ) を参照してください。

ネットワーク オブジェクトの編集

ネットワーク オブジェクトを編集するには、以下の手順に従います。

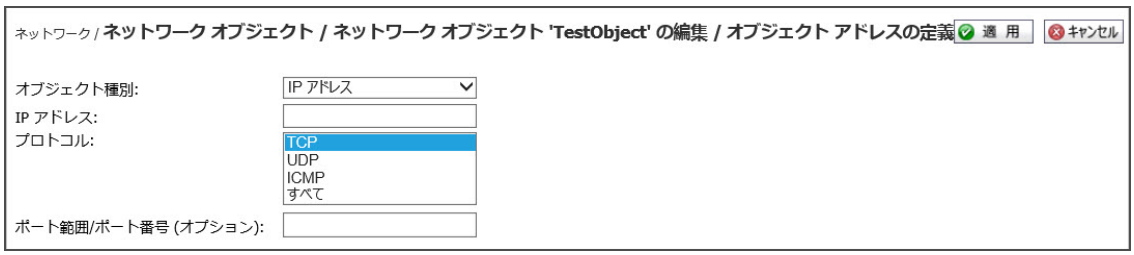
1 既存のネットワーク オブジェクトを編集するには、「**ネットワーク > ネットワーク オブジェクト**」ページにナビゲートして、設定アイコンを選択するか、「**未完了**」リンクを選択します。「**ネットワーク オブジェクトの編集**」画面が表示されます。

ネットワーク オブジェクトを作成した直後の場合は、「**適用**」の選択後すぐに「**ネットワーク オブジェクトの編集**」画面が表示されます。

「**ネットワーク オブジェクトの編集**」には、ネットワーク オブジェクト名とそれに関連付けられたサービスが示されます。また、ネットワーク オブジェクトにマップされた既存のアドレスを示すアドレス リストも表示されます。

2 サービスを変更するには、「**サービス**」ドロップダウン リストからサービスを選択し、「**サービスの更新**」を選択します。「ネットワーク オブジェクト」テーブルの「サービス」カラムに新しいサービスが表示されます。「**ネットワーク オブジェクトの編集**」ダイアログ ボックスは開いたままです。編集を終了する場合は、「**完了**」を選択します。

3 このネットワーク オブジェクトの「**オブジェクト種別**」と「**IP アドレス**」の値を追加または編集するには、「**追加**」をクリックします。「**オブジェクト アドレスの定義**」ページが表示されます。



4 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

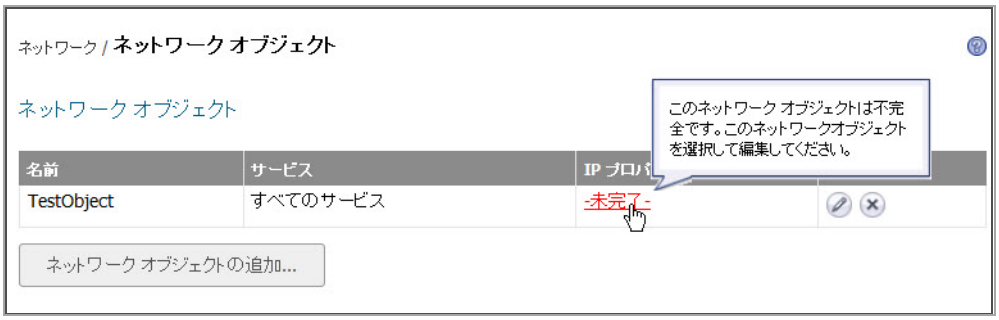
ⓘ **メモ**：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

5 「**適用**」を選択して、オブジェクト アドレスをネットワーク オブジェクトに追加します。

6 アドレスの追加が終了したら、オブジェクト アドレスの定義ページで「**完了**」を選択します。

7 「**ネットワーク > ネットワーク オブジェクト**」ページが表示され、「**ネットワーク オブジェクト**」のリストに新しいオブジェクトが表示されます。

8 オブジェクトが最低でも 1 つの IP アドレスかネットワーク範囲を用いて完全に定義されていない場合、「**未完了**」ステータスが表示されます。このネットワーク オブジェクトを再度編集するには、「**未完了**」リンクを選択するか、設定アイコンを選択してから、このネットワーク オブジェクトに対する種別とアドレスの値を追加するために「**追加**」を選択します。「**オブジェクト アドレスの定義**」ページが表示されます。



ⓘ **メモ**：未完了なネットワーク オブジェクトにはポリシーを作成できません。

オブジェクト アドレスの定義

1 「**オブジェクト アドレスの定義**」ページで、「**オブジェクト種別**」ドロップダウン リストを選択し、オブジェクトのタイプを選択します。オブジェクトには次の 4 つのタイプがあります。

- 「**IP アドレス**」- 単一の IP アドレス

- 「**IP ネットワーク**」- 開始アドレスとサブネット マスクで定義される IP アドレスの範囲
- 「**IPv6 アドレス**」- 単一の IPv6 アドレス
- 「**IPv6 ネットワーク**」- IPv6 アドレスの範囲

2 選択したオブジェクトのタイプに関する適切な情報を入力します。

- オブジェクトのタイプが **IP アドレス**の場合は、「**IP アドレス**」フィールドに IP アドレスを入力します。
- オブジェクトのタイプが **IP ネットワーク**の場合、「**ネットワーク アドレス**」フィールドに希望のネットワーク サブネットに存在する IP アドレスを入力し、「**サブネット マスク**」フィールドにサブネット マスクを入力します。オプションとして「**ポート範囲/ポート番号**」フィールドにポート範囲 80 ～ 443 の形式または特定のポート番号を入力します。
- オブジェクトのタイプが **IPv6 アドレス**の場合は、「**IPv6 アドレス**」フィールドに IP アドレスを入力します。
- オブジェクトのタイプが **IPv6 ネットワーク**の場合は、「**IPv6 ネットワークアドレス**」フィールドに希望のネットワーク サブネットに存在する IPv6 アドレスを入力し、「**接頭辞**」フィールドに接頭辞として使用するビット数を入力します。

3 アドレスを追加する操作が完了したら、「ネットワーク オブジェクトの編集」ダイアログ ボックスの「**完了**」を選択します。

5

ポータルの設定

このセクションでは、ウェブ ベースの Secure Mobile Access 管理インターフェースの「**ポータル**」ページで行う、ポータルの設定、ポータルの割り当て、認証ドメイン (RADIUS、LDAP、アクティブ ディレクトリなど) の定義などの設定タスクについて説明します。

トピック:

ポータル > ポータル

このセクションでは、「**ポータル > ポータル**」ページの概要と、このページで実行できる設定タスクについて説明します。

アプリケーション オフローダと「**ウェブ アプリケーションのオフロード**」の詳細については、ポータル > アプリケーション オフロード (164 ページ) を参照してください。

ポータル > ポータル の概要

「**ポータル > ポータル**」ページでは、Secure Mobile Access ポータルのログイン ページとホーム ページに個別のポータルを設定できます。

「ポータル > ポータル」ページ

ポータル設定

ポータル設定セクションでは、ポータル名、ポータル サイト タイトル、ポータル バナー タイトル、ログイン メッセージ、仮想ホスト/ドメイン名、およびポータル URL を指定することによって、個別のポータルを設定できます。また、ログイン時およびログアウト時に表示/ロードする項目を制御する個別ログイン オプション、キャッシュ制御用の HTTP メタ タグ、ActiveX ウェブ キャッシュ クリーナ、ログインの一意性、およびクライアント送信元の一意性を設定することもできます。

ポータルのホームページに関するその他の情報

通常の Secure Mobile Access 管理者の場合は、プレーン テキストのホームページ メッセージとネットワーク リソースへのリンクのリストがあれば十分です。ユーザ ポータルに他のコンテンツを表示する必要がある場合は、以下の情報を参照してください。

- ヒント/ヘルプのサイドバーを有効にすると、ワークスペース幅は 561 ピクセル
- ヒント/ヘルプのサイドバーを無効にすると、ワークスペース幅は 712 ピクセル
- IFRAME は使っていない
- ホームページの他のすべてのコンテンツの最後に表示する個別 HTML ファイルをアップロードできる「**ホームページ メッセージ**」フィールドに HTML タグと JavaScript を追加することもできる
- アップロードした HTML ファイルは他のコンテンツの後ろに表示されるので、このファイルに <head> タグや <body> タグを入れてはならない

ポータルの追加

管理者は、ポータルを個別化することで、ユーザが認証のために SMA/SRA 装置にリダイレクトされたときにユーザごとに個別の待ち受けページを表示できます。

ネットワーク管理者は、ポータルに個別のレイアウトを定義することができます。レイアウトの設定には、メニュー レイアウト、表示するポータル ページ、表示するポータル アプリケーションのアイコン、およびウェブ キャッシュ制御オプションが含まれます。

既定ポータルは **Virtual Office** ポータルです。別のポータルを追加したり、修正したりすることもできます。

ポータルを追加するには:

1 「**ポータル > ポータル**」ウィンドウにナビゲートし、「**ポータルの追加**」を選択します。「**ポータル設定**」ウィンドウが表示されます。

次の表に、「**一般**」セクションで設定できるフィールドの説明を示します。独自のポータルを設定するために必要な手順については、一般ポータル設定の設定 (151 ページ) を参照してください。

「一般」セクションのフィールド

フィールド	説明
ポータル名	このポータルを参照する場合に使うタイトル。内部参照専用で、ユーザには表示されない
ポータル サイト タイトル	ユーザがこのポータルにアクセスしたときにウェブ ブラウザのタイトル バーに表示されるタイトル
ポータル バナー タイトル	ポータル画面の一番上に表示されるウェルカム テキスト
ログイン メッセージ	ポータル ログイン ページで認証エリアの上に表示されるオプション テキスト
ポータル URL	この特定のポータルにアクセスする場合に使う URL
個別ログイン ページを表示する	このポータルの既定ログイン ページではなく個別のログイン ページを表示する
個別ログイン ページにログイン メッセージを表示する	ログイン メッセージ テキスト ボックスに指定されたメッセージを表示する
ポータル ログイン ページのドメイン リストを非表示にする	有効な場合、ログイン ページの「ドメイン」リスト ボックスをテキスト ボックスに置き換える。ユーザは正しいドメイン名を入力できます。このオプションは、ウェブからのポータル ログインに対してのみ有効です。
キャッシュ制御のための HTTP メタ タグを有効にする	すべての HTTP/HTTPS ページに HTTP メタ タグを埋め込み、リモート ユーザのブラウザのキャッシュにコンテンツが保管されないようにする
ActiveX ウェブ キャッシュ クリーナを有効にする	Secure Mobile Access セッションの終了後にすべてのセッションのコンテンツを消去する ActiveX コントロール (ブラウザのサポートが必要) をロードします。

「一般」セクションのフィールド (続き)

フィールド	説明
多重ログインを禁止する	多重ログインを禁止すると、アカウントは一度に 1 つのセッションにしか使用できない。優先される強制方式として、「**既存のセッションから自動的にログアウトします**」または「**既存のセッションからログアウトしたことを確認します**」を選択します。 禁止しないと、アカウントは同時に複数のセッションで使用できる
クライアント送信元の一意性の強制	強制すると、クライアント送信元の一意性により、ユーザが SonicWall Inc. クライアント (NetExtender、Mobile Connect、仮想アシストなど) を使用して接続するときに、同じクライアント送信元アドレスを使った 1 ユーザからの複数接続を防ぐことができます。これにより、ネットワークの予期しない中断の後にユーザが再接続を行うとき、ライセンスを複数消費することが防げます。
小さなロゴ	小さなロゴのリンクを指定する。推奨サイズは 128 x 128 です。
中程度のロゴ	中程度のロゴのリンクを指定する。推奨サイズは 270 x 270 です。
幅広のロゴ	幅広のロゴのリンクを指定する。推奨サイズは 558 x 270 です。
大きなロゴ	大きなロゴのリンクを指定する。推奨サイズは 558 x 558 です。
背景色	ライブ タイルの背景色を指定する。#0085C3 が既定で設定される
サイト名	ブックマークの表示名を指定する。ポータル名が既定で設定される

一般ポータル設定の設定

ポータルの主な設定オプションは、次の 2 つです。

- 既存のレイアウトを変更する
- 新しいポータルを設定する

「一般」セクションで新しいポータルの設定を行うには:

1 「**ポータル > ポータル**」ページを開きます。

2 「**ポータルの追加**」を選択するか、設定するポータルの横にある「設定」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。

3 「一般」セクションの「**ポータル名**」フィールドに、そのポータルを表すわかりやすい名前を入力します。この名前は、Secure Mobile Access ポータルの URL パスの一部になります。例えば、Secure Mobile Access ポータルが **https://vpn.company.com** でホストされていて、ポータル名を "sales" にした場合、ユーザは **https://vpn.company.com/portal/sales** でサブサイトにアクセスできます。

> **メモ**:「**ポータル名**」フィールドには、英数字、ハイフン (-)、および下線 (_) しか使用できません。これ以外の文字やスペースを入力すると、ポータル名は最初の英数字以外の文字の前で切り捨てられます。

4 「**ポータル サイト タイトル**」フィールドに、ウェブ ブラウザ ウィンドウのタイトルを入力します。

5 ユーザがポータルにログインする前にバナー メッセージを表示するには、「**ポータル バナー タイトル**」フィールドにバナー タイトルのテキストを入力します。

6 「**ログイン メッセージ**」フィールドに HTML 準拠メッセージを入力するか、既定で入力されているメッセージを編集します。このメッセージは、個別のログイン ページに表示されます。

7 「**ポータル URL**」フィールドには、SMA/SRA 装置のネットワーク アドレスとポータル名に基づいて値が自動的に設定されます。

8 個別のロゴ、メッセージ、およびタイトル情報をログイン ページに表示するには、「**個別ログイン ページを表示する**」をオンにします。

> **メモ**：個別のロゴは、既存のポータルにのみ追加できます。個別のロゴを新しいポータルに追加するには、最初に一般ポータル設定を完了してから、個別ポータル ロゴの追加 (162 ページ) の手順に従ってロゴを追加します。

9 「**キャッシュ制御のための HTTP メタ タグを有効にする**」をオンにして、このポータルに HTTP メタ タグ キャッシュ制御ディレクティブを適用します。キャッシュ制御ディレクティブには、次のものが含まれます。

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
```

これらのディレクティブを適用することで、SMA ポータル ページとその他のウェブ コンテンツのキャッシングを防ぐことができます。

> **メモ**：セキュリティ上の理由に加え、古いウェブ ページやデータがユーザのウェブ ブラウザのキャッシュに保管されることを防ぐために、HTTP メタ タグを有効にすることを強くお勧めします。

10 「**ActiveX ウェブ キャッシュ クリーナを有効にする**」をオンにして、ユーザが SMA/SRA 装置にログインしたときに、ActiveX キャッシュ コントロールがロードされるようにします。ウェブ キャッシュ クリーナにより、ユーザがログアウトしたとき、またはウェブ ブラウザ ウィンドウを閉じたときに、すべてのセッションの一時インターネット ファイル、Cookie、およびブラウザ履歴を削除することを求めるプロンプトが表示されます。ActiveX をサポートしていないウェブ ブラウザでは、ActiveX ウェブ キャッシュ コントロールは無視されます。

11 多重ログインの禁止 (152 ページ) を参照してください。

12 クライアント送信元の一意性の強制 (153 ページ) を参照してください。

13 ライブ タイルで使用する**小さな/中程度の/幅広の/大きな**ロゴのリンクを指定します。

14 ライブ タイルの**背景色**を指定します。値を指定しない場合、既定色は #0085C3 です。

15 ライブ タイルに対して表示される**サイト名**を指定します。値を指定しない場合、既定値はポータル名です。

多重ログインの禁止

多重ログインを禁止すると、アカウントは一度に 1 つのセッションにしか使用できません。禁止しない場合は、アカウントは同時に複数のセッションで使用できます。

多重ログインを禁止するには:

1 「**ポータル > ポータル**」にナビゲートします。

2 既存のポータルの場合は、設定するポータルの横にある設定アイコンを選択します。新しいポータルの場合は、「**ポータルの追加**」を選択します。

3 「**多重ログインを禁止する**」をオンにします。

4 「**適用**」を選択します。

クライアント送信元の一意性の強制

クライアント送信元の一意性を強制すると、SonicWall Inc. クライアント (NetExtender、Mobile Connect、仮想アシストなど) を使用して接続するときに同じクライアント送信元アドレスを使った 1 ユーザからの複数接続を防ぐことができます。これにより、ネットワークの予期しない中断の後にユーザが再接続を行うとき、ライセンスを複数消費することが防げます。

例えば、信頼性の低いネットワーク上のユーザがネットワークの問題により切断されたとします。もし多重ログインの禁止が有効になっていない場合、この種の切断に対しては、タイムアウト値に到達するまで装置上のユーザ セッションはアクティブなままです。ユーザは再接続して、タイムアウトで切断される前に潜在的により多くのライセンスを消費する可能性がある状態で 2 個目のライセンスを消費します。

クライアント送信元の一意性を強制するには:

1 「**ポータル > ポータル**」にナビゲートします。

2 既存のポータルの場合は、設定するポータルの横にある設定アイコンを選択します。新しいポータルの場合は、「**ポータルの追加**」を選択します。

3 「**クライアント送信元の一意性の強制**」をオンにします。

4 「**適用**」を選択します。

ログイン スケジュールの設定

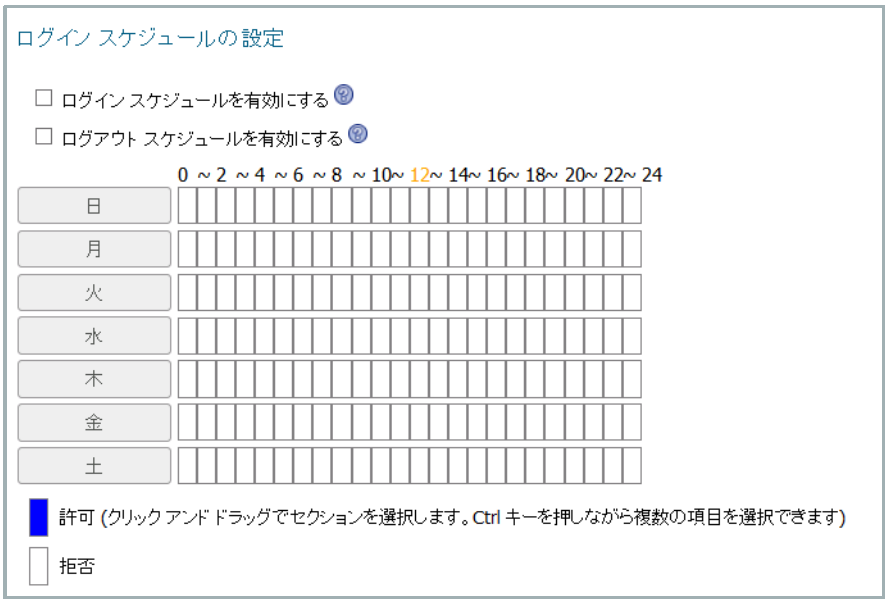
「ログイン スケジュール」セクションでは、時間を指定してポータルへのアクセスを制限できます。

ログイン スケジュールを有効にするには:

1 「**ポータル > ポータル**」にナビゲートします。

2 設定する既存のポータルを選択します。

3 「**ログイン スケジュール**」セクションに移動します。ログイン スケジュールが表示されます。



4 「**ログイン スケジュールを有効にする**」をオンにします。

5 1 日のうちのアクセスを許可または禁止する時間を選択することにより、ログイン スケジュールを設定します。複数の項目を選択するには、Ctrl キーを押しながら選択します。「**曜日**」を選択して、1 日全体を選択することもできます。

6 「**適用**」を選択して、ログイン スケジュールの変更を保存します。

ホームページの設定

ホームページは、Secure Mobile Access 装置ポータルのオプションの開始ページです。ホームページを設定することで、モバイル ユーザがポータルにログインしたときに表示する個別ページを作成できます。ホームページは個別化できるので、リモート アクセス手順、サポート情報、技術に関する問い 合わせ先情報、Secure Mobile Access 関連の更新などをリモート ユーザに伝える理想的な方法となります。

ホームページは、アクセスに制限があるユーザの開始ページとして最適です。モバイル ユーザやビジネス パートナがアクセスを許可されているファイルやウェブ URL が限られている場合、ホームページを設定すれば、対象ユーザにはそれらの関連リンクしか表示されません。

ページのタイトルを編集したり、ページの一番上に表示するホーム ページ メッセージを作成したり、ユーザごとに該当するすべてのブックマーク (ユーザ、グループ、およびグローバル) を表示したり、必要に応じて HTML ファイルをアップロードしたりできます。

参考資料:

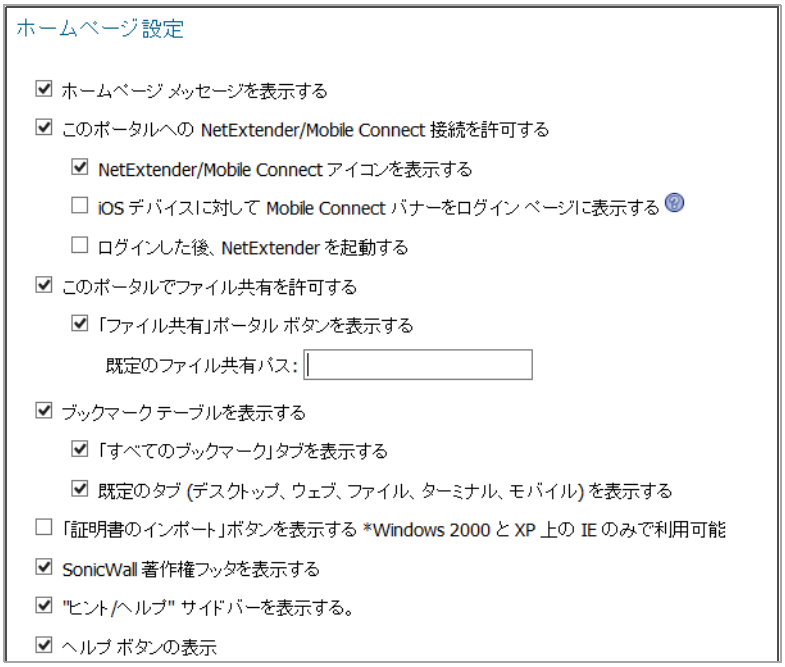
- ユーザ ポータルでの NetExtender の自動起動 (156 ページ)
- “既定でアプレットを使用”するファイル共有 (157 ページ)

ホームページを設定するには:

1 「**ポータル > ポータル**」ページを開きます。

2 「**ポータルの追加**」を選択するか、設定するポータルの横にある「**設定**」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。

3 「**ホームページ**」セクションに移動します。



次の表に、「ホームページ」セクションで設定できるオプションの説明を示します。

「ホームページ」セクションのフィールド

フィールド	説明
ホームページ メッセージを表示する	ユーザが SMA/SRA 装置に対する認証に成功した後で個別のホームページ メッセージを表示します。
このポータルへの NetExtender/Mobile Connect 接続を許可する	選択した場合は、その下にある 2 つのチェックボックス オプションが利用できます。選択しない場合、NetExtender と Mobile Connect はこのポータルで利用できません。
NetExtender/Mobile Connect アイコンを表示する	NetExtender または Mobile Connect のアイコンを表示し、クライアントレスの NetExtender 仮想アダプタ、またはモバイル機器用の Mobile Connect アプリケーションを、ユーザがインストールして起動できるようにします。
iOS デバイスに対して Mobile Connect バナーをログインページに表示する	iOS 6 以降を搭載するデバイスに対し、ログイン ページに Mobile Connect バナーを表示します。
ログインした後、NetExtender を起動する	ユーザが SMA/SRA 装置に対する認証に成功した後で NetExtender を自動的に起動します。ユーザ ポータルでの NetExtender の自動起動 (156 ページ) を参照してください。
このポータルでファイル共有を許可する	選択した場合は、その下にある 2 つのチェックボックス オプションが利用できます。選択しない場合、ファイル共有はこのポータルで利用できません。
「ファイル共有」ポータル ボタンを表示する	ファイル共有 (Windows CIFS/SMB) ウェブ インターフェースへリンクするボタンを、ドメイン許可に従って提供します。“既定でアプレットを使用”するファイル共有 (157 ページ) を参照してください。
ポータル ボタンにアプレットを使用する	Java ファイル共有アプレットを有効にして、ドラッグ アンド ドロップ、複数ファイル選択、コンテキスト依存の選択操作などの簡単で強力なファイル操作インターフェースを利用できるようにします。
既定のファイル共有パス	ポータル上でファイル共有を許可する場合の具体的なファイル共有パスを指定します。何も指定されていない場合、ファイル共有はすべての利用可能なドメインを検索するためのリンクをユーザに提供します。また、すべての利用可能なファイル共有ブックマークを一覧表示し、ユーザが起動できるようにします。
ブックマーク テーブルを表示する	選択した場合は、その下にある 2 つのチェックボックス オプションが利用できます。選択しない場合、ブックマークはこのポータルで利用できません。
「すべてのブックマーク」タブを表示する	管理者によって提供されたブックマークを含むタブを表示し、ユーザがネットワーク リソースへの独自のブックマークを定義できるようにします。
既定のタブ (デスクトップ、ウェブ、ファイル、ターミナル)、モバイル を表示する	既定のブックマーク タブを表示します。
「証明書のインポート」ボタンを表示する	SSL セキュリティ証明書を永続的にインポートできるボタンを表示します。
SonicWall Inc. 著作権フッタを表示する	ポータルに SonicWall Inc. 著作権フッタを表示します。オフにすると、フッタは表示されません。

「ホームページ」セクションのフィールド (続き)

フィールド	説明
〝ヒント/ヘルプ〟サイドバーを表示する	ポータルにヒントとヘルプのリンクを持つサイドバーを表示します。「一般」タブで「**従来の外観と操作性**」をオンにした場合、このオプションは使用できません。
ヘルプ ボタンの表示	「**ヘルプ**」ボタンを表示します。
ヘルプ ページ URL	ヘルプ ページの URL を指定します。既定の SonicWall Inc. ヘルプ ページを使用する場合は、このフィールドを空白のままにします。
オプション ボタンを表示する	選択すると、「**オプション**」ボタンが表示されます。
ホームページ メッセージ	ユーザ認証の成功後にホームページ上に表示できるオプション テキストです。

メモ：

- ファイル共有を作成するときは、DFS (Distributed File System) サーバをウィンドウズ ドメイン ルート システムに設定しないでください。ドメイン ルートはドメイン内の Windows コンピュータへのアクセスのみを提供するので、DFS サーバをドメイン ルートに設定すると、他のドメインから DFS ファイル共有にアクセスできません。SMA/SRA 装置は、ドメイン メンバではないので、DFS ファイル共有に接続できません。スタンドアロン ルート上の DFS ファイル共有には、Microsoft の制限は適用されません。
- ActiveX アプリケーションの中には、ActiveX ターミナル サービス RDP クライアントなど、信頼できるルート CA からの証明書でサーバに接続しなければ機能しないものもあります。SMA/SRA 装置に付属のテスト用 SSL 証明書を使っている場合、「**自己署名証明書インポートのリンクを表示する**」をオンにすると、Windows ユーザが自己署名証明書を簡単にインポートできるようになります。
- Verisign、Thawte などの信頼できるルート CA からの有効な SSL 証明書をアップロードすることを強くお勧めします。有効な SSL 証明書がある場合は、「**自己署名証明書インポートのリンクを表示する**」をオンにしないでください。

4 「**適用**」を選択してホームページのコンテンツを更新します。

ユーザ ポータルでの NetExtender の自動起動

ユーザがユーザ ポータルにログインしたときに自動的に起動されるように NetExtender を設定できます。また、Virtual Office ポータル に NetExtender を表示するかどうかも設定できます。

NetExtender ポータル オプションを設定するには:

1 「**ポータル > ポータル**」にナビゲートします

2 「**ポータルの追加**」を選択するか、設定するポータルの横にある「**設定**」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。

3 「**ホームページ**」セクションを選択します。

4 ユーザがこのポータルから NetExtender にアクセスできないようにするには、「**このポータルへの NetExtender 接続を許可する**」をオフにします。Mobile Connect は接続時に NetExtender クライアントとして動作するため、このチェックボックスをオフにすると、このポータル上の Mobile Connect ユーザもアクセスできなくなります。

5 ユーザがポータルにログインしたときに NetExtender を自動的に起動するには、「**ログインした後、NetExtender を起動する**」をオンにします。

6 「**適用**」を選択します。

“既定でアプレットを使用”するファイル共有

ファイル共有 Java アプレット オプションを使うと、標準の HTML ベースのファイル共有では利用できない以下の機能がユーザに提供されます。

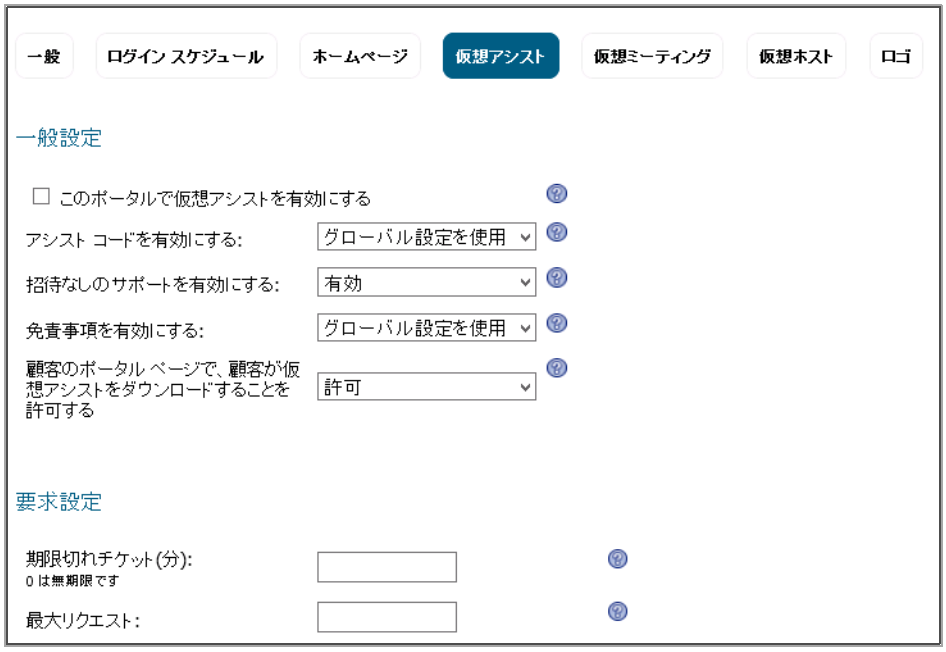
- 既存のファイルの上書き
- ディレクトリのアップロード
- ドラッグ アンド ドロップ機能
- 複数ファイル選択
- 状況に依存する選択機能
- 並べ替え可能なファイル リスト
- パス入力による直接フォルダ移動機能
- ドロップダウン履歴メニューと進む/戻るボタン
- フォルダ サイズを表示するプロパティ ウィンドウ

このポータルでファイル共有 Java アプレットを使用するには:

1. 「**ポータル > ポータル**」にナビゲートします。
2. 「**ポータルの追加**」を選択するか、設定するポータルの横にある「**設定**」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。
3. 「**ホームページ**」セクションを選択します。
4. 「**「ファイル共有」ポータル ボタンを表示する**」をオンにします。
5. 「**ポータル ボタンにアプレットを使用する**」をオンにします。
6. 「**適用**」ボタンを選択して、変更内容を保存します。

ポータルごとの仮想アシスト設定の設定

管理者はポータルごとにセキュア仮想アシストを有効にできます。



「ポータルの追加」画面の「仮想アシスト」セクションには、グローバルな「**セキュア仮想アシスト > 設定**」ページとほぼ同じ設定オプションがこのポータル用に表示されます。

ポータルに対する仮想アシスト設定を行うには:

1 「**ポータル > ポータル**」にナビゲートします。

2 「**ポータルの追加**」を選択するか、設定するポータルの横にある「**設定**」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。

3 「**仮想アシスト**」セクションに移動します。

4 このポータルで仮想アシストを有効にするには、「**このポータルで仮想アシストを有効にする**」をオンにします。

5 「**技術者ボタンを表示する**」をオンにします。このチェックボックスがオンになっていないと、「**仮想アシスト**」が表示されず、技術者はダウンロードしたクライアントを通して直接ログインする必要があります。

6 「**「サポートの要求」ボタンを表示する**」をオンにして、ユーザがポータルからアシストを要求できるようにします。

7 このポータルへのセキュア仮想アクセス接続を許可するには、「**仮想アクセス モードを有効にする**」をオンにします。これは、セキュア仮想アクセスを実行するポータル単位で有効にする必要があります。このチェックボックスがオンになっていると、ポータル上に対応するリンクを表示するための「**仮想アクセスの設定リンクを表示する**」をオンに設定できます。セキュア仮想アクセスの機能性の詳細情報については、セキュア仮想アクセス用のシステムの有効化 (67 ページ) を参照してください。

8 「**セキュア仮想アシストをインストールせずに起動する**」機能を使用すると、ユーザは仮想アシストを、クライアント マシンにインストールすることなく起動できます。この機能はグローバルまたはポータルごとに有効化できます。ドロップダウン リストで次のいずれかを選択します。

- このポータルにグローバル設定を適用するには、「**グローバル設定を使用**」を選択します。
- グローバル設定に関係なく、このポータルにおいて仮想アシストをインストールせずにウェブから起動するには、「**有効**」を選択します。
- グローバル設定に関係なく、このポータルにおいて仮想アシストをウェブからアクセスする際にインストールするには、「**無効**」を選択します。

9 「**LAN 上の顧客の PC を起動する**」機能を使用すると、技術者は仮想アシストを実行する LAN 上のクライアントを起動できます。クライアント PC は、電源がオフの場合も、スリープ状態の場合も、休止状態の場合も起動できます。この機能はグローバルまたはポータルごとに有効化できます。

- このポータルにグローバル設定を適用するには、「**グローバル設定を使用**」を選択します。
- グローバル設定に関係なく、この機能を有効にするには、「**有効**」を選択します。
- グローバル設定に関係なく、この機能を無効にするには、「**無効**」を選択します。

> **メモ**：クライアント起動を使用するには、この機能をクライアント マシン上で設定する必要があります。『*Secure Mobile Access ユーザ ガイド*』を参照してください。

10 「**サポート セッション数の制限**」フィールドに、このポータルで許可するアクティブなサポート セッションの数を入力します。制限を設けない場合は、0 を入力します。

11 「**アシスト コードを有効にする**」をオンにすると、アシストを要求する前に指定されたコードを入力することがユーザに求められます。このチェックボックスをオンにすると、「**アシスト コード**」フィールドが表示されるので、そこにユーザが入力するコードを指定します。

12 「仮想アシスト」セクションの他の設定については、セキュア仮想アシスト > 設定 (291 ページ) を参照してください。

13 ページの各セクションを展開して、関連するオプションを設定します。

14 「**適用**」ボタンを選択して、変更内容を保存します。

仮想ミーティングの設定

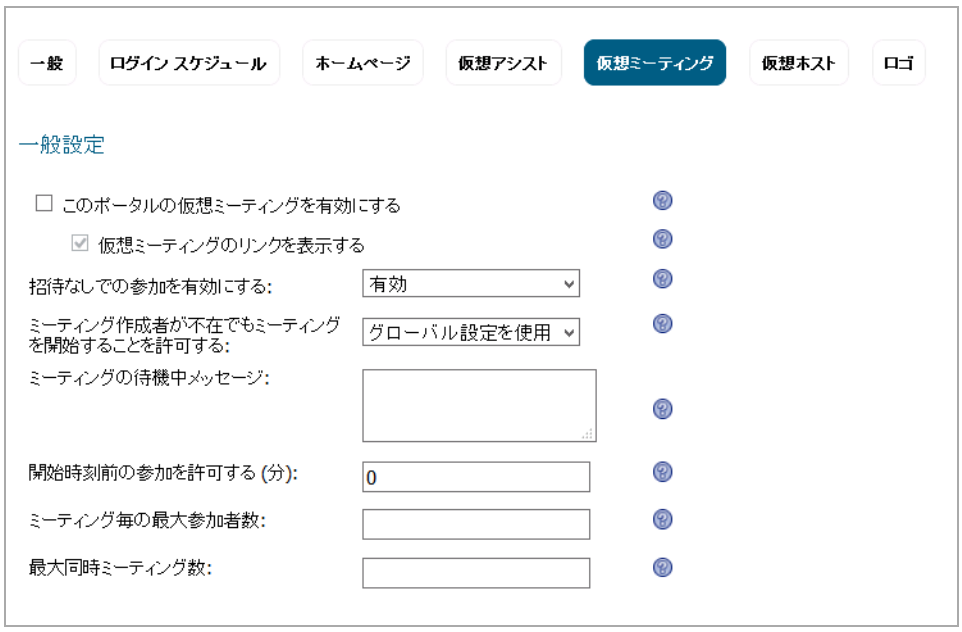
「仮想ミーティング」セクションでは、ポータルの仮想ミーティングの設定を行うことができます。このタブでは、「一般設定」セクションと「通知設定」セクションの両方を設定できます。

仮想ミーティングの設定を行うには:

1 「**ポータル > ポータル**」にナビゲートします。

2 「**ポータルの追加**」を選択するか、設定するポータルの横にある「**設定**」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。

3 「**仮想ミーティング**」セクションに移動します。



4 「**一般設定**」セクションに移動します。

5 このポータルからログインするユーザに対して仮想ミーティングを制御できるようにするには、「**このポータルの仮想ミーティングを有効にする**」をオンにします。

「このポータルの仮想ミーティングを有効にする」オプションが有効な状態で、「**仮想ミーティングのリンクを表示する**」をオンにすると、ダウンロードまたはインストール用の仮想ミーティング アイコンが表示されます。

6 責任者からの招待なしで参加者がミーティングに参加できるようにするには、「**招待なしでの参加を有効にする**」フィールドで「グローバル設定を使用する」、「有効」、または「無効」を選択します。このオプションが無効な場合、参加者はミーティング作成者からの招待によってのみミーティングに参加できます。

7 ミーティング開始時に責任者が不在の場合、参加者がミーティング責任者の役割を果たせるようにするには、「**ミーティング作成者が不在でもミーティングを開始することを許可する**」フィールドで「グローバル設定を使用する」、「有効」、または「無効」を選択します。

8 ミーティングが始まっていないときに表示する既定のメッセージを「**ミーティングの待機中メッセージ**」フィールドに作成します。このフィールドが空欄のままの場合、仮想ミーティングではこのオプションに対するグローバル設定が使用されます。

9 「開始時刻前の参加を許可する」フィールドに値 (分単位) を設定します。これは、ミーティング開始予定時刻の何分前に参加者がミーティングに参加できるかを示す数値です。参加者がミーティング ロビーに入ると、ライセンスは使用中と見なされます。ミーティングに参加する時間を無制限に許可するには、このフィールドを 0 に設定してください。このフィールドが空欄のままの場合、仮想ミーティングではこのオプションに対するグローバル設定が使用されます。

10 「**ミーティング毎の最大参加者数**」フィールドに、ミーティングの最大同時システム数を設定します。ミーティング参加者を無制限に許可するには、このフィールドを 0 に設定してください。このフィールドが空欄のままの場合、仮想ミーティングではこのオプションに対するグローバル設定が使用されます。

11 「**最大同時ミーティング数**」フィールドに、この装置の最大同時ミーティング数を設定します。ミーティング数を無制限に許可するには、このフィールドを 0 に設定してください。このフィールドが空欄のままの場合、仮想ミーティングではこのオプションに対するグローバル設定が使用されます。

12 続いて「**通知設定**」セクションに移動します。

13 「**招待の件名**」フィールドに、仮想ミーティングへの電子メールの招待状の件名を指定します。このフィールドには以下の変数を使用できます。

- %COORDINATOR% - 責任者名
- %MEETINGNAME%- ミーティング名
- %MEETINGCODE% - ミーティング コード
- %STARTTIME% - ミーティングの開始日時
- %ENDTIME% - ミーティングの終了日時
- %MEETINGDESCRIPTION% - ミーティングの説明

変数は大文字と小文字が区別されます。このフィールドが空欄のままの場合、仮想ミーティングではこのオプションに対するグローバル設定が使用されます。

14 「**招待メッセージ**」フィールドに、仮想ミーティングへの招待状の本文を指定します。このフィールドには以下の変数を使用できます。

- %COORDINATOR% - 責任者名
- %MEETINGNAME%- ミーティング名
- %MEETINGCODE% - ミーティング コード
- %STARTTIME% - ミーティングの開始日時
- %ENDTIME% - ミーティングの終了日時
- %MEETINGDESCRIPTION% - ミーティングの説明

変数は大文字と小文字が区別されます。このフィールドが空欄のままの場合、仮想ミーティングではこのオプションに対するグローバル設定が使用されます。

15 「**適用**」ボタンを選択して、変更内容を保存します。

仮想ホストの設定

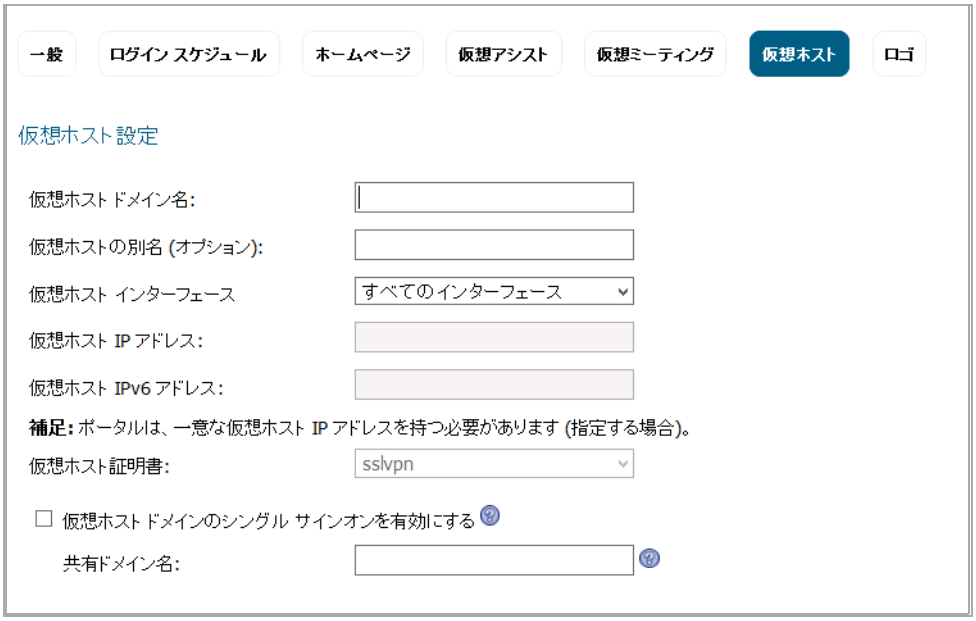
仮想ホストを作成すると、ユーザは既定 URL とは異なる別のホスト名を使ってログインできるようになります。例えば、販売担当者は、管理用の既定ドメイン〈**https://vpn.company.com**〉ではなく、〈**https://sales.company.com**〉にアクセスできます。仮想ホスト名を定義しても、ポータル URL (例えば、**https://vpn.company.com/portal/sales**) は存在します。仮想ホスト名を作成することで、管理者はユーザ グループごとに別個のログイン URL を提供できます。

仮想ホスト ドメイン名を作成するには:

1 「**ポータル > ポータル**」にナビゲートします。

2 「**ポータルの追加**」を選択するか、設定するポータルの横にある「**設定**」を選択します。「**ポータルの追加**」または「**ポータルの編集**」画面が表示されます。

3 「**仮想ホスト**」セクションに移動します。



4 ホスト名を「**仮想ホスト ドメイン名**」フィールドに入力します。例えば、**sales.company.com** と入力します。このフィールドはオプションです。

「**仮想ホスト ドメイン名**」フィールドには、英数字、ハイフン (-)、および下線 (_) しか使用できません。

5 IP ベースの仮想ホスティングを使う場合は、ポータルに固有の「**仮想ホスト インターフェース**」を選択します。

名前ベースの仮想ホスト (1 つの IP アドレスに対して複数のホスト名が存在する仮想ホスト形式) を使用している場合は、「仮想ホスト インターフェース」から「**すべてのインターフェース**」を選択します。

6 ポータルに固有の仮想ホスト インターフェースを選択した場合は、使用する IP アドレスを「**仮想ホスト IP アドレス**」フィールドに入力します。ユーザは、この IP アドレスを使って仮想オフィス ポータルにアクセスすることになります。

> ⓘ **メモ**：仮想ホスト名とドメイン名を SMA/SRA 装置の外部 IP アドレスに解決できるように、外部 DNS サーバにエントリを追加してください。

7 ポータルに固有の仮想ホスト インターフェースを選択した場合は、IPv6 アドレスを「**仮想ホスト IPv6 アドレス**」フィールドに指定できます。このアドレスを使って仮想ホストにアクセスできます。IPv6 アドレスは 10 進数または 16 進数を使って次の形式で入力します。

2001::A987:2:3:4321

8 このサブドメインに個別のセキュリティ証明書を使用する予定であれば、それに対応するポート インターフェース アドレスを「**仮想ホスト証明書**」リストから選択します。

仮想ホスト ドメイン名ごとに証明書を用意しない場合 (つまり *.domain SSL 証明書を購入した場合) は、ユーザが Secure Mobile Access 仮想オフィス ポータルにログインしたときに**証明書ホ**

スト名の不一致警告が表示されることがあります。証明書ホスト名の不一致の影響を受けるのはログイン ページ、NetExtender、およびセキュア仮想アクセス/アシスト/ミーティングで、その他の Secure Mobile Access クライアント アプリケーションはホスト名不一致の影響を受けません。

ユーザに対して単一ポイントのアクセスを実現するには、アプリケーション オフロード ポータルに対する外部ウェブ サイト ブックマークを設定して、クロス ドメイン SSO を有効にするために「**仮想ホスト ドメインのシングル サインオンを有効にする**」をオンにします。クロス ドメイン SSO は、同一の共有ドメイン内のすべてのポータルで認証情報を共有します。「**仮想ホスト ドメインのシングル サインオンを有効にする** 」は、自動的に共有ドメイン名を「仮想ホスト ドメイン名」の 1 階層上から設定し、「**共有ドメイン名**」フィールド内に表示します。例えば、仮想ホスト ドメイン名が webmail.example.com の場合、共有ドメイン名は example.com です。

メモ : 以前のリリースでは、ユーザは 2 回ログインする必要がありました - 1 回目は通常のポータルに対してで、もう 1 回は外部ウェブサイト ブックマークのリダイレクト後のアプリケーション オフローダ ポータルに対してです。クロス ドメイン SSO 機能により、ユーザはメイン ポータルにログインした後に、同じ仮想ホストドメインを共有しているアプリケーション オフローダ ポータルやウェブ サイトに自動的にログインすることが可能になります。

9 「**SSL/TLS の詳細設定**」セクションの「前方秘匿性を強制する」フィールドで、「**グローバル設定を使用**」、「**有効**」、または「**無効**」を選択できます。このオプションを有効にすると、秘密鍵が盗まれるようなことがあった場合でも、現在の情報の機密性を守ることができます。前方秘匿性をサポートしないブラウザは、SMA/SRA 装置に接続できない可能性があります。また、クライアント ブラウザがサポートする暗号化によっては、この機能のパフォーマンスが低下する可能性もあります。

10 **プロキシ接続のバックエンド SSL サーバ証明書を確認** - このオプションを有効にすると、バックエンド SSL/TLS サーバ証明書が信頼できなければ、接続が破棄されます。確認の深度は 10 です。このオプションを有効にすると、警告レベルのログ メッセージも生成されます。

11 「**プロキシ接続に対する SSL/TLS バージョンの強制**」を有効にして、仮想ホストとバックエンド サーバが通信できるようにします。

個別ポータル ロゴの追加

個別ロゴ設定セクションでは、個別ロゴをアップロードし、これを既定のSonicWall Inc.ロゴと切り替えることができます。このセクションでは、個別ポータル ファビコンもアップロードできます。個別ロゴまたは個別ファビコンをアップロードするためには、ポータルを追加しておかなければなりません。「ポータルの追加」画面の「ロゴ」セクションには、個別ロゴまたは個別ファビコンをアップロードするためのオプションがありません。

メモ：ロゴまたはファビコンは、OWA アクセスに合わせてカスタマイズすることもできます。

個別ポータル ロゴを追加するには:

1 「**ポータル > ポータル**」に移動し、独自のロゴを追加する既存のポータルの横にある「**設定**」を選択します。「**ポータルの編集**」画面が表示されます。

2 「**ロゴ**」セクションに移動します。

3 「**ロゴのアップロード**」フィールドの横にある「**Browse**」をクリックします。ファイル ブラウザのウィンドウが表示されます。

4 適切なサイズで作成された GIF 形式のロゴをファイル ブラウザで選択し、「**開く**」を選択します。

> ⓘ **メモ**：個別のロゴは GIF 形式でなければなりません。新式のポータルでは、155x68 ピクセルというサイズ制限があります。これより大きいものは、ページ上のロゴ スペースに収まるように切り詰められます。従来のポータルでは、最適な表示結果を得るため、背景が透明か薄い色になっているロゴをインポートしてください。推奨サイズ (必須ではない) は 155x36 ピクセルです。

5 「**背景**」ドロップダウン リストから「**暗い**」または「**明るい**」を選択します。ポータル ページの中でロゴが目立つように、うまく濃淡を選んでください。

6 「**ロゴの更新**」を選択すると、そのロゴが SMA/SRA 装置に転送されます。

7 「**既定のロゴ**」を選択すると、既定の SonicWall Inc. ロゴに戻ります。

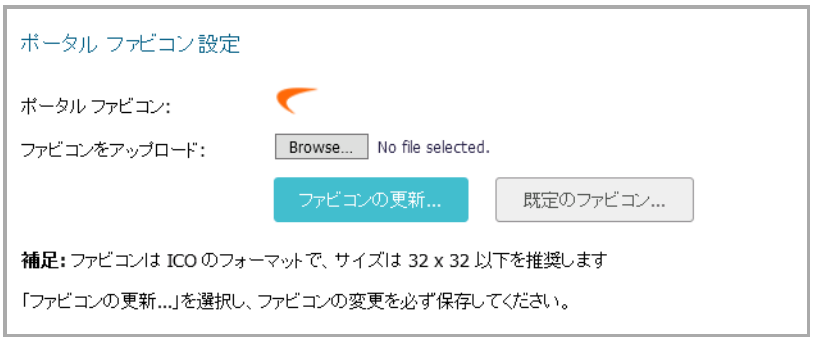
8 「**適用**」ボタンを選択して、変更内容を保存します。

個別ファビコンを追加するには:

1 「**ポータル > ポータル**」に移動し、個別ファビコンを追加する既存のポータルの横にある「**設定**」を選択します。「**ポータルの編集**」画面が表示されます。

2 「**ロゴ**」セクションに移動します。「**ポータル ファビコン設定**」セクションに移動します。

3 「**ファビコンをアップロード**」フィールドの横にある「**Browse**」をクリックします。ファイル ブラウザのウィンドウが表示されます。



4 適切なサイズで作成された ICO 形式のファビコンをファイル ブラウザで選択し、「**開く**」を選択します。

メモ：個別ファビコンは ICO 形式でなければなりません。個別ファビコンのサイズは最大 32 x 32 ピクセルにしてください。

5 「**ファビコンの更新**」を選択すると、そのファビコンが SMA/SRA 装置に転送されます。

6 「**既定のファビコン**」を選択すると、既定の SonicWall Inc. ファビコンに戻ります。

7 ポータルの認証制御が無効の場合、「**オフロード サーバのファビコンを再利用**」チェックボックスが表示されます。このオプションを有効にすると、バックエンド サーバのファビコンをクライアントのブラウザに表示できます。

8 「**適用**」ボタンを選択して、変更内容を保存します。

メモ：ファビコンの動作は、ファビコンがキャッシュされている場合は特に、ブラウザごとに異なる可能性があります。ファビコンを正しく表示するために、キャッシュの更新または消去が必要な場合があります。

ポータル > アプリケーション オフロード

Secure Mobile Access 管理インターフェースの「**ポータル > アプリケーション オフローダ**」ページでは、「**ポータル > ポータル**」ページから利用できるアプリケーション オフローダ機能の概要が説明されています。設定はこのページでは行えません。

このページのスクリーンショットのいずれかを選択すると、「**ポータル > ポータル**」ページに移動します。この移動先のページでは、「**ウェブ アプリケーションのオフロード**」を選択して、オフロードされたアプリケーションを設定できます。

以下のセクションを参照してください。

- アプリケーション オフロードの概要 (165 ページ)
- HTTP/HTTPS アプリケーション オフロード ポータルの設定 (166 ページ)
- オフロード ポータル ウィザードを使った設定 (170 ページ)

アプリケーション オフロードの概要

アプリケーション オフロードは、内部および公開されているホストのウェブ アプリケーションへの安全なアクセスを提供します。アプリケーション オフロード ホストは、バックエンド ウェブ アプリケーションのプロキシとして機能する仮想ホストを持つ専用のポータルとして作成されます。

HTTP(S) ブックマークと異なり、オフロードされたアプリケーションへのアクセスはリモート ユーザに制限されません。管理者は特定のユーザやグループに対して強力な認証とアクセス ポリシーを強制することができます。例えば、組織では一定のゲスト ユーザは Outlook Web Access (OWA) へのアクセスに二段階認証やクライアント証明書認証が必要なこともありますが、OWA パブリック フォルダへのアクセスは許されません。認証が有効なら、オフロードされたホストにはワンタイム パスワード、二段階認証、クライアント証明書認証、シングル サイン オンといった SonicWall の高度な認証機能を積層することができます。

このポータルは、適切な Secure Mobile Access ドメインを持つ仮想ホストとして設定しなければなりません。このようなオフロードされたホストに対しては、認証とアクセス ポリシーの強制を無効にすることが可能です。

ウェブ トランザクションは、ログを確認することで集中監視することができます。さらに、ウェブ アプリケーション ファイアウォールによって、クロスサイト スクリプティングや SQL インジェクションなどの予期せぬ侵入からこれらのホストを保護することができます。

プロキシされたページ内の URL は HTTP ブックマークや HTTPS ブックマークで使われる方法で書き換えられないので、オフロードされたウェブ アプリケーションへのアクセスはシームレスに行われます。

ウェブ アプリケーションを Secure Mobile Access の HTTP(S) ブックマークとして設定するのに比べて、オフロードされたウェブ アプリケーションには次の利点があります。

- URL 書き換えが必要ないので、スループットが著しく向上する。
- 元のウェブ アプリケーションの機能がほぼ完全に維持される。それに対し、HTTP(S) ブックマークは最大努力型のソリューションにすぎない。
- アプリケーション オフロードは Secure Mobile Access のセキュリティ機能を公開ホストのウェブサイトに拡張する。

アプリケーション オフロードは次のシナリオのいずれにも使用できます。

- SSL オフローダとして機能し、オフロードされたウェブ アプリケーションに HTTPS サポートを追加する。これには SMA/SRA 装置の統合 SSL アクセラレータ ハードウェアを使用する。
- ウェブ アプリケーション ファイアウォール購読サービスと共に、オフロードされたウェブ アプリケーションに悪質なウェブ攻撃からの継続的な保護を提供する。
- 二段階認証、ワンタイム パスワード、クライアント証明書認証など、強力な認証や積層された認証をオフロードされたウェブ アプリケーションに追加する。
- グローバルなグループまたはユーザをベースにしたアクセス ポリシーを使って、オフロードされたウェブ アプリケーションへのアクセスをきめ細かに制御する。
- HTTP/HTTPS ブックマークで現在サポートされていないウェブ アプリケーションをサポートする。アプリケーション オフロードでは URL 書き換えが必要ないので、スループットに悪影響を与えずに完全なアプリケーション機能を提供できる。

メモ：

- サポートされるユーザの最大数は、アクセスされているアプリケーション数と送信されているアプリケーション トラフィック量によって制限されます。
- アプリケーションが絶対 URL を使って同じホスト内のリソースを参照していると、アプリケーション オフローダ機能は正常に機能しません。その場合、絶対 URL 参照を相対参照形式に変換する必要があります。
- 特定のバックエンド ウェブ アプリケーションの設定についての詳細情報は、www.sonicwall.com の「**Support**」にある『*Secure Mobile AccessApplication Offloading and HTTP(S) Bookmarks*』機能モジュール内で参照可能です。

HTTP/HTTPS アプリケーション オフロード ポータルの設定

ウェブ アプリケーションをオフロードして、そのためのポータルを作成するには:

1 「**ポータル > ポータル**」を開いて「**仮想ホスト**」セクションに移動します。「仮想ホスト設定」画面が表示されます。この画面から直接ポータルにアクセスできます。

2 わかりやすい名前を「**仮想ホスト ドメイン名**」フィールドに入力します。

3 「**オフロード**」タブで、オフロードされたアプリケーション サーバ間で負荷分散するための「**負荷分散を有効にする**」をオンにします。

4 「**仕組み**」ドロップダウン リストから次のいずれかを選択します。

- **ウェブ (HTTP)** - HTTP を使ってウェブ アプリケーションにアクセスします (既定の仕組み)。
- **セキュア ウェブ (HTTPS)** - HTTPS を使ってウェブ アプリケーションにアクセスします。
- **自動 (HTTP/HTTPS)** - オフロードされたポータルにアクセスする際にバックエンド サーバと通信するための実際の仕組みを、ユーザが決定できます。この場合もアクセスには、アクセス ポリシーが適用されます。

  「自動」の仕組みを使用する場合、ユーザはブラウザのアドレス バーに「http://www.example.virtual.host.com」または「https://www.example.virtual.host.com」と入力することによって、この機能をテストできます。仕組みを「自動」に設定した場合でも、アクセス ポリシーが適用されます。

△ 注意：**バックエンド サーバとの通信に使用する正しい仕組みを設定するのは、管理者の責任です。自動 (HTTP/HTTPS) スキームは、仮想ホストに対して HTTP アクセスが有効 (「仮想ホスト」タブの下) で、かつ、認証が無効 (「オフロード」タブの下) の場合のみ機能しますが、これでは安全でない可能性があります。そのため、仮想ホストに対して HTTP を有効にするため、確認として「OK」を選択することが求められます。**

- **一般 (SSL オフローダ)** - SSL オフローダを使って個別の SSL アプリケーション (非 HTTP(S) アプリケーション) にアクセスします。

  「**一般 (SSL オフローダ)**」オプションの詳細については、オフロード ポータル ウィザードを使った設定 (170 ページ) を参照してください。

5 「**アプリケーション サーバ ホスト**」フィールドに、バックエンド ホストのホスト名またはプライベート IP アドレスを入力します。

6 「**アプリケーション サーバ IPv6 アドレス**」フィールドに、バックエンド ホストの IPv6 アドレスを入力します (オプション)。

7 「**ポート番号 (オプション)**」フィールドに、アプリケーションへのアクセスに使用する個別ポート番号を入力します (オプション)。

8 「**ホームページ URL (オプション)**」フィールドに、ユーザがこのアプリケーション オフローダ ポータルに最初にアクセスを試みたときに転送されるウェブ サーバ上の特定のリソースの URL を入力します (オプション)。これは次の形式の文字列です。**/exch/test. cgi?key1=value1&key2=value2**

このフィールドが設定されていると、ユーザがこのポータルに最初にアクセスしたときに、ユーザをウェブ サイトのホームページにリダイレクトします。これは、ユーザが URL パス無しでサイトにアクセスしたとき(例えば https://www/google.com/ のようなルート フォルダにアクセスしたとき)のみ動作します。これはルート フォルダに対するエイリアスではありません。ユーザは URL を編集してルート フォルダに戻ることができます。

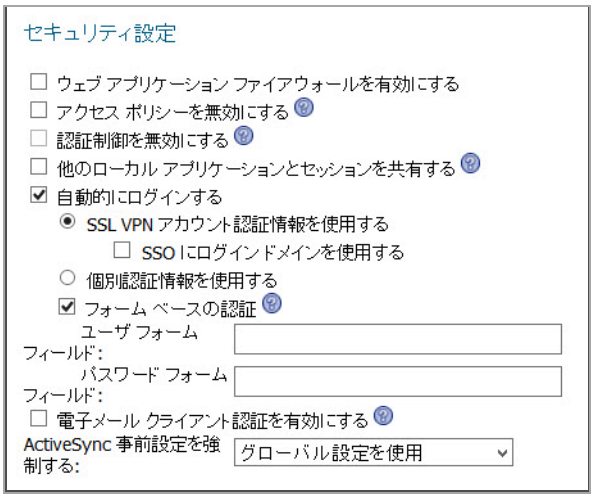
この Key=値 の組により、URL 内の URL クエリ パラメータを指定できます。ルート フォルダからホームページ URL への既定のリダイレクトを持たない、どのようなウェブ サイトに対しても、これらを使用できます。Outlook Web Access は一つの例ですが、ほとんどの公開サイトに既定のリダイレクトがあります。

a 「セキュリティ設定」の下で「**ウェブ アプリケーション ファイアウォールを有効にする**」をオンにして、この機能を有効にします。

b 認証、アクセス ポリシー、および CSRF 防御を適用する必要がない場合は、「認証制御を無効にする」と「アクセス ポリシーを無効にする」をオンにし、**CSRF 防御が有効になっている場合は無効**にします。これは公開ホストのウェブ サイトに便利です。

a ActiveSync 認証を設定するには、「**認証制御を無効にする**」をオフにして、認証に関するフィールドを表示させます。「**ActiveSync 認証を有効にする**」をオンにして、既定のドメイン名を入力します。この既定のドメイン名は、電子メール クライアントの設定内にドメイン名が設定されている場合は使用されません。

9 シングル サイン オンを設定するには、「**自動的にログインする**」をオンにします。



10 SSO を用いた自動ログインに対して、次のラジオ ボタンのいずれかを選択します。

- **SSL-VPN アカウント認証情報を使用する** - SMA/SRA 装置上で設定された認証情報による、オフロードされたアプリケーションへのログインを許可します。
- **個別認証情報を使用する** -「**ユーザ名**」、「**パスワード**」、「**ドメイン**」の各フィールドを表示します。これらのフィールドにアプリケーションの個別認証情報を入力するか、動的な変数を使用できます。「**パスワード**」フィールドには、提示する個別パスワードを入力するか、空白のままにして現在のユーザのパスワードをオフロードされたアプリケーション ポータルに提示します。その他のフィールドに対しては、次の表に示す動的な変数が使用できます。

サポートされている動的な変数

用途	変数	使用例
ログイン名	%USERNAME%	US\%USERNAME%
ドメイン名	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
グループ名	%USERGROUP%	%USERGROUP%\%USERNAME%

11 「**自動的にログインする**」を選択している場合は、「**フォーム ベースの認証**」をオンにしてシングル サイン オンをフォーム ベース認証用に設定します。

- 「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の‘name’または‘id’属性と同じになるように設定します。

  例えば、<input type=text name='userid'> のようにします。

- 「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の ‘name’ または ‘id’ 属性と同じになるように設定します。

  例えば、`<input type=password name=PASSWORD id=PASSWORD maxlength=128>` のようにします。

12 「**仮想ホスト**」セクションの「**仮想ホスト ドメイン名**」フィールドでアプリケーションのホスト名を設定し、オプションで「**仮想ホストの別名**」フィールドにわかりやすい別名を入力します。

このホストに証明書を関連付ける必要がある場合は、さらに仮想インターフェースを設定し、該当する SSL 証明書をインポートしてください。SMA/SRA 装置のすべての仮想ホストに使用できるワイルドカードの証明書をインポートすれば、仮想インターフェースを作成せずに済みます。

このセクションにあるフィールドの設定方法の詳細については、仮想ミーティングの設定 (159 ページ) を参照してください。

13 このポータルで認証が無効の場合、このアプリケーション オフロード ポータルで「**HTTP アクセスを有効にする**」オプションが利用できます。この機能は試験用環境内でのオフロード設定に有用です。

14 「**適用**」を選択します。これで「**ポータル > ポータル**」ページに戻ります。ここでウェブ アプリケーションが「説明」の下に「**オフロードされたウェブ アプリケーション**」として表示されるのが確認できます。

15 認証を無効にしていなければ、「**ポータル > ドメイン**」ページにナビゲートし、このポータルのドメインを作成します。ドメインの作成については、ポータル > ドメイン (186 ページ) を参照してください。

16 この仮想ホストのドメイン名とエイリアス (もしあれば) に関して DNS サーバを更新します。

メモ: 将来は、WAF がライセンスされていない場合に匿名オフロード アクセスがサポートされなくなる予定です。「**システム > ライセンス**」ページで WAF 購読サービスを有効にするか、試用版を使用してください。

オフロード ポータル ウィザードを使った設定

オフロード ポータル ウィザードを使ってポータルを設定するには:

1 「**ポータル > ポータル**」を表示し、「**ウェブ アプリケーションのオフロード**」を選択します。オフロード ポータル ウィザードが表示されます。

2 最初の画面ではアプリケーション オフロードのタイプを選択します。オプションは以下を含みます。

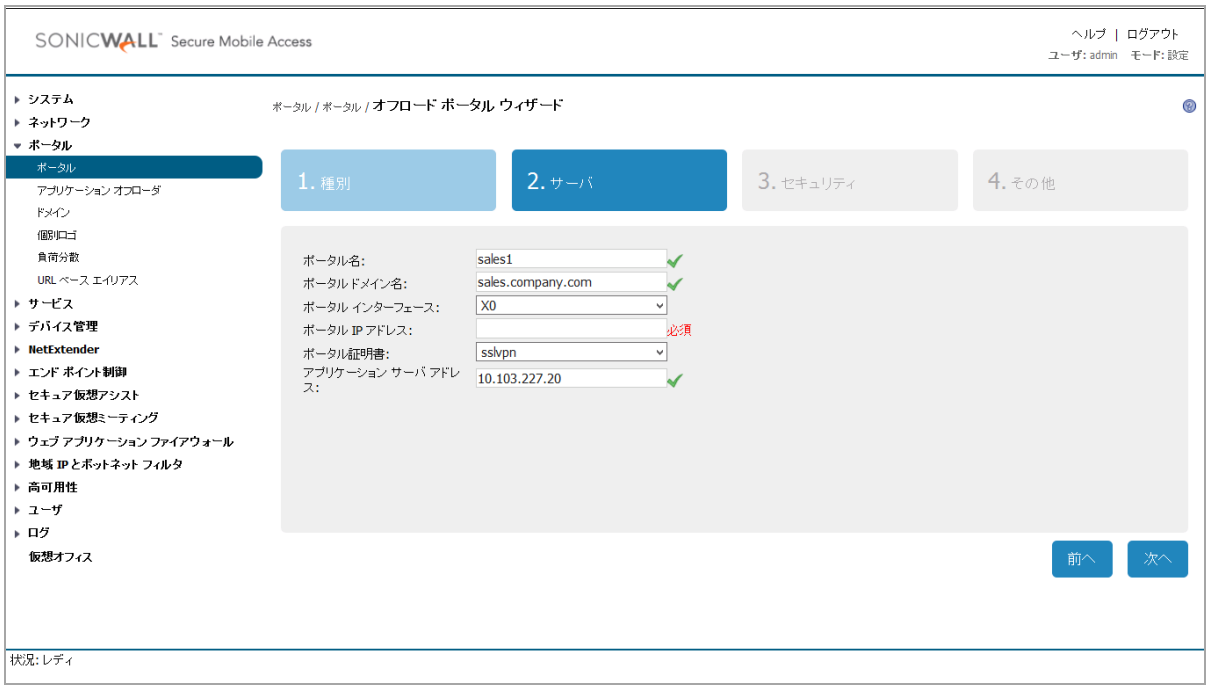
- **一般**ポータル - ほとんどの状況で選択できます。
- **負荷分散**ポータル - 負荷分散オフロード ポータルをセットアップする場合に使用するポータル タイプです。
- **URL ベース エイリアス** ポータル - URL ベース エイリアス オフロード ポータルをセットアップする場合に使用します。1 つのポータルとドメイン名を使って複数のウェブ サイトにアクセスする必要があれば、「**URL ベース エイリアス**」を選択します。このオプションを有効にすると、画面に表示されるオプションが変わります。
- **リモート デスクトップ ウェブ アクセス (RD Web Access)** - リモート デスクトップ (RD) ウェブ アクセス ページでは、RD ウェブ サイト上のリソース リストがより効率的に機能するように、SMA Agent を使用してプライベート ネットワークへの RDP 接続をプロキシ処理します。「RD Web Access」オプションを使用するもう 1 つのメリットは、すべてのブラウザ (Chrome、Firefox、および Internet Explorer) に対応していることです。

3 Exchange ポータルを使用する場合は、「**これは、OWA、ActiveSync、または Outlook Anywhere によってアクセスされる Exchange ポータルです**」を選択します。

4 「**次へ**」ボタンを選択します。

一般サーバ設定

「**一般**」を最初のページで選択した場合、「**サーバ**」ページが次に表示されます。ポータルおよびアプリケーション サーバの設定は、このページで行うことができます。



1 「**ポータル名**」フィールドに、ポータルを識別するための一意の名前を入力します。

2 「**ポータル ドメイン名**」フィールドに、オフロード ポータルへのアクセスに使用するドメイン名を入力します。

3 「**ポータル インターフェース**」フィールドに、ポータルが結合されているネットワーク インターフェースを入力します。ある特定のネットワーク インターフェースが選択されている場合は、新しい IP アドレスがポータルに割り当てられます。

4 「**ポータル IP アドレス**」フィールドに、ポータルがある IP アドレスを入力します。

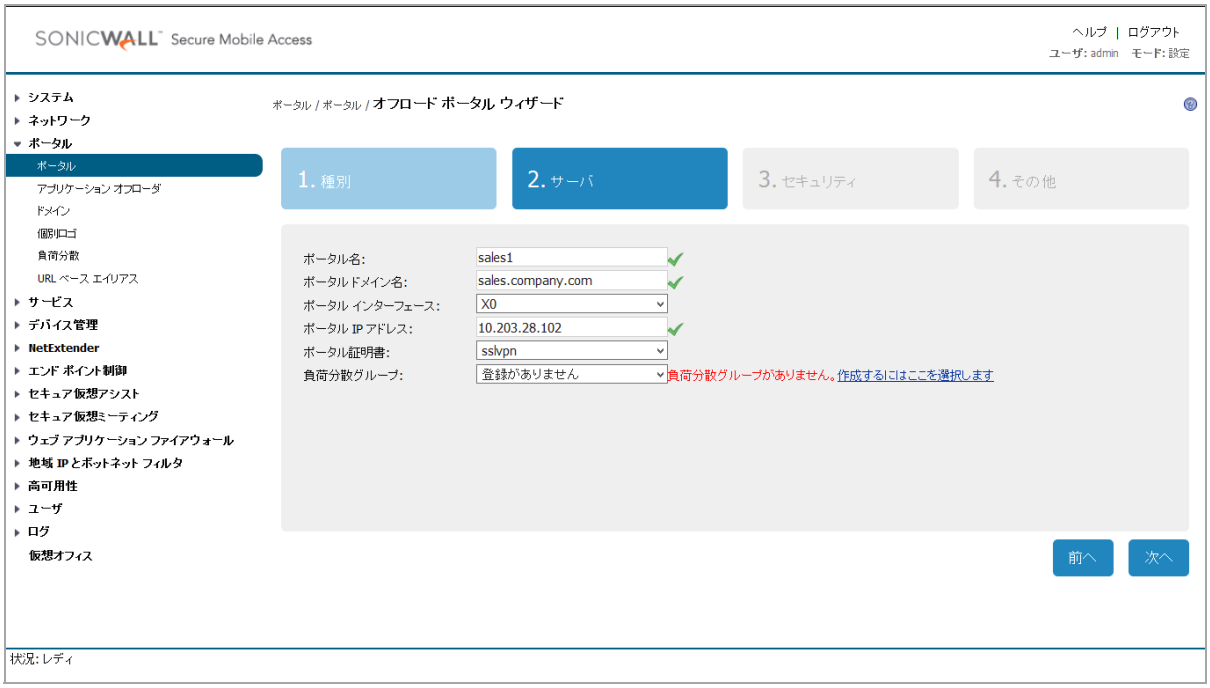
5 「**ポータル証明書**」ドロップダウンには、それまでにインポートされたすべての証明書のリストが表示されます。

6 「**アプリケーション サーバ アドレス**」フィールドには、アプリケーション サーバに関する設定が反映されます。アプリケーション サーバの IP アドレスがそのまま表示されることがあります。アドレスのスキームは既定で "HTTPS" になっています。ポートおよび既定のパスもこの 1 つのフィールドで設定できます。

これらすべての設定は、マウス ポインタが入力テキスト ボックスから離れるとすぐに、装置側からの検証が行われます (緑色のチェックマーク)。入力内容に問題がある場合は、その理由が表示されます。すべてのフィールドに問題がない場合に限り、「**次へ**」をクリックして次のタブに進むことができます。

負荷分散サーバ設定

「**負荷分散**」を最初のページで選択した場合、「**サーバ**」ページが次に表示されます。



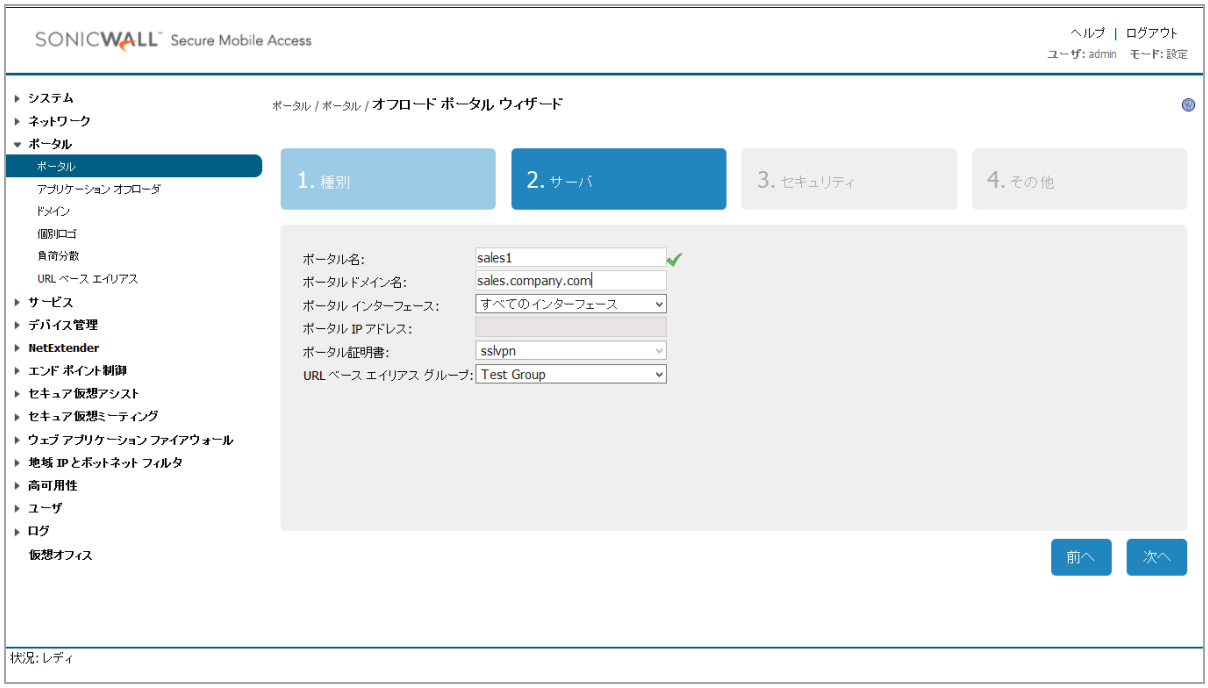
1. 「**ポータル名**」フィールドに、ポータルを識別するための一意の名前を入力します。
2. 「**ポータル ドメイン名**」フィールドに、オフロード ポータルへのアクセスに使用するドメイン名を入力します。
3. 「**ポータル インターフェース**」フィールドに、ポータルが結合されているネットワーク インターフェースを入力します。ある特定のネットワーク インターフェースが選択されている場合は、新しい IP アドレスがポータルに割り当てられます。
4. 「**ポータル IP アドレス**」フィールドに、ポータルがある IP アドレスを入力します。
5. 「**ポータル証明書**」ドロップダウンには、それまでにインポートされたすべての証明書のリストが表示されます。
6. 「**負荷分散グループ**」フィールドは、「**アプリケーション サーバ アドレス**」フィールドに代わるものとして、このポータルに割り当てることができる既存の負荷分散グループを表示します。負荷分散グループが存在しない場合は、「作成するにはここを選択します」をクリックすると、新しい負荷分散グループを作成できます。

これらすべての設定は、マウス ポインタが入力テキスト ボックスから離れるとすぐに、装置側からの検証が行われます (緑色のチェックマーク)。入力内容に問題がある場合は、その理由が表示されます。すべてのフィールドに問題がない場合に限り、「**次へ**」をクリックして次のタブに進むことができます。

URL ベース エイリアス サーバ設定

1 つのポータルとドメイン名を使って複数のウェブ サイトにアクセスする必要があれば、最初のページで「**URL ベース エイリアス**」を選択します。このオプションを有効にすると、画面に表示されるオプションが変わります。ドロップダウン リストから「**URL ベースのエイリアス グループ**」を選択す

る必要があります。「**URL ベースのエイリアス**」を最初のページで選択した場合、「**サーバ**」ステップが次に表示されます。



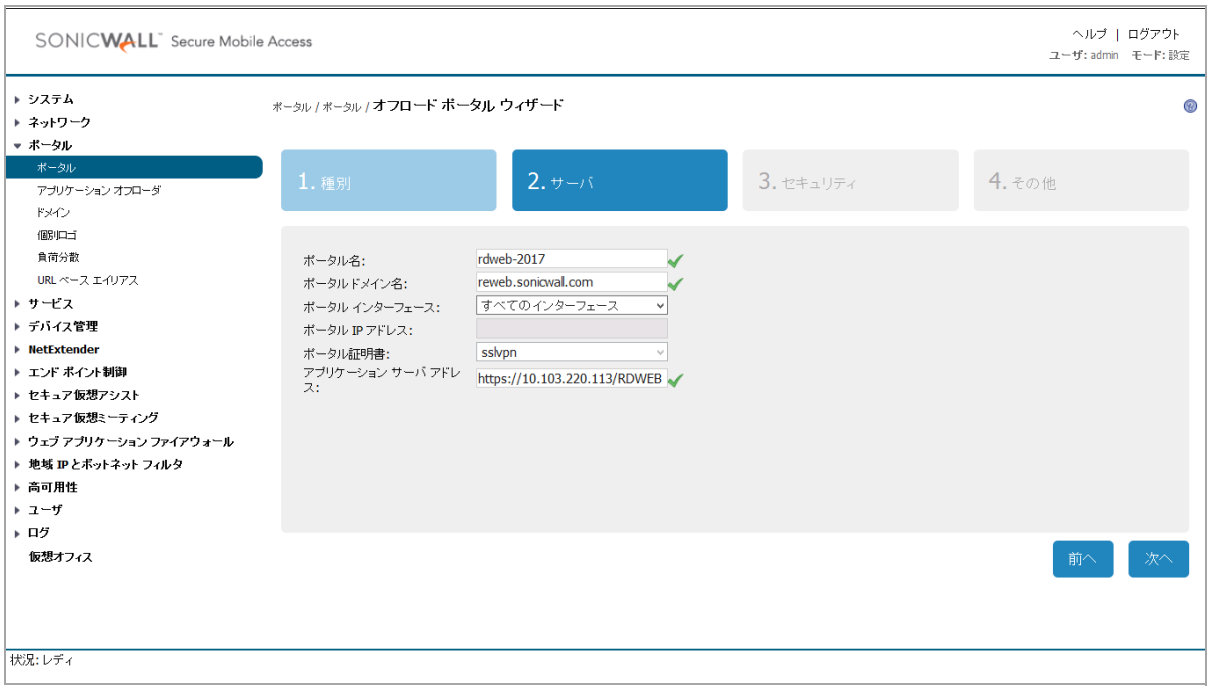
1. 「**ポータル名**」フィールドに、ポータルを識別するための一意の名前を入力します。
2. 「**ポータル ドメイン名**」フィールドに、オフロード ポータルへのアクセスに使用するドメイン名を入力します。
3. 「**ポータル インターフェース**」フィールドに、ポータルが結合されているネットワーク インターフェースを入力します。ある特定のネットワーク インターフェースが選択されている場合は、新しい IP アドレスがポータルに割り当てられます。
4. 「**すべてのインターフェース**」が「**ポータル インターフェース**」フィールドで選択されている場合、「**ポータル IP アドレス**」フィールドの入力は不要ですが、X0、X1、X2、および X3 インターフェースの「**ポータル IP アドレス**」は入力する必要があります。
5. 「**ポータル証明書**」ドロップダウンには、それまでにインポートされたすべての証明書のリストが表示されます。
6. 既存の「**URL ベースエイリアス グループ**」は、ドロップダウンにリストで表示され、このポータルに割り当てることができます。**URL ベース エイリアス グループ**が存在しない場合は、"**ここをクリックして作成**" ハイパーリンクをクリックすると、新しいグループを作成できます。

これらすべての設定は、マウス ポインタが入力テキスト ボックスから離れるとすぐに、装置側からの検証が行われます (緑色のチェックマーク)。入力内容に問題がある場合は、その理由が表示されます。すべてのフィールドに問題がない場合に限り、「**次へ**」をクリックして次のタブに進むことができます。

リモート デスクトップ ウェブ アクセス サーバの設定

リモート デスクトップ (RD) ウェブ サイト上のリソース リストがより効率的に機能するように、SMA Agent を使用してプライベート ネットワークへの RDP 接続をプロキシ処理したい場合は、最初のペー

ジで「**リモート デスクトップ ウェブ アクセス (RD Web Access)**」を選択します。このオプションを有効にすると、画面に表示されるオプションが変わります。ドロップダウン リストから「**リモート デスクトップ ウェブ アクセス (RD Web Access)**」を選択する必要があります。最初のページで「**リモート デスクトップ ウェブ アクセス (RD Web Access)**」を選択すると、「**サーバ**」ステップが次のように表示されます。



1 「**ポータル名**」フィールドに、ポータルを識別するための一意の名前を入力します。

2 「**ポータル ドメイン名**」フィールドに、オフロード ポータルへのアクセスに使用するドメイン名を入力します。

3 「**ポータル インターフェース**」フィールドに、ポータルが結合されているネットワーク インターフェースを入力します。ある特定のネットワーク インターフェースが選択されている場合は、新しい IP アドレスがポータルに割り当てられます。

4 「**すべてのインターフェース**」が「**ポータル インターフェース**」フィールドで選択されている場合、「**ポータル IP アドレス**」フィールドの入力は不要ですが、X0、X1、X2、および X3 インターフェースの「**ポータル IP アドレス**」は入力する必要があります。

5 「**ポータル証明書**」ドロップダウンには、それまでにインポートされたすべての証明書のリストが表示されます。

6 「**アプリケーション サーバ アドレス**」フィールドには、アプリケーション サーバに関する設定が反映されます。アプリケーション サーバの IP アドレスがそのまま表示されることがあります。アドレスのスキームは既定で "HTTPS" になっています。ポートおよび既定のパスもこの 1 つのフィールドで設定できます。

これらすべての設定は、マウス ポインタが入力テキスト ボックスから離れるとすぐに、装置側からの検証が行われます (緑色のチェックマーク)。入力内容に問題がある場合は、その理由が表示されます。すべてのフィールドに問題がない場合に限り、「**次へ**」をクリックして次のタブに進むことができます。

セキュリティ設定の構成

3 番目のステップでは、「**ウェブ アプリケーション ファイアウォールを有効にする**」、「**認証制御を無効にする**」などのセキュリティ設定を行います。ただし、どちらのオプションも使用するにはウェブ アプリケーション ファイアウォールのライセンスが必要です。

その他の設定の構成

4 番目 (最後) のステップには、全般的なポータル設定が含まれています。

「**ポータル サイト タイトル**」、「**ポータル バナー タイトル**」、「**ログイン メッセージ**」は既定で設定されていますが、任意に変更できます。

今すぐ再起動 -「**完了**」のクリック後、装置のスムーズな再起動をただちに行います。

ウィザードの終了後にこのポータルを編集することで、より詳細なオプションを調整できます。ポータル設定を変更するには、ウェブ サーバを再起動する必要があります。再起動により、アクティブな NetExtender 接続や特定のブックマークが切断状態になる可能性があります。設定した内容をただちに有効にするために、ウェブ サーバの再起動に進む場合は、「**今すぐ再起動**」にチェックを入れます。それ以外の場合は、このチェック ボックスをオフにして、ウェブ サーバを再起動せずに変更内容を保存します。装置の再起動は、後で「**システム > 再起動**」ページから行うことができます。

「**完了**」をクリックすると、ウィザードは終了します。アプリケーション オフロード ポータルが正しく作成された後、ページは遮断され、ポータル リスト ページにリダイレクトされます。

一般設定の変更

一般設定を編集するには:

1 必要に応じて、「**ポータル名**」、「**ポータル サイト タイトル**」、「**ポータル バナー タイトル**」、および「**ログイン メッセージ**」を編集できます。

2 個別のロゴ、メッセージ、およびタイトル情報をログイン ページに表示するには、「**個別ログイン ページを表示する**」をオンにします。

> **メモ**：個別のロゴは、既存のポータルにのみ追加できます。個別のロゴを新しいポータルに追加するには、最初に一般ポータル設定を完了してからロゴを追加します。

3 ユーザが個別ログイン ページにログインしたときにログイン メッセージ (「**ログイン メッセージ**」フィールドの内容) を表示するには、「**個別ログイン ページにログイン メッセージを表示する**」をオンにします。

4 ログイン ページに表示される「ドメイン」リスト ボックスの代わりに、適切なドメイン名を入力できるテキスト ボックスを表示するには、「**ポータル ログイン ページのドメイン リストを非表示にする**」をオンにします。

5 HTTPOnly フラグを使って SMA クッキーを保護するには、「**SMA クッキーの HttpOnly を有効化**」をオンにします。

Java アプレットなどクライアント側のテクノロジーの一部には、HTTPOnly とマーク付けされたクッキーにアクセスできないものがあります。このため、HTTP/HTTPS ブックマークやアプリケーション オフロード ポータルを使用していると、ウェブ アプリケーションにアクセスできない可能性があります。このようなウェブ アプリケーションに再度アクセスするには、このオプションを無効にしてください。

6 「**キャッシュ制御のための HTTP メタ タグを有効にする**」をオンにして、このポータルに HTTP メタ タグ キャッシュ制御ディレクティブを適用します。キャッシュ制御ディレクティブには、次のものが含まれます。

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
```

これらのディレクティブを適用することで、SMA/SRA 装置ポータル ページとその他のウェブ コンテンツがクライアント ブラウザ側でキャッシュされるのを防ぐことができます。

メモ：セキュリティ上の理由に加え、古いウェブ ページやデータがユーザのウェブ ブラウザのキャッシュに保管されることを防ぐために、HTTP メタ タグを有効にすることを強くお勧めします。

7 各アカウントに一度に 1 つのセッションのみを許可するには、「**多重ログインを禁止する**」(既定では無効) をオンにします。禁止しない場合は、ActiveSync または Outlook Anywhere クライアントは同時に複数のセッションを使用できます。

8 「**強制適用手順**」をオンにします。「**既存のセッションから自動的にログアウトします**」や「**既存のセッションからログアウトしたことを確認します**」などのオプションを選択できます。

9 SonicWall Inc. クライアント (NetExtender、Mobile Connect、Virtual Assist など) の使用時に、同じクライアント送信元アドレスによる複数の接続を禁止するには、「**クライアント送信元の一意性の強制**」をオンにします。これにより、ネットワークの予期しない中断の後にユーザが再接続を行うとき、ライセンスを複数消費することが防げます。

例えば、信頼性の低いネットワーク上のユーザがネットワークの問題が原因で切断されたとします。もし多重ログインの禁止が有効になっていない場合、この種の切断に対しては、タイムアウト値に到達するまで装置上のユーザ セッションはアクティブなままです。ユーザは再接続し、元の接続がタイムアウトで切断される前に、潜在的により多くのライセンスを消費する可能性がある状態で 2 個目のライセンスを消費します。

10 ライブ タイルで使用する**小さな/中程度の/幅広の/大きな**ロゴのリンクを指定します。

11 ライブ タイルの**背景色**を指定します。値を指定しない場合、既定色は #0085C3 です。

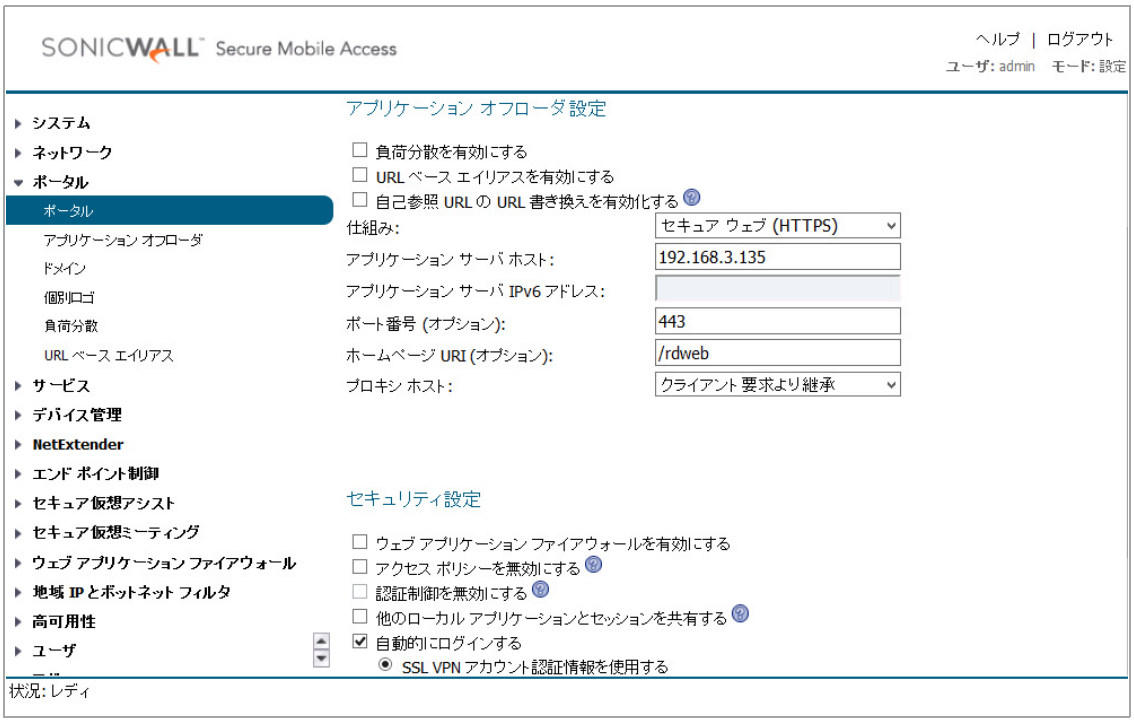
12 ライブ タイルに対して表示される**サイト名**を指定します。値を指定しない場合、既定値はポータル名です。

13 「**適用**」を選択して設定を保存します。

オフロード設定の構成

1 編集が必要なポータルで、「**ポータル > ポータル**」にナビゲートし、「**設定**」アイコンを選択します。「ポータル設定」画面の「**一般**」タブが表示されます。

2 「**アプリケーション オフロードの設定**」セクションに移動します。



3 「**オフロード**」タブで、オフロードされたアプリケーション サーバ間で負荷分散するための「**負荷分散を有効にする**」をオンにします。

4 「**URL ベース エイリアスを有効にする**」をオンにします。これにより、いくつかのフィールドが非表示になり、「**自己参照 URL の URL 書き換えを有効化する**」が自動的にオンになります。

5 ポータルを追加したいグループを「**URL ベース エイリアス グループ**」ドロップダウン リストから選択します。

6 「**URL ベース エイリアス グループ**」を使用しない場合は、「**仕組み**」ドロップダウン リストから次のオプションのいずれかを選択します。

- **ウェブ (HTTP)** - HTTP を使ってウェブ アプリケーションにアクセスします (既定の仕組み)。
- **セキュア ウェブ (HTTPS)** - HTTPS を使ってウェブ アプリケーションにアクセスします。
- **自動 (HTTP/HTTPS)** - オフロードされたポータルにアクセスする際にバックエンド サーバと通信するための実際の仕組みを、ユーザが決定できます。この場合もアクセスには、アクセス ポリシーが適用されます。

  「自動」の仕組みを使用する場合、ユーザはブラウザのアドレス バーに「http://www.example.virtual.host.com」または「https://www.example.virtual.host.com」と入力することによって、この機能をテストできます。仕組みを「自動」に設定した場合でも、アクセス ポリシーが適用されます。

△ **注意：バックエンド サーバとの通信に使用する正しい仕組みを設定するのは、管理者の責任です。仕組みは、仮想ホストに対して HTTP アクセスが有効 (「仮想ホスト」タブの下) で、かつ、認証が無効 (「オフロード」タブの下) の場合のみ機能しますが、これでは安全でない可能性があります。そのため、仮想ホストに対して HTTP を有効にするため、確認として「OK」を選択することが求められます。**

7 「**アプリケーション サーバ ホスト**」フィールドに、バックエンド ホストのホスト名またはプライベート IP アドレスを入力します。

8 「**アプリケーション サーバ IPv6 アドレス**」フィールドに、バックエンド ホストの IPv6 アドレスを入力します (オプション)。

9 「**ポート番号 (オプション)**」フィールドに、アプリケーションへのアクセスに使用する個別ポート番号を入力します (オプション)。

10 「**ホームページ URL (オプション)**」フィールドに、ユーザがこのアプリケーション オフロード ポータルに最初にアクセスを試みたときに、ユーザがログイン後に転送されるウェブ サーバ上の特定のリソースの URL を入力します (オプション)。これは次の形式の文字列です。
/exch/test. cgi?key1=value1&key2=value2

このフィールドが設定されていると、ユーザがこのポータルに最初にアクセスしたときに、ユーザをウェブ サイトのホームページにリダイレクトします。これは、ユーザが URL パス無しでサイトにアクセスしたとき (例えば `https://www/google.com/` のようなルート フォルダにアクセスしたとき) のみ動作します。これはルート フォルダに対するエイリアスではありません。ユーザは URL を編集してルート フォルダに戻ることができます。

この Key=値 の組により、URL 内の URL クエリ パラメータを指定できます。ルート フォルダからホームページ URL への既定のリダイレクトを持たない、どのようなウェブ サイトに対しても、これらを使用できます。Outlook Web Access は一つの例ですが、ほとんどの公開サイトに既定のリダイレクトがあります。

11 ドロップダウン メニューから「**プロキシ ホスト**」を選択して、バックエンド サーバに送信されるホスト名を選択できるようにします。ほかにも「**クライアント要求より継承**」、「**仮想ホスト名**」、「**アプリケーション サーバ ホスト (バックエンド)**」といったオプションがあります。「**クライアント要求から継承する**」オプションが既定で選択されます。

セキュリティ設定

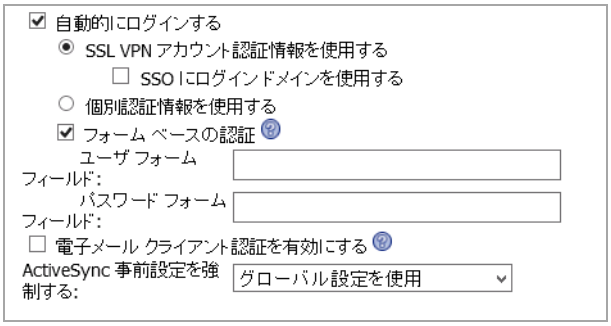
1 「セキュリティ設定」の下で「**ウェブ アプリケーション ファイアウォールを有効にする**」をオンにして、この機能を有効にします。

2 「**アクセス ポリシーを無効にする**」を選択して、既存のアクセス ポリシーが優先されないようにします。

3 認証、アクセス ポリシー、および CSRF 防御を適用する必要がない場合は、「認証制御を無効にする」と「アクセス ポリシーを無効にする」をオンにし、**CSRF 防御が有効になっている場合は無効**にします。これは公開ホストのウェブ サイトに便利です。

4 ActiveSync 認証を設定するには、「**認証制御を無効にする**」チェックボックスを非選択にして認証に関するフィールドを表示させます。「**ActiveSync 認証を有効にする**」をオンにして、既定のドメイン名を入力します。この既定のドメイン名は、電子メール クライアントの設定内にドメイン名が設定されている場合は使用されません。

5 シングル サイン オンを設定するには、「**自動的にログインする**」をオンにします。



6 SSO を用いた**自動ログイン**の場合は、次のラジオ ボタンのいずれかを選択します。

- **SSL-VPN アカウント認証情報を使用する** - SMA/SRA 装置上で設定された認証情報による、オフロードされたアプリケーションへのログインを許可します。
- **個別認証情報を使用する** -「**ユーザ名**」、「**パスワード**」、「**ドメイン**」の各フィールドを表示します。これらのフィールドにアプリケーションの個別認証情報を入力するか、動的な変数を使用できます。「**パスワード**」フィールドには、提示する個別パスワードを入力するか、空白のままにして現在のユーザのパスワードをオフロードされたアプリケーション ポータルに提示します。その他のフィールドに対しては、以下の動的な変数が使用できます。

サポートされている動的な変数

用途	変数	使用例
ログイン名	%USERNAME%	US\%USERNAME%
ドメイン名	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
グループ名	%USERGROUP%	%USERGROUP%\%USERNAME%

7 「**自動的にログインする**」をオンにした場合は、「**フォーム ベースの認証**」をオンにしてシングル サイン オンをフォーム ベースの認証用に設定します。

- 「**ユーザ フォーム フィールド**」は、ログイン フォーム内のユーザ名を表す HTML 要素の 'name' または 'id' 属性と同じになるように設定します。

  例えば、`<input type=text name='userid'>` のようにします。

- 「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の 'name' または 'id' 属性と同じになるように設定します。

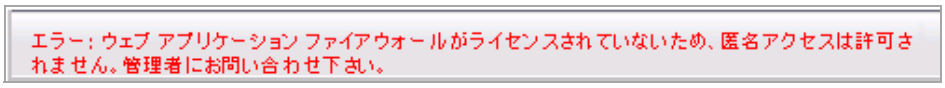
  例えば、`<input type=password name=PASSWORD id=PASSWORD maxlength=128>` のようにします。

8 ActiveSync、Outlook、OWA などの電子メール クライアントから Exchange ポータルにアクセスできるようにするには、「**電子メール クライアント認証を有効にする**」をオンにします。オンになっている場合は、ドロップダウン リストから「**既定のドメイン名**」を選択します。「**既定のドメイン名**」は、ドメインを作成または編集する際に自動的に設定されます。ドメイン名が電子メール クライアントで指定されていない場合は、このドメイン名が SMA 認証の既定のドメインとして使用されます。

ⓘ **メモ**：このオプションは OWA の場合は不要です。

認証制御が既に無効になっていて (さらに WAF がライセンスされていない) 場合は、8.5 へのアップグレード後に「操作が必要」というメッセージがポータル ページに表示されます。「**認証制御を無効にする**」オプションも無効になっています。「保存」をクリックして、認証制御の設定を確定させます。

これらの条件の下にポータルにアクセスした場合、エラー メッセージが表示されます。



次のようなログ メッセージが通告のレベルで生成されます。「*WAF がライセンスされていないため、匿名オフロード接続を処理できませんでした。*」「***システム > ライセンス***」*ページ*」*で WAF 購読サービスまたは無料試用版を有効にしてください。*

「**認証制御**」が無効になっている場合は、同様のことが Exchange ポータルへのアクセスについて当てはまります。

その場合、ログ メッセージには「匿名 Exchange アクセスを処理できませんでした。ポータルの認証制御を有効にしてください」と表示されます。

HTTP/HTTPS アプリケーション オフロード ポータルの設定

ウェブ アプリケーションをオフロードして、そのためのポータルを作成するには:

1 「**ポータル > ポータル**」を開いて「**仮想ホストの設定**」セクションまでスクロールします。この画面から直接ポータルにアクセスできます。

2 わかりやすい名前を「**仮想ホスト ドメイン名**」フィールドに入力します。

3 「**仮想ホスト**」タブの「**仮想ホスト ドメイン名**」フィールドでアプリケーションのホスト名を設定し、「**仮想ホスト の別名**」フィールドにオプションでわかりやすいエイリアスを入力します。ActiveSync アクセスが有効になっていれば、「**仮想ホストの別名**」が ActiveSync の Autodiscover アドレスに設定されています。Autodiscover アドレスは、「**仮想ホスト ドメイン名**」から自動的に生成されます。

このホストに証明書を関連付ける必要がある場合は、さらに仮想インターフェースを設定し、該当する SSL 証明書をインポートしてください。SMA/SRA 装置のすべての仮想ホストに使用できるワイルドカードの証明書をインポートすれば、仮想インターフェースを作成せずに済みます。

4 このポータルで認証が無効の場合、このアプリケーション オフロード ポータルで「**HTTP アクセスを有効にする**」オプションが利用できます。この機能は試験用環境内でのオフロード設定に有用です。

5 「**適用**」を選択します。これで「**ポータル > ポータル**」ページに戻ります。ウェブ アプリケーションが「説明」の下に「**オフロードされたウェブ アプリケーション**」として表示されるのが確認できます。

6 認証を無効にしていなければ、「**ポータル > ドメイン**」ページにナビゲートし、このポータルのドメインを作成します。

7 この仮想ホストのドメイン名とエイリアス (もしあれば) に関して DNS サーバを更新します。

オフロードされたアプリケーションの使用

オフロードされたアプリケーションには、SMA/SRA 装置に固有のポータル ページが作成されます。このポータルには、URL をウェブ ブラウザに入力すると直接アクセスできます。また、オフロードされたアプリケーションのポータルに移動するために使用できる外部ウェブ サイト ブックマークを SMA 仮想オフィス ポータルに作成することもできます。

オフロードされたアプリケーションを使用するには:

1 直接アクセスする場合は、オフロードされたアプリケーションのポータルの URL をウェブ ブラウザに入力します。

2 外部ウェブ サイト ブックマークを使ってアクセスする場合は、SonicWall Inc. 仮想オフィスにログインしてからブックマークをクリックします。

既定のブラウザで新しいウィンドウが表示され、ブックマークで指定した、オフロードされたアプリケーションのポータルに接続されます。

3 認証が必要な場合は、アプリケーションにアクセスするためにポータル ページでログイン資格情報を入力します。

SharePoint 2013 を使用するアプリケーション オフローダの設定

オフロードされたポータルを通じて SharePoint 2013 サーバにアクセスする場合、ドキュメント、タスク、またはカレンダー イベントの追加、編集、削除などの基本機能がサポートされます。クライアント統合は、オフロードされたポータルの認証制御が有効か無効かにかかわらず、サポートされます。ただし、認証制御が有効な場合、クライアントは以下の条件を満たす Internet Explorer でのみサポートされます。

- SharePoint 用に作成されたオフロード ポータルが、有効な証明書を使用している。
- オフロード ポータルとバックエンドの SharePoint で使用されるスキームが同一である。バックエンドの SharePoint が HTTP 上で動作している場合、オフロード ポータルは HTTP アクセスが有効で、HTTP によってアクセスされる必要があります。
- オフロード ポータルとバックエンドの SharePoint のスキームが同一であるということは、オフロード ポータルの URL の書き換えを有効にする*必要がない*ということです。
- 「**他のローカル アプリケーションとセッションを共有する**」オプションを有効にする必要があります。このチェックボックスは、「**ポータル** > **ポータル** > **オフロード**」タブにあります。
- 「**要求ヘッダを制限する**」オプションを無効にする必要があります。このチェックボックスは、「**サービス** > **設定**」ページにあります。
- クライアントで Windows Vista または Windows 7 を使用している場合は、オフロードされたポータルを“信頼されたサイト”として Internet Explorer ブラウザに追加する必要があります。信頼されたサイトを設定するには、「**ツール** > **インターネット オプション**」に移動します。「**セキュリティ**」タブの「**信頼されたサイト**」アイコンを選択します。
- 「**他のローカル アプリケーションとセッションを共有する**」オプションがログイン時に有効になっている必要があります。

Microsoft Outlook Anywhere with Autodiscover の概要

Outlook Anywhere with Autodiscover アプリケーション オフローダは、Outlook 2013、Outlook 2010、または Outlook 2007 を使用しているクライアントがインターネットから Outlook Exchange サーバにアクセスできるようにする機能です。Autodiscover サポートは、ユーザの電子メール アドレスとパスワードのみを要求することによって、ユーザのアカウントの設定を容易にします。Autodiscover はまた、Outlook Exchange サーバの設定が変更された場合に、クライアント上の設定を更新できるようにします。

Outlook Anywhere with Autodiscover は、アプリケーション オフローダ ポータルでサポートされ、アクセス ポリシーと認証の両方を強制できます。

メモ：SMA/SRA 装置の認証制御が有効な場合は、Outlook Anywhere 向けの基本認証のみをサポートできます。

Outlook Anywhere ポータルの設定

Outlook Anywhere アプリケーション オフローダ ポータルを設定するには:

1 Exchange サーバ上で Outlook Anywhere を有効にします。Outlook Anywhere が正しく設定されていることを確認します。

2 以下の設定に基づいて、アプリケーション オフローダ ポータルを作成します。

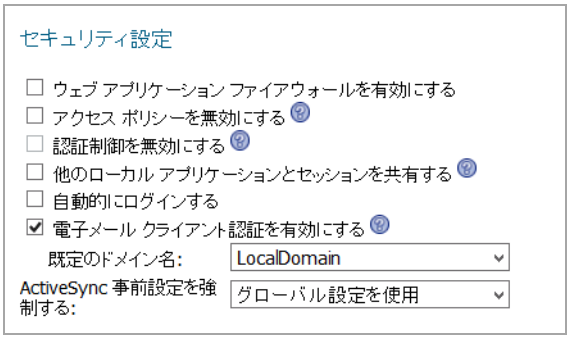
Autodiscover は設定の取得に異なる URL を使用するので、Autodiscover URL を**仮想ホスト の別名**として設定します。Autodiscover URL が Exchange サーバの設定と一致していることを確認してください。

3 **仮想ホスト証明書**を指定します。Autodiscover が有効な場合、ワイルドカード証明書が優先されます。

4 「**オフロード**」タブを開きます。

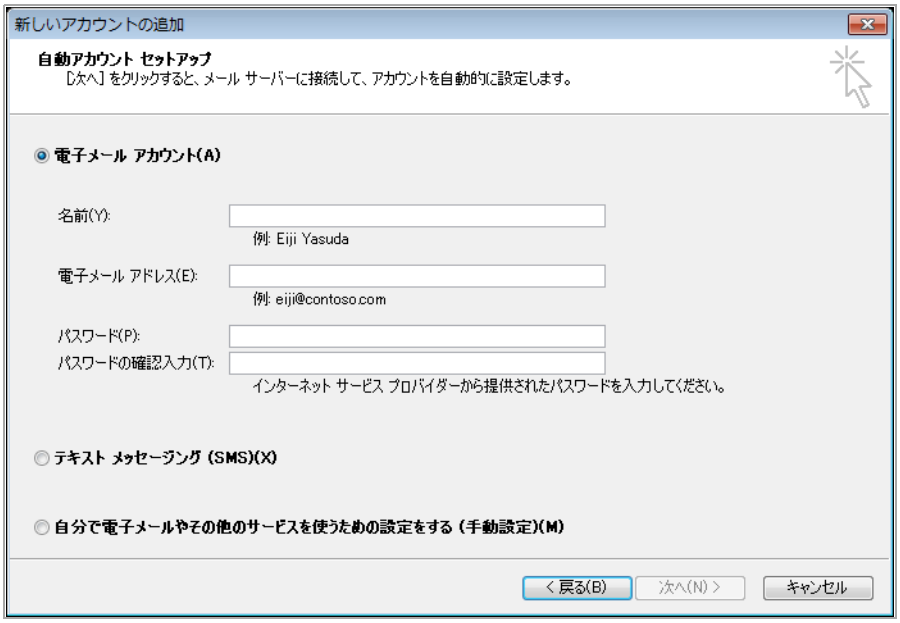
5 「**電子メール クライアント認証を有効にする**」を選択します。

6 「**既定のドメイン名**」をドロップダウン リストから選択します。ドメイン名が Outlook で指定されていない場合は、このドメイン名が Secure Mobile Access 認証の既定のドメインとして使用されます。



7 Microsoft Outlook を起動します。

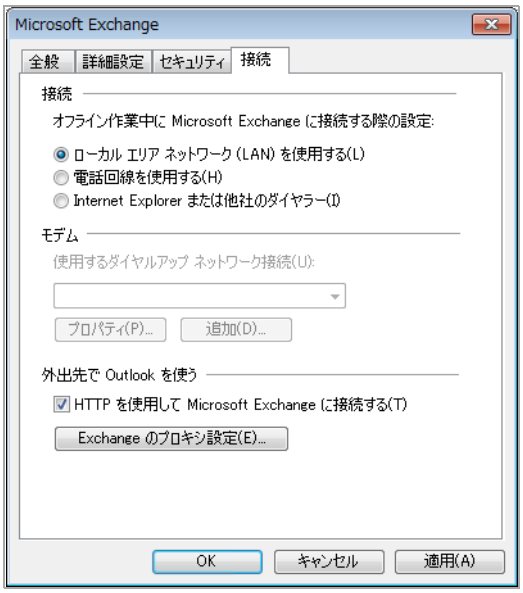
8 「**ファイル** > **情報**」ページの「**アカウントの追加**」を選択します。「新しいアカウントの追加」ウィンドウが表示されます。



電子メール アカウントを追加するには、「**自動アカウント セットアップ**」または「**サーバ設定または追加のサーバ種別を手動で設定する**」を選択できます。Autodiscover が設定されている場合は、「**自動アカウント セットアップ**」を選択します。Autodiscover が有効でない場合、または正しく機能していない場合は、「**サーバ設定または追加のサーバ種別を手動で設定する**」をオンにして、Outlook Anywhere の設定を手動で指定します。「**次へ**」を選択します。

9 「Microsoft Exchange 設定」ウィンドウで「**詳細設定**」を選択します。

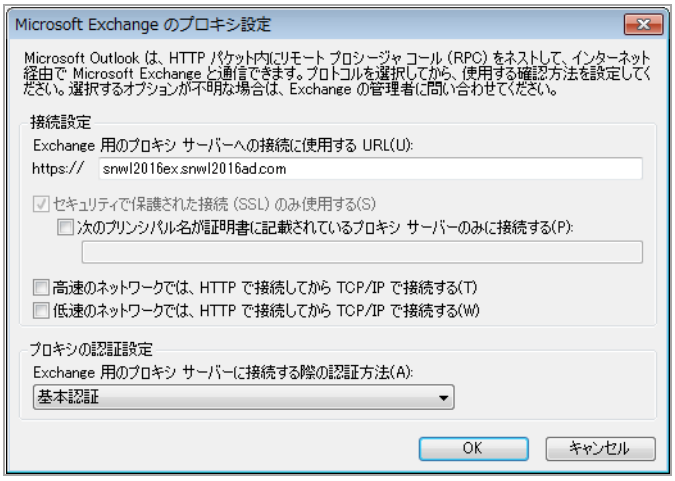
10 「接続」タブの「Outlook Anywhere」セクションで「**HTTP を使用して Microsoft Exchange に接続する**」をオンにします。



11 次に、「**Exchange のプロキシ設定**」を選択します。

12 「Microsoft Exchange のプロキシ設定」画面で、「**Exchange用のプロキシ サーバーへの接続に使用する URL**」フィールドに Outlook Anywhere ポータルのホスト名を指定します。

13 ドロップダウン リストからプロキシ認証設定を選択します。Secure Mobile Access 認証が有効な場合は、「**基本認証**」を選択します。



14 「**OK**」を選択して設定を保存し、Microsoft Outlook を終了します。

15 Microsoft Outlook を起動して新しいセッションを開始します。Outlook Anywhere ポータルにアクセスすると、ログ メッセージが生成されます。

メモ：Secure Mobile Access ポータルの認証制御が有効な場合は、基本認証のみをサポートできます。Outlook Anywhere 用の Exchange サーバで、必ず「**基本認証**」を選択してください。Secure Mobile Access の認証制御が無効な場合は、その他の認証方式がサポートされます。

メモ：Exchange Server のセキュリティを向上するため、匿名 Outlook Anywhere アクセスはサポートされていません。

ポータル > ドメイン

このセクションでは、「**ポータル > ドメイン**」ページの概要と、このページで実行できる設定タスクについて説明します。

「ポータル > ドメイン」の概要

「**ポータル > ドメイン**」ページでは、以下の設定を含み、ドメインの追加および設定ができます。

- 認証種別 (ローカル ユーザ データベース、アクティブ ディレクトリ、LDAP、または RADIUS)

- ドメイン名
- ポータル名
- グループ (アクティブ ディレクトリ、RADIUS) または組織単位 (LDAP) のサポート (オプション)
- クライアント デジタル証明書の要求 (オプション)
- ワンタイム パスワード (オプション)

「ポータル > ドメイン」ページ

ドメイン テーブルの参照

設定されたすべてのドメインは、「**ポータル > ドメイン**」ウィンドウ内のテーブルにリストされます。ドメインは、作成された順番でリストされます。「**ドメイン名**」列ヘッダの隣の上/下の矢印を選択することにより、順番を逆にできます。

ドメインの削除

ドメインを削除するには:

1 「**ポータル > ドメイン**」にナビゲートします。

2 テーブル内で、削除したいドメインと同じ行の削除アイコンを選択します。

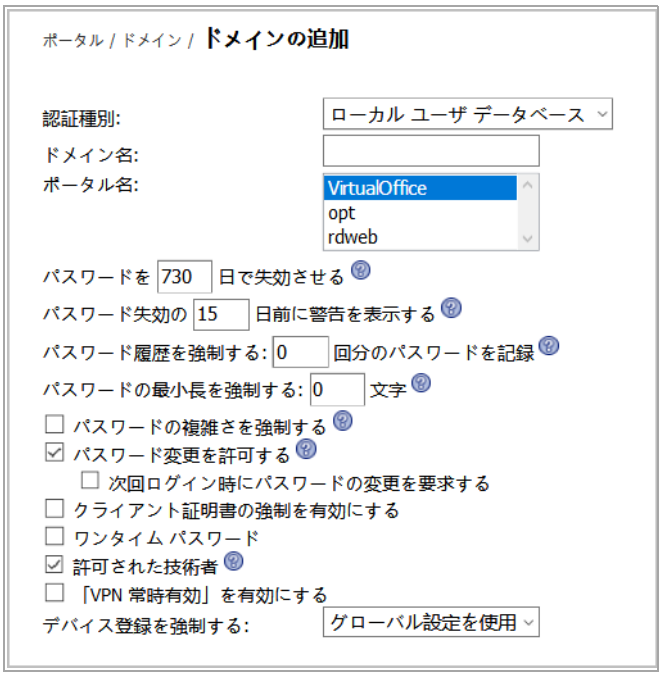
3 確認のダイアログ ボックスで、「**OK**」を選択します。

SMA/SRA 装置が更新されると、削除されたドメインはこのテーブルに表示されなくなります。

メモ：既定の「**LocalDomain**」ドメインは削除できません。

ドメインの追加と編集

「**ポータル > ドメイン**」ページから、新しいドメインの追加と既存のドメインの編集ができます。ドメインを追加するには、「**ドメインの追加**」を選択してドメインの追加ウィンドウを表示します。



既存のドメインを編集するには、編集したいドメインの右側の「**設定**」アイコンを選択します。

インターフェースには、ドメインの追加と編集の両方で、同じフィールドがありますが、既存のドメインの編集時には、「**認証種別**」と「**ドメイン名**」フィールドは変更できません。

メモ：新しいポータル ドメインを追加した後で、そのドメインのユーザ グループ設定を「**ユーザ > ローカル グループ**」ページで設定します。グループを設定する手順については、ユーザ > ローカル グループ (440 ページ) を参照してください。

アクセス ポリシーを作成するには、まず認証ドメインを作成しなければなりません。既定では、*LocalDomain* 認証ドメインが既に定義されています。LocalDomain ドメインは、内部ユーザ データベースです。リモート認証サーバに対する認証を要求する追加ドメインを作成することもできます。SMA/SRA 装置は、内部ユーザ データベース認証のほかに、RADIUS、LDAP、アクティブ ディレクトリ、およびデジタル証明書の認証をサポートしています。

メモ：ドメインにポータルを適用するには、新しいドメインを追加し、「**ドメインの追加**」ウィンドウの「ポータル名」ドロップダウン リストからポータルを選択します。選択したポータルは、新しいドメインのすべてのユーザに適用されます。ドメインの選択は、選択したポータルのログイン ページに表示されます。ログイン時に、ドメインは大文字と小文字を区別します。

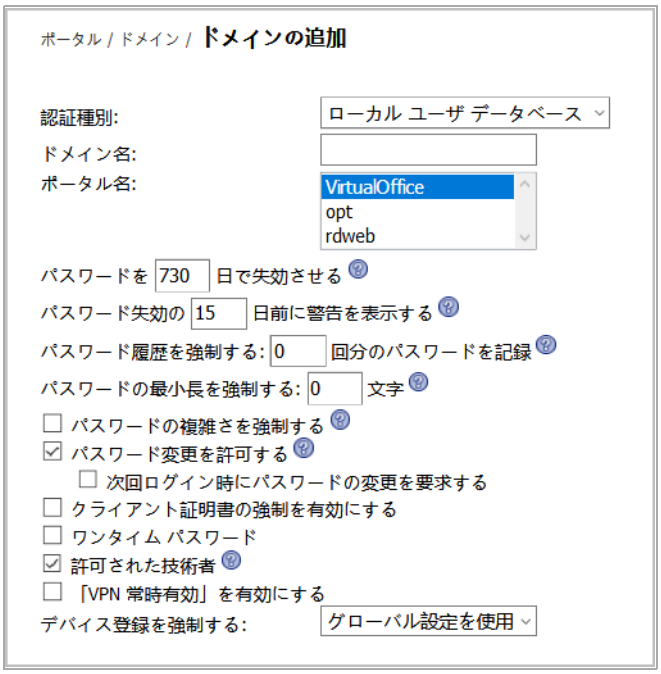
SMA/SRA 装置に保管されているユーザ名とパスワードを使ってユーザを認証する複数のドメインを作成することができます。こうすることで、ユーザごとに異なるポータル (Secure Mobile Access ポータル ページなど) を表示できます。

SMA/SRA 装置の管理者アカウントを簡単に設定するために、ドメインにログインしたすべてのユーザに管理者アクセスを提供するドメインを作成できます。この種のドメインに対しては LDAP またはアクティブ ディレクトリ認証のどちらかを使います。

ローカル ユーザ認証を使用するドメインの追加と編集

ローカル データベース認証用のドメインを追加または編集するには:

1 「**ポータル > ドメイン**」ウィンドウにナビゲートし、「**ドメインの追加**」を選択、または編集するドメインの編集アイコンを選択します。「**ドメインの追加**」または、「**ドメインの編集**」ウィンドウが表示されます。



2 ドメインを追加する場合は、「**認証種別** 」ドロップダウン リストから「**ローカル ユーザ データベース**」を選択します。

3 ドメインを追加する場合は、「**ドメイン名**」フィールドに認証ドメインのわかりやすい名前を入力します(最大 24 文字)。これは、Secure Mobile Access ポータルにログインするためにユーザが選択するドメイン名です。

4 「**ポータル名**」フィールドでレイアウトの名前を選択します。他のレイアウトを「**ポータル > ポータル**」ページで追加定義することもできます。

5 ローカル データベースのユーザ種別で新しく作成されたすべてのドメインには、既定のパスワード有効期限の値が設定され、「有効期限の警告を表示する日数」オプションが 15 に設定されます。この設定は作成時に手動で変更できます。必要に応じて、ローカル ユーザ データベースのすべてのユーザに対し、設定された間隔で、または次回のログイン時に、必ずパスワードを変更するよう求めます。設定された間隔で必ずパスワードを変更させるには、「**パスワードを *x* 日で失効させる**」フィールドに失効間隔を入力します。次回のログイン時に必ずパスワードを変更させるには、「**次回ログイン時にパスワードの変更を要求する**」をオンにします。

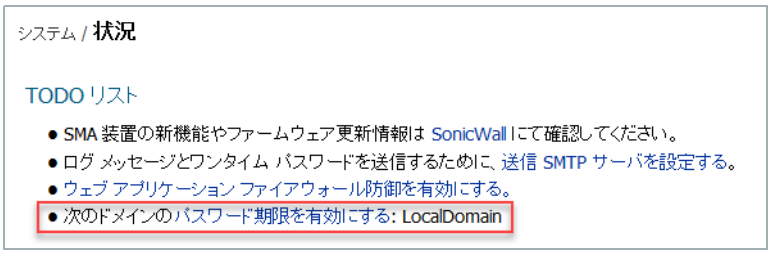
> ⓘ **メモ :** 特定のローカル ドメインのユーザにパスワードの変更を求めることもできます。「**ユーザ > ローカル ユーザ > 編集**」ページの「一般」タブを使用してください。

ドメインに具体的なパスワード有効期限の日数が設定されている場合は、ユーザ側の有効期限を 0 に設定する必要もあります。これは、ドメインの有効期限の設定を使用することを意味します。ドメイン設定の検出は、「ユーザの追加」要求の送信後、自動的に行われます。この設定も作成時に手動で変更できます。

既定のパスワード有効期限の値は 2 年 (730 日) です。

アップグレードを行っても、パスワード有効期限の既存の値はそのまま維持されます。

「**システム > 状況**」ページには、すべてのローカル データベース ドメインから有効期限の設定を行うことを推奨する通告が追加されました。この通告には、そうした設定が必要なドメインのリスト (上位 5 件) が付随しています。すべてのドメインについて既定のパスワード有効期限を設定した場合は、このメッセージ表示が解除されます。



6 パスワードの失効間隔を設定する場合は、「**パスワード失効の *x* 日前に警告を表示する**」フィールドに、失効の何日前にユーザに通知を送信するかを入力します。

これを設定し、パスワードの失効が近づくと、ユーザの「仮想オフィス」ページ、または管理者の管理コンソールに、パスワード失効までの日数を示す通知が表示されます。通知とともに、パスワードを変更する画面へのリンクも表示されます。

7 必要に応じて、古いパスワードをもう一度使用できるようになるまで、ユーザ アカウントに対して記憶される、重複しない新しいパスワードの数を、「**パスワード履歴を強制する: *x* 回分のパスワードを記録**」フィールドに追加します。0 ～ 10 の間の値を指定する必要があります。

8 必要に応じて、「**最小パスワード長**」として 1 ～ 14 の値を入力します。この値は、ユーザ パスワードとして許可される最小文字数になります。

9 必要に応じて、「**パスワードの複雑さを強制する**」をオンにします。このオプションをオンにすると、パスワードの設定時に次の 4 種類のうちの少なくとも *3* 種類の文字を含める必要があります。

- 英大文字 (A ～ Z)
- 英小文字 (a ～ z)
- 10 進数 (0 ～ 9)
- アルファベット以外の文字 (!、$、#、% など)

10 必要に応じて、「**パスワード変更を許可する**」をオンにします。これにより、ユーザはアカウントを設定した後でパスワードを任意に変更できます。

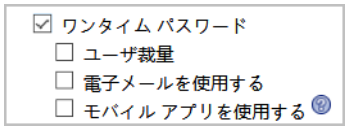
11 必要に応じて、「**次回のログイン時にパスワードの変更を要求する**」を選択します。これにより、ユーザーは次にログインするときパスワードを変更する必要があります。

12 必要に応じて、「**クライアント証明書の強制を有効にする**」をオンにして、ログインに際してクライアント証明書を要求するようにします。このチェックボックスをオンにすることによって、強力な相互認証のためにクライアント証明書を提示することをクライアントに要求します。さらに次の 2 つのフィールドが表示されます。

- **ユーザ名がクライアント証明書の一般名 (CN) と一致していることを確認する** - ユーザのアカウント名がクライアント証明書と一致することを要件とする場合は、このチェックボックスをオンにします。
- **サブジェクト内の部分 DN を確認する** - 次の変数を使ってクライアント証明書と一致する部分 DN を設定します。
  - ユーザ名: %USERNAME%

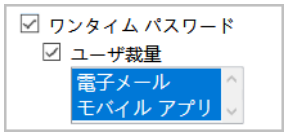
- ドメイン名: %USERDOMAIN%
- アクティブ ディレクトリ ユーザ名: %ADUSERNAME%
- ワイルドカード: %WILDCARD%

13 必要に応じて、「**ワンタイム パスワード**」をオンにしてワンタイム パスワード機能を有効にします。ドロップダウン リストが表示されます。ここで「**ユーザ裁量**」、「**電子メールを使用する**」、「**モバイル アプリを使用する**」を選択できます。



各オプションには次の機能があります。

- **ユーザ裁量** - このドメインのユーザは「**ポータル > ドメイン > ドメインの追加**」ページからワンタイム パスワード設定を編集できます。

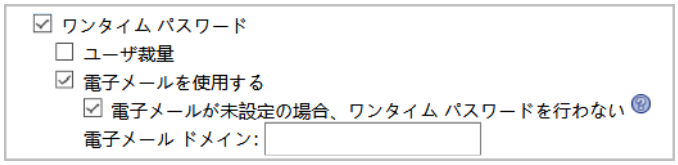


ユーザは、以下のワンタイム パスワード方式のどちらか一方または両方を選択できます。

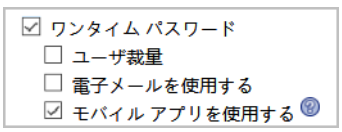
- 「**電子メールを使用する**」は、ユーザが「**電子メールを使用する**」を選択してこのワンタイム パスワード方式を有効化できるようにします。
- 「**モバイル アプリを使用する**」は、ユーザが「モバイル アプリを使用する」を選択してこのワンタイム パスワード方式を有効化できるようにします。

> **メモ**：両方の方式が有効化されている場合は、ユーザに対して既定の (優先) ワンタイム パスワード方式を指定します。

- **電子メールを使用する** - 必要に応じて「**電子メールを使用する**」を選択して、このワンタイム パスワード方式を有効化します。「**電子メール ドメイン:**」ウィンドウが表示されます。ここで、ワンタイム パスワードを送信する電子メール アドレスを入力できます。



- **モバイル アプリを使用する** - 必要に応じて「**モバイル アプリを使用する**」を選択します。これで、このワンタイム パスワード方式を有効化してユーザにワンタイム パスワードを強制的に使用させることができます。ユーザは Google Authenticator、Duo Mobile、またはその他の適合二段階認証サービスを利用できます。



14 「**許可された技術者**」を有効にすると、セキュア仮想アシストは技術担当者の役割としてこのドメインにログインできます。

15 「**VPN 常時有効を有効にする**」が有効化されている場合、ユーザはネットワークに中断されずにアクセスできます。

16 必要に応じて「**VPN 常時有効を有効にする**」を選択して「VPN 常時有効」機能を有効化します。ドロップダウン リストが表示されます。ここで、以下のいずれかを選択できます。

- **ユーザに切断を許可する。**この場合は、「**電子メール ドメイン:**」ウィンドウにドメインを入力します。
- **VPN が接続に失敗した場合にネットワークへのアクセスを許可する。**
- **信頼済みネットワークで VPN に接続しない。**

17 「**デバイス登録を強制する**」ドロップダウン メニューから以下のいずれかのオプションを選択します。

- このドメインにグローバル設定を適用するには「**グローバル設定を使用する**」を選択します。
- グローバル設定に関係なく、この機能を有効にするには、「**有効**」を選択します。
- グローバル設定に関係なく、この機能を無効にするには、「**無効**」を選択します。

18 「**適用**」を選択して設定を更新します。ドメインが追加されると、「**ポータル > ドメイン**」ページのテーブルにそのドメインが追加されます。

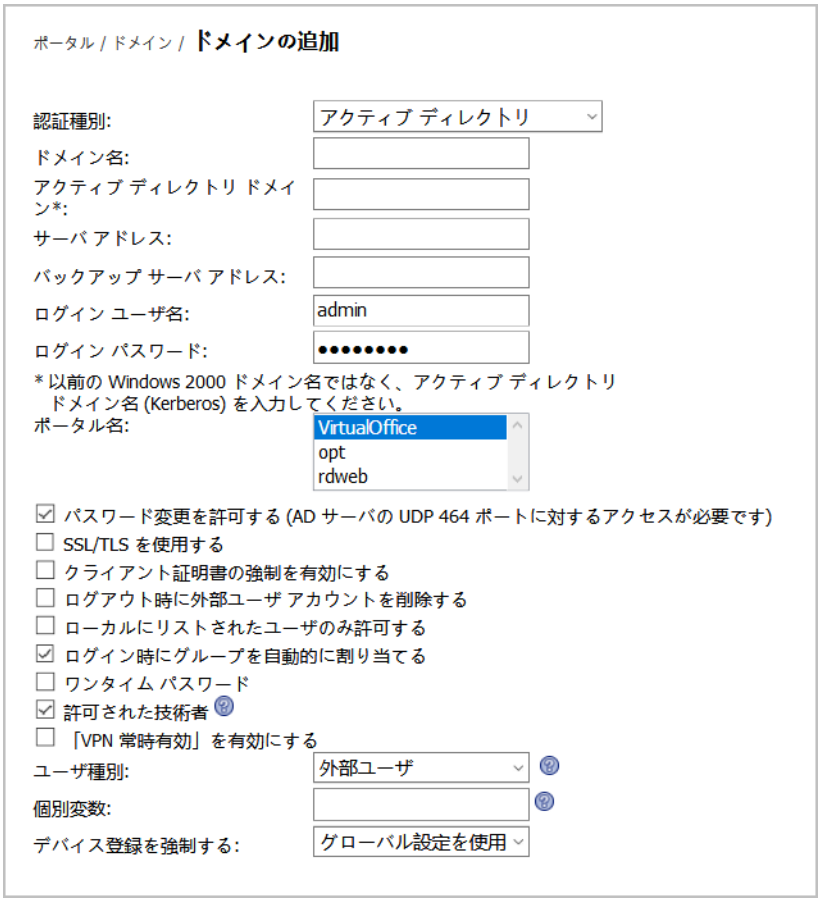
アクティブ ディレクトリ認証を使用するドメインの追加と編集

Windows アクティブ ディレクトリ認証を設定するには:

1 「**ドメインの追加**」ボタンを選択、または編集するドメインの編集アイコンを選択します。「**ドメインの追加**」または、「**ドメインの編集**」ウィンドウが表示されます。

> **メモ**：あらゆる認証方法の中でも、アクティブ ディレクトリ認証が、クロック スキュー、つまり SMA/SRA 装置とアクティブ ディレクトリ サーバとの時間のずれに最も敏感です。アクティブ ディレクトリを使って認証できない場合は、アクティブ ディレクトリのトラブルシューティング (196 ページ) を参照してください。

2 ドメインを追加する場合は、「**認証種別**」ドロップダウン リストから「**アクティブ ディレクトリ**」を選択します。アクティブ ディレクトリ設定フィールドが表示されます。



3 ドメインを追加する場合は、「**ドメイン名**」フィールドに認証ドメインの説明的な名前を入力します。これは、SMA/SRA 装置ポータルにログインするためにユーザが選択するドメイン名です。これは、ネットワーク設定に応じて、「**サーバ アドレス**」フィールドまたは「**アクティブ ディレクトリ ドメイン**」フィールドと同じ値でも構いません。

4 「**アクティブ ディレクトリ ドメイン**」フィールドにアクティブ ディレクトリ ドメイン名を入力します。

5 「**サーバ アドレス**」フィールドに、アクティブ ディレクトリ サーバの IP アドレスまたはホストとドメイン名を入力します。

6 「**バックアップ サーバ アドレス**」フィールドに、バックアップ サーバの IP アドレスまたはホストとドメイン名を入力します。

7 ログイン用のユーザ名を「**ログイン ユーザ名**」フィールドに入力します。

8 ログイン用のパスワードを「**ログイン パスワード**」フィールドに入力します。

9 必要に応じて、「**パスワード変更を許可する**」をオンにします。この機能を有効にすると、ユーザが仮想オフィス ポータルのページの上部にある「**オプション**」を選択することで自分のパスワードを変更できるようになります。ユーザは新しいパスワードと共に古いパスワードを入力し、新しく選択したパスワードの再確認を行う必要があります。

10 必要に応じて、「**SSL/TLS を使用する**」をオンにします。このオプションを選択すると、アクティブ ディレクトリのパスワード交換で必要な SSL/TLS 暗号化を使用できます。このチェックボックスは、アクティブ ディレクトリ認証を使用したドメインの設定時に有効にする必要があります。

11 必要に応じて、「**クライアント証明書の強制を有効にする**」をオンにして、ログインに際してクライアント証明書を要求するようにします。このチェックボックスをオンにすることによって、強力な相互認証のためにクライアント証明書を提示することをクライアントに要求します。さらに次の 2 つのフィールドが表示されます。

- **ユーザ名がクライアント証明書の一般名 (CN) と一致していることを確認する** - ユーザのアカウント名がクライアント証明書と一致することを要件とする場合は、このチェックボックスをオンにします。
- **サブジェクト内の部分 DN を確認する** - 次の変数を使ってクライアント証明書と一致する部分 DN を設定します。
  - ユーザ名: %USERNAME%
  - ドメイン名: %USERDOMAIN%
  - アクティブ ディレクトリ ユーザ名: %ADUSERNAME%
  - ワイルドカード: %WILDCARD%

12 ドメイン アカウントにログインしなかったユーザをログアウト後に削除するには、「**ログアウト時に外部ユーザ アカウントを削除する**」をオンにします。

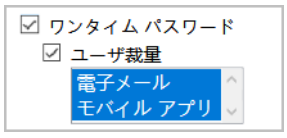
13 「**ローカルにリストされたユーザのみ許可する**」をオンにして、アクティブ ディレクトリにローカル レコードを持つユーザのみにログインを許可します。

14 「**ログイン時にグループを自動的に割り当てる**」をオンにして、ユーザをログイン時にグループに割り当てるようにします。

アクティブ ディレクトリ ドメインにログインするユーザは、外部 AD グループ メンバーシップに基づいて、リアルタイムで Secure Mobile Access グループに自動的に割り当てられます。ユーザの外部グループ メンバーシップが変更された場合は、Secure Mobile Access グループ メンバーシップが外部グループ メンバーシップに対応するように自動的に変更されます。

15 オプションで、ワンタイム パスワード機能を有効にするには、「**ワンタイム パスワード**」をオンにします。ドロップダウン リストが表示されます。ここで、「**ユーザ裁量**」、「**電子メールを使用する**」、「**モバイル アプリを使用する**」を選択できます。各オプションには次の機能があります。

- **ユーザ裁量** - このドメインのユーザは「**ポータル > ドメイン > ドメインの追加**」ページからワンタイム パスワード設定を編集できます。

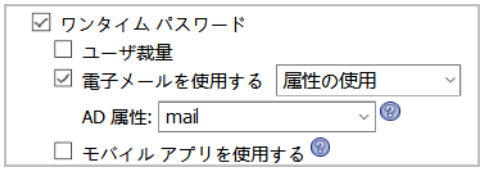


ユーザは、以下のワンタイム パスワード方式のどちらか一方または両方を選択できます。

- 「**電子メールを使用する**」は、ユーザが「**電子メールを使用する**」を選択してこのワンタイム パスワード方式を有効化できるようにします。
- 「**モバイル アプリを使用する**」は、ユーザが「モバイル アプリを使用する」を選択してこのワンタイム パスワード方式を有効化できるようにします。

> **メモ**：両方の方式が有効化されている場合は、ユーザに対して既定の (優先) ワンタイム パスワード方式を指定します。

- **電子メールを使用する** - 必要に応じて「**電子メールを使用する**」を選択して「**属性の使用**」または「**AD 属性**」をドロップダウン メニューから選択します。



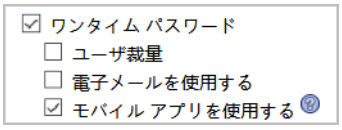
  - 「**AD 属性**」を選択し、ドロップダウン メニューから以下のいずれかの AD 属性を選択します。
    - **mail** - ユーザが「**電子メールを使用する**」を選択してこのワンタイム パスワード方式を有効化できるようにします。

      メモ： mail 属性は、有効な電子メール アドレスが含まれている場合にのみ使用できます。

    - **mobile** - ユーザが「**モバイル**」を選択してこのワンタイム パスワード方式を有効化できるようにします。

      メモ: 書式付きでない生の電話番号は使用できませんが、SMS 電子メールアドレスは使用できます。

    - **pager** - ユーザが「**ポケベル**」を選択してこのワンタイム パスワード方式を有効化できるようにします。
    - **userPrincipalName** - ユーザが「**ユーザ プリンシパル名**」を選択してこのワンタイム パスワード方式を有効化できるようにします。
    - **custom** - ユーザが「**個別**」を選択してこのワンタイム パスワード方式をカスタマイズできるようにします。
  - 「**ドメイン名を使用する**」を選択します。
- **モバイル アプリを使用する** - 必要に応じて「**モバイル アプリを使用する**」を選択します。これで、このワンタイム パスワード方式を有効化してユーザにワンタイム パスワードを強制的に使用させることができます。ユーザは Google Authenticator、Duo Mobile、またはその他の適合二段階認証サービスを利用できます。



16 「**ワンタイム パスワード**」ドロップダウン リストで「**設定する場合**」または「**全てのユーザに必要**」を選択した場合は、アクティブ ディレクトリの「**AD 電子メール属性**」ドロップダウン リストが表示され、そこで「**mail**」、「**mobile**」、「**pager**」、「**userPrincipalName**」、または「**個別**」を選択できます。各オプションには次の機能があります。

- **mail** - AD サーバが mail 属性を使って電子メール アドレスを保存するように設定されている場合は、「**mail**」を選択します。
- **mobile** または **pager** - AD サーバが mobile 属性または pager 属性を使ってそれらの番号を保存するように設定されている場合は、それぞれ「mobile」、「pager」を選択します。処理されていない番号は使えませんが、SMS アドレスは使えます。
- **userPrincipalName** - AD サーバが userPrincipalName 属性を使って電子メール アドレスを保存するように設定されている場合は、「**userPrincipalName**」を選択します。

- **個別** - AD サーバが個別属性を使って電子メール アドレスを保存するように設定されている場合は、「**個別**」を選択します。ユーザに指定された属性が見つからない場合は、個別のユーザ ポリシーの設定で割り当てられた電子メール アドレスが使われます。「**個別**」を選択すると、「**個別属性**」フィールドが表示されます。AD サーバで電子メール アドレスの保存に使用される個別属性を入力します。ユーザに指定された属性が見つからない場合は、個別のポリシーの設定で割り当てられた電子メール アドレスが使われます。

「**ドメイン名を使用**」を選択すると、ドロップダウン リストの後に「**電子メール ドメイン**」フィールドが表示されます。ワンタイム パスワード電子メールの送信先となるドメイン名 (例えば、abc.com) を入力してください。

17 「**許可された技術者**」を有効にすると、セキュア仮想アシストは技術担当者の役割としてこのドメインにログインできます。

18 「**ユーザ種別**」ドロップダウン リストからユーザの種別を選択します。このドメインを通してログインするすべてのユーザは、このユーザ種別として扱われます。選択肢は既に定義されたユーザ種別に依存します。いくつかの利用可能な選択肢は、以下の通りです。

- **外部ユーザ** - このドメインにログインするユーザは、管理権限の無い一般ユーザとして扱われます。
- **外部管理者** - このドメインにログインするユーザは、ローカルの Secure Mobile Access 管理資格のある管理者として扱われます。これらのユーザには、管理者ログイン ページが表示されます。

  このオプションにより Secure Mobile Access 管理者は、ドメインにログインするすべてのユーザに Secure Mobile Access 管理権限を許可するドメインを設定することが可能です。

  SonicWall Inc. は、正しいグループ内のユーザにのみ管理アクセスを許可するフィルタを追加することを推奨します。これは、「**ユーザ > ローカル グループ**」ページ上でドメインを編集することで可能です。
- **読み込み専用管理者** - このドメインにログインするユーザは、読み込み専用管理者として扱われ、すべての情報と設定を参照できますが、設定の変更は一切適用できません。これらのユーザには、管理者ログイン ページが表示されます。

19 「**適用**」を選択して設定を更新します。ドメインが追加されると、「**ポータル > ドメイン**」ページのテーブルにそのドメインが追加されます。

アクティブ ディレクトリのトラブルシューティング

アクティブ ディレクトリを使って接続できない場合は、以下の設定を確認してください。

- アクティブ ディレクトリ サーバの時間設定と SMA/SRA 装置の時間設定は同期していなければなりません。アクティブ ディレクトリがクライアントを認証する場合に使う Kerberos 認証では、Windows サーバとクライアント (SMA/SRA 装置) との時間のずれが最大 15 分まで認められています。この問題を解決する一番簡単な方法は、ウェブ ベースの Secure Mobile Access 管理インターフェースの「**システム > 時間**」ページでネットワーク タイム プロトコルを設定し、さらにアクティブ ディレクトリ サーバの時間設定が正しいかどうかを確認することです。
- ウィンドウズ サーバがアクティブ ディレクトリ認証に対応していることを確認します。

LDAP 認証を使用するドメインの追加と編集

LDAP 認証を使用するドメインを設定するには:

1 「**ドメインの追加**」ボタンを選択、または編集するドメインの編集アイコンを選択します。「**ドメインの追加**」または、「**ドメインの編集**」ウィンドウが表示されます。

2 ドメインを追加する場合は、「**認証種別**」メニューから「**LDAP**」を選択します。LDAP ドメイン設定フィールドが表示されます。

3 ドメインを追加する場合は、「**ドメイン名**」フィールドに認証ドメインの説明的な名前を入力します。これは、SMA/SRA 装置のユーザ ポータルにログインするためにユーザが選択するドメイン名です。「プライマリ LDAP サーバ」の「**サーバ アドレス**」フィールドと同じ値でも構いません。

4 「**LDAP BaseDN**」フィールドに LDAP 問い合わせの検索ベースを入力します。検索ベースの文字列としては、例えば **CN=Users**, **DC=yourdomain**, **DC=com** などがあります。

> ⓘ **ヒント**：単一のドメインに対して複数の OU を設定することが可能です。それには、「**LDAP BaseDN**」フィールドで各 OU を別個の行に入力します。さらに、このフィールドに追加した OU にサブ OU がある場合には、自動的に含まれます。

メモ :「**LDAP BaseDN**」フィールドに入力する場合は、引用符 (“”) を省いてください。

5 「**サーバ アドレス**」フィールドに、プライマリ LDAP サーバの IP アドレスまたはドメイン名を入力します。

6 「**ログイン ユーザ名**」フィールドと「**ログイン パスワード**」フィールドに、プライマリ サーバの制御を委譲されたユーザの共通名とパスワードを入力します。

メモ :「**ログイン ユーザ名**」と「**ログイン パスワード**」を入力すると、SMA/SRA 装置と LDAP ツリーはこれらの資格情報でバインドされ、ユーザは sAMAccountName を使ってログインできます。

7 必要に応じて、「バックアップ LDAP サーバ」セクションの下の「**サーバ アドレス**」フィールドに、バックアップ LDAP サーバの IP アドレスまたはドメイン名を入力します。

8 必要に応じて、「バックアップ LDAP サーバ」セクションの下の「**ログイン ユーザ名**」フィールドと「**ログイン パスワード**」フィールドに、バックアップ サーバの制御を委譲されたユーザの共通名とパスワードを入力します。

9 「**ポータル名**」フィールドにレイアウトの名前を入力します。他のレイアウトを「**ポータル > ポータル**」ページで追加定義することもできます。

10 必要に応じて、「**パスワード変更を許可する (LDAP サーバに許可された場合)**」をオンにします。このオプションは、LDAP サーバ側で許可されている場合、Secure Mobile Access セッション中にユーザが LDAP パスワードを変更できるようにします。

11 必要に応じて、「**SSL/TLS を使用する**」をオンにします。このオプションは、LDAP パスワード交換で SSL/TLS 暗号化を使うことを許可します。すべての LDAP サーバで SSL/TLS の設定がされているわけではないので、このオプションは既定で無効です。

12 必要に応じて、「**クライアント証明書の強制を有効にする**」をオンにして、ログインに際してクライアント証明書を要求するようにします。このチェックボックスをオンにすることによって、強力な相互認証のためにクライアント証明書を提示することをクライアントに要求します。さらに次の 2 つのフィールドが表示されます。

- **ユーザ名がクライアント証明書の一般名 (CN) と一致していることを確認する** - ユーザのアカウント名がクライアント証明書と一致することを要件とする場合は、このチェックボックスをオンにします。
- **サブジェクト内の部分 DN を確認する** - 次の変数を使ってクライアント証明書と一致する部分 DN を設定します。
  - ユーザ名: %USERNAME%
  - ドメイン名: %USERDOMAIN%
  - アクティブ ディレクトリ ユーザ名: %ADUSERNAME%
  - ワイルドカード: %WILDCARD%

13 「**ログイン時にグループを自動的に割り当てる**」をオンにして、ユーザをログイン時にグループに割り当てるようにします。

LDAP ドメインにログインするユーザは、外部 LDAP 属性に基づいて、リアルタイムで Secure Mobile Access グループに自動的に割り当てられます。ユーザの外部グループ メンバーシップが変更された場合は、Secure Mobile Access グループ メンバーシップが外部グループ メンバーシップに対応するように自動的に変更されます。

14 オプションで、ワンタイム パスワード機能を有効にするには、「**ワンタイム パスワード**」をオンにします。表示されるドロップダウン リストから「**設定する場合**」、「**全てのユーザに必要**」、または「**ドメイン名を使用**」を選択できます。各オプションには次の機能があります。

- **設定する場合** - ワンタイム パスワード電子メール アドレスが設定されているユーザだけがワンタイム パスワード機能を使用します。
- **全てのユーザに必要** - すべてのユーザがワンタイム パスワード機能を使わなければなりません。ワンタイム パスワード電子メール アドレスが設定されていないユーザはログインを許可されません。
- **ドメイン名を使用** - ドメインに所属するユーザはワンタイム パスワード機能を使用します。ドメイン内のすべてのユーザのワンタイム パスワード電子メールが username@domain.com に送信されます。

「**ワンタイム パスワード**」ドロップダウン リストで「**設定する場合**」または「**全てのユーザに必要**」を選択すると、「**LDAP の電子メール属性**」ドロップダウン リストが表示され、「**mail**」、「**userPrincipalName**」、または「**個別**」を選択できます。各オプションには次の機能があります。

- **mail** - LDAP サーバが“mail”属性を使って電子メール アドレスを保存するように設定されている場合は、「**mail**」を選択します。
- **mobile** または **pager** - AD サーバが mobile 属性または pager 属性を使ってそれらの番号を保存するように設定されている場合は、それぞれ「mobile」、「pager」を選択します。処理されていない番号は使えませんが、SMS アドレスは使えます。
- **userPrincipalName** - LDAP サーバが“userPrincipalName”属性を使って電子メール アドレスを保存するように設定されている場合は、「**userPrincipalName**」を選択します。
- **個別** - LDAP サーバが個別属性を使って電子メール アドレスを保存するように設定されている場合は、「**個別**」を選択します。ユーザに指定された属性が見つからない場合は、個別のユーザ ポリシーの設定で割り当てられた電子メール アドレスが使われます。「**個別**」を選択すると、「**個別属性**」フィールドが表示されます。LDAP サーバで電子メール アドレスの保存に使用される個別属性を入力します。ユーザに指定された属性が見つからない場合は、個別のポリシーの設定で割り当てられた電子メール アドレスが使われます。

「**ワンタイム パスワード**」ドロップダウン リストで「**ドメイン名を使用**」を選択すると、「**LDAP の電子メール属性**」ドロップダウン リストではなく「**電子メール ドメイン**」フィールドが表示されます。ワンタイム パスワード電子メールの送信先となるドメイン名 (例えば、abc.com) を入力してください。

15 「**ユーザ種別**」ドロップダウン リストからユーザの種別を選択します。このドメインを通してログインするすべてのユーザは、このユーザ種別として扱われます。選択肢は既に定義されたユーザ種別に依存します。いくつかの利用可能な選択肢は、以下の通りです。

- **外部ユーザ** - このドメインにログインするユーザは、管理権限の無い一般ユーザとして扱われます。
- **外部管理者** - このドメインにログインするユーザは、ローカルの Secure Mobile Access 管理資格のある管理者として扱われます。これらのユーザには、管理者ログイン ページが表示されます。

  このオプションにより Secure Mobile Access 管理者は、ドメインにログインするすべてのユーザに Secure Mobile Access 管理権限を許可するドメインを設定することが可能です。

  SonicWall Inc. は、正しいグループ内のユーザにのみ管理アクセスを許可するフィルタを追加することを推奨します。これは、「**ユーザ > ローカル グループ**」ページ上でドメインを編集することで可能です。
- **読み込み専用管理者** - このドメインにログインするユーザは、読み込み専用管理者として扱われ、すべての情報と設定を参照できますが、設定の変更は一切適用できません。これらのユーザには、管理者ログイン ページが表示されます。

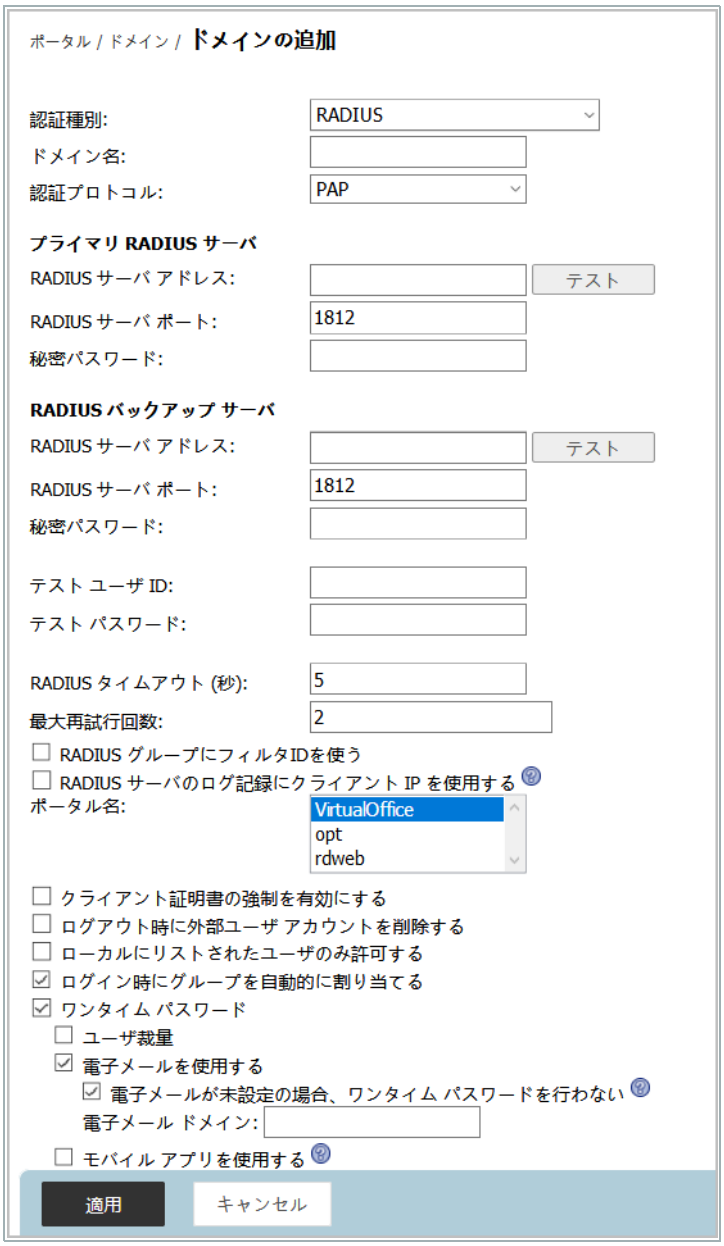
16 「**適用**」を選択して設定を更新します。ドメインが追加されると、「**ポータル > ドメイン**」ページのテーブルにそのドメインが追加されます。

RADIUS 認証を使用するドメインの追加と編集

RADIUS 認証を使用するドメインを設定するには:

1 「**ポータル > ドメイン**」ページで、「**ドメインの追加**」ボタンを選択、または編集するドメインの編集アイコンを選択します。「**ドメインの追加**」または、「**ドメインの編集**」ウィンドウが表示されます。

2 ドメインを追加する場合は、「**認証種別**」メニューから「**RADIUS**」を選択します。「**RADIUS の設定**」フィールドが表示されます。



3 ドメインを追加する場合は、「**ドメイン名**」フィールドに認証ドメインの説明的な名前を入力します。これは、Secure Mobile Access ポータルにログインするためにユーザが選択するドメイン名です。

4 RADIUS サーバの**認証プロトコル**を適切に選択します。**PAP**、**CHAP**、**MSCHAP**、または **MSCHAPV2** のいずれかを選択できます。

5 「**プライマリ RADIUS サーバ**」の「**RADIUS サーバ アドレス**」フィールドに、RADIUS サーバの IP アドレスまたはドメイン名を入力します。

6 「**RADIUS サーバ ポート**」フィールドに、RADIUS サーバ ポートを入力します。

7 RADIUS 設定で要求される場合は、「**秘密パスワード**」フィールドに認証の秘密パスワードを入力します。

8 「**RADIUS バックアップサーバ**」の「**RADIUS サーバ アドレス**」フィールドに、バックアップ RADIUS サーバの IP アドレスまたはドメイン名を入力します。

9 「**RADIUS サーバ ポート**」フィールドに、バックアップ RADIUS サーバ ポートを入力します。

10 バックアップ RADIUS サーバで要求される場合は、「**秘密パスワード**」フィールドにバックアップ RADIUS サーバの認証の秘密パスワードを入力します。

11 「**テスト ユーザ ID**」フィールドにテスト ユーザ ID を入力します。

12 「**テスト パスワード**」フィールドにテスト パスワードを入力します。

13 RADIUS タイムアウトの数値 (秒) を「**RADIUS タイムアウト (秒)**」フィールドに入力します。

14 「**最大再試行回数**」フィールドに再試行の最大数を入力します。

15 RADIUS をグループ ベースのアクセスに使用する場合は、「**RADIUS グループにフィルタ ID を使う**」をオンにします。

16 必要に応じて、「**RADIUS サーバのログ記録にクライアント IP を使用する**」を選択して RADIUS ログで SMA IP アドレスの代わりにクライアント IP を使用します。

17 「**ポータル名**」ドロップダウン リストでレイアウトの名前を選択します。

18 RADIUS サーバの認証プロトコルとして MSCHAP または MSCHAPV2 を選択した場合は、「**パスワード変更を許可する**」をオンにすることができます。パスワード変更を許可する場合は、LAN Manager 認証も導入する必要があります。

19 必要に応じて、「**クライアント証明書の強制を有効にする**」をオンにして、ログインに際してクライアント証明書を要求するようにします。このチェックボックスをオンにすることによって、強力な相互認証のためにクライアント証明書を提示することをクライアントに要求します。さらに次の 2 つのフィールドが表示されます。

- **ユーザ名がクライアント証明書の一般名 (CN) と一致していることを確認する** - ユーザのアカウント名がクライアント証明書と一致することを要件とする場合は、このチェックボックスをオンにします。
- **サブジェクト内の部分 DN を確認する** - 次の変数を使ってクライアント証明書と一致する部分 DN を設定します。
    - ユーザ名: %USERNAME%
    - ドメイン名: %USERDOMAIN%
    - アクティブ ディレクトリ ユーザ名: %ADUSERNAME%
    - ワイルドカード: %WILDCARD%

20 ドメイン アカウントにログインしなかったユーザをログアウト後に削除するには、「**ログアウト時に外部ユーザ アカウントを削除する**」をオンにします。

21 「**ローカルにリストされたユーザのみ許可する**」を選択して、ローカルで構成したユーザのみを許可します。ただし、RADIUS による認証はまだ可能です。

22 「**ログイン時にグループを自動的に割り当てる**」をオンにして、ユーザをログイン時にグループに割り当てるようにします。

RADIUS ドメインにログインするユーザは、外部 RADIUS フィルタ ID に基づいて、リアルタイムで Secure Mobile Access グループに自動的に割り当てられます。ユーザの外部グループ メンバーシップが変更された場合は、Secure Mobile Access グループ メンバーシップが外部グループ メンバーシップに対応するように自動的に変更されます。

23 必要に応じて、「**ワンタイム パスワード**」をオンにしてワンタイム パスワード機能を有効にします。表示されるドロップダウン リストから「**設定する場合**」、「**全てのユーザに必要**」、または「**ドメイン名を使用**」を選択できます。各オプションには次の機能があります。

- **設定する場合** - ワンタイム パスワード電子メール アドレスが設定されているユーザだけがワンタイム パスワード機能を使用します。
- **全てのユーザに必要** - すべてのユーザがワンタイム パスワード機能を使わなければなりません。ワンタイム パスワード電子メール アドレスが設定されていないユーザはログインを許可されません。
- **ドメイン名を使用** - ドメインに所属するユーザはワンタイム パスワード機能を使用します。ドメイン内のすべてのユーザのワンタイム パスワード電子メールが username@domain.com に送信されます。

24 「**ドメイン名を使用**」を選択すると、ドロップダウン リストの後に「**電子メール ドメイン**」フィールドが表示されます。ワンタイム パスワード電子メールの送信先となるドメイン名 (例えば、abc.com) を入力してください。

25 「**許可された技術者**」をオンにすると、セキュア仮想アシストは技術担当者の役割としてこのドメインにログインできます。

26 必要に応じて「**VPN 常時有効**」を選択して中断のない VPN アクセスを許可します。さらに次の 3 つのフィールドが表示されます。

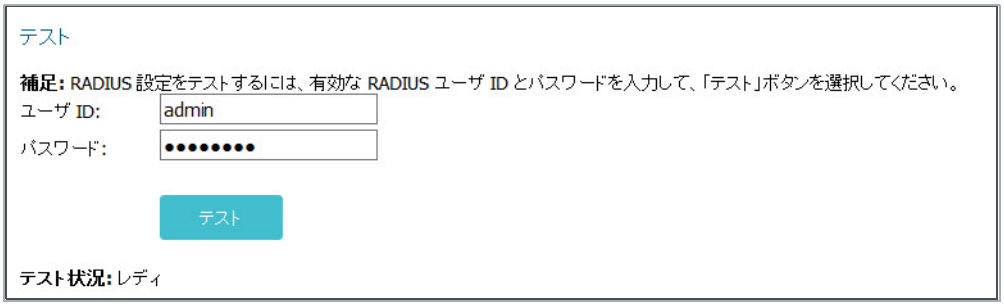
- **ユーザに切断を許可する。**この場合は、「**電子メール ドメイン:**」ウィンドウにドメインを入力します。
- **VPN が接続に失敗した場合にネットワークへのアクセスを許可する。**
- **信頼済みネットワークで VPN に接続しない。**

27 「デバイス登録を要求」ドロップダウン メニューからオプションを選択します。

- グローバル設定をドメインに適用するには、「**グローバル設定を使用する**」を選択します。
- グローバル設定に関係なく、この機能を有効にするには、「**有効化**」を選択します。
- グローバル設定に関係なく、この機能を無効化するには、「**無効化**」を選択します。

28 「**適用**」を選択して設定を更新します。ドメインが追加されると、「**ポータル > ドメイン**」ページのテーブルにそのドメインが追加されます。

29 追加した RADIUS ドメインの横にある「**設定**」を選択します。「**ドメインの編集**」ページの「**テスト**」タブが表示されます。



30 「**ユーザ ID**」フィールドに RADIUS ユーザ名を入力し、「**パスワード**」フィールドに RADIUS パスワードを入力します。

31 「**テスト**」を選択します。SMA/SRA 装置が RADIUS サーバに接続します。

32 「**サーバが応答しません**」というメッセージを受け取った場合は、ユーザ ID とパスワードをチェックし、「**一般**」タブを選択して RADIUS 設定を確認してください。テストを再度実行します。

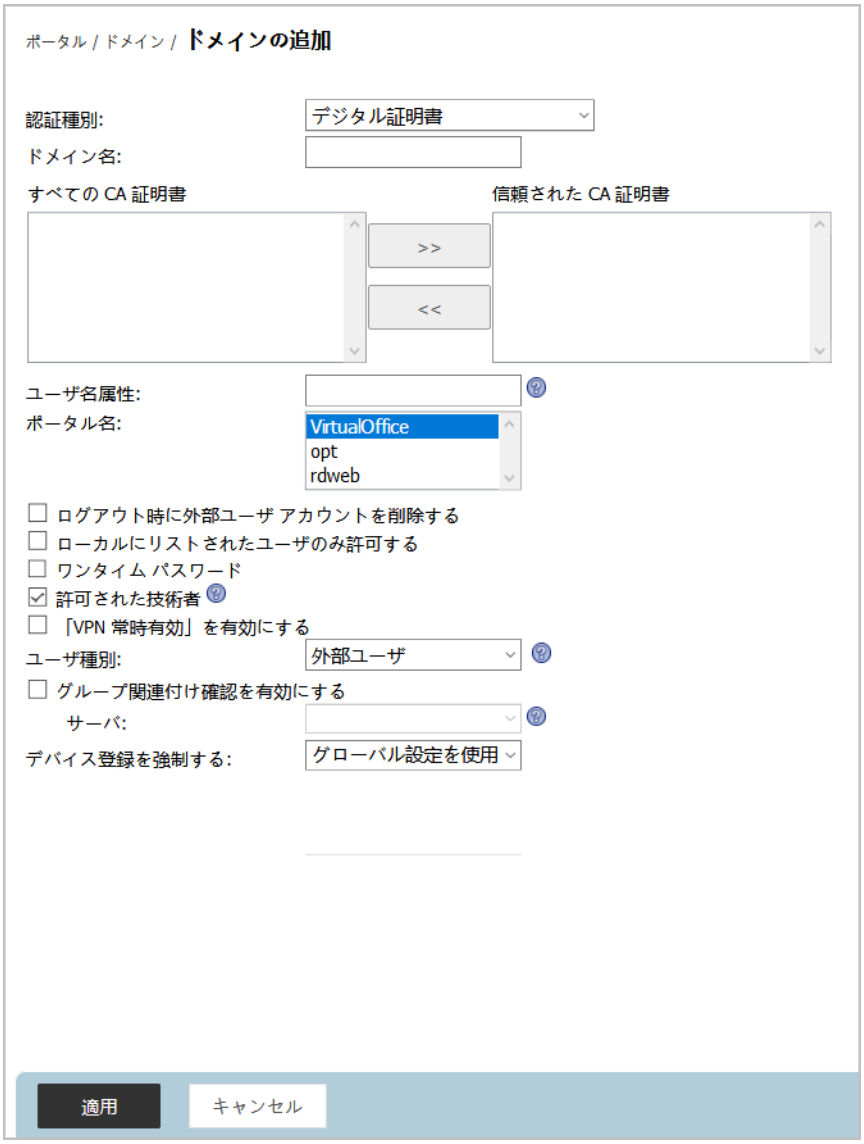
> ⓘ **メモ**：SMA/SRA 装置は、PAP 認証を使って、指定された RADIUS サーバに対する認証を試みます。通常、RADIUS サーバは、SMA/SRA 装置からの RADIUS クライアント接続を受け入れるように設定する必要があります。一般に、この接続の発信元は SMA/SRA 装置の X0 インターフェースの IP アドレスに見えます。設定の手順については、ご使用の RADIUS サーバのマニュアルを参照してください。

デジタル証明書を使用するドメインの追加と編集

デジタル証明書認証用のドメインを追加または編集するには:

1 「**ポータル > ドメイン**」ウィンドウを開き、「**ドメインの追加**」を選択するか、または編集するドメインの**設定**アイコンをクリックします。「**ドメインの追加**」または、「**ドメインの編集**」ウィンドウが表示されます。

2 ドメインを追加する場合は、「**認証種別**」メニューから「**デジタル証明書**」を選択します。「**デジタル証明書の設定**」フィールドが表示されます。



3 ドメインを追加する場合は、「**ドメイン名**」フィールドに認証ドメインの説明的な名前を入力します。これは、Secure Mobile Access ポータルにログインするためにユーザが選択するドメイン名です。

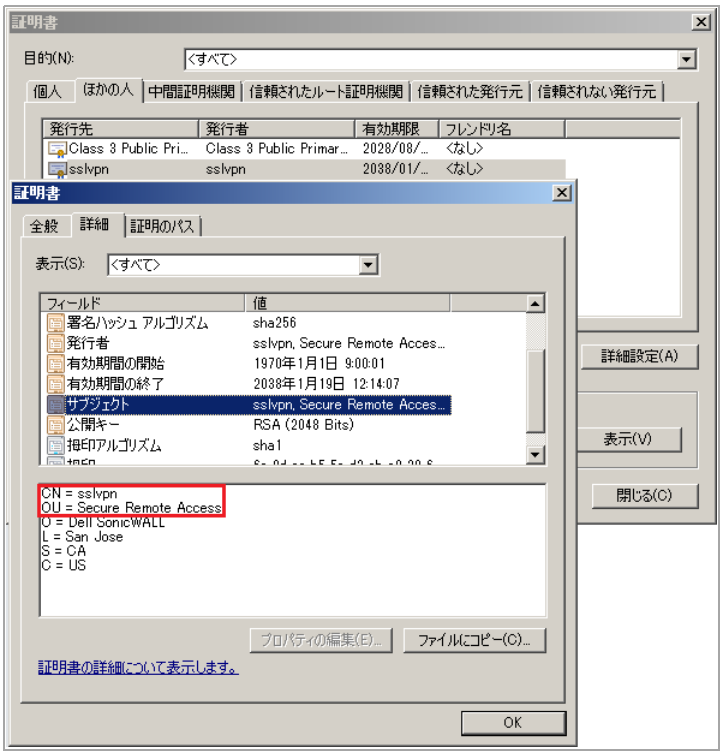
4 1 つ以上の証明書を「**すべての CA 証明書**」リストから選択して、「**信頼された CA 証明書**」リストに追加します。「すべての CA 証明書」リストには、システム証明書設定からインポートされた、SMA/SRA 装置で使用可能なすべての証明書が含まれています。

5 「**ユーザ名属性**」に「**CN**」と入力します。これにより、クライアント証明書の CN 属性がログイン ユーザ名として使用されます。

6 「**適用**」ボタンを選択して、変更内容を保存します。次に、クライアント証明書をウェブ ブラウザにインポートする必要があります。

クライアント証明書をインポートするには:

1 ウェブ ブラウザの設定の証明書の詳細に移動します。



2 CA ドメインを選択します。ダイアログ ウィンドウが表示されます。認証するクライアント証明書を選択します。「**OK**」を選択します。

クライアント証明書の CA が「信頼された CA 証明書」リスト上に存在する場合、認証は完了します。クライアント証明書が「信頼された CA 証明書」リストに含まれていない場合、アクセスは遮断され、エラー メッセージが表示されます。

3 次に、クライアント証明書ユーザを承認する必要があります。

クライアント証明書を承認するには:

1 「**ポータル > ドメイン**」ウィンドウを開き、編集するドメインの設定アイコンを選択します。

2 「**グループ関連付け確認を有効にする**」をオンにします。

3 ドロップダウン リストから使用可能ないずれかのドメインを選択し、**サーバ**として指定します。

4 「**適用**」を選択します。

メモ：アクティブ ディレクトリまたは LDAP サーバおよびドメインのみがサポートされています。

二段階認証の設定

二段階認証とは、2 つの個別の情報を要求して ID と権限を確立する認証方式です。二段階認証は、1 段階 (ユーザのパスワード) だけを要求する従来のパスワード認証より強力で、厳密です。

二段階認証の仕組みの詳細については、二段階認証の概要 (49 ページ) を参照してください。

SonicWall Inc. が実装している二段階認証は、2 台の別々の RADIUS 認証サーバを使うか、高度なユーザ認証で業界の先端をいく RSA および VASCO と提携しています。RSA を使用する場合は、RSA 認証マネージャ トークンと RSA SecurID トークンが必要です。VASCO を使用する場合は、VASCO IdentiKey と Digipass トークンが必要です。

二段階認証を設定するには、最初に RADIUS ドメインを設定する必要があります。詳しくは、RADIUS 認証を使用するドメインの追加と編集 (200 ページ) を参照してください。

以下のセクションでは、サポートされているサードパーティ認証サーバの設定方法を説明します。

- RSA Authentication Manager の設定 (207 ページ)
- VASCO IdentiKey ソリューションの設定 (211 ページ)

RSA Authentication Manager の設定

以下のセクションでは、RSA Authentication Manager バージョン 6.1 を設定して、SMA/SRA 装置で二段階認証を実行する手順を説明します。

- SMA/SRA 装置のエージェント ホスト レコードを追加する (207 ページ)
- SMA/SRA 装置を RADIUS クライアントとして追加する (208 ページ)
- 時刻と日付を設定する (209 ページ)
- トークンのインポートとユーザの追加 (209 ページ)

メモ：この設定手順は、RSA Authentication Manager バージョン 6.1 に固有のものです。別のバージョンの RSA Authentication Manager を使用している場合は、やや手順が異なります。

RSA ではなく VASCO を使用する場合は、VASCO IdentiKey ソリューションの設定 (211 ページ) を参照してください。

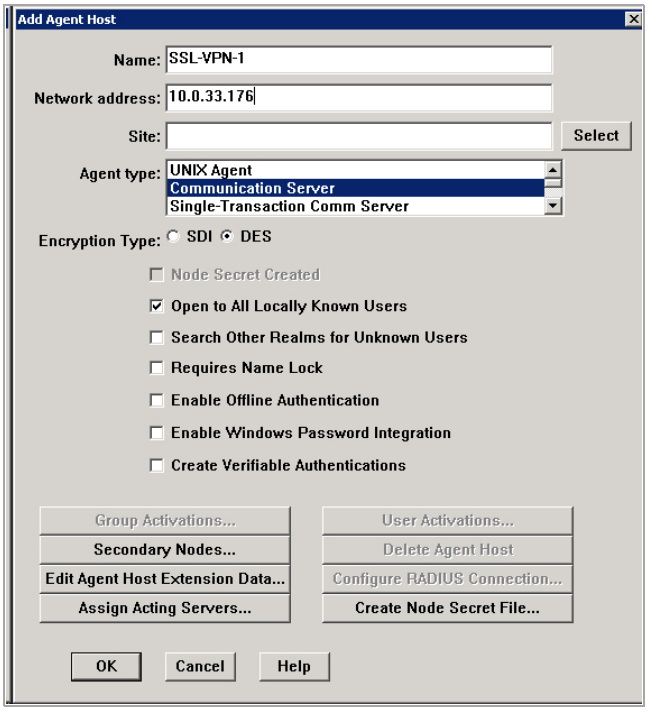
SMA/SRA 装置のエージェント ホスト レコードを追加する

SMA/SRA 装置と RSA Authentication Manager の接続を確立するには、エージェント ホスト レコードを RSA Authentication Manager のデータベースに追加する必要があります。エージェント ホスト レコードは、データベース内で SMA/SRA 装置を識別するための手段であり、通信と暗号に関する情報が含まれます。

SMA/SRA 装置のエージェント ホスト レコードを作成するには:

1 RSA Authentication Manager を起動します。

2 「**Agent Host (エージェント ホスト)**」メニューから「**Add Agent Host (エージェント ホストの追加)**」を選択します。「**Add Agent Host (エージェント ホストの追加)**」ウィンドウが表示されます。



3 SMA/SRA 装置のホスト名を「**Name (名前)**」フィールドに入力します。

4 SMA/SRA 装置の IP アドレスを「**Network address (ネットワーク アドレス)**」フィールドに入力します。

5 「**Agent type (エージェント種別)**」リストで「**Communication Server (通信サーバ)**」を選択します。

6 既定で、「**Enable Offline Authentication (オフライン認証を有効にする)**」オプションと「**Enable Windows Password Integration (ウィンドウズ パスワード統合を有効にする)**」オプションが有効になります。SonicWall Inc. は、「**Open to All Locally Known Users (すべてのローカルの既知ユーザに開放する)**」以外のすべてのオプションを無効にすることを推奨します。

7 「**OK**」を選択します。

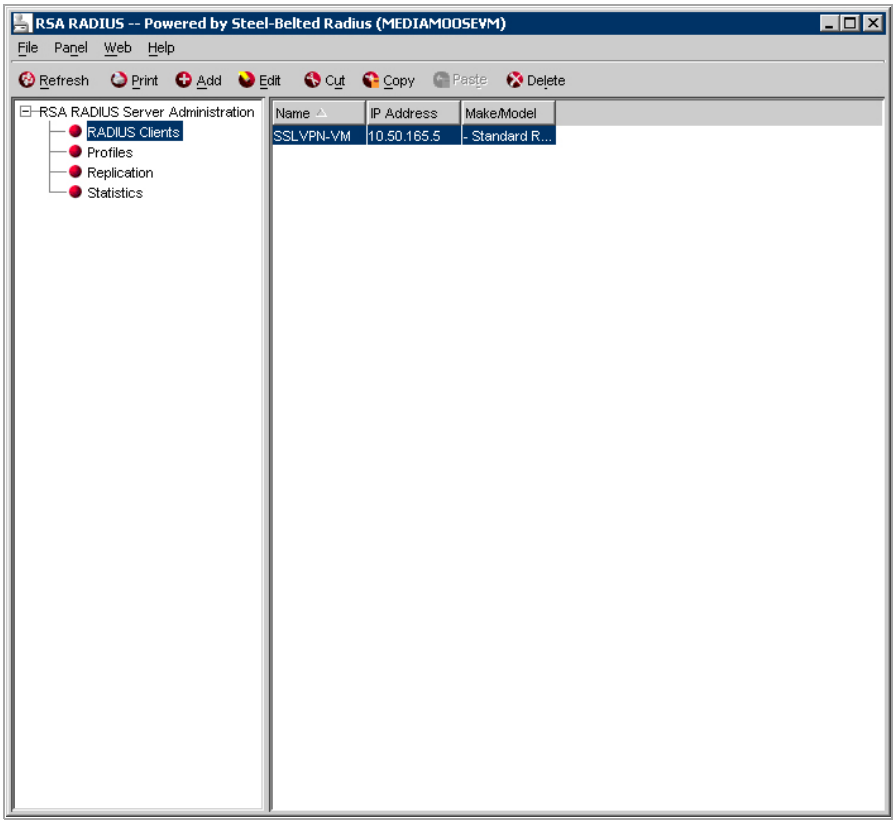
SMA/SRA 装置を RADIUS クライアントとして追加する

エージェント ホスト レコードを作成した後で、SMA/SRA 装置を RADIUS クライアントとして RSA Authentication Manager に追加する必要があります。

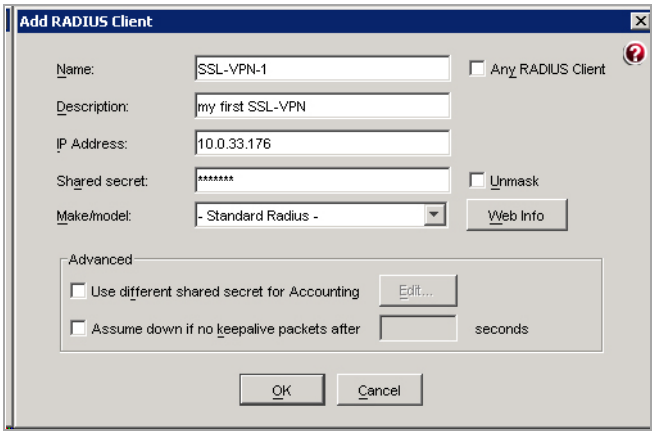
この設定を行うには、以下の手順に従います。

1 RSA Authentication Manager で、「**RADIUS**」メニューから「**Manage RADIUS Server (RADIUS サーバの管理)**」を選択します。**RSA RADIUS Manager (RSA RADIUS マネージャ)**が表示されます。

2 「**RSA RADIUS Server Administration (RSA RADIUS サーバ管理)**」ツリーを展開し、「**RADIUS Clients (RADIUS クライアント)**」を選択します。



3 「**Add (追加)**」を選択します。「**Add RADIUS Client (RADIUS クライアントの追加)**」ウィンドウが表示されます。



4 SMA/SRA 装置の説明的な名前を入力します。

5 SMA/SRA 装置の IP アドレスを「**IP Address (IP アドレス)**」フィールドに入力します。

6 SMA/SRA 装置で設定した共有鍵を「**Shared secret (共有鍵)**」フィールドに入力します。

7 「**OK**」を選択し、RSA RADIUS Manager を閉じます。

時刻と日付を設定する

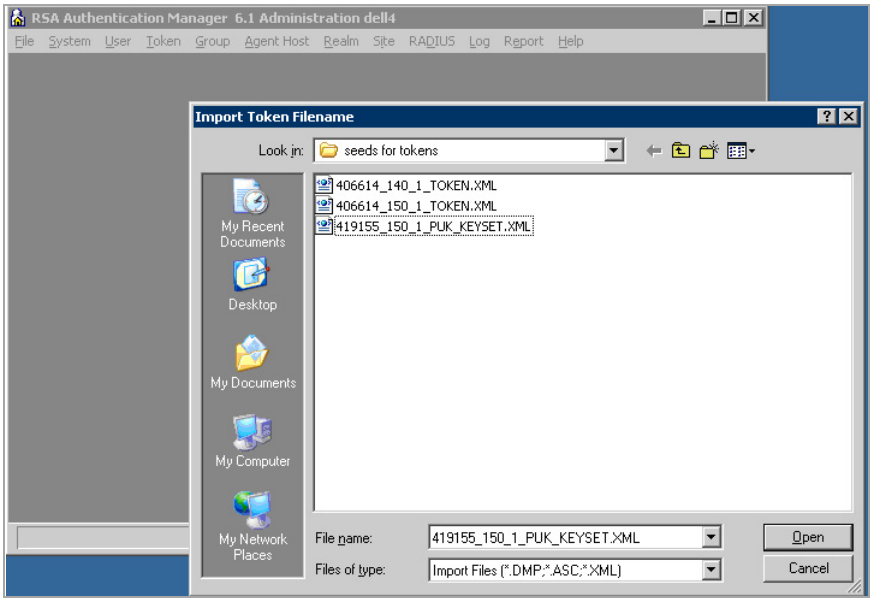
二段階認証は時間の同期に基づいて機能するので、RSA Authentication Manager と SMA/SRA 装置の内部クロックを正しく設定する必要があります。

トークンのインポートとユーザの追加

SMA/SRA 装置と通信するための設定を RSA Authentication Manager で行った後で、トークンをインポートし、ユーザを RSA Authentication Manager に追加する必要があります。

トークンをインポートし、ユーザを追加するには:

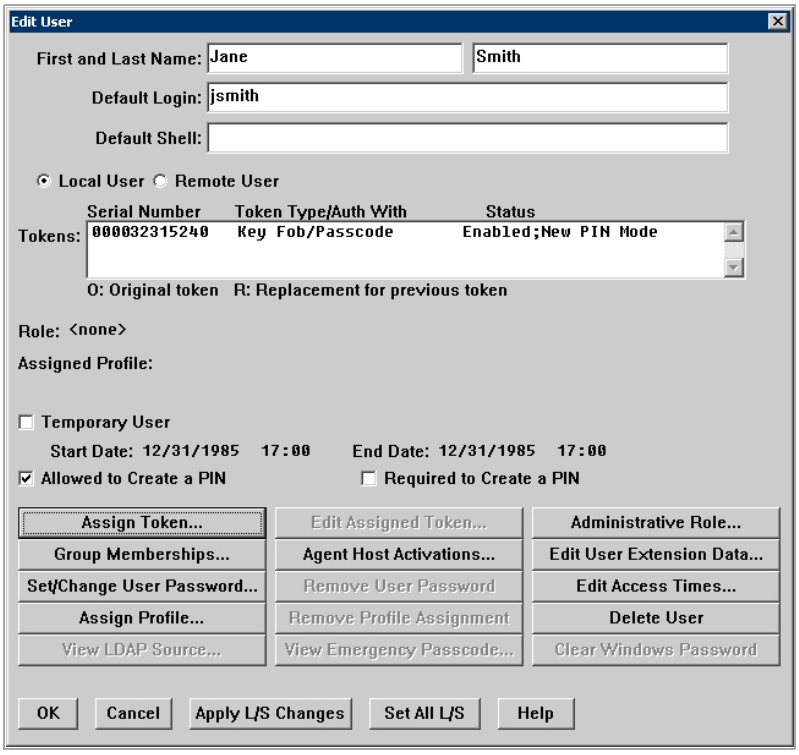
1 トークン ファイルをインポートするには、「**Token > Import Tokens (トークン > トークンのインポート)**」を選択します。



2 RSA SecurID トークンを購入すると、トークンに関する情報が含まれる XML ファイルも提供されます。トークン XML ファイルにナビゲートし、「**Open (開く)**」を選択します。トークン ファイルがインポートされます。

3 「**Import Status (インポートの状況)**」ウィンドウに、RSA Authentication Manager にインポートされたトークンの数に関する情報が表示されます。

4 RSA Authentication Manager にユーザを作成するには、「**User > Add user (ユーザ > ユーザの追加)**」を選択します。

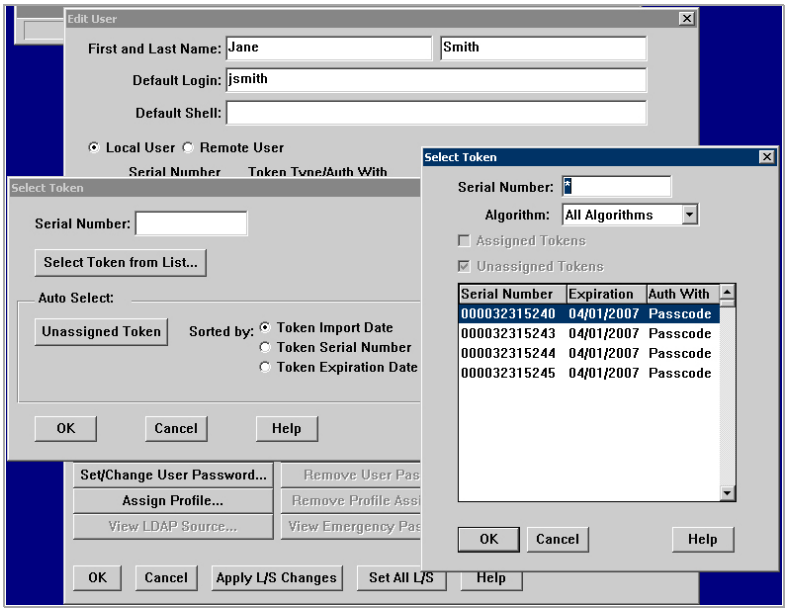


5 ユーザの **First and Last Name (名と姓)**を入力します。

6 ユーザのユーザ名を「**Default Login (既定のログイン)**」フィールドに入力します。

7 「**Allowed to Create a PIN (PIN の作成を許可する)**」または「**Required to Create a PIN (PIN の作成を要求する)**」を選択します。「**Allowed to Create a PIN (PIN の作成を許可する)**」を選択すると、ユーザは PIN を独自に作成するか、無作為な PIN の生成をシステムに任せるかを選択できます。「**Required to Create a PIN (PIN の作成を要求する)**」を選択すると、ユーザは PIN の作成を要求されます。

8 トークンをユーザに割り当てるには、「**Assign Token (トークンの割り当て)**」を選択します。表示される確認用ウィンドウで「**Yes (はい)**」を選択します。「**Select Token (トークンの選択)**」ウィンドウが表示されます。



9 トークンは手動で選択するか、自動的に割り当てることができます。

- ユーザのトークンを手動で選択するには、「**Select Token from List (リストからトークンを選択する)**」を選択します。表示されるウィンドウで、トークンの Serial Number (シリアル番号) を選択し、「**OK**」を選択します。
- トークンを自動的に割り当てるには、トークンを並べ替えるオプションとしてToken Import Date (トークンのインポート日付)、Token Serial Number (トークンのシリアル番号)、またはToken Expiration Date (トークンの失効日)を選択できます。その後で「**Unassigned Token (未割り当てトークン)**」を選択すると、RSA Authentication Manager によってトークンがユーザに割り当てられます。「**OK**」を選択します。

10 「**Edit User (ユーザの編集)**」ウィンドウの「**OK**」を選択します。ユーザが RSA Authentication Manager に追加されます。

11 ユーザに RSA SecurID Authenticator を渡し、ログイン方法、PIN 作成方法、RSA SecurID Authenticator の使用方法を伝えます。詳細については、『*Secure Mobile Access ユーザ ガイド*』を参照してください。

VASCO IdentiKey ソリューションの設定

VASCO IdentiKey ソリューションは、Secure Mobile Access で動作します。以下のセクションでは、VASCO の IdentiKey バージョン 3.2 を使った二段階認証の設定方法を説明します。

- 二段階認証を検証する (214 ページ)

メモ：この設定手順は、VASCO IdentiKey バージョン 3.2 に特化しています。異なるバージョンの VASCO IdentiKey を使う場合は、手順は若干異なります。

VASCO ではなく RSA を使用する場合は、RSA Authentication Manager の設定 (207 ページ) を参照してください。

時刻を設定する

DIGIPASS トークンは時刻同期に基づいています。二段階認証は時刻同期に依存しているので、SMA/SRA 装置の内部時計と VASCO IdentiKey の内部時計が正しく設定されていることが重要です。

SMA/SRA 装置で「**システム > 時間**」に移動して、正しいタイム ゾーンを設定します。

DNS とデフォルト ルートを設定する

SMA/SRA 装置のデフォルト ルートは、DMZ ゾーンに相当するファイアウォール上のインターフェースです。このファイアウォール DMZ インターフェースの IP アドレスが、SMA/SRA 装置のデフォルト ルートとして設定されている必要があります。

DNS とデフォルト ルートを設定するには、以下の手順に従います。

1 Secure Mobile Access 管理インターフェース上で、「**ネットワーク > DNS**」に移動して、DNS 設定 および/または WINS 設定を構成します。

2 「**ネットワーク > ルート**」に移動して、**Secure Mobile Access X0** インターフェースに対して正しい**デフォルト ルート**を設定します。

NetExtender クライアント アドレス範囲とルートを設定する

SMA/SRA 装置で NetExtender クライアント アドレス範囲とルートを設定するには、以下の手順に従います。

1 「**ユーザ > ローカル ユーザ > クライアント**」に移動して「**クライアント アドレス範囲**」を設定します。

クライアント アドレスは、SMA/SRA X0 インターフェースと同じサブネット内に割り当てられます。SMA/SRA 装置の X0 インターフェースとファイアウォール DMZ インターフェース IP アドレスは除外します。

2 「**ユーザ > ローカル ユーザ > クライアント > ルート**」に移動します。

「**クライアント ルートの追加**」を選択して、SMA/SRA 接続によってプライベート ネットワークにアクセスする認証されたリモート ユーザに対する正しいクライアント ルートを選択します。

クライアント ルートは、SonicWall Inc. NSA、TZ、または SuperMassive 9000 シリーズの X0 (LAN) インターフェースに接続されたサブネットに対応します。

RADIUS 認証を使うポータル ドメインを作成する

SMA/SRA 装置上に RADIUS 認証を使うドメインを作成するには、以下の手順に従います。

1 「**ポータル > ドメイン**」に移動して、「**ドメインの追加**」を選択します。

2 「**認証種別**」ドロップダウン リストから「**RADIUS**」を選択します。

3 ユーザが Secure Mobile Access ポータルにログインするために使用する「**ドメイン名**」を入力します。

VASCO IdentiKey 上でポリシーを設定する

VASCO Identikey Web Administration インターフェースで新しいポリシーを追加するには:

1 Vasco Identikey Web Administration ウィンドウにログインします。

2 「**Policies (ポリシー)**」タブを選択して、「**Create (作成)**」を選択します。

> ⓘ **メモ**：既定で利用可能なポリシーがあり、必要に応じて新しいポリシーを作成することもできます。

3 ポリシー名を入力して、あなたの状況にもっとも適切なオプションを選択します。ポリシーに別のポリシーから設定を引き継ぎたい場合は、引継ぎのオプションを選択します。既存のポリシーを複製したい場合は、複製のオプションを選択し、また新しいポリシーを作成したい場合は、作成のオプションを選択します。

> ⓘ **メモ**：適切なバックエンド サーバを使うためにポリシー プロパティを設定します。これは、SMA/SRA 装置で先程使用した認証サービスと同じにすることができます。

ポリシーに対して以下の設定を使用します。

ポリシー設定

Local Auth	Default (DIGIPASS/Password)
Back-End Auth	Default (None)
Dynamic User Registration	Default (No)
Password Autolearn	Default (No)
Stored Password Proxy	Default (No)
Windows Group Check	Default (No Check)

SMA/SRA を VASCO クライアントとして登録する

SMA/SRA 装置を VASCO クライアントとして登録するには、以下の手順に従います。

1 Vasco Identikey Web Administration ウィンドウで、「**Clients**」タブを選択して「**Register**」を選択します。

2 「**Client Type**」に「**RADIUS Client**」を選択します。

3 SMA/SRA 装置の IP アドレスを入力します。

4 「**Policy ID**」フィールドで、あなたの新しいポリシーを選択します。

5 SMA/SRA 装置上で RADIUS サーバ プロパティに対して入力した「**Shared Secret**」を入力します。

6 「**Create**」を選択します。

VASCO IdentiKey ユーザを設定する

新しいユーザを作成するには、以下の手順に従います。

1 Vasco Identikey Web Administration ウィンドウで、「**Users (ユーザ)**」タブを選択して「**Create (作成)**」を選択します。

2 「**User ID (ユーザ ID)**」フィールドを入力します。

3 「**Domain (ドメイン)**」を選択します。

4 「**Organization Unit (部門/部署)**」を選択します。

5 「**Create (作成)**」を選択します。

作成したユーザが、Vasco Identikey Web Administration 管理インターフェースのユーザ リストに表示されます。

DIGIPASS をインポートする

DIGIPASS をインポートするには、以下の手順に従います。

1 Vasco Identikey Web Administration ウィンドウで、「**DIGIPASS**」タブを選択して「**Import (インポート)**」を選択します。

2 「***.DPX**」ファイルをブラウズします。

3 「**Transport Key (転送キー)**」を入力します。

4 「**Upload (アップロード)**」を選択します。

DIGIPASS が正しくインポートされると、確認のメッセージがポップアップします。

DIGIPASS をユーザに割り当てる

DIGIPASS をユーザに割り当てる方法は 2 通りあります。DIGIPASS を検索してからそれをユーザに割り当てるか、ユーザを検索してからそれを DIGIPASS に割り当てます。

1 以下のいずれかを実行します。

- 「**Users (ユーザ)**」タブでユーザの隣のチェックボックスを選択してから、「**Assign DIGIPASS (DIGIPASS の割り当て)**」を選択します。
- 「**DIGIPASS**」タブで DIGIPASS の隣のチェックボックスを選択してから、「**NEXT (次へ)**」を選択します。

メモ：「**User ID (ユーザ ID)**」が空欄のままの場合は、「**Find (検索)**」を選択すると同一ドメイン内の利用可能なすべてのユーザが表示されます。ユーザが表示されない場合は、DIGIPASS のドメインとユーザが一致していることを確認します。

ユーザが DIGIPASS に割り当てられると、確認のメッセージがポップアップします。

二段階認証を検証する

VASCO IdentiKey を用いた二段階認証の SMA/SRA 接続を試験するには、以下の手順に従います。

1 ブラウザで IP アドレスを指定して、PC を SMA/SRA の WAN (X1) インターフェースに接続します。

2 管理者として LocalDomain にログインします。

3 「**ポータル > ドメイン**」に移動し、「**設定**」を選択して、RADIUS から VASCO IdentiKey への接続を試験します。

4 RADIUS 認証が成功した場合は、管理者アカウントからログアウトして、Secure Mobile Access の WAN (X1) インターフェースに、作成したユーザ名でログインします。

ポータル > 個別ロゴ

ポータル ロゴは「**ポータル > 個別ロゴ**」ページでグローバルに設定されなくなりました。個別ロゴは、「**ポータル ロゴ設定**」ダイアログの「**ロゴ**」タブでポータル別にアップロードされます。個別ポータル ロゴの詳細については、個別ポータル ロゴの追加 (162 ページ) を参照してください。

ポータル > 負荷分散

このセクションでは、「**ポータル > 負荷分散**」ページの概要と、このページで利用可能な設定タスクの説明を提供します。

- ポータル > 負荷分散 の概要 (215 ページ)
- 負荷分散グループの設定 (216 ページ)

ポータル > 負荷分散 の概要

「**ポータル > 負荷分散**」ページでは、管理者はバックエンド ウェブ サーバを負荷分散配備するための設定ができます。負荷分散機能に対するこの既定の開始ページでは、管理者は負荷分散グループの設定と、既存の負荷分散グループすべてのプロパティ概要の一覧ができます。

メモ：この機能にはまた、「**ポータル > 負荷分散**」ページで設定される仮想ホストを持つ負荷分散ポータルが必要です。

「ポータル > 負荷分散」ページ

設定シナリオ

Secure Mobile Access 向けの負荷分散は、多様な用途を持つ強固な機能で、次のような用途があります。

ウェブ サーバ ファームの分散 - 高パワーの SMA/SRA 装置が、比較的低パワーのウェブ サーバ ファームの防御と負荷分散を提供している場合に有用です。この場合、ウェブ アプリケーション ファイアウォール、URL 書き換え、およびその他の CPU 負荷の高い作業が、負荷分散装置上で利用可能です。

低パワー クラスタの分散 - 比較的低パワーの SMA/SRA クラスタを負荷分散して拡張性を向上できます。この場合、ウェブ アプリケーション ファイアウォール、URL 書き換え、およびその他の可変機能が、低パワーの SMA/SRA 装置群で利用可能です。

負荷分散ペア - このシナリオでは、負荷分散装置はポータル 1 つをフロントエンド用に設定し、別のアプリケーション オフロード ポータルを仮想バックエンド サーバとして動作するように設定することができます。この仮想バックエンド サーバおよび 2 台目の SMA/SRA 装置は、負荷分散メンバとして設定され、またセキュリティ サービスの負荷も請け負います。前の 2 つのシナリオ内の負荷分散装置は、本質的にはセキュリティ サービスの負荷を負わないダミー プロキシです。

負荷分散の設定

以下のテーブルは、「**ポータル > 負荷分散**」の設定オプションの一覧です。追加のグループ毎設定オプションは、負荷分散グループの設定 (216 ページ) で説明します。

負荷分散の設定オプション

オプション	説明
負荷分散を有効にする	現在アクティブなすべてのグループに渡って、負荷分散機能を有効にする。
フェイルオーバーを有効にする	すべてのプローブ、監視、およびフェイルオーバー機能を有効/無効にする。
プローブ間隔	負荷分散機能がバックエンド ノードの状況を確認する頻度 (秒) を決定する。

負荷分散グループの設定

このセクションは、新しい負荷分散グループの作成の設定詳細を提供し、以下のセクションから構成されます。

新しい負荷分散グループの追加

1 「**ポータル > 負荷分散**」ページで、「**グループの追加**」を選択します。新規負荷分散グループの設定情報が表示されます。

2 この負荷分散グループに対して、わかりやすい「**負荷分散グループ名**」を入力します。

3 「**負荷分散方式**」ドロップダウン リストから、負荷分散方式を選択します。オプションは以下を含みます。

- **重み付き要求数** - 着信要求 (正しく完了した要求を含む) の数を追跡することで、どのメンバが次の着信要求を処理するかを決定します。負荷分散率によって分配パーセンテージが決まります。
- **重み付きトラフィック量** - 着信/発信データのバイト数を追跡することで、どのメンバが次の着信要求を処理するかを決定します。
- **最小要求数** - 現在サービスされている着信要求 (正しく完了した要求を除く) の数を追跡することで、どのメンバが次の着信要求を処理するかを決定します。

4 「**負荷分散を有効にする**」を選択して、このグループで負荷分散を有効にします。

5 グループを有効にした際に「**セッションの恒久化を有効にする**」オプションは、自動的に選択されます。このオプションにより、管理者は同一セッションの”要求”部分を同一バックエンドサーバへ転送することによる、継続的なユーザ セッションを有効にすることができます。

6 プローブ、監視、およびフェイルオーバー機能を有効にするには、「**フェイルオーバーを有効にする**」を選択します。

> **メモ**：認証されたユーザを保持するために、同じメンバがすべてのクッキーを受け取ることを確実にすることが重要です。しかしながら、特定の状況下でのパフォーマンス向上のために、すべてのバックエンド メンバがすべてのユーザのセッション Cookie を受諾できる場合があります。この場合、管理者はセッション恒久化をオフにすることができます。そうすると負荷分散装置は、負荷を分散するための負荷分散方式と負荷分散要因を厳密に固守します。

7 グループに新しいメンバーを追加するには、負荷分散グループへの新メンバの追加 (218 ページ)を参照してください。

プローブ設定の構成

この負荷分散グループに対して「**ポータル > 負荷分散**」画面の「**プローブ設定**」セクションでプローブ設定を構成するには、以下の手順に従います。

1 「**プローブ方式**」をドロップダウン リストから選択します。オプションは以下を含みます。

- **HTTP/HTTPS GET** - 負荷分散装置は、HTTP 応答ステータス コードが 500 以上ではないかどうかを見て、ウェブ サーバ エラーが無いことを確かにするために、HTTP(S) GET 要求を定期的に (設定したプローブ間隔に基づいて) 送信します。これは、ウェブ サーバが活動しているかどうかを判断する、最も確実な方式です。この方式は、プローブ中の SSL 証明書警告を無視します。
- **TCP Connect** - 負荷分散装置は、バックエンド ノードの健康状態を監視するために、定期的に 3 ウェイ TCP ハンドシェークを完了します。
- **ICMP Ping** - 負荷分散装置は、バックエンド ノードが活動しているかどうかを監視するために、単純な ICMP Ping 要求を送信します。

2 「**メンバを停止するまでの無応答回数**」フィールドに、ノードを停止するまでに必要な無応答回数を入力します。既定値は 2 です。

3 「**停止したメンバを再度有効にするまでの応答回数**」フィールドに、停止ノードを動作中として復帰させるまでに必要な成功応答回数を入力します。既定値は 2 です。

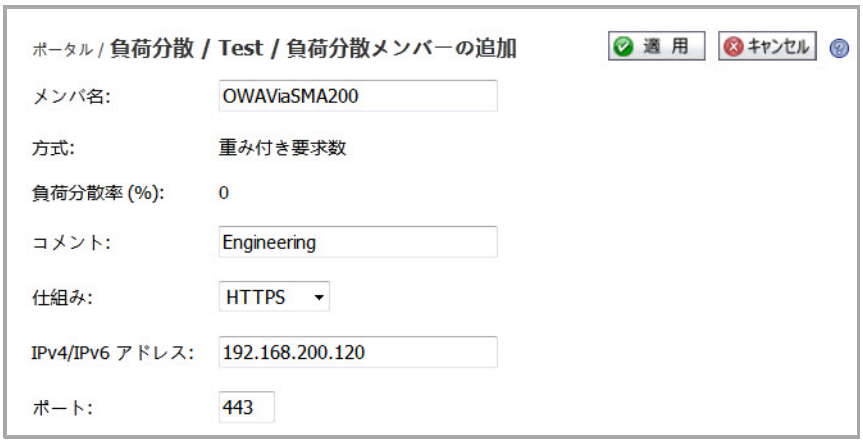
4 「**フェイルオーバーするリソースが存在しない場合にエラー ページを表示する**」テキストボックスに、設定したすべてのバックエンド ノードが失敗した場合に表示する個別メッセージやウェブ ページを入力します。このフィールドでは HTML 形式を使用できます。

負荷分散グループへの新メンバの追加

> **メモ**：負荷分散グループを作成してからでなければ、そのグループへのメンバーの追加を開始することはできません。

新しい、または既存の負荷分散グループにメンバを追加するには、以下の手順に従います。

1 「**ポータル > 負荷分散**」ページからグループの編集や追加を行う場合は、「**メンバの追加**」を選択します。負荷分散メンバの追加画面が表示されます。



2 負荷分散グループ内でこのメンバを一意に識別するための「**メンバ名**」を入力します。

3 グループのページでマウスオーバーすることによりこのグループを判別するための、わかりやすい名前や説明を「**コメント**」フィールドに入力します。

4 バックエンド サーバに接続するための**仕組み**を選択します。次のいずれかのオプションをドロップダウン リストで選択します。「**HTTP**」、「**HTTPS**」、または「**自動**」。既定値は HTTPS です。

「自動」を選択した場合は、HTTPS 用と HTTP 用の 2 つのポート番号を指定します。

メモ：アプリケーション オフローダ ポータルに対して HTTP アクセスを有効にするには、ポータルの「**仮想ホスト**」タブにある「**HTTP アクセスを有効にする**」をオンにします。

5 バックエンド HTTP(S) サーバの IP アドレスを、「**IPv4/IPv6 アドレス**」フィールドに入力します。

6 バックエンド サーバの**ポート**を入力します。HTTPS 接続の既定値は 443 です。仕組みが「自動」である場合は、HTTPS 用と HTTP 用の 2 つのポート番号を指定します。

7 「**適用**」を選択して、このメンバをグループに追加します。

ポータル > URL ベース エイリアス

このセクションでは、「**ポータル > URL ベース エイリアス**」ページの概要と、このページで利用可能な設定タスクについて説明します。

- URL ベース エイリアスの概要 (220 ページ)
- URL ベース エイリアス グループの追加 (220 ページ)
- 既定のサイト設定 (223 ページ)

URL ベース エイリアスの概要

URL ベース エイリアスは、1 つのドメイン名を使用して、1 つのポータルをから複数の異なるウェブ サイトにアクセスできます。この機能は、負荷分散設定と一致するように設計されています。URL ベース エイリアスは、バックエンド ウェブ サーバが提供するコンテンツ内の URL の書き換えを伴うので、バックエンド ウェブ アプリケーションにはサードパーティのプロキシとの互換性が必要です。ウェブ アプリケーションが URL ベース エイリアスを使用して正しく表示されない場合は、URL の書き換えや NetExtender を使用することなく、アプリケーション オフローダでそのアプリケーションへのアクセスを設定しなければならないことがあります。

URL ベース エイリアス グループの追加

参考資料:

- メンバーの追加 (221 ページ)
- グループの削除 (222 ページ)
- メンバーの削除 (223 ページ)

URL ベース エイリアス グループを追加するには:

1 「**ポータル** > **URL ベース エイリアス**」ページを開きます。

2 「URL ベース エイリアス グループ」セクションの「**グループの追加**」を選択します。「新規 URL ベース エイリアス グループ」ページが表示されます。

3 表示されるフィールドに**グループ名**を入力します。「**適用**」をクリックします。新規に追加されたグループが、「URL ベース エイリアス グループ」のリストに表示されます。

メンバーの追加

メモ：URL ベース エイリアス グループを作成してからでなければ、そのグループへのメンバーの追加を開始することはできません。

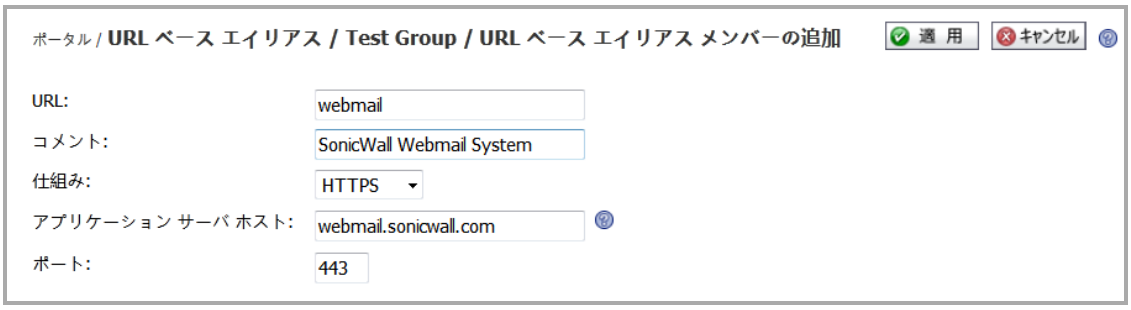
URL ベース エイリアスを使用すると、最大 100 名のメンバーをグループに追加できます。

URL ベース エイリアス グループにメンバーを追加するには:

1 「**ポータル** > **URL ベース エイリアス**」ページを開きます。

2 編集したいグループの**設定**アイコンを選択します。「グループの URL ベース エイリアス設定」ページが表示されます。

3 「**メンバの追加**」を選択します。「URL ベース エイリアス メンバーの追加」ページが表示されます。



以下のフィールドを設定します。

- **URL** - メンバーの URL または名前を入力します。
- **コメント** - 追加情報があれば入力します。このフィールドに入力した内容はすべて、索引ページに表示されます。
- **仕組み** - ドロップダウン リストからバックエンド サーバのスキームを選択します。「HTTP」、「HTTPS」、または「自動」から選択します。
- **アプリケーション サーバ ホスト** - ホストのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。
- **ポート** - ポート番号を指定します。既定値は 443 です。

4 「**適用**」を選択して、変更を保存し、グループにメンバーを追加します。新規追加されたメンバーが、「**URL ベース エイリアス設定**」ページに表示されます。

グループに追加したいメンバーごとに手順 2 から 4 を繰り返します。

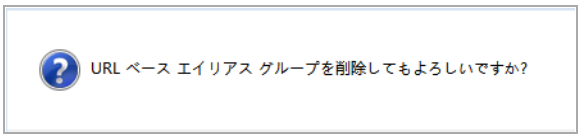
グループの削除

特定のグループを削除するには:

1 「**ポータル** > **URL ベース エイリアス**」ページを開きます。

2 削除したいグループの **削除**アイコンを選択します。

3 グループの削除の確認メッセージが表示されます。「**OK**」を選択します。



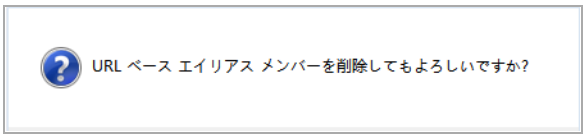
メンバーの削除

グループから特定のメンバーを削除するには:

1 メンバーが所属する URL ベース エイリアス グループの設定ページを表示します。

2 削除したいメンバーの**削除**アイコンを選択します。

3 メンバーの削除の確認メッセージが表示されます。「**OK**」を選択します。削除したいグループごとにこれらの手順を繰り返します。

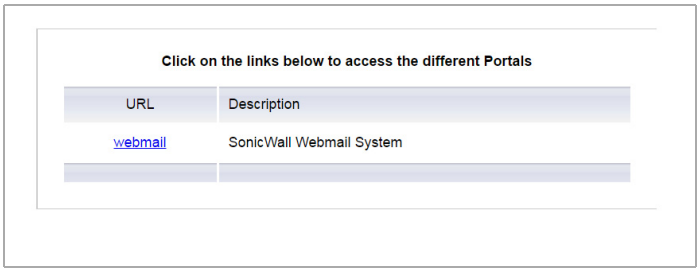


既定のサイト設定

「既定のサイト設定」セクションでは、URL を指定せずにポータルにアクセスする場合の既定のサイトを設定できます。ドロップダウン リストの既定値は「索引ページ」です。

「既定のサイト設定」は、HTML を編集し、「**適用**」を選択することによってカスタマイズできます。

- 「**プレビュー**」を選択して、索引ページを表示します。このページの見え方を変更するには、「既定のサイト設定」セクションで HTML を編集し、「**適用**」を選択します。



- 「**既定の索引ページ**」を選択し、既定のページを表示します。

メモ：URL webmail.sonicwall.com を使用してください。設定済みサイトへのハイパーリンク アクセスが設定された索引ページが表示されます。

第 3 部

サービスとクライアントの設定

- サービスの設定
- デバイス管理の設定
- クライアントの構成
- エンド ポイント制御
- セキュア仮想アシストの設定
- セキュア仮想ミーティング
- ウェブ アプリケーションファイアウォールの設定
- キャプチャ ATP
- 地域 IP とボットネット フィルタ
- 高可用性の設定

6

サービスの設定

このセクションでは、ウェブ ベースの Secure Mobile Access 管理インターフェースの「**サービス**」ページで行う、HTTP/HTTPS、Citrix、RDP、VNC といった多種のアプリケーション レイヤのサービスに対する設定、ブックマークとポリシーの設定などの設定タスクについて説明します。

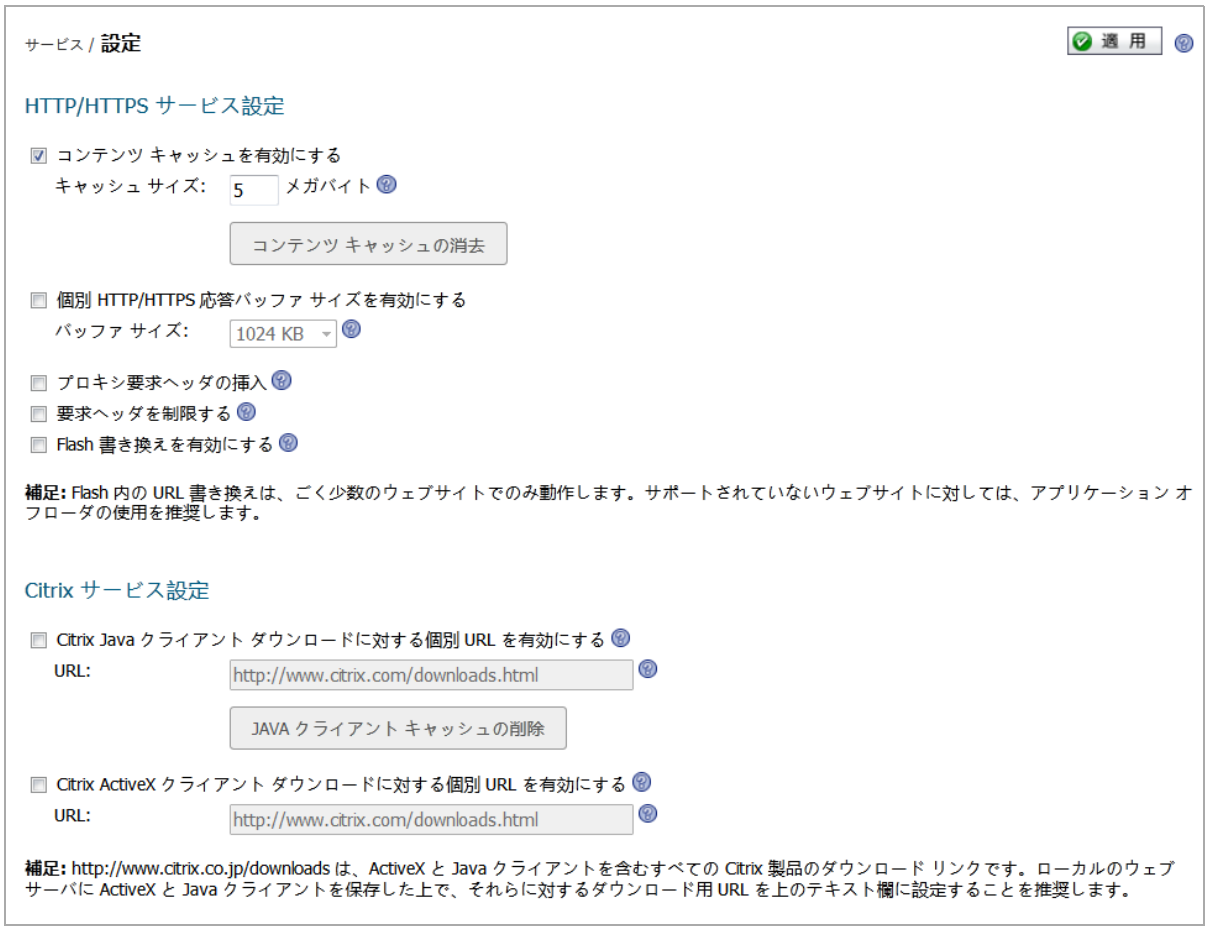
トピック:

サービス > 設定

このセクションでは、「**サービス > 設定**」ページの概要と、このページで利用できる設定タスクについて説明します。

「**サービス > 設定**」ページで、管理者は HTTP/HTTPS、Citrix、グローバル ポータル文字セット、およびワンタイム パスワードに関するさまざまな設定を行うことができます。

「サービス > 設定」ページ



HTTP/HTTPS サービス設定

管理者は、以下の手順に従って HTTP/HTTPS サービスを設定できます。

1 既定では、「**コンテンツ キャッシュを有効にする**」がオンになっています。管理者はこのチェックボックスをオフにすることでこの設定を無効にできます。ただし、「コンテンツ キャッシュを有効にする」の設定を変更すると、ウェブ サーバを含む Secure Mobile Access サービスが再起動されます。

「**キャッシュ サイズ**」フィールドで、必要なコンテンツ キャッシュのサイズを定義します。5MB が既定の設定ですが、管理者は 2 ～ 20MB の範囲で任意のサイズを設定できます。「**消去**」を選択すると、コンテンツ キャッシュが消去されます。

2 応答バッファを設定する場合は、「**個別 HTTP/HTTPS 応答バッファ サイズを有効にする**」をオンにします。「**バッファ サイズ**」ドロップダウン メニューを使用して適切なバッファ サイズを設定します。この制限は、プレーン テキスト、Flash、および Java アプレットを対象としたバックエンド ウェブ サーバからの HTTP および HTTPS 応答に適用されます。バッファの既定のサイズは 1024KB です。

3 プロキシ要求ヘッダをバックエンド ウェブ サーバに対する HTTP/HTTPS 要求に挿入するには、「**プロキシ要求ヘッダの挿入**」をオンにします。以下のヘッダーが挿入されます。

- X-**Forwarded-For**: 元の HTTP/HTTPS 要求のクライアント IP アドレスを指定します。
- X-**Forwarded-Host**: クライアントからの HTTP/HTTPS 要求で“ホスト”を指定します。

- X-**Forwarded-Server**: SMA/SRA プロキシ サーバのホスト名を指定します。

4 識別不能な HTTP 要求ヘッダを除去するには、「**要求ヘッダを制限する**」をオンにします。

5 Flash ファイルに含まれる URL を書き換えるには、「**Flash 書き換えを有効にする**」をオンにします。Flash 内の URL 書き換えは、ごく少数のウェブ サイトでしか動作しない場合があります。サポートされていないウェブ サイトに対しては、アプリケーション オフローダの使用を推奨します。この機能は、既定では無効になっています。

Citrix サービス設定

管理者はローカル ウェブ サーバ上に Citrix クライアントをホストして、そこから Secure Mobile Access にこれらのクライアントをダウンロードさせる必要があります。例えば、以下の Citrix Receiver クライアントをウェブ サーバ上に配置します。

- ActiveX に対して: Receiver for Windows 3.0 - CitrixReceiver.exe
- Java に対して: Receiver for Java 10.1 - JICAComponents.zip

Citrix サービス設定を構成するには、以下の手順に従います。

1 独自の HTTP URL を使用して Citrix Java クライアントをダウンロードする場合は、「**Citrix Java クライアント ダウンロードに対する個別 URL を有効にする**」をオンにします。「**URL**」フィールドに個別 URL を入力します。このオプションを有効にしない場合は、既定の URL が使用されます。

2 独自の HTTP URL を使用して Citrix ActiveX クライアントをダウンロードする場合は、「**Citrix ActiveX クライアント ダウンロードに対する個別 URL を有効にする**」をオンにします。「**URL**」フィールドに個別 URL を入力します。このオプションを有効にしない場合は、既定の URL が使用されます。

NetExtender/Mobile Connect サービス設定

1 必要に応じて圧縮を有効にし、ファイル サイズを縮小します。

2 NetExtender の詳細なデバッグ ログを有効にします。mcd.log ファイルは「**システム > 診断**」ページで生成されるテクニカル サポート レポート (TSR) の一部になります。「**ログ レベル**」ドロップダウン メニューから既定のログ レベルを選択します。レベルは最も低いものから最も高いものまで順に表示されます。

   - デバッグ
   - 情報
   - 通告 – 既定
   - 警告
   - エラー

   すべてのログは、特にオーバーライドされない限り、ここで設定されている既定のレベルに従います。

3 「上書き」セクションでログに対する変更を行う場合は、「既定レベルに従う」チェックボックスをオフにします。すべてのサービス種別ですべてのドロップダウン メニューがアクティブになります。

4 NetExtender/Mobile Connect 接続の「**パケット キャプチャを有効にする**」をオンにします。保存されたすべてのパケット キャプチャをダウンロードするには、「**すべてダウンロード**」を選択

します。保存されたすべてのパケット キャプチャを削除するには、「**すべて削除**」を選択します。このオプションはスループットに悪影響を与える可能性があるので、トラブルシューティングにのみ使用してください。

メモ：IPv4/IPv6 ストリームをキャプチャするには、「**圧縮**」オプションを無効にします。

5 指定したパケット キャプチャ種別に基づいて、一意の Pcap ファイルが保存されます。キャプチャ種別は「**キャプチャ種別**」ドロップダウン メニューから選択します。次のような種別があります。

- **ユーザごと** -「**ユーザごと**」を選択すると、パケット キャプチャがオンの間はユーザごとに一意の Pcap ファイルが保存されます。
- **NetExtender クライアント IP ごと** -「**NetExtender クライアント IP ごと**」を選択すると、SMA によって割り当てられたリモート IP ごとに一意の Pcap ファイルが保存されます。
- **ユーザ セッションごと** -「**ユーザ セッションごと**」を選択すると、ユーザ セッションごとに一意の Pcap ファイルが保存されます。
- **クライアント IP ごと** -「**クライアント IP ごと**」を選択すると、SMA への接続を最初に開始したクライアント IP ごとに一意の Pcap ファイルが保存されます。

Mobile Connect の既定のポリシー設定

Mobile Connect の既定のポリシー設定を次の中から選択します。

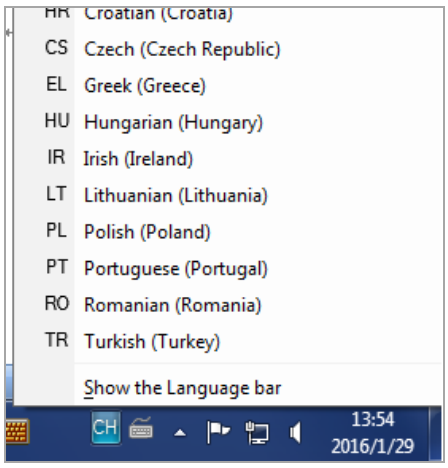
- **オープンを許可** - ファイルを他のアプリケーションで開くことを許可します。ただし、Mobile Connect のポリシーは他のアプリケーションから適用されません。
- **コピーを許可** - ファイルの一部をクリップボードにコピーすることを許可します。
- **印刷を許可** - ファイルの印刷を許可します。
- **キャッシュを許可** - ファイルをクライアントにキャッシュし、安全に保存し、暗号化することを許可します。

グローバル ポータル設定

標準および非標準の FTP サーバで言語互換性文字セットが使用されるように設定するには、「**既定の文字セット**」ドロップダウン メニューを使用します。この文字セットは FTP セッションとブックマークだけに適用されます。ほとんどの FTP サーバは、既定の設定である標準のエンコード (UTF-8) に対応しています。

欧州向けのキーボード

米国向けのキーボードでは、一部の欧州文字を入力することができません。キーボード種別を設定し、リモート サーバ、HTML5 サーバ、ローカル クライアント コンピュータで一致させる必要があります。



使用できるキーボードを以下に示します。

国	キーボード	外国語
ボスニア	ボスニア語 (キリル)	ボスニア語 (キリル、ボスニア・ヘルツェゴビナ)
ブルガリア	ブルガリア語	ブルガリア語 (ブルガリア)
クロアチア	クロアチア語	クロアチア語 (クロアチア)
チェコ共和国	チェコ語	チェコ語 (チェコ共和国)
ギリシャ	ギリシャ語	ギリシャ語 (ギリシャ)
ハンガリー	ハンガリー語	ハンガリー語 (ハンガリー)
アイルランド	アイルランド語	アイルランド語 (アイルランド)
リトアニア	リトアニア語	リトアニア語 (リトアニア)
ポーランド	ポーランド語 (214)	ポーランド語 (ポーランド)
ポルトガル	ポルトガル語	ポルトガル語 (ポルトガル)
ルーマニア	ルーマニア語 (レガシー)	ルーマニア語 (ルーマニア)
トルコ	トルコ語 F	トルコ語 (トルコ)
トルコ	トルコ語 Q	トルコ語 (トルコ)
英語	米国 - インターナショナル	英語 (米国)

入力の解析を適切に行うには、HTML5 のキャンバス要素 (<canvas>) に同じ言語を設定します。そのためには、S シールド ("S" と記された盾のマーク) の横にある言語識別子をクリックして、言語選択メニューを開きます。

言語選択メニュー

次の 3 つの領域でキーボードの言語設定が同じになるようにしてください。

1 ローカル クライアント マシン

2 HTML5 の設定

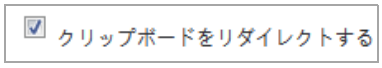
3 リモート RDP サーバ マシン

ブックマーク管理者は、ブックマーク設定で既定の言語キーボードを設定できます。ブックマークを開くと、既定の言語の識別子が S シールドの横に表示されます。

RDP セッション間でのテキストのコピーと貼り付け

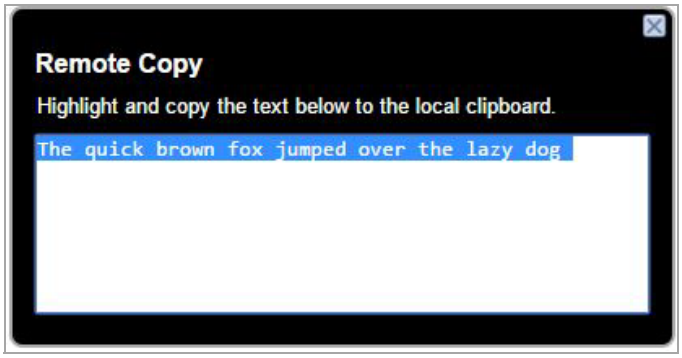
メモ：Chrome、Edge、または Firefox ブラウザで HTML5 クライアントを使用している場合は、リモート コンピュータとの間でテキストのコピーと貼り付けを行うことはできません。

ブックマーク管理者は、ブックマーク設定の「クリップボードのリダイレクト」オプションを使用して、コピーと貼り付けの機能を有効または無効にできます。同様に、「**クリップボードのリダイレクト**」と「**リモート コピー**」を使ってローカル セッションとリモート セッション間のコピーと貼り付けの機能も有効または無効にできます。



有効になっている場合、ブックマークを起動してリモート サーバにテキストをコピーしようとすると、S シールドの下にあるアイコンが点滅します。

点滅しているアイコンをクリックすると、ダイアログがポップアップ表示されます。入力フィールドにはコピーされたテキストが示されています。テキストは、そこから手動でコピーしてローカル マシンにペーストする (貼り付ける) ことができます。



反対方向へのコピー/ペーストは、ローカルでのコピー/ペーストのように非常にスムーズに行えます。ローカルの文字列をコピーし、リモート マシン上にペーストするだけです。

ワンタイム パスワード設定

「**ワンタイム パスワード設定**」セクションでは、管理者がワンタイム パスワードの作成と通信に関する設定を行うことができます。ワンタイム パスワードは、文字、数字、またはその両方を組み合わせて動的に生成される文字列です。電子メールの件名の文字数を制限できるメール サービス (SMS など) との互換性のために、管理者は電子メールの件名をカスタマイズして、ワンタイム パスワードを含めるか除外することができます。電子メール メッセージの本文についても同様の設定ができます。また、管理者はパスワードの形式 (文字や番号など) を選択できます。

ワンタイム パスワード電子メールの件名の形式と本文の形式を設定し、ワンタイム パスワードの生成で使用する既定の文字タイプを変更するには、以下のタスクを実行します。

1 「**電子メール件名**」フィールドに、適切なテキストをワンタイム パスワード電子メールの件名として入力します。既定の件名は、**OTP** に実際のワンタイム パスワード (ここではパラメータ プレースホルダ **%OneTimePassword%** として表示) が付加された文字列です。

2 「**電子メール本文**」フィールドに、適切なテキストをワンタイム パスワード電子メール メッセージの本文として入力します。既定のメッセージは、ワンタイムパスワードそのもの (ここでは **%OneTimePassword%** として表示) です。

ワンタイム パスワード電子メールの件名や本文では変数が使えます。

- **%OneTimePassword%** - ユーザのワンタイム パスワードです。電子メールの件名または本文のどちらかで少なくとも 1 回は現れるはずです。
- **%AD:mobile%** - アクティブ ディレクトリ (AD) で設定されているユーザの携帯電話です。
- **%AD:_____%** - その他の任意のアクティブ ディレクトリ (AD) ユーザ属性です。その他の属性については、「**電子メール本文**」フィールドの下にある Microsoft ドキュメント リンクを参照してください。

3 「**ワンタイム パスワード形式**」ドロップダウン リストから、次の 3 つのオプションのいずれかを選択します。

- **英字** - ワンタイム パスワードの生成時にアルファベットのみを使用します。
- **英数字** - ワンタイム パスワードの生成時にアルファベットと数字を使用します。
- **数字** - ワンタイム パスワードの生成時に数字のみを使用します。

4 「**ワンタイム パスワード長**」フィールドを使用して、ワンタイム パスワードで使用できる文字数の範囲を調整します。

5 「**サービス > 設定**」ページの右上にある「**適用**」を選択して、変更内容を保存します。

ワンタイム パスワード機能の詳細については、ワンタイム パスワードの概要 (52 ページ) を参照してください。

ポリシー一致のログ設定

ポリシー一致のログ設定を使用して、ポリシーの静的情報にアクセスできます。ポリシー一致のログ設定は、一連のポリシーに一致するユーザ、そのユーザのアクセス元、およびそのユーザのアクセス先を記録します。この情報は、「**サービス > ポリシー**」ページに記録されます。

ポリシー一致のログを有効にするには:

1 「**サービス > 設定**」ページを表示し、「ポリシー一致のログ設定」セクションまでスクロールします。

2 「**ポリシー一致を有効にする**」チェックボックスをオンにします。

3 「**動作を許可するためにポリシー一致を有効にする**」を使用して、許可種別ごとにサーバ ログ一致情報を設定できます。

4 「**動作を拒否するためにポリシー一致を有効にする**」を使用して、拒否種別ごとにサーバ ログ一致情報を設定できます。

5 「**ログ データの保存**」フィールドに、データをログに保存する日数を指定します。既定値は 0 です。

サービス > ブックマーク

ウェブベースの Secure Mobile Access 管理インターフェース内の「**サービス > ブックマーク**」ページは、ブックマークを表示するための単一のインターフェースであり、ユーザおよびグループのブックマークを設定できます。

メモ：安全でないことで知られる Java ブックマークに取って代わるソリューション (HTML5 ブックマーク) が開発されました。SMA 8.6 リリースでは、Java ブックマークが廃止され、既定で無効になっています。Java ブックマークがまだ必要な場合は、ブックマークを有効にするための手順をサポートにお問い合わせください。

これに合わせてすべてのブックマーク オプションが調整されており、Java 関連のオプションは削除されています。

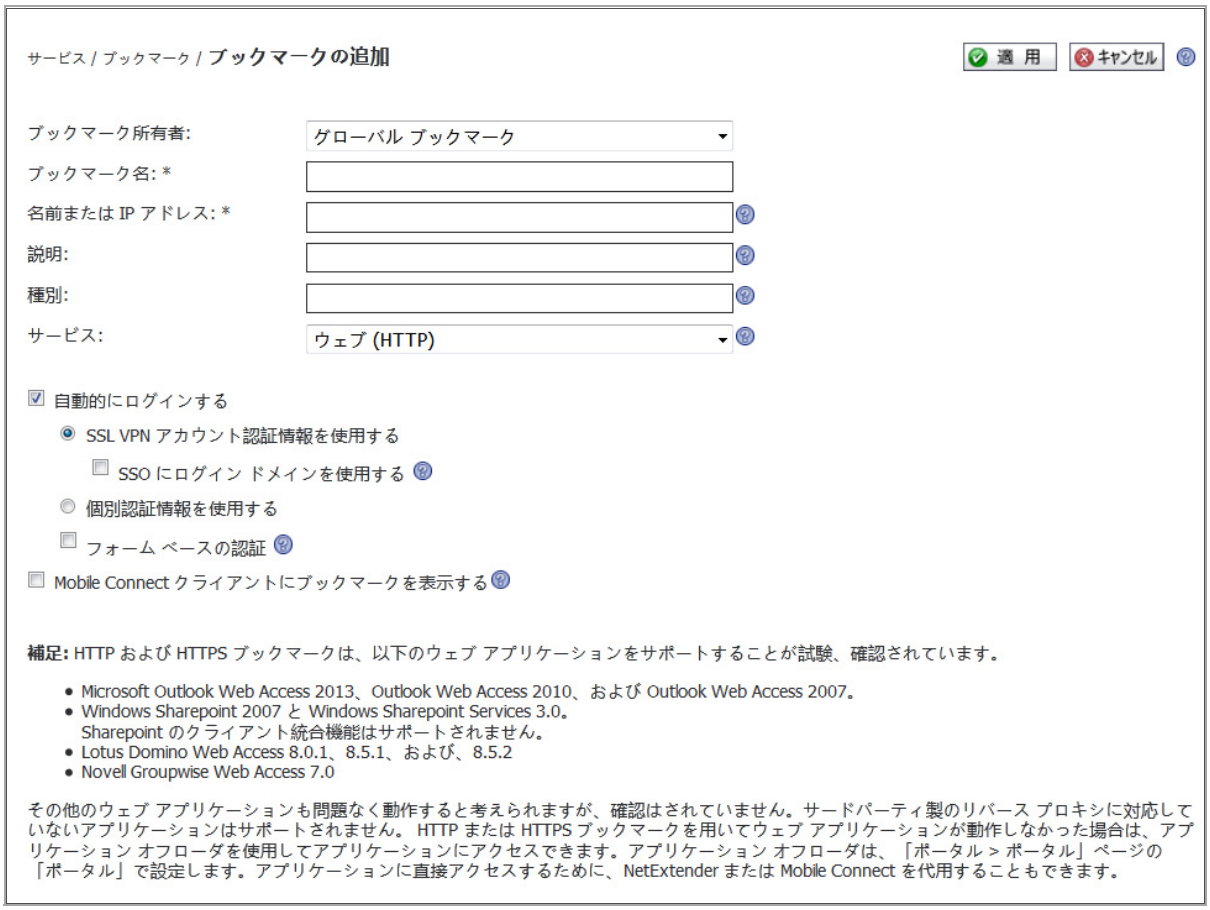
メモ: セキュア シェル バージョン 1 (SSHv1) サービス種別も削除されています。既存の SSHv1 ブックマークはシステム内にはまだ存在しますが、ポータル ページでは非表示です。Java ブックマークを手動で有効にすると、SSHv1 ブックマークが表示されます。

次を参照してください。

- ブックマークの追加または編集 (234 ページ)

ブックマークの追加または編集

ブックマークを追加するには、Secure Mobile Access 管理インターフェース内の「**サービス > ブックマーク**」画面に移動し、「**ブックマークの追加...**」を選択します。「**ブックマークの追加**」ウィンドウが開きます。



サービス ブックマークを追加するには、以下の手順を実行します。

1. 「**ブックマーク所有者**」ドロップダウン メニューを使って、ブックマークが「**グローバル ブックマーク**」、「**ローカル ドメイン グループ ブックマーク**」、または個々の「**ユーザ**」に割り当てられたブックマークのいずれの形で所有されるかを選択します。
2. 「**ブックマーク名**」フィールドに、サービス ブックマークのわかりやすい名前を指定します。
3. 「**名前または IP アドレス**」フィールドに、設定するブックマークのホスト名、IP アドレス、または IPv6 アドレスを入力します。IPv6 アドレスは“［“と“］”で囲む必要があります。

   メモ：IPv6 はファイル共有ではサポートされません。

サービスによっては、非標準ポートで動作し、接続時にパスを要求することがあります。「サービス」フィールドで選択したオプションによって、サービス種別に基づく名前と IP アドレスの形式 表に示した例のいずれかの形式で「**ホスト名または IP アドレス**」フィールドに入力します。

サービス種別に基づく名前と IP アドレスの形式

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
RDP - HTML5	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
VNC VNC - HTML5	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (セッションへ割り当て済み)	10.20.30.4:5901 (セッション 1 へ割り当て済み)
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
	メモ：ポートの代わりにセッション番号または表示番号を使用しないでください。	**メモ**：10.20.30.4:1 を使用しないでください。 **ヒント**：Linux サーバへのブックマークについては、この表の後にヒントがあります。
FTP	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818 または [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
Telnet	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818 または [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
SSHv2	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818 または [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC

サービス種別に基づく名前と IP アドレスの形式 (続き)

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
HTTP HTTPS	URL	www.sonicwall.com
	URL の IP アドレス	204.212.170.11
	IPv6 アドレス	2008::1:2:3:4
	URL:パスまたはファイル	www.sonicwall.com/index.html
	IP:パスまたはファイル	204.212.170.11/フォルダ/
	URL:ポート	www.sonicwall.com:8080
	IP:ポート	204.212.170.11:8080 または [2008::1:2:3:4]:8080
	URL:ポート:パスまたはファイル	www.sonicwall.com:8080/フォルダ/index.html
	IP:ポート:パスまたはファイル	www.sonicwall.com:8080/index.html
ファイル共有	ホスト\フォルダ\	server-3\共有フォルダ\
	ホスト\フォルダ	server-3\inventory.xls
	完全修飾名\フォルダ	server-3.company.net\共有フォルダ\
	完全修飾名\ファイル	server-3.company.net\inventory.xls
	IP\フォルダ\	10.20.30.4\共有フォルダ\
	IP\ファイル	10.20.30.4\status.doc
		メモ：Linux や Mac コンピュータでもファイル共有に Windows API が使用されるため、\ 記号を使用してください。
Citrix (Citrix ウェブインターフェース)	IP アドレス	172.55.44.3
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート	172.55.44.3:8080 または [2008::1:2:3:4]:8080
	IP:パスまたはファイル	172.55.44.3/フォルダ/file.html
	IP:ポート:パスまたはファイル	172.55.44.3:8080/report.pdf
	FQDN	www.citrixhost.company.net
	URL:パスまたはファイル	www.citrixhost.net/フォルダ/
	URL:ポート	www.citrixhost.company.net:8080
	URL:ポート:パスまたはファイル	www.citrixhost.com:8080/フォルダ/index.html
	メモ：ポートは、Citrix クライアント ポートではなく、Citrix ウェブ インターフェースの HTTP(S) ポートです。	

ヒント：Linux サーバへの **Virtual Network Computing (VNC)** ブックマークを作成するときは、「**ホスト名または IP アドレス**」フィールドで、Linux サーバの IP アドレスとともにポート番号とサーバ番号を**ipaddress:port:server**の形式で指定する必要があります。例えば、Linux サーバの IP アドレスが 192.168.2.2、ポート番号が 5901、サーバ番号が 1 の場合は、「**ホスト名または IP アドレス**」フィールドに**192.168.2.2:5901:1**を指定します。

4 「**サービス**」ドロップダウン メニューを使って、適切なブックマーク サービスを選択します。ブックマークの作成を完了するには、選択したサービスに関する次の情報を使います。

ターミナル サービス (RDP - HTML5 およびネイティブ)

- 「**画面サイズ**」ドロップダウン リストで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。

画面サイズはコンピュータによって異なるので、リモート デスクトップ アプリケーションを使用するときは、リモート デスクトップ セッションの実行元のコンピュータ画面のサイズを選択する必要があります。また、場合によっては「**アプリケーション パス**」フィールドでリモート コンピュータ上のアプリケーションのパスを指定する必要があります。

- 「**カラー**」ドロップダウン リストで、このブックマークの実行時に使用されるターミナル サービス画面の既定の色深度を選択します。
- オプションで、このアプリケーションへのローカル パスを「**アプリケーションおよびパス**」フィールドに入力します。
- 「**次のフォルダから開始**」フィールドに、アプリケーション コマンドを実行するローカル フォルダをオプションで入力します。
- 「**コンソール / 管理者セッションとしてログインする**」をオンにすると、コンソールまたは管理者としてログインできます。RDC 6.1 以降では、admin セッションへのログインは、コンソール セッションへのログインに置き換わります。
- 「**Wake on LAN を有効にする**」をオンにすると、ネットワーク接続を介してコンピュータの電源を投入できます。このチェックボックスをオンにした場合、以下の新しいフィールドが表示されます。
  - **MAC/イーサネット アドレス** - 電源を投入するホストの 1 つ以上の MAC アドレスをスペースで区切って入力します。
  - **起動待ち時間 (秒)** - WoL 操作を中止するまでターゲット ホストの起動完了を待機する時間を秒単位で入力します。
  - **WOL パケットをホスト名または IP アドレスに送信する** - WOL パケットをこのブックマークのホスト名または IP アドレスに送信するには、「**WOL パケットをホスト名または IP アドレスに送信する**」をオンにします。この設定は、WOL で電源を投入する別のコンピュータの MAC アドレスと併用して適用できます。
- ブックマークを使用してターミナル サービス ファームを起動する場合は、「**サーバは TS ファーム**」をオンにします。ターミナル サービス ブックマークによってクライアントをターミナル サーバに接続するには、互換性のあるクライアントがインストールされている必要があります。

ターミナル サービス (RDP - HTML5)

- 「**画面サイズ**」ドロップダウン リストで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。

画面サイズはコンピュータによって異なるので、リモート デスクトップ アプリケーションを使用するときは、リモート デスクトップ セッションの実行元のコンピュータ画面のサイズを選択する必要があります。また、場合によっては「**アプリケーション パス**」フィールドでリモート コンピュータ上のアプリケーションのパスを指定する必要があります。

メモ：RDP - HTML5 ブックマークは、iOS および Android 機器上の既定のブラウザを使用してサポートされます。

- 「**カラー**」ドロップダウン リストで、このブックマークの実行時に使用されるターミナル サービス画面の既定の色深度を選択します。
- 「**Wake on LAN を有効にする**」をオンにすると、ネットワーク接続を介してコンピュータの電源を投入できます。このチェックボックスをオンにした場合、以下の新しいフィールドが表示されます。
  - **MAC/イーサネット アドレス** - 電源を投入するホストの 1 つ以上の MAC アドレスをスペースで区切って入力します。
  - **起動待ち時間 (秒)** - WoL 操作を中止するまでターゲット ホストの起動完了を待機する時間を秒単位で入力します。
  - **WOL パケットをホスト名または IP アドレスに送信する** - WOL パケットをこのブックマークのホスト名または IP アドレスに送信するには、「**WOL パケットをホスト名または IP アドレスに送信する**」をオンにします。この設定は、WOL で電源を投入する別のコンピュータの MAC アドレスと併用して適用できます。
- 「**コンソール / 管理者セッションとしてログインする**」をオンにすると、コンソールまたは管理者としてログインできます。RDC 6.1 以降では、admin セッションへのログインは、コンソール セッションへのログインに置き換わります。
- ブックマークを使用してターミナル サービス ファームを起動する場合は、「**サーバは TS ファーム**」をオンにします。ターミナル サービス ブックマークによってクライアントをターミナル サーバに接続するには、互換性のあるクライアントがインストールされている必要があります。
- 「**詳細な Windows オプションを表示**」を選択して、**デスクトップ背景、メニューとウインドウ アニメーション、ドラッグ/リサイズの間にウィンドウの内容を表示する、クリップボードをリダイレクトする、ポートをリダイレクトする、接続バーを表示する、プリンタをリダイレクトする、リモート音声、自動再接続、表示スタイル、リモート コピー、ドライブをリダイレクトする、スマートカードをリダイレクトする、ビットマップのキャッシュ**。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ)を参照してください。

仮想ネットワーク コンピューティング (VNC)

- 「**エンコード**」ドロップダウン メニューで、適切なエンコード転送形式を選択します。Raw、RRE、CoRRE、Hextile、Zlib、Tight などのオプションがあります。
- 「**圧縮レベル**」ドロップダウン メニューを使って、データの適切な圧縮レベルを選択します。
- 「**JPEG イメージ品質**」ドロップダウン メニューを使って、JPEG 画像ファイルの品質レベルを選択します。
- 「**カーソル状態更新**」ドロップダウン メニューで、これらの更新の「**有効化**」、「**無効化**」、または「**無視**」を選択します。
- 「**リモート貼り付けキー**」ドロップダウン メニューで、**Ctrl + V**、**Meta + V**、または **Alt + V** を選択します。
- 対応するチェックボックスを使って「**CopyRect を使用**」機能を有効または無効にします。

- 対応するチェックボックスを使って「**制限された色数 (256色)**」のみの使用を有効または無効にします。

  メモ：制限された色数は、Mac の画面共有ではサポートされていないので、Mac の画面共有が利用されている場合はこのオプションを有効にしないでください。

- VNC を介した制御が行われないようにするには、「**表示のみ**」を有効にします。
- VNC を介したデスクトップ表示の共有を許可する場合は、「**デスクトップ共有**」を有効にします。
- VNC クライアントとサーバの間でテキストをコピーする場合は、「**リモート コピー**」を有効にします。
- 「**Mobile Connect クライアントにブックマークを表示する**」オプションを選択すると、Mobile Connect クライアントにこのブックマークが表示されます。このブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

HTML5 ブックマークの機能

利用できる機能

機能	HTML5 バージョン
エンコード	はい (設定は可能ではなく、VNC サーバによって決定。サポートされているエンコード: Raw、CopyRect、RRE、Hextile、Tight、TightPNG、Zlib)
圧縮レベル	いいえ
JPEG イメージ品質	いいえ
カーソル状態更新	はい (既定で有効。IE ではサポートされていません。モバイル ブラウザの場合、"カーソル形状更新" は常に無効)
CopyRect の使用	はい (設定は不可)
制限された色数 (256 色)	いいえ
表示のみ	はい
デスクトップ共有	はい
Mobile Connect クライアントにブックマークを表示する	はい

仮想ネットワーク コンピューティング (VNC - HTML5)

- VNC を介した制御が行われないようにするには、「**表示のみ**」を有効にします。
- VNC を介したデスクトップ表示の共有を許可する場合は、「**デスクトップ共有**」を有効にします。

Citrix Portal (Citrix)

- 「**リソース ウィンドウ サイズ**」ドロップダウン リストから、ユーザがこのブックマークを実行した際に Citrix セッションで使用する既定の画面サイズを選択します。
- このブックマークで「**スマート**」と「**手動**」のどちらのアクセス タイプを使用するかを選択します。新しい Citrix ブックマークは既定で「**スマート**」になります。起動シーケ

ンスは、「HTML5」、「Native」、「ActiveX」です。「手動」を選択すると、アクセスタイプの起動方法を変更、有効化、または無効化できます。

- 「**Citrix サーバによるクライアント検知を無効にする**」をオンにして、ブックマークを使用する場合に Citrix サーバによるクライアント検知を無効にします。SMA/SRA 装置は Citrix を使用する場合、Citrix クライアント検知を必ず実行します。Citrix サーバでクライアント検知を有効にすると、このクライアント検知が冗長になります。

メモ：この機能は、ActiveX クライアントを使用することで Citrix XenApp 5.0 以降に対応します。

- Citrix ウェブ サーバが SSL を使用して、SMA/SRA 装置と Citrix サーバ間の通信に対して SSL 暗号化を有効にするよう設定されている場合は、「**HTTPS モード**」をオンにします。
- Citrix ICA セッションの Citrix ICA サーバ アドレスを明示的に設定するには、「**指定した Citrix ICA サーバを常に使用する**」をオンにして、「**Citrix ICA サーバ アドレス**」フィールドにサーバの IP アドレスを入力します。

  Citrix 配備の中には、1 つの IP アドレスに Citrix ウェブ インターフェースを持ち、別のアドレスで ICA サーバを待機するものがあります。Citrix ウェブ インターフェースと Citrix ICA サーバが同じ IP アドレスを共有しない場合は、この設定を使用して、ICA サーバのアドレスを明示的に設定してください。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ)を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアントにこの Citrix ブックマークが表示されます。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

メモ：Citrix ブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

- Mobile Connect ユーザに、設定されているサードパーティ アプリケーションではなく、アプリケーション内セキュア ウェブ ブラウザを強制的に使用させるには、「**MC セキュア ウェブ ブラウザを強制する**」を選択します。このオプションを有効にするには、Mobile Connect は、バージョン 5.0 以降である必要があります。この設定は、HTTP と HTTPS ブックマークのユーザ設定よりも優先されます。また、RDP、VNC、SSH、Telnet、HTTP、HTTPS、および外部ウェブサイト サービスに対してのみ使用できます。
  - ユーザが Mobile Connect セキュア ウェブ ブラウザにおいて URL を編集できるようにするには、「**セキュア ウェブ ブラウザにおける URL 編集を許可する**」オプションを選択します。このオプションを適用するには、Mobile Connect はバージョン 5.0 以降である必要があります。このオプションを有効にすると、ウェブ ブックマーク (HTTP および HTTPS) に対する Mobile Connect クライアントのブックマーク設定よりも優先されます。この設定は、HTTP/HTTPS ブックマークに対してのみ使用できます。
-

ウェブ (HTTP)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ)を参照してください。
- シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の'name'または'id'属性と同じになるように設定します。例えば、<input type=text name='userid'> のようにします。「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の 'name' または 'id' 属性と同じになるように設定します。例えば、<input type=password name='PASSWORD' id='PASSWORD' maxlength=128> のようにします。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアントに、このブックマークが表示されます。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

メモ：このウェブ (HTTP) ブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

- Mobile Connect ユーザに、設定されているサードパーティ アプリケーションではなく、アプリケーション内セキュア ウェブ ブラウザを強制的に使用させるには、「**MC セキュア ウェブ ブラウザを強制する**」を選択します。このオプションを有効にするには、Mobile Connect は、バージョン 5.0 以降である必要があります。この設定は、HTTP および HTTPS ブックマークに対するユーザ設定よりも優先されます。
    - ユーザが Mobile Connect セキュア ウェブ ブラウザにおいて URL を編集できるようにするには、「**セキュア ウェブ ブラウザにおける URL 編集を許可する**」オプションを選択します。このオプションを適用するには、Mobile Connect はバージョン 5.0 以降である必要があります。このオプションを有効にすると、ウェブ ブックマーク (HTTP および HTTPS) に対する Mobile Connect クライアントのブックマーク設定よりも優先されます。

セキュア ウェブ (HTTPS)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の'name'または'id'属性と同じになるように設定します。例えば、<input type=text name='userid'> のようにします。「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の 'name' または 'id' 属性と同じになるように設定します。例えば、<input type=password name='PASSWORD' id='PASSWORD' maxlength=128> のようにします。

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアントにこの HTTPS ブックマークが表示されます。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

メモ：この HTTPS ブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

- Mobile Connect ユーザに、設定されているサードパーティ アプリケーションではなく、アプリケーション内セキュア ウェブ ブラウザを強制的に使用させるには、「**MC セキュア ウェブ ブラウザを強制する**」を選択します。このオプションを有効にするには、Mobile Connect は、バージョン 5.0 以降である必要があります。この設定は、HTTP および HTTPS ブックマークに対するユーザ設定よりも優先されます。
    - ユーザが Mobile Connect セキュア ウェブ ブラウザにおいて URL を編集できるようにするには、「**セキュア ウェブ ブラウザにおける URL 編集を許可する**」オプションを選択します。このオプションを適用するには、Mobile Connect はバージョン 5.0 以降である必要があります。このオプションを有効にすると、ウェブ ブックマーク (HTTP および HTTPS) に対する Mobile Connect クライアントのブックマーク設定よりも優先されます。

外部ウェブ サイト

- **HTTPS モード** - SSL プロトコルを使用してウェブ通信を暗号化する場合に選択します。
- **セキュリティ警告を無効にする** - このブックマークがアプリケーション オフロードされたウェブ サイトを参照しておらず、このチェックボックスが無効である場合は、セキュリティ警告ダイアログが表示されます。
- **自動的にログインする** - このブックマークの仮想ホスト ドメイン SSO を有効にします。ブックマーク内のホストが、このポータルと同一の共有ドメインを持つポータルを参照する場合、このポータルの認証情報で自動的にログインすることができます。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアントにこの外部ウェブ サイト ブックマークが表示されます。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

メモ：この外部ウェブ サイト ブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

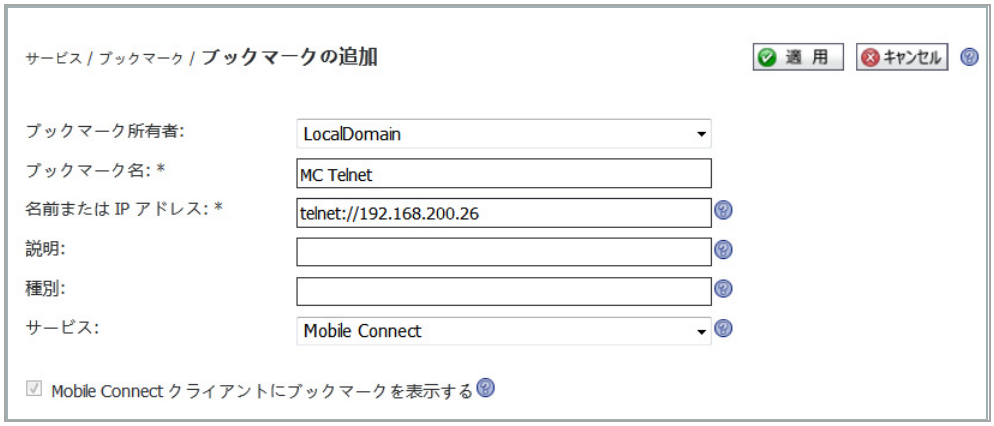
- Mobile Connect ユーザに、設定されているサードパーティ アプリケーションではなく、アプリケーション内セキュア ウェブ ブラウザを強制的に使用させるには、「**MC セキュア ウェブ ブラウザを強制する**」を選択します。このオプションを有効にするには、Mobile Connect は、バージョン 5.0 以降である必要があります。この設定は、HTTP および HTTPS ブックマークに対するユーザ設定よりも優先されます。
    - ユーザが Mobile Connect セキュア ウェブ ブラウザにおいて URL を編集できるようにするには、「**セキュア ウェブ ブラウザにおける URL 編集を許可する**」オプションを選択します。このオプションを適用するには、Mobile Connect はバージョン 5.0 以降である必要があります。このオプションを有効にすると、ウェブ ブックマーク (HTTP および HTTPS) に対する Mobile Connect クライアントのブックマーク設定よりも優先されます。

Mobile Connect

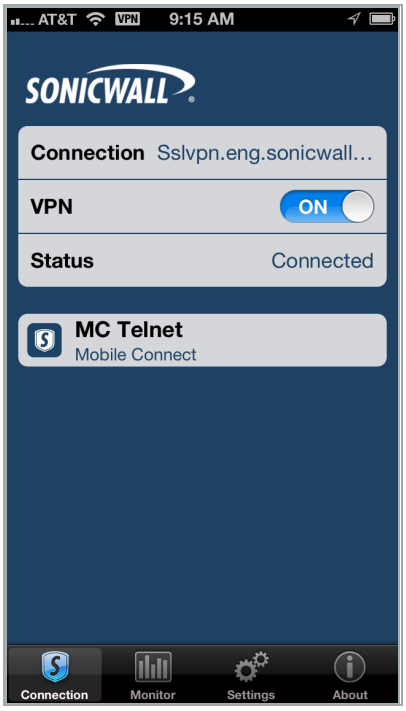
Mobile Connect ブックマークにより、ユーザが接続した後に Mobile Connect に表示する個別ブックマークを定義できます。このブックマークは、社内アプリや、App Store または Google Play の公開アプリを含む、任意のサードパーティ アプリをサポートするためのものです。またこのブックマークにより、Google Earth に対する 'comgoogleearth://' といった、カスタム URL スキームが定義されているサードパーティ アプリを呼び出すことも可能です。Mobile Connect ブックマークは、通常のブラウザからの編集のみが可能で、モバイル機器上のみで使用します。

メモ：Mobile Connect ブックマークは、'http://' または 'https://' のURL スキームに対しても使用できますが、SonicWall Inc. では、これらのスキームに対して HTTP または HTTPS ブックマークを使用することを推奨します。

- 「**ブックマーク名**」と「**ホスト名または IP アドレス**」を入力します。「名前または IP アドレス」フィールドは、カスタム URL スキームです。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

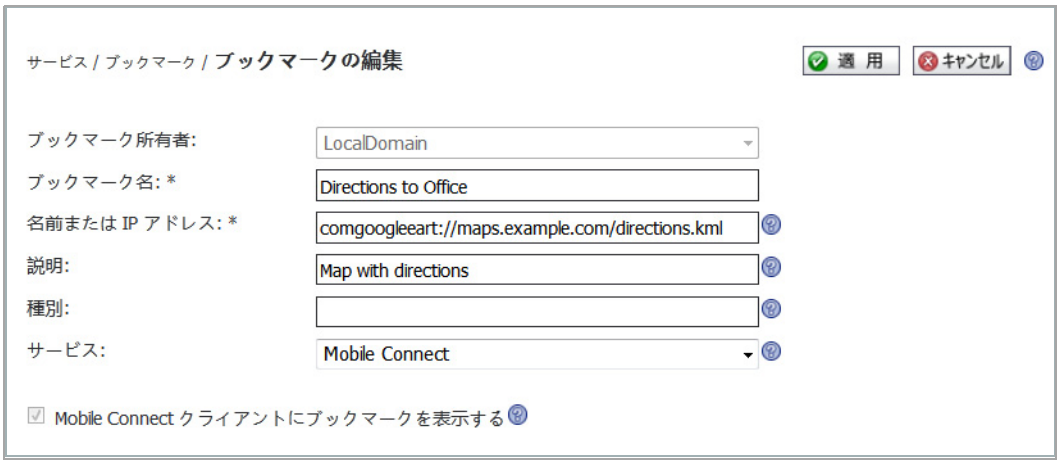


Secure Mobile Access 上の Mobile Connect ブックマークが正しく設定されると、ブックマークがお使いのモバイル機器上に表示されます。

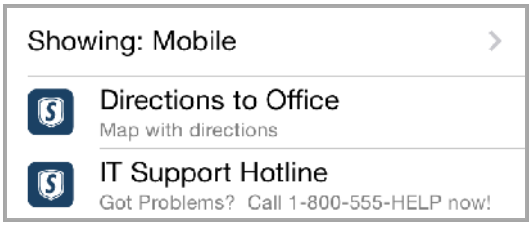


Mobile Connect ブックマークの以下の例では、Google Earth を使用するブックマークを作成して、特定の道順を示す地図を表示する方法を示します。

まず、URL スキームを使用してブックマークを作成する必要があります。

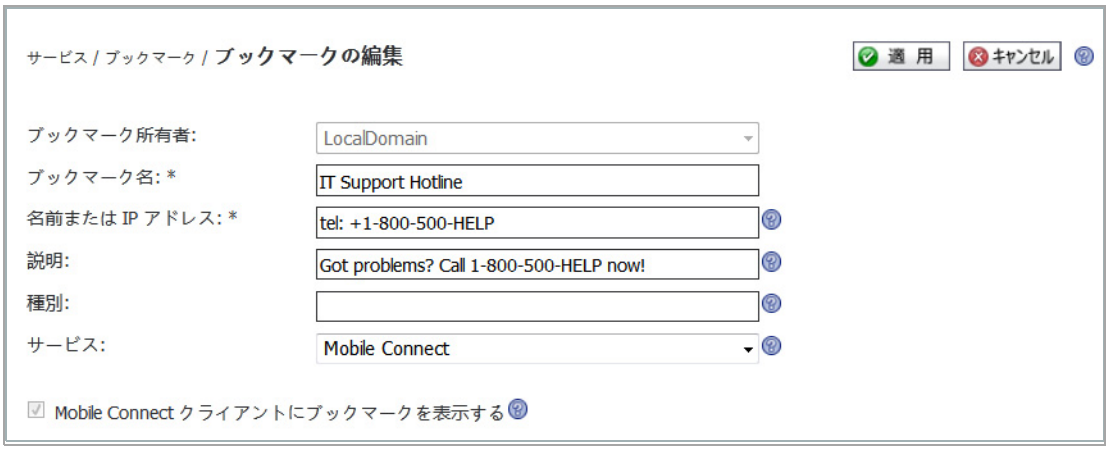


このブックマークが、お使いのモバイル機器からアクセス可能になります。

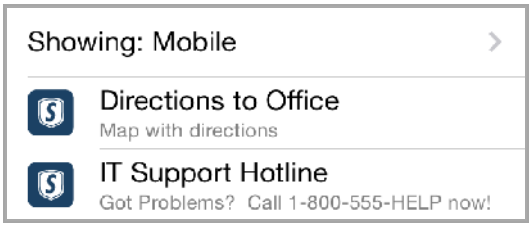


新しく追加されたブックマークを選択します。「オフィスへの道順」ブックマークに対し、以下のように Google Map が表示されます。

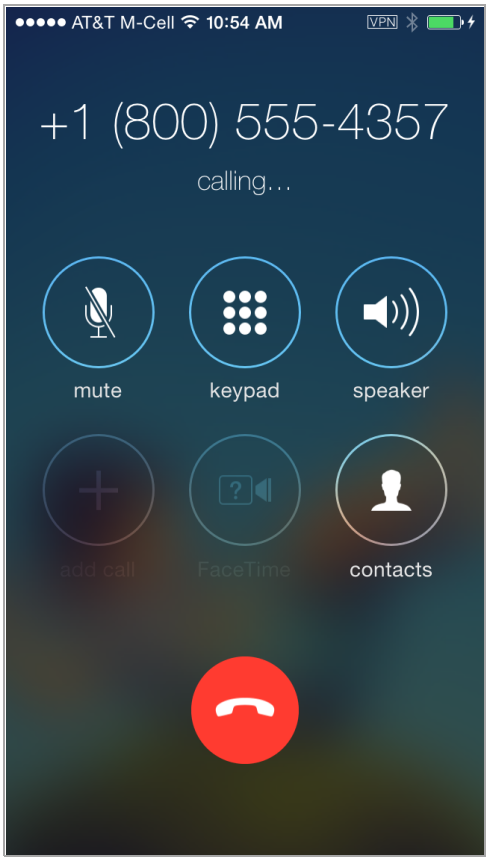
次の例は、Mobile Connect ブックマークの別の使用方法を示したものです。この例では、iOS の電話アプリを起動して IT サポート ホットラインに電話をかけるブックマークを追加します。



このブックマークが、お使いのモバイル機器からアクセス可能になります。



新しく追加されたブックマークを選択します。「IT サポート ホットライン」ブックマークに対し、以下のように iOS の電話アプリによる IT サポート ホットラインへの発信が開始します。



ファイル共有 (CIFS)

メモ：SMB2 および SMB3 プロトコルは現在サポートされていません。サーバは、Linux ベースのクライアントからの通信を許可するよう設定する必要があります。

- クライアント UI へのアクセスを制限するには、「**特定のファイル/フォルダにアクセスするユーザを設定する**」をオンにします。完全にアクセスを制限するには、「**サービス > ポリシー**」ページに移動して、アクセス制限のポリシーを設定します。詳細については、ポリシーの追加 (249 ページ) を参照してください。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

  ファイル共有を作成するときは、DFS (Distributed File System) サーバをウィンドウズ ドメイン ルート システムに設定しないでください。ドメイン ルートはドメイン内の Windows コンピュータへのアクセスのみを提供するので、DFS サーバをドメイン ルートに設定すると、他のドメインから DFS ファイル共有にアクセスできません。SMA/SRA 装置は、ドメイン メンバではなく、このような DFS 共有に接続できません。

  スタンドアロン ルート上の DFS ファイル共有には、Microsoft の制限は適用されません。

ファイル転送プロトコル (FTP) と SSH ファイル転送プロトコル (SFTP)

- 「**詳細なサーバ設定を表示**」を展開して、代替値を「**文字エンコード**」ドロップダウンリストで選択します。既定値は「**標準 (UTF-8)**」です。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから FTP サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

Telnet HTML5 設定

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアントにこの外部ウェブ サイト ブックマークが表示されます。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

メモ：この外部ウェブ サイト ブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

- Mobile Connect ユーザに、設定されているサードパーティ アプリケーションではなく、アプリケーション内セキュア ウェブ ブラウザを強制的に使用させるには、「**MC セキュア ウェブ ブラウザを強制する**」を選択します。このオプションを有効にするには、Mobile Connect は、バージョン 5.0 以降である必要があります。この設定は、HTTP および HTTPS ブックマークに対するユーザ設定よりも優先されます。
    - ユーザが Mobile Connect セキュア ウェブ ブラウザにおいて URL を編集できるようにするには、「**セキュア ウェブ ブラウザにおける URL 編集を許可する**」オプションを選択します。このオプションを適用するには、Mobile Connect はバージョン 5.0 以降である必要があります。このオプションを有効にすると、ウェブ ブックマーク (HTTP および HTTPS) に対する Mobile Connect クライアントのブックマーク設定よりも優先されます。

セキュア シェル バージョン 2 (SSHv2)

SSHv2 HTML5 設定

- 「**既定のフォント サイズ**」を選択します。サポートされているオプションは、12 ～ 99 ポイントの範囲です。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。

SSHv2 共通設定

- 必要に応じて、「**自動的にホスト キーを受け入れる**」をオンにします。このオプションを選択すると、ブラウザは、サーバの公開ホスト キーをローカル ストレージに自動的に保持します。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアントにこの外部ウェブ サイト ブックマークが表示されます。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

ⓘ **メモ**：この外部ウェブ サイト ブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

- Mobile Connect ユーザに、設定されているサードパーティ アプリケーションではなく、アプリケーション内セキュア ウェブ ブラウザを強制的に使用させるには、「**MC セキュア ウェブ ブラウザを強制する**」を選択します。このオプションを有効にするには、Mobile Connect は、バージョン 5.0 以降である必要があります。この設定は、HTTP および HTTPS ブックマークに対するユーザ設定よりも優先されます。
    - ユーザが Mobile Connect セキュア ウェブ ブラウザにおいて URL を編集できるようにするには、「**セキュア ウェブ ブラウザにおける URL 編集を許可する**」オプションを選択します。このオプションを適用するには、Mobile Connect はバージョン 5.0 以降である必要があります。このオプションを有効にすると、ウェブ ブックマーク (HTTP および HTTPS) に対する Mobile Connect クライアントのブックマーク設定よりも優先されます。

- SSHv2 サーバを認証なしで使用している場合 (SonicWall Inc. ファイアウォールなど)、「**ユーザ名をバイパスする**」をオンにできます。
- 「**適用**」を選択して設定を更新します。設定が更新されると、新しいグループ ブックマークが「**ローカル グループの編集**」ページに表示されます。

ブックマークの編集

サービス ブックマークを編集するには、「**サービス > ブックマーク**」画面に移動します。「**設定**」カラムにある**鉛筆アイコン**を選択します。新しい「**ブックマークの編集**」ウィンドウが開き、ブックマークの現在の設定が表示されます。必要な調整をすべて行い、「**OK**」を選択します。編集されたブックマークが「**サービス > ブックマーク**」ウィンドウに表示されます。

ブックマークの削除

設定済みのブックマークを削除するには、「**サービス > ブックマーク**」画面に移動します。「**設定**」カラムにある"**X**"アイコンを選択します。ダイアログ ボックスが開き、指定したブックマークを本当に削除するかどうかを尋ねられます。「**OK**」を選択すると、ブックマークが削除されます。削除したブックマークは「**サービス > ブックマーク**」画面に表示されなくなります。

サービス > ポリシー

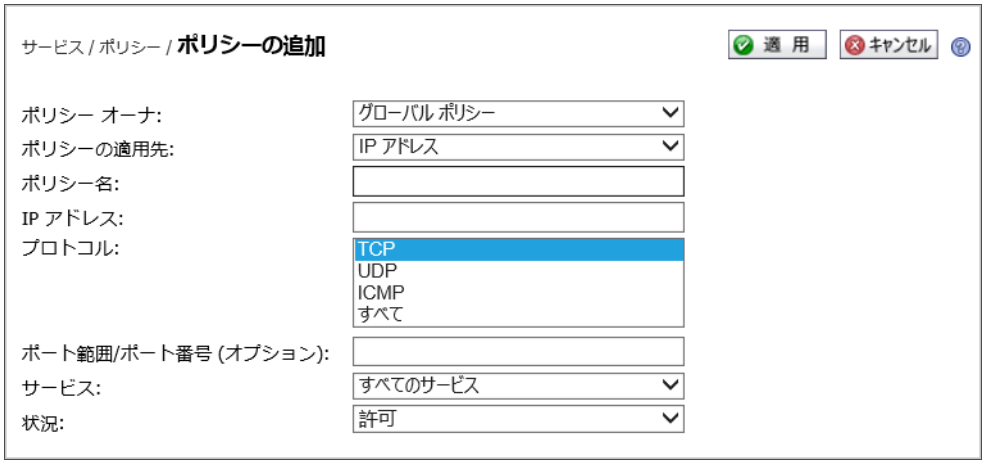
ウェブベースの Secure Mobile Access 管理インターフェース内の「**サービス > ポリシー**」ページは、サービス ポリシーを表示するための単一のインターフェースであり、ユーザおよびグループのポリシーを設定できます。

次を参照してください。

- ポリシーの追加 (249 ページ)
- ポリシーの編集 (251 ページ)
- ポリシーの削除 (251 ページ)

ポリシーの追加

ポリシーを追加するには、Secure Mobile Access 管理インターフェース内の「**サービス > ポリシー**」画面に移動し、「**ポリシーの追加...**」を選択します。「**ポリシーの追加**」ウィンドウが開きます。



管理者は、以下の手順に従ってサービス ポリシーを追加できます。

1 「**ポリシー オーナ**」ドロップダウン メニューを使って、ポリシーが「**グローバル ポリシー**」、「**LocalDomain**」グループ ポリシー、または個々の「**ユーザ**」に割り当てられたポリシーのいずれの形で所有されるかを選択します。

2 「**ポリシーの適用先**」ドロップダウン メニューで、ポリシーの適用先として、個別ホスト、ネットワーク アドレスの範囲、すべてのアドレス、ネットワーク オブジェクト、サーバ パス、または URL オブジェクトのいずれかを選択します。単一の IPv6 ホスト、IPv6 アドレス範囲、またはすべての IPv6 アドレスの選択もできます。「**ポリシーの追加**」ダイアログ ボックスの内容は、「**ポリシーの適用先**」ドロップダウン リストで選択したオブジェクトの種別に応じて変化します。

> **メモ:** これらの Secure Mobile Access のポリシーは Secure Mobile Access 接続の送信元アドレスではなく送信先アドレスに適用されます。インターネット上の特定の IP アドレスが「**ポリシー**」タブ上で作成されたポリシーを用いて SMA/SRA ゲートウェイの認証を受けることを許可または阻止することはできません。ただし、ユーザの「**ログイン ポリシー**」タブ上で作成されたログイン ポリシーを用いて IP アドレスにより送信元ログインを制御することが可能です。詳細については、ログイン ポリシーの設定 (434 ページ) を参照してください。

3 「**ポリシーの適用先**」メニューで選択した内容に応じて、次のうち適切な手順を実行します。

- **IP アドレス** - 特定のホストにポリシーを適用する場合は、ローカル ホスト コンピュータの IP アドレスを「**IP アドレス**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IP アドレスのポリシーの追加 (404 ページ) を参照してください。
- **IP ネットワーク** - アドレス範囲にポリシーを適用する場合は、IP アドレス範囲の開始アドレスを「**IP ネットワーク アドレス**」フィールドに入力し、IP アドレス範囲を定義するサブネットを「**サブネット マスク**」フィールドに入力します。または、ポート範囲 (例えば 4100 - 4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IP ネットワークに対するポリシーの追加 (405 ページ) を参照してください。

- **すべてのアドレス** - ポリシーをすべての IPv4 アドレスに適用する場合は、IP アドレス情報を入力する必要はありません。すべてのアドレスのポリシーの追加 (405 ページ) を参照してください。
- **ネットワーク オブジェクト** - 定義済みネットワーク オブジェクトにポリシーを適用する場合は、「**ネットワーク オブジェクト**」ドロップダウン リストでオブジェクトの名前を選択します。ネットワーク オブジェクトを定義するときにポートまたはポート範囲を指定できます。ネットワーク オブジェクトの追加 (145 ページ) を参照してください。
- **サーバ パス** -サーバ パスにポリシーを適用する場合は、「**リソース**」フィールドで以下のラジオ ボタンの 1 つを選択します。
  - 共有 (サーバ パス) - このオプションを選択するときは、パスを「サーバ パス」フィールドに入力します。
  - ネットワーク (ドメイン リスト)
  - サーバ (コンピュータ リスト)

  ファイル共有アクセス ポリシーの設定 (406 ページ) を参照してください。
- **URL オブジェクト** - 定義済みの URL オブジェクトにポリシーを適用する場合は、URL を「**URL**」フィールドに入力します。URL オブジェクトのポリシーの追加 (407 ページ) を参照してください。
- **すべての IPv6 アドレス** - すべての IPv6 アドレスにポリシーを適用する場合は、IP アドレス情報を入力する必要はありません。ユーザ ブックマークの追加または編集 (409 ページ) を参照してください。
- **IPv6 アドレス** - 特定のホストにポリシーを適用する場合は、ローカル ホスト マシンの IPv6 アドレスを「**IPv6 アドレス**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IPv6 アドレスに対するポリシーの追加 (408 ページ) を参照してください。
- **IPv6 ネットワーク** - アドレス範囲にポリシーを適用する場合は、先頭の IPv6 アドレスを「**IPv6 ネットワーク アドレス**」フィールドに入力して、この IPv6 アドレス範囲を定義する接頭辞を「**IPv6 接頭辞**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IPv6 ネットワークに対するポリシーの追加 (409 ページ) を参照してください。

4 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

メモ：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

5 サービスの種類を「**サービス**」ドロップダウン リストで選択します。ポリシーの適用先がネットワーク オブジェクトの場合は、そのネットワーク オブジェクトで定義されたサービスが使用されます。

6 「**状況**」ドロップダウン リストから「**許可**」または「**拒否**」を選択し、指定したサービスおよびホスト コンピュータの SMA 接続を許可または拒否します。

メモ：ウィザードの実行中に選択した特定のアクセス方式を拒否する内容のポリシーを 1 つ以上追加できます。

ヒント：Citrix ブックマークを使用するときには、ホストへのプロキシ アクセスを制限するために、Citrix サービスと HTTP サービスの両方に対して拒否ルールを設定する必要があります。

7 「**適用**」を選択して設定を更新します。設定を更新すると、新しいポリシーが「**サービス > ポリシー**」ウィンドウに表示されます。

メモ：SonicWall Inc. では、管理者が、信頼済みホストへのアクセスのみを許可するグローバルな「すべて拒否」ポリシーを設定することを推奨します。これによって、Secure Mobile Access から悪意のあるホストへの発信要求を防御できます。

グローバルな「すべて拒否」ポリシーを作成するには:

1 「**サービス > ポリシー**」ページで、「**ポリシーの追加**」を選択します。

2 「**ポリシー所有者**」で、ドロップダウン リストから「**グローバル ポリシー**」を選択します。

3 「**ポリシーの適用先**」で、ドロップダウン リストから「**すべてのアドレス**」を選択します。

4 「**ポリシー名**」で、このポリシーのわかりやすい名前 (「すべて拒否」など) を作成します。

5 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

メモ: プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

6 「**IP アドレス範囲**」は、自動的に既定の「**すべての IP アドレス**」になります。

7 「**サービス**」で、ドロップダウン リストから「**すべてのサービス**」を選択します。

8 「**状況**」で、ドロップダウン リストから「**拒否**」を選択します。

ポリシーの編集

サービス関連のポリシーを編集するには、「**サービス > ポリシー**」画面に移動します。「**設定**」カラムにある**鉛筆アイコン**を選択します。新しい「**ポリシーの編集**」ウィンドウが開き、ブックマークの現在の設定が表示されます。必要な調整をすべて行い、「**適用**」を選択します。編集されたブックマークが「**サービス > ポリシー**」ウィンドウに表示されます。

ポリシーの削除

設定済みのポリシーを削除するには、「**サービス > ポリシー**」画面に移動します。「**設定**」カラムにある“**X**”アイコンを選択します。ダイアログ ボックスが開き、指定したポリシーを本当に削除するかどうかを尋ねられます。「**OK**」を選択すると、ポリシーが削除されます。削除したポリシーは「**サービス > ポリシー**」画面に表示されなくなります。

7

デバイス管理の設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「デバイス管理」ページと、このページで行う設定タスクについて説明します。

トピック:

デバイス管理 > デバイス

Secure Mobile Access は、クライアント デバイスの一意なデバイス ID を取得します。この情報を使うと、すべての機器の表示、機器の状況の変更、不要な機器の削除を行うことができます。このセクションでは、「**デバイス管理 > デバイス**」ページの概要を説明します。

このセクションは次のサブセクションで構成されています。

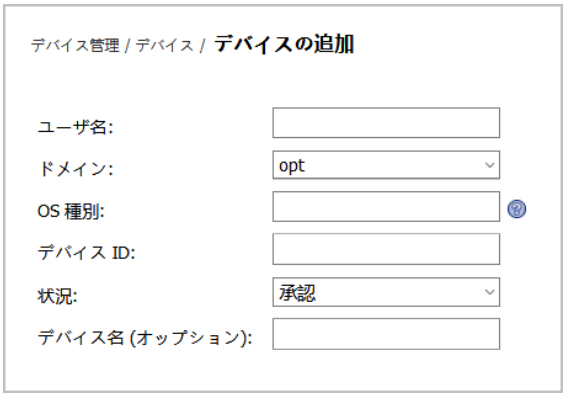
- デバイスの追加
- デバイスのインポート
- 選択したデバイスのエクスポート
- 選択したデバイスの削除
- 選択したデバイスの承認
- 選択したデバイスの拒否

デバイスの追加

「**デバイス管理 > デバイス**」ページでは、クライアント デバイスの追加、インポート、エクスポート、削除、承認、拒否を行うことができます。

新しいデバイスを追加するには:

1 「**デバイス管理 > デバイス**」ページに移動し、「**デバイスの追加**」をクリックします。「デバイスの追加」ウィンドウが表示されます。



2 「**デバイスの追加**」ウィンドウで、「**ユーザ名**」フィールドにユーザのユーザ名を入力します。これは、Secure Mobile Access ユーザ ポータルにログインするためにユーザが入力する名前です。

3 ユーザが所属するドメインの名前を「**ドメイン**」ドロップダウン リストで選択します。

4 「**OS 種別**」ウィンドウで、デバイスのオペレーティング システム情報を入力します。適合するオペレーティングシステムは、Windows、Android、iOS です。

5 「デバイス ID」ウィンドウにデバイス ID を入力します。

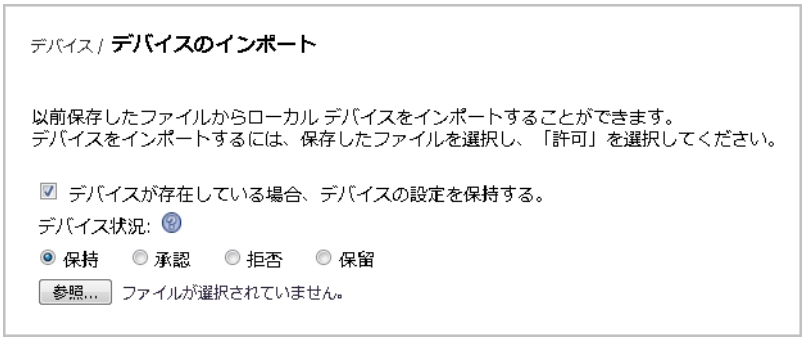
6 「**状況**」ドロップダウン メニューからデバイス状況を選択します。使用可能な状況のタイプは、「**拒否**」、「**承認**」、「**保留**」です。

7 「**適用**」を選択して設定を更新します。新しいデバイスが「**デバイス管理 > デバイス**」ページに表示されます。

デバイスのインポート

新しいデバイスをインポートするには:

1 「**デバイス管理 > デバイス**」ページに移動し、「**デバイスのインポート**」をクリックします。「**デバイスのインポート**」ページが表示されます。



2 デバイスの設定を保持するには「**デバイスが存在している場合、デバイスの設定を保持する**」を有効化します。そうしないと、削除したデバイスの設定は削除されます。

3 「**デバイス状況**」セクションで、インポートされたデバイスに対して以下のいずれかのデバイス状況を選択します。

- **保持** - インポートしたすべてのデバイスの状況がファイル内の状況のまま保持されます。
- **承認** - インポートしたすべてのデバイスの状況が「承認」に設定されます。
- **拒否** - インポートしたすべてのデバイスの状況が「拒否」に設定されます。
- **保留** - インポートしたすべてのデバイスの状況が「保留」に設定されます。

4 「**ファイルの選択**」をクリックして、以前保存した JSON ファイルからローカル デバイスをインポートします。

5 ファイルを選択し、「**開く**」をクリックしてデバイスをインポートします。

6 「**適用**」を選択して設定を更新します。インポートされたデバイスは、「**デバイス管理 > デバイス**」ページに表示されます。

選択したデバイスのエクスポート

選択したデバイスをエクスポートするには:

1 「**デバイス管理 > デバイス**」ページに移動します。

2 デバイスをエクスポートするには、デバイスのユーザ名の横にあるチェックボックスを選択し、「**デバイスのエクスポート**」をクリックします。拡張子が .json のファイルがハード ドライブに保存されます。

選択したデバイスの削除

選択したデバイスを削除するには:

1 「**デバイス管理 > デバイス**」ページに移動します。

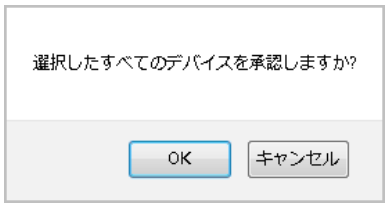
2 デバイスを削除するには、デバイスのユーザ名の横にあるチェックボックスを選択し、「**選択したデバイスの削除**」をクリックします。「**デバイス管理 > デバイス**」ページにある表からデバイスが削除されます。

選択したデバイスの承認

選択したデバイスを承認するには:

1 「**デバイス管理 > デバイス**」ページに移動します。

2 デバイスを承認するには、デバイスのユーザ名の横にあるチェックボックスを選択し、「**選択したデバイスの承認**」をクリックします。ウィンドウが表示され、「**選択したすべてのデバイスを承認しますか?**」と問われます。



3 「**OK**」をクリックします。「**デバイス管理 > デバイス**」ページで、デバイス状況が「承認」と表示されます。

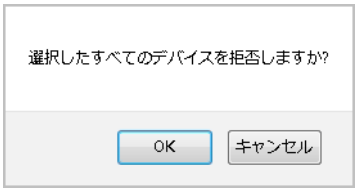
4 必要に応じて、デバイスの「**状況**」ドロップダウン メニューから「**承認**」を選択してデバイスを承認します。

選択したデバイスの拒否

選択したデバイスを拒否するには:

1 「**デバイス管理 > デバイス**」ページに移動します。

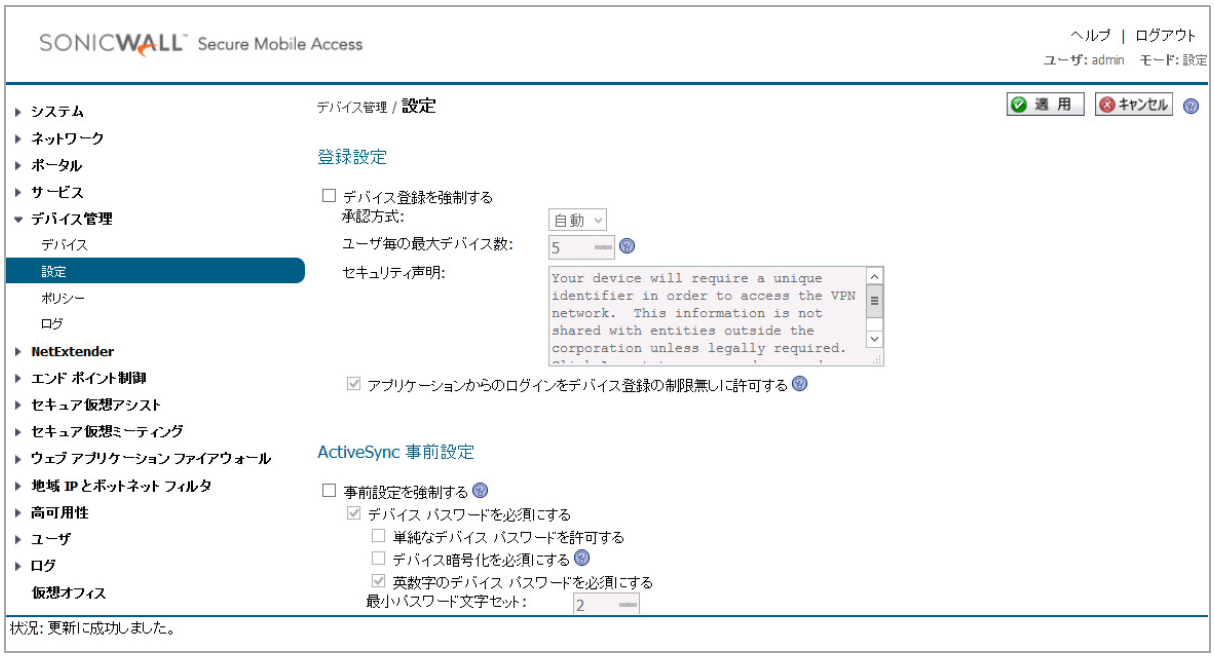
2 デバイスを拒否するには、デバイスのユーザー名の横にあるチェックボックスを選択し、「**選択したデバイスの拒否**」をクリックします。ウィンドウが表示され、「**選択したすべてのデバイスを拒否しますか?**」と問われます。



3 「**デバイス 管理 > デバイス**」ページで、デバイス状況が「拒否」と表示されます。

4 必要に応じて、デバイスの「**状況**」ドロップダウン メニューから「**拒否**」を選択してデバイスを拒否します。

デバイス管理 > 設定



登録の設定

デバイス登録を強制する

このオプションを使用して、個人用デバイスの認証 (PDA) を有効または無効にします。既定では無効になっています。

承認方式

2 つの方式として、**自動**と**手動**があります。1) **手動**モードにすると、各デバイスはユーザによる初回登録時に "保留" または "管理者による承認待ち" の状況になります。2) システムが自動モードの状態にあると、デバイスは承認済みに設定されます。自動モードは、管理者の負担を減らすことができます。

ユーザ毎の最大デバイス数

このオプションは、各ユーザが登録できるデバイスの最大数を制限します。

セキュリティ声明

この警告メッセージは、ユーザがログインする際にクライアントに表示されます。このセキュリティ声明はカスタマイズできます。

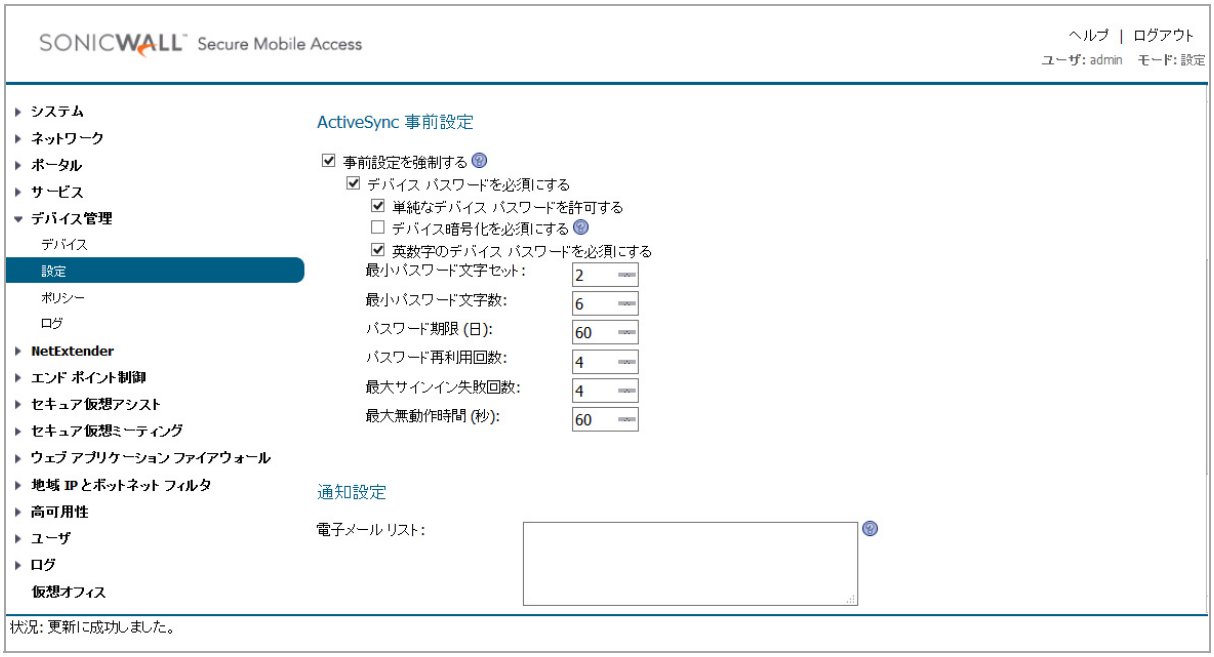
アプリケーションからのログインをデバイス登録の制限無しに許可する

このオプションは、SMA Connect Agent (接続エージェント) デバイス (Linux/Android/iOS/Windows Phone など) に適用されます。このオプションを有効にすると、デバイス登録を行わなくてもデバイスは装置にアクセスできます。

上記はグローバルな設定に関する説明です。デバイス登録を有効化する際に、登録の設定はドメインレベルでカスタマイズすることができます。ドメイン レベルの設定は、グローバル レベルの設定よりも優先されます。

ActiveSync 事前設定

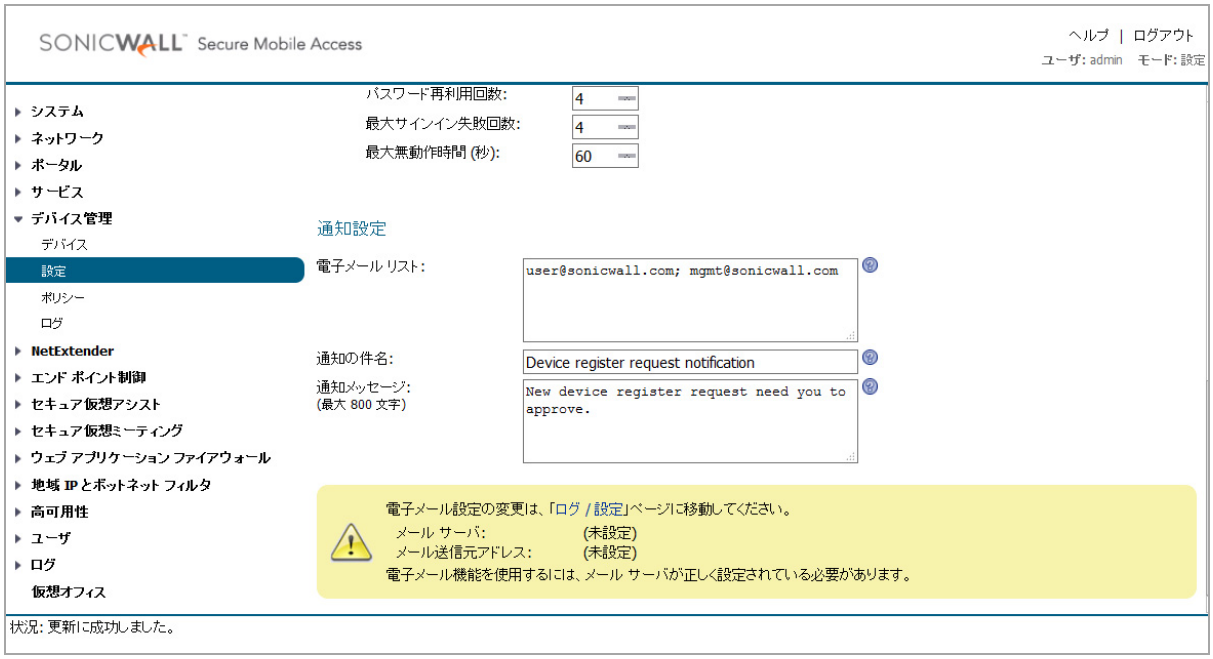
ActiveSync 事前設定は、ActiveSync デバイスのみに適用できます。事前設定によってバックエンド Exchange サーバ上の設定をオーバーライドできます。事前設定が満たされていない場合、モバイルデバイスは同期をとることができません。



通知設定

ここでは、一連の電子メール アドレスのリストを表示できます。新しい登録要求が届くと、これらのアドレスに電子メール通知が送信され、要求が処理されていることが受信者に通知されます。

この通知電子メールの件名とメッセージは、カスタマイズできます。



デバイス管理 > ポリシー

デバイス ポリシーはグローバルに有効なポリシーで、デバイスの登録が要求されたときに初めて適用されます。デバイスは、ポリシーが一致した場合に、そこに定義された動作を実行します。不一致であれば、デバイスは、承認済みの方式のオプションに従ってその状態を変更します。これにより、管理者の負担を減らすことができます。

機器ポリシーには、**機器 ID** と **OS** の 2 種類があります。既定では、機器 ID の優先順位のほうが OS よりも高くなっています。

演算子についても、**正規表現に一致**と**文字列に等しい**の 2 つがあります。文字列一致では、大文字と小文字が区別されます。既定では、文字列一致が正規表現一致よりも優先されます。

動作オプションには、3 つの選択肢、「**拒否**」、「**承認**」、「**保留**」があります。ポリシーに一致した場合、機器はここで定義されている動作を実行します。

デバイス管理 > ログ

デバイス管理のログは、機器についての詳しい情報を得るのに役立ちます。新しい機器の登録要求、機器の状況変化、機器の削除、電子メール通知などに関するログがあります。

8

クライアントの構成

このセクションでは、Secure Mobile Access ウェブベース管理インターフェースの「クライアント」ページに固有の情報と設定タスクについて説明します。

NetExtender/MobileConnect は、Windows、Mac、Linux、Android スマートフォン ユーザ用の Secure Mobile Access クライアントであり、透過的にダウンロードされ、会社のネットワーク上で任意のアプリケーションを安全に実行できるようにします。

接続にはポイント ツー ポイント プロトコル (PPP) が使用されます。NetExtenderr/MobileConnect によって、リモート クライアントはローカル ネットワーク上のリソースにシームレスにアクセスできます。

ユーザは NetExtender/MobileConnect に次の 3 つの方法でアクセスできます: (1) Secure Mobile Access ユーザ ポータル上で **NetExtender/MobileConnect** を使用する、(2) Microsoft インストーラ (MSI) を使用する、(3) Secure Mobile Access ウェブベース管理インターフェースのいずれかの **NetExtender クライアント**をクリックしてインストールした NetExtender スタンドアロン クライアントを使用する。NetExtender/MobileConnect スタンドアロン クライアントは、Windows システムでは「スタート」メニューから、Mac システムではアプリケーション フォルダまたはドックから、Linux システムではパス名によって、あるいはショートカット バーから、Android スマートフォンではアイコンから直接アクセスできます。

SMA/SRA 装置は、スタンドアロンの Windows NetExtender/MobileConnect クライアントと NetExtender/MobileConnect Mobile クライアントの両方でクライアント証明書をサポートしています。

ウィンドウズ システム上で、NetExtender/MobileConnect はウィンドウズにログインする前の VPN セッション確立をサポートします。NetExtenderr/MobileConnect は、Vista またはそれよりも新しいウィンドウズ システムと Linux クライアントからの IPv6 クライアント接続をサポートしています。NetExtender/MobileConnect 用の IPv6 アドレス プールはオプションですが、IPv4 アドレス プールは必須です。

NetExtender/MobileConnect の概念の詳細については、NetExtender の概要 (43 ページ) を参照してください。NetExtender/MobileConnect、NetExtender/MobileConnect Mobile、または NetExtender/MobileConnect Android クライアントの使い方とインストール方法については、最新の『*Secure Mobile Access ユーザ ガイド*』を参照してください。このドキュメントは次の場所にある SonicWall Inc. サポート ウェブ サイトの Secure Mobile Access ページで参照できます。参照先: SMA ドキュメント。

トピック:

クライアント > 状況

このセクションでは、「**クライアント > 状況**」ページの概要と、このページで実行できる設定タスクについて説明します。

「クライアント > 状況」の概要

「**クライアント > 状況**」ページで管理者はアクティブな NetExtender/MobileConnect セッションを表示できます。この情報には、名前、IP アドレス、ログイン時間、ログイン経過時間、ログアウト時間が含まれます。

クライアント > 状況

NetExtender/MobileConnect 状況の表示

「**クライアント > 状況**」ページで管理者はアクティブな NetExtender/MobileConnect セッションを表示できます。この情報には、名前、IP アドレス、ログイン時間、ログイン経過時間、管理用ログアウトコントロールが含まれます。次のNetExtender/MobileConnect 状況 表に、状況の各項目の説明を示します。

NetExtender/MobileConnect 状況

状況の項目	説明
名前	ユーザの名前
NetExtender/MobileConnect クライアントの IP アドレス	NetExtender/MobileConnect によってクライアント マシンに割り当てられた IP アドレス
ユーザの送信元 IP アドレス	ユーザがログインしているワークステーションの IP アドレス
場所	各セッションの送信元 IP の地理的な場所
接続開始時間	ユーザが SMA/SRA 装置との接続を最初に確立した時間 (曜日、日付、および時刻 (HH:MM:SS) の形式)
接続継続時間	ユーザが SMA/SRA 装置との接続を最初に確立してからの経過時間 (日数、時間、分、秒 (HH:MM:SS) の形式)
統計	セッション中に転送された送信、受信、合計のパケット数およびバイト数と、現在、最大、平均のスループットを示すツール チップを表示
切断	NetExtender/MobileConnect セッションを管理者が切断できるようにする

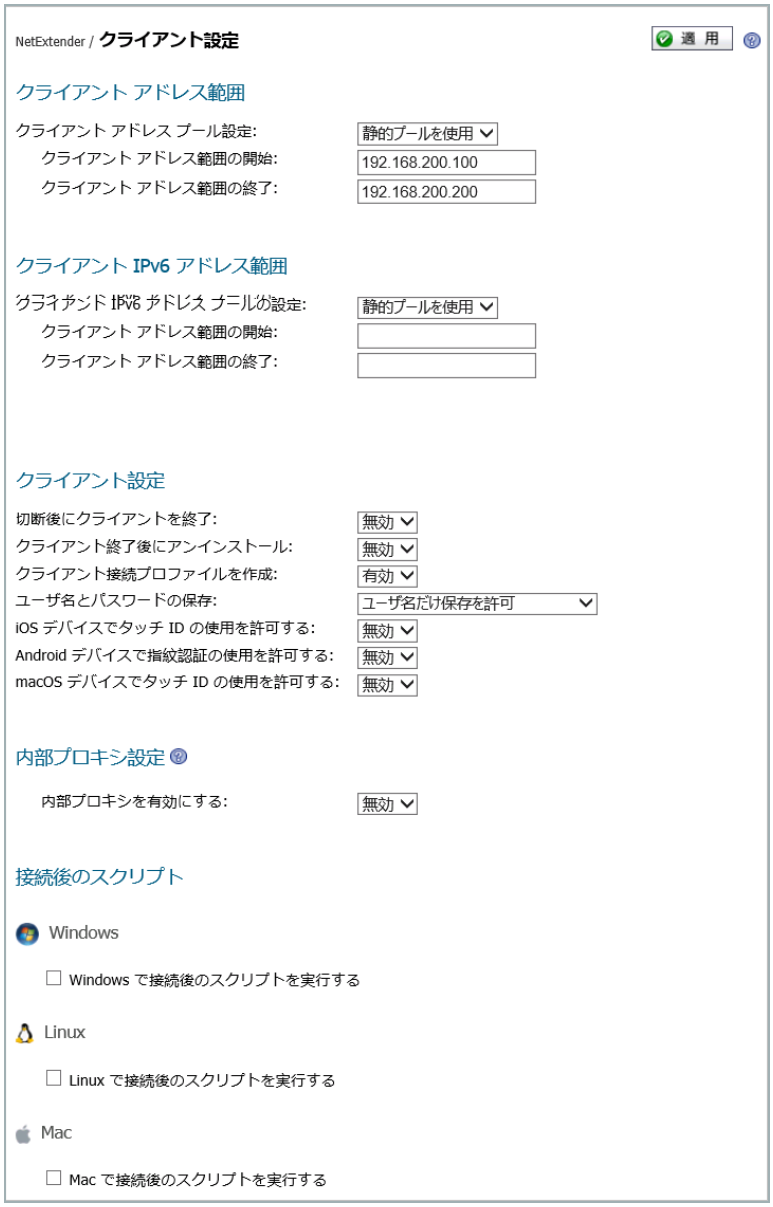
クライアント > 設定

このセクションでは、「**クライアント > 設定**」ページの概要と、このページで利用できる設定タスクについて説明します。

「クライアント > 設定」の概要

「**クライアント > 設定**」ページで管理者はクライアント アドレス範囲を指定できます。

クライアント > 設定



NetExtender/MobileConnect のグローバルな IP アドレス範囲を構成する

「**クライアント > 設定**」ページで管理者はグローバルなクライアント アドレス範囲を指定できます。IPv4 と IPv6 の両方についてアドレス範囲を指定できます。NetExtender/MobileConnect の IPv6 アドレス プールはオプションですが、IPv4 アドレス プールは必須です。NetExtender/MobileConnect のグローバルな IP 範囲は、IP アドレス プールを定義します。NetExtender/MobileConnect セッション中に、このプールからリモート ユーザにアドレスが割り当てられます。この範囲には、NetExtender/MobileConnect でサポートする同時実行ユーザ数の最大値に 1 を加えた大きさが必要です (例えば 15 人のユーザの場合には、192.168.200.100 ～ 192.168.200.115 のように 16 個のアドレスが必要です)。

この範囲は、SMA/SRA 装置の接続先インターフェースと同じサブネットに含まれる必要があります。SMA/SRA 装置と同じセグメント上に他のホストが存在する場合は、アドレス範囲が割り当て済みのアドレスと部分的に重なったり、衝突したりしないようにしてください。適切なサブネットを決定するには、次の方法のいずれかを使用します。

- NetExtender/MobileConnect 既定の範囲 (192.168.200.100 ～ 192.168.200.200) をそのまま使用できます。
- 使用する既存の DMZ サブネット内の範囲を選択します。例えば、DMZ で 192.168.50.0/24 サブネットを使用していて、最大 30 の NetExtender/MobileConnect 同時セッションをサポートする場合、192.168.50.220～192.168.50.250 (これらが未使用の場合) を使用できます。
- 使用する既存の LAN サブネット内の範囲を選択します。例えば、LAN で 192.168.168.0/24 サブネットを使用していて、最大 10 の NetExtender/MobileConnect 同時セッションをサポートする場合、192.168.168.240～192.168.168.250 (これらが未使用の場合) を使用できます。

静的 IP を使用して NetExtender/MobileConnect のグローバルなアドレス範囲を指定するには:

1 「**クライアント > 設定**」ページに移動します。

2 「**クライアント アドレス範囲**」の下で、ドロップダウン リストから「**静的プールを使用**」を選択します。

3 「**クライアント アドレス範囲の開始**」フィールドに、クライアント IPv4 アドレス範囲の開始アドレスを入力します。

4 「**クライアント アドレス範囲の終了**」フィールドに、クライアント IPv4 アドレス範囲の終了アドレスを入力します。

5 「**クライアント IPv6 アドレス範囲**」の下で、必要に応じて、ドロップダウン リストから「**静的プールを使用**」を選択します。

6 「**クライアント アドレス範囲の開始**」フィールドに、クライアント IPv6 アドレス範囲の開始アドレスを入力します。

7 IPv6 を使用する場合は、「**クライアント アドレス範囲の終了**」フィールドに、クライアント IPv6 アドレス範囲の終了アドレスを入力します。

8 「**適用**」を選択します。

9 「**状況**」メッセージに「**更新成功」と表示されます。 再起動すると現在のクライアントが新しいアドレスを取得します。**

DHCP を使用して NetExtender/MobileConnect のグローバルなアドレス範囲を指定するには:

1 「**クライアント > 設定**」ページに移動します。

2 「**クライアント アドレス範囲**」の下で、ドロップダウン リストから「**DHCP を使用**」を選択します。

3 「**インターフェースの選択**」の下で、ドロップダウン リストから DHCP に使用するインターフェースを選択します。

4 **DHCP サーバ**をフィールドに入力します。

5 「**クライアント IPv6 アドレス範囲**」の下で、必要に応じて、ドロップダウン リストから「**DHCP を使用**」を選択します。

6 「**インターフェースの選択**」の下で、ドロップダウン リストから DHCPv6 に使用するインターフェースを選択します。

7 **DHCPv6 サーバ**をフィールドに入力します。

8 「**適用**」を選択します。

9 「**状況**」メッセージに「**更新成功**」と表示されます。 再起動すると現在のクライアントが新しいアドレスを取得します。

Framed IP Address を使用して NetExtender/MobileConnect のグローバルなアドレス範囲を指定するには:

1 「**ユーザ > ローカル ユーザ > ユーザの編集 (Radius ドメイン ユーザ) > クライアント**」ページまたは「**ユーザ > ローカル グループ > ドメインの編集 (Radius) > クライアント**」ページに移動します。

2 「**クライアント アドレス プールの設定**」で、ドロップダウン リストから「**ユーザに割り当てられたアドレスを使用する**」を選択します。

3 「**クライアント IPv6 アドレス プール設定**」で、「**グローバル設定を使用**」、「**DHCPv6 を使用**」または「**静的プールを使用**」を選択します。

4 **プライマリ DNS サーバ**をフィールドに入力します。

5 **セカンダリ DNS サーバ**をフィールドに入力します。

6 **DNS 検索リスト** (検索順) をフィールドに入力します。

7 「**適用**」を選択します。

NetExtender/MobileConnect のグローバルな設定を構成する

SMA/SRA 装置には、ユーザが接続および切断するときの NetExtender/MobileConnect の動作を指定するさまざまな設定が用意されています。

NetExtender/MobileConnect のグローバルなクライアント設定を構成するには、以下の手順を実行します。

1 「**クライアント > 設定**」ページに移動します。

すべてのユーザに対して、以下のオプションを有効または無効にできます。

- **切断後にクライアントを終了** - SMA/SRA サーバから切断された NetExtender/MobileConnect クライアントは終了されます。再接続するには、Secure Mobile Access ポータルに戻るか、「プログラム」メニューから NetExtender/MobileConnect を起動する必要があります。このオプションは、Android スマートフォンを除き、サポートされるすべてのプラットフォームに適用されます。
- **クライアント終了後にアンインストール** - ユーザがクライアント ユーザ インターフェースを終了した際に、NetExtender/MobileConnect クライアントが自動的にアンインストールされます。これは、ユーザが NetExtender/MobileConnect トレイ アイコンを右クリックして「終了」を選択したときに起こります。再接続するには、Secure Mobile Access ポータルに戻って NetExtender/MobileConnect を選択して再インストールする必要があります。このオプションは、Windows クライアントにのみ適用されます。Android、Mac、または Linux クライアントには適用されません。
- **自動更新のオフを許可する** - NetExtender/MobileConnect クライアントが自動更新機能を無効にします。
- **クライアント接続プロファイルを作成** - NetExtender クライアントは、SMA/SRA サーバ名、ドメイン名、およびオプションでユーザ名とパスワードを記録した接続プロファイルを作成します。

2 「**ユーザ名とパスワードの保存**」オプションでは、ユーザが NetExtender/MobileConnect クライアントにユーザ名とパスワードをキャッシュできるようにするかどうかを設定できます。選択できるオプションは、「**ユーザ名だけ保存を許可**」、「**ユーザ名とパスワードの保存を許可**」、「**ユーザ名とパスワードの保存は不可**」の 3 つです。これらのオプションによって、セキュリティの必要性とユーザの使い勝手の両方に配慮した設定を実現できます。

3 このオプションが無効になっている場合、「**iOS デバイスでタッチ ID の使用を許可する**」では、iOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

4 このオプションが無効になっている場合、「**Android デバイスで指紋認証の使用を許可する**」では、Android デバイスでの指紋認証による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

5 このオプションが無効になっている場合、「**macOS デバイスでタッチ ID の使用を許可する**」では、macOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

6 「**iOS デバイスで Face ID の使用を許可する**」(macOS デバイスで Face ID 技術を使用して今後のログイン試行を遮断するコントロール) が無効化されていると、サーバはクライアントが接続を試みるまでクライアントの設定を変更する手段がありません。

7 「**無動作タイムアウトで切断**」で、NetExtender/MobileConnect クライアントは、セッションがあらかじめ定義された非アクティブ制限に達すると切断します。再接続するには、Secure Mobile Access ポータルに戻るか、「プログラム」メニューから NetExtender/MobileConnect を起動する必要があります。このオプションは、NetExtender Windows クライアントにのみ適用されます。

8 「**適用**」を選択します。

内部プロキシ設定の構成

NetExtender/MobileConnect では、すべてのユーザ トラフィックが指定された内部プロキシ サーバを経由するように、接続をプロビジョニングすることができます。内部プロキシ機能を有効にすると、使用するプロキシ サーバが指定できます。NetExtender/MobileConnect が SMA/SRA 装置に接続した後、内部プロキシ設定がクライアントにプッシュされ、NetExtender/MobileConnect 仮想アダプタのプロキシ設定として使用されます。

内部プロキシ設定を構成するには:

1 「**クライアント > 設定**」ページに移動します。

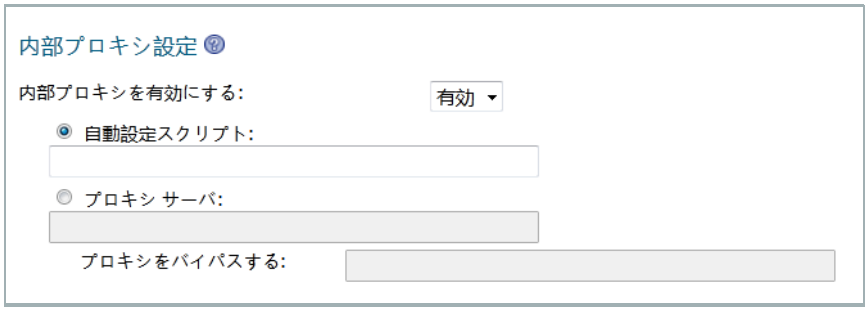
2 「**内部プロキシ設定**」の下の「内部プロキシを有効にする」で、「**有効**」を選択します。

3 内部プロキシ サーバに対して以下のいずれかを選択します。

- **自動設定スクリプト** - プロキシを自動設定するようにスクリプトを設定します。
- **プロキシ サーバ** - プロキシ サーバを手動で設定します。
- **プロキシをバイパスする** - プロキシ サーバを使用しないようにホストを設定します。

4 「**適用**」を選択してすべての変更を保存します。

クライアント > 設定 > 内部プロキシ設定



接続後スクリプトの設定

Windows、Linux、または Mac システムで接続後スクリプトを実行するには:

1 「**クライアント > 設定**」ページに移動します。

2 「**接続後スクリプト**」の下で、接続後スクリプトを実行するオペレーティング システムのセクションを探します。そのオペレーティング システムのセクションで、「**接続後のスクリプトを実行する**」をオンにします。

3 接続後スクリプトがローカルのクライアント マシン上に存在する場合は、「**ローカル ファイルを実行する**」を選択します。接続後スクリプトがサーバにアップロードされている場合は、「**リモート スクリプトを実行**」のラジオ ボタンを選択します。

4 ローカル ファイルの場合は、「**このファイルを実行する**」フィールドにスクリプト パスを設定します。

5 ローカル ファイルの場合は、「**コマンドライン引数**」を設定します。

6 ローカルファイルの場合は、「**作業ディレクトリ**」フィールドにディレクトリを設定します。

7 リモート ファイルについては、**利用可能なファイル**のボックスと**使用中のファイル**のボックスの間でファイルを移動することができます。クライアント接続後に、使用ファイルのボックスに含まれるスクリプト ファイルが実行されます。

8 「**適用**」を選択して設定を保存します。

クライアント > 設定 > 接続後スクリプト

クライアント > ルート

このセクションでは、「**クライアント > ルート**」ページの概要と、このページで利用できる設定タスクについて説明します。

「クライアント > ルート」の概要

「**クライアント > ルート**」ページで管理者はクライアント ルートを追加して構成することができます。

クライアント > ルート

クライアント ルートの追加

クライアント ルートは、すべての NetExtender/MobileConnect クライアントに渡されます。これはリモート ユーザが Secure Mobile Access 接続を利用してアクセスできるプライベートなネットワークやリソースの決定に用いられます。

「**クライアント ルートの追加**」に対してユーザ レベルのオプションを有効化する場合は、プライマリ グループと追加グループの両方からグループ レベルのルートを割り当ててください。ユーザ レベルの**ルート**を常に NX クライアントにプッシュする必要があります。それでもグローバル ルートは「**クライアント ルートの追加**」オプションに以前と同様に依存します。IPv4 と IPv6 ルートの両方がこれらのルールに従います。

メモ：グループ アクセス ポリシーでは、すべてのトラフィックが既定で許可されます。これは SonicWall Inc. 装置の既定の動作 (すべての着信トラフィックを既定で拒否する) と反対の動作です。SMA/SRA 装置用のポリシーを作成しない場合、すべての NetExtender/MobileConnect ユーザが内部ネットワーク上のすべてのリソースにアクセスできるようになります。

追加の許可および拒否ポリシーを、送信先アドレスまたはアドレス範囲か、サービス種別ごとに作成することができます。

メモ：ポリシーは限定的な方が優先されます。例えば、特定の IP アドレスに適用されるポリシーは、IP アドレス範囲に適用されるポリシーよりも優先されます。特定の IP アドレスに適用されるポリシーが 2 つあるときは、特定のサービス (RDP など) に関するポリシーがすべてのサービスに関するポリシーよりも優先されます。

ユーザ ポリシーはグループ ポリシーよりも優先され、グループ ポリシーはグローバル ポリシーよりも優先されます。これはポリシーの定義と関係ありません。すべての IP アドレスへのアクセスを許可するユーザ ポリシーは、特定の IP アドレスへのアクセスを拒否するグループ ポリシーよりも優先されます。

クライアント ルートを追加するには:

1 「**クライアント > ルート**」ページに移動します。

2 「**強制トンネル方式**」ドロップダウン　リストから「**有効**」を選択します。これにより、このユーザへのすべてのトラフィック (リモート ユーザのローカル ネットワーク宛てのトラフィックも含む) で Secure Mobile Access NetExtenderr/MobileConnect トンネルが使用されます。

3 「**クライアント ルートの追加**」を選択します。「**クライアント ルートの追加**」ダイアログ ボックスが表示されます。

4 「**クライアント ルートの追加**」ダイアログ ボックスの「**送信先ネットワーク**」フィールドに、NetExtender/MobileConnect でアクセスできるようにする信頼済みネットワークの IP アドレスを入力します。例えば、ネットワーク 192.168.50.0/24 の既存の DMZ に接続し、LAN ネットワーク 192.168.168.0/24 へ のアクセスを可能にする場合、192.168.168.0 と入力します。

「**送信先ネットワーク**」フィールドに、IPv6 ルートを、2007::1:2:3:0 の形式で入力できます。

5 IPv4 の送信先ネットワークに対しては、「**サブネット マスク/接頭辞**」フィールドに、サブネット マスクを 10 進形式 (255.0.0.0、255.255.0.0、または 255.255.255.0) で入力します。IPv6 の送信先ネットワークに対しては、112 のように接頭辞を入力します。

6 「**適用**」を選択します。

7 必要なすべてのルートについて、この手順を繰り返します。

クライアント > 詳細設定

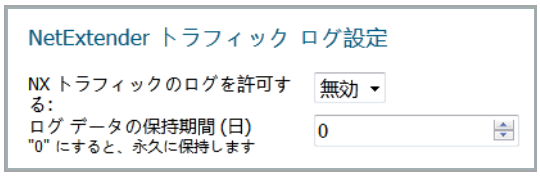
「**クライアント > 詳細設定**」ページでは、トラフィック ログを設定し、接続後スクリプト ファイルをアップロードすることができます。

トピック:

NetExtender/MobileConnect トラフィック ログ

「**NX トラフィックのログを許可する**」で有効を選択することにより、NetExtender/MobileConnect トンネルを経由するトラフィック情報を記録できます。ログ データの保存日数を設定することがで

き、期限が切れたデータは自動的に削除されます。ログ データを永久保存する場合は、値を 0 のままにします。ログ データは、「**クライアント > ログ**」ページで参照できます。



接続後のスクリプト ファイル

管理者は、NetExtender/MobileConnect 用の接続後スクリプト ファイルをアップロードまたは削除することができます。「**クライアント > 詳細設定**」ページに移動し、「接続後のスクリプト ファイル」のセクションまで下方向にスクロールします。

「**ファイルの選択**」をクリックして、ローカル システムからファイルをアップロードします。その後、「**アップロード**」をクリックします。アップロードされたファイルは、一覧に表示されます。

メモ：最大スクリプト サイズは 1024 KB です。スクリプト ファイルの最大数は 30 です。

スクリプト ファイルを削除するには、削除するファイルの横にある削除アイコン「**X**」をクリックします。

クライアント > ダウンロード

「**クライアント > ダウンロード**」ページでは、使用可能な NetExtender/MobileConnect クライアントと Mobile Connect クライアントを装置やモバイル機器にダウンロードできます。ファイル拡張子のリンクを選択するだけで、ローカル システムへのダウンロードが開始します。

メモ：クライアントは software.sonicwall.com からダウンロードする必要があります。クライアントが利用できない場合は、ページにダウンロード リンクの代わりに「(利用できません)」と表示されます。装置から software.sonicwall.com にアクセスできること、および装置が「**システム > ライセンス**」で正しく登録されていることを確認してください。

以下のシステム/モバイル機器がサポートされています。

- Windows
- Mac OS X
- Linux 32 ビット
- Linux 64 ビット

- Android
- Apple iOS

クライアント > ログ

「**クライアント > ログ**」ページでは、データ ログの表示と検索ができます。「**クライアント > 詳細設定**」ページで NetExtender/MobileConnect トラフィックのログ記録を有効化した場合、このページでデータ ログを表示することができます。

使用できるオプションは次のとおりです。

- **検索** - ログで検索する値を入力し、「**検索**」を選択します。必要に応じて、ドロップダウン リストで検索対象の列を選択することができます。
  - すべてのフィールド
  - ユーザ
  - ドメイン
  - 送信元
  - プラットフォーム
  - ログイン時間
  - 送信
  - 受信

- **除外** - 検索値を含まないログを表示します。
- **リセット** - 検索フィールドと検索結果をすべて消去します。
- **エクスポート** - 現在のログをローカル システムにエクスポートします。
- **ログの消去** - 現在のログ エントリを消去します。
- **電子メール ログ** - 現在のログをメール送信します。送信先の電子メール アドレスの入力を求められます。

ログは、要約ログまたは詳細ログとして表示できます。要約ログでは、NetExtender/MobileConnect セッションごとにトラフィック情報を表示できます。詳細ログでは、ユーザごとにトラフィック情報を表示します。

NetExtender/MobileConnect のユーザおよびグループ設定

NetExtender/MobileConnect の複数範囲およびルートのサポートでは、ネットワーク管理者がグループとユーザを簡単にセグメント分割できます。アクセスを制御するファイアウォールのルールを設定する必要はありません。アクセスを制御するファイアウォールのルールを設定する必要はありません。このユーザのセグメント化によって、ネットワークへのアクセスを細かく制御できます。ユーザに対しては必要なリソースへのアクセスを認め、機密性の高いリソースへのアクセスは必要最小限のユーザのみに制限できます。このセクションは、次のサブセクションから構成されています。

- ユーザ レベルの NetExtender/MobileConnect 設定を構成する (272 ページ)
- グループ レベルの NetExtender/MobileConnect 設定を構成する (276 ページ)

ユーザ レベルの NetExtender/MobileConnect 設定を構成する

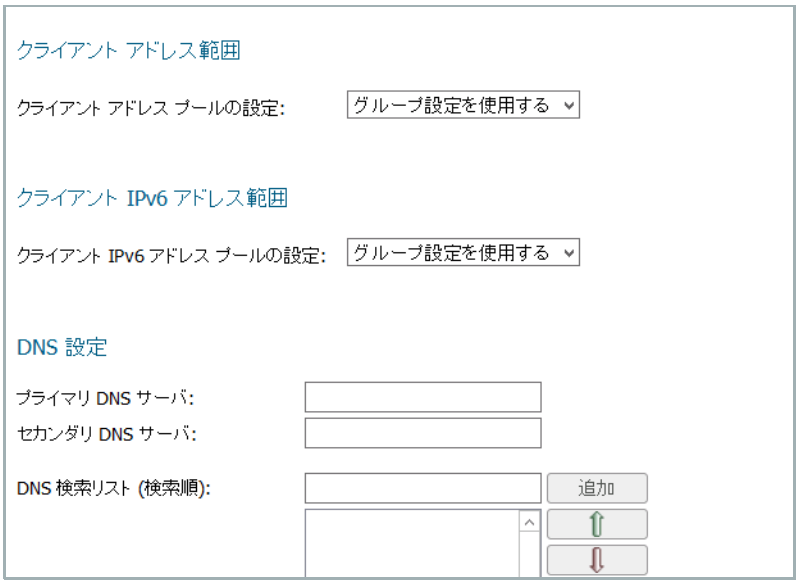
NetExtender/MobileConnect のすべてのグローバル設定 (IP アドレス範囲、DNS 設定、クライアント ルート、およびクライアント接続設定)　はユーザおよびグループ　レベルで構成できます。NetExtender/MobileConnect の複数範囲およびルートのサポートでは、ネットワーク管理者がグループとユーザを簡単にセグメント分割できます。アクセスを制御するファイアウォールのルールを設定する必要はありません。アクセスを制御するファイアウォールのルールを設定する必要はありません。このユーザのセグメント化によって、ネットワークへのアクセスを細かく制御できます。ユーザに対しては必要なリソースへのアクセスを認め、機密性の高いリソースへのアクセスは必要最小限のユーザのみに制限できます。

個々のユーザの個別設定を構成するには:

1 「**ユーザ > ローカル ユーザ**」ページに移動します。

2 編集するユーザの設定アイコン  を選択します。「**ユーザの編集**」ウィンドウが表示されます。

3 「**クライアント**」セクションに移動します。



参考資料:

- ユーザのクライアント IP アドレス範囲の設定 (273 ページ)
- ユーザ DNS 設定の構成 (274 ページ)
- ユーザの NetExtender/MobileConnect 設定を構成する (274 ページ)
- ユーザ の NetExtender/MobileConnect ルートを構成する (275 ページ)

ユーザのクライアント IP アドレス範囲の設定

クライアント IP アドレス範囲を設定するには、以下の手順に従います。

1 このユーザの IPv4 アドレス範囲を設定するには、「**クライアント アドレス範囲の開始**」フィールドに範囲の開始アドレスを入力し、「**クライアント アドレス範囲の終了**」フィールドに範囲の終了アドレスを入力します。

2 このユーザに毎回同じ IP アドレスを付与するには、その IP アドレスを両方のフィールドに入力します。

3 このユーザの IPv6 アドレス範囲を設定するには、「**クライアント IPv6 アドレス範囲の開始**」フィールドに範囲の開始アドレスを入力し、「**クライアント IPv6 アドレス範囲の終了**」フィールドに範囲の終了アドレスを入力します。IPv6 設定はオプションです。

このユーザに毎回同じ IP アドレスを付与するには、その IP アドレスを両方のフィールドに入力します。

ⓘ **ヒント**：複数のユーザが同じユーザ名を共用するという方法 (推奨されない方法) を使っていない場合は、ユーザのクライアント IP アドレス範囲に複数の IP アドレスを設定する必要はありません。

4 「**適用**」を選択します。

ユーザ DNS 設定の構成

特定のユーザの個別 NetExtender/MobileConnect DNS 設定を構成するには:

1 「**プライマリ DNS サーバ**」フィールドに、プライマリ DNS サーバの IP アドレスを入力します。

2 オプションで、「**セカンダリ DNS サーバ**」フィールドに、セカンダリ DNS サーバの IP アドレスを入力します。

3 「**DNS ドメイン**」フィールドに、DNS サーバのドメイン名を入力します。

4 「**適用**」を選択します。

ユーザの NetExtender/MobileConnect 設定を構成する

ユーザに対して以下の NetExtender/MobileConnect 設定を構成できます。

- **切断後にクライアントを終了** - SMA/SRA サーバから切断された NetExtender/MobileConnect クライアントは終了されます。再接続するには Secure Mobile Access ポータルに戻って NetExtender/MobileConnect をクリックするか、「プログラム」メニューから NetExtender/MobileConnect を起動する必要があります。
- **クライアント終了後にアンインストール** - 終了される、またはユーザが終了を選択 (単に切断するのとは対照的に) した際に NetExtender/MobileConnect クライアントが自動的にアンインストールされます。再接続するには、Secure Mobile Access ポータルに戻って NetExtender/MobileConnect を選択する必要があります。このオプションは、Windows クライアントにのみ適用されます。Android、Mac、または Linux クライアントには適用されません。
- **自動更新のオフを許可する** - NetExtender/MobileConnect クライアントが自動更新機能をオフにすることができます。
- **クライアント接続プロファイルを作成** - NetExtender クライアントは、SMA/SRA サーバ名、ドメイン名、およびオプションでユーザ名とパスワードを記録した接続プロファイルを作成します。
- 「**ユーザ名とパスワードの保存**」オプションでは、ユーザが NetExtender/MobileConnect クライアントにユーザ名とパスワードをキャッシュできるようにするかどうかを設定できます。選択できるオプションは、「**ユーザ名だけ保存を許可**」、「**ユーザ名とパスワードの保存を許可**」、「**ユーザ名とパスワードの保存は不可**」の 3 つです。これらのオプションによって、セキュリティの必要性とユーザの使い勝手の両方に配慮した設定を実現できます。
- このオプションが無効になっている場合、「**iOS デバイスでタッチ ID の使用を許可する**」では、iOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。
- このオプションが無効になっている場合、「**Android デバイスで指紋認証の使用を許可する**」では、Android デバイスでの指紋認証による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。
- このオプションが無効になっている場合、「**macOS デバイスでタッチ ID の使用を許可する**」では、macOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段が

ないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

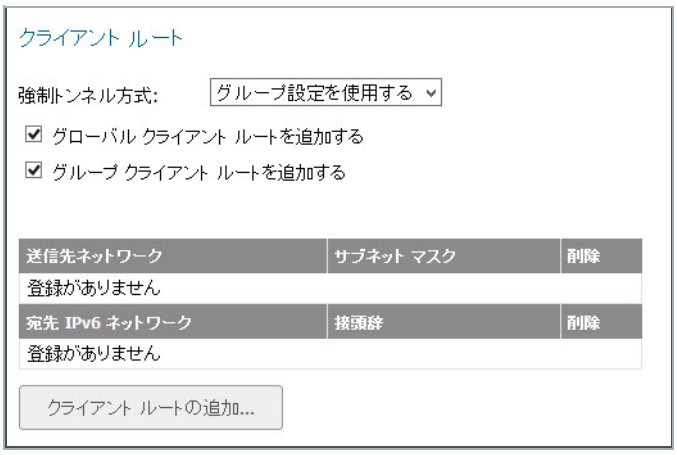
- 「**iOS デバイスで Face ID の使用を許可する**」(macOS デバイスで Face ID 技術を使用して今後のログイン試行を遮断するコントロール) が無効化されていると、サーバはクライアントが接続を試みるまでクライアントの設定を変更する手段がありません。

ユーザの所属グループの NetExtender/MobileConnect 設定 (ユーザがグループに属していない場合はグローバル NetExtender/MobileConnect 設定) を適用するには、上記の各オプションで「**グループ設定を使用する**」を選択します。

ユーザ の NetExtender/MobileConnect ルートを構成する

ユーザの NetExtender/MobileConnect ルートを構成するには:

1 「**クライアント > ルート**」ページに移動します。



2 「**クライアント ルートの追加**」を選択します。

3 「**送信先ネットワーク**」に、NetExtender/MobileConnect でアクセスできるようにする信頼済みネットワークの IPv4 または IPv6 アドレスを入力します。

4 IPv4 の送信先ネットワークに対しては、「**サブネット マスク/接頭辞**」フィールドに、サブネット マスクを 10 進形式 (255.0.0.0、255.255.0.0、または255.255.255.0) で入力します。IPv6 の送信先ネットワークに対しては、112 のように接頭辞を入力します。

5 「**適用**」を選択します。

6 必要なルートすべてに対して、ステップ 1～5 を繰り返します。

7 「**強制トンネル方式**」ドロップダウン リストから「**有効**」を選択します。これにより、このユーザへのすべてのトラフィック (リモート ユーザのローカル ネットワーク宛てのトラフィックも含む) で Secure Mobile Access NetExtenderr/MobileConnect トンネルが使用されます。

8 ユーザにグローバルな NetExtender/MobileConnect クライアント ルート (「**クライアント > ルート**」ページで構成する) も追加する場合は、「**クライアント ルートの追加**」を選択します。

9 ユーザの所属するグループにグループの NetExtender/MobileConnect クライアント ルートも追加する場合は、「**グループの NetExtender/MobileConnect クライアント ルートの追加**」を選択します。グループの NetExtender/MobileConnect ルートは、「**ローカル グループの編集**」ウィンドウの「**ルート**」ページ (「**ユーザ > ローカル グループ**」ページからアクセスする) で構成します。

10 「**適用**」を選択します。

メモ：外部認証サーバを使用するときには、通常は SMA/SRA 装置にローカル ユーザ名は設定されていません。この場合、ユーザの認証が成功すると、ローカル ユーザ アカウントが作成され、「**グローバルな NetExtender/MobileConnect クライアント ルートの追加**」設定と「**グループの NetExtender/MobileConnect クライアント ルートの追加**」設定が有効化されます。

グループ レベルの NetExtender/MobileConnect 設定を構成する

NetExtender/MobileConnect の複数範囲およびルートのサポートでは、ネットワーク管理者がグループとユーザを簡単にセグメント分割できます。アクセスを制御するファイアウォールのルールを設定する必要はありません。アクセスを制御するファイアウォールのルールを設定する必要はありません。このユーザのセグメント化によって、ネットワークへのアクセスを細かく制御できます。ユーザに対しては必要なリソースへのアクセスを認め、機密性の高いリソースへのアクセスは必要最小限のユーザのみに制限できます。

グループの個別設定を構成するには:

1 「**ユーザ > ローカル グループ**」ページに移動します。

2 編集するグループの設定アイコン を選択します。「**ローカル グループの編集**」ウィンドウが表示されます。

3 「**クライアント**」ページをクリックします。

参考資料:

- グループのクライアント IP アドレス範囲の構成 (277 ページ)
- グループ DNS 設定の構成 (277 ページ)
- グループ クライアント設定の構成 (277 ページ)
- グループの NetExtender/MobileConnect ルートを構成する (278 ページ)

グループのクライアント IP アドレス範囲の構成

グループレベルの NetExtender/MobileConnect アドレス範囲を構成するには:

1 このグループの IPv4 アドレス範囲を構成するには、「**クライアント アドレス プールの設定**」ドロップダウン メニューから「**静的プールを使用**」を選択し、「**クライアント アドレス範囲の開始**」フィールドに範囲の開始アドレスを、「**クライアント アドレス範囲の終了**」フィードに範囲の終了アドレスをそれぞれ入力します。

2 このグループの IPv6 アドレス範囲を構成するには、「**Client IPv6 アドレス プール設定**」ドロップダウン メニューから「**静的プールを使用**」を選択し、「**クライアント IPv6 アドレス範囲の開始**」フィールドに範囲の開始アドレスを、「**クライアント IPv6 アドレス範囲の終了**」フィールドに範囲の終了アドレスをそれぞれ入力します。IPv6 設定はオプションです。

3 「**適用**」を選択します。

グループ DNS 設定の構成

特定のグループの個別 NetExtender DNS 設定を構成するには:

1 「**プライマリ DNS サーバ**」フィールドに、プライマリ DNS サーバの IP アドレスを入力します。

2 オプションで、「**セカンダリ DNS サーバ**」フィールドに、セカンダリ DNS サーバの IP アドレスを入力します。

3 「**DNS ドメイン**」フィールドに、DNS サーバのドメイン名を入力します。

4 「**適用**」を選択します。

グループ クライアント設定の構成

グループに対して次のクライアント設定を構成できます。

- **切断後にクライアントを終了** - SMA/SRA サーバから切断された NetExtender/MobileConnect クライアントは終了されます。再接続するには、グループ内のユーザが Secure Mobile Access ポータルに戻って NetExtender/MobileConnect をクリックするか、「プログラム」メニューから NetExtender/MobileConnect を起動する必要があります。
- **クライアント終了後にアンインストール** - 終了される、またはユーザが終了を選択 (単に切断するのとは対照的に) した際に NetExtender/MobileConnect クライアントが自動的にアンインストールされます。再接続するには、グループ内のユーザが Secure Mobile Access ポータルに戻って NetExtenderr/MobileConnect を選択する必要があります。このオプションは、Windows クライアントにのみ適用されます。Android、Mac、または Linux クライアントには適用されません。
- **クライアント接続プロファイルを作成** - NetExtender/MobileConnect クライアントは、SMA/SRA サーバ名、ドメイン名、およびオプションでユーザ名とパスワードを記録した接続プロファイルを作成します。
- 「**ユーザ名とパスワードの保存**」オプションでは、ユーザが NetExtender/MobileConnect クライアントにユーザ名とパスワードをキャッシュできるようにするかどうかを設定できます。選択できるオプションは、「**ユーザ名だけ保存を許可**」、「**ユーザ名とパスワードの保存を許可**」、「**ユーザ名とパスワードの保存は不可**」の 3 つです。これらのオプションによって、セキュリティの必要性とユーザの使い勝手の両方に配慮した設定を実現できます。

- このオプションが無効になっている場合、「**iOS デバイスでタッチ ID の使用を許可する**」では、iOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。
- このオプションが無効になっている場合、「**Android デバイスで指紋認証の使用を許可する**」では、Android デバイスでの指紋認証による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。
- このオプションが無効になっている場合、「**macOS デバイスでタッチ ID の使用を許可する**」では、macOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。
- 「**iOS デバイスで Face ID の使用を許可する**」(macOS デバイスで Face ID 技術を使用して今後のログイン試行を遮断するコントロール) が無効化されていると、サーバはクライアントが接続を試みるまでクライアントの設定を変更する手段がありません。

ユーザにグローバルな NetExtender/MobileConnect 設定から NetExtender/MobileConnect 設定を継承させる場合は、上記の各オプションで「**グローバル設定を使用する**」を選択します。

グループの NetExtender/MobileConnect ルートを構成する

グループの NetExtender/MobileConnect クライアント ルートを構成するには:

1 このユーザにのみ追加される NetExtender/MobileConnect クライアント ルートを追加する場合は、「**ユーザ > ローカル ユーザ > ユーザの編集**」に移動し、「**ユーザ設定の編集**」ウィンドウの「**ルート**」ページをクリックします。

2 このグループのユーザにのみ追加される NetExtender/MobileConnect クライアント ルートを追加するには、「**クライアント ルートの追加**」を選択します。

3 「**送信先ネットワーク**」に、NetExtender/MobileConnect でアクセスできるようにする信頼済みネットワークの IPv4 または IPv6 アドレスを入力します。

4 IPv4 のルートに対しては、「**サブネット マスク/接頭辞**」フィールドに、サブネット マスクを入力します。IPv6 のルートに対しては、「**サブネット マスク/接頭辞**」フィールドに接頭辞を入力します。

5 「**適用**」を選択します。必要なすべてのルートについて、この手順を繰り返します。

6 「**強制トンネル方式**」ドロップダウン リストから「**有効**」を選択します。これにより、このユーザへのすべてのトラフィック (リモート ユーザのローカル ネットワーク宛てのトラフィックも含む) で Secure Mobile Access NetExtenderr/MobileConnect トンネルが使用されます。

7 このグループのユーザにグローバルな NetExtender/MobileConnect クライアント ルート (「**クライアント > ルート**」ページで構成する) も追加する場合は、「**クライアント ルートの追加**」を選択します。

8 「**適用**」を選択します。

9

エンド ポイント制御

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**エンド ポイント制御**」ページと、このページで行う設定タスクについて説明します。

トピック:

エンド ポイント制御の設定

従来の VPN ソリューションでは、あなたのネットワークに社員個人所有のコンピュータ、空港、またはホテルといった信頼していない場所からアクセスすることにより、ネットワーク資源に対する危険が増大します。SMA/SRA 装置は、信頼していない環境内の機器など、あらゆるウェブ対応システムからの安全なアクセスを提供します。Secure Mobile Access では、エンド ポイント制御 (EPC) をサポートしています。これは、SMA 400/200、SRA 4600/1600、および SMA 500v Virtual Appliance で利用できる既定のサービスです。

EPC は接続を確立する前にユーザの環境が安全かどうかを確認するエンド ポイント制御 (EPC) をサポートします。EPC は機密性の高いデータを保護し、信頼していない環境内の機器からアクセスされる際にネットワークに危険が及ばないように防御します。EPC はまた、SMA/SRA に参加しているクライアント機器を起源とする脅威からネットワークを保護します。

EPC は、ユーザがウェブ ブラウザからウェブ ポータルにログインする際に確認され、信頼されていないサイトからのプライベート ネットワークへのアクセスをすべて遮断します。EPC は、システム上のブラウザ プラグインを使用してポータル確認を行います。

EPC は、Mobile Connect を用いる iOS および Android モバイル機器でサポートされており、これらのモバイル機器に対してデバイス プロファイルの作成が可能です。これによって、クライアント機器を脅威から保護するとともに、SSL VPN に参加しているクライアント機器を起源とする脅威から SMA/SRA 装置を保護します。Mobile Connect の詳細については、Mobile Connect の各種ユーザ ガイドを参照してください。

Secure Mobile Access は、これらのエンド ポイント セキュリティ制御を、トンネル セッションが開始される前にホストの健全性確認とセキュリティ防御機構を実行することで提供します。ホストの健全性確認は、クライアント システムが組織のセキュリティ ポリシーに沿っていることを確認する助け

になります。SonicWall Inc. エンド ポイント セキュリティ制御はアクセス制御と堅く統合されており、クライアント システムを分析して、その結果を基にアクセス制御を適用します。

EPC は、Windows、Linux、および Mac NetExtender クライアントをサポートします。また、iOS、Android、OSX、Windows Phone、および Windows Next 向けの Mobile Connect もサポートします。ウェブ ポータル ログインに関して、EPC は Windows プラットフォーム上でのみサポートされます。EPC 拡張は SonicWall Inc. SMA 400/200、SRA 4600/1600 および SMA 500v Virtual Appliance プラットフォームでサポートされます。

メモ：EPC 機能がアクティブな場合、増加したトラフィックのために他の機能の動作が遅くなることがあります。

EPC を設定するには:

1. ご使用の装置の導入ガイドで説明されているように、装置を最新の Secure Mobile Access ファームウェア イメージで起動します。
2. 様々なグローバル、グループ、またはユーザ属性に基づいてユーザ認証を許可または禁止するデバイス プロファイルを設定します。エンド ポイント制御 > デバイス プロファイル (280 ページ) を参照してください。
3. エンド ポイント制御プロファイルを許可または禁止するグループとユーザを追加して設定します。エンド ポイント制御 > 状況 (287 ページ) を参照してください。
4. グループ プロファイルを継承するようにユーザを設定します。ユーザ > ローカル グループ > EPC 設定の編集 (282 ページ) を参照してください。
5. エンド ポイント制御を有効にします。エンド ポイント制御 > 状況 (287 ページ) を参照してください。
6. NetExtender に接続して、エンド ポイント制御のログを監視します。エンド ポイント制御 > ログ (288 ページ) を参照してください。

エンド ポイント制御 > デバイス プロファイル

様々なグローバル、グループ、またはユーザ属性に基づいて、ユーザまたはグループに対する認証指針を設定するためのデバイス プロファイルを作成します。例えば、あるアンチウィルス プログラムを使用するグループ、特定の Windows バージョンのユーザなどを選択できます。

プロファイルには、**許可**プロファイルと**禁止**プロファイルの 2 種類があります。**許可**プロファイルはユーザが認証される前に提示する必要があるクライアント ネットワークの属性を確認し、**禁止**プロファイルは提示できない ネットワークの属性を確認します。あるグループまたはユーザに対して複数のプロファイルが定義されている場合、SMA/SRA 装置への接続は、クライアント環境がグループまたはユーザに対するすべての**許可**プロファイルを満たし、かつ、どの**禁止**プロファイルも満たさない場合のみ許可されます。

「**エンド ポイント制御 > デバイス プロファイル**」ページを使用して、デバイス プロファイルを管理します。

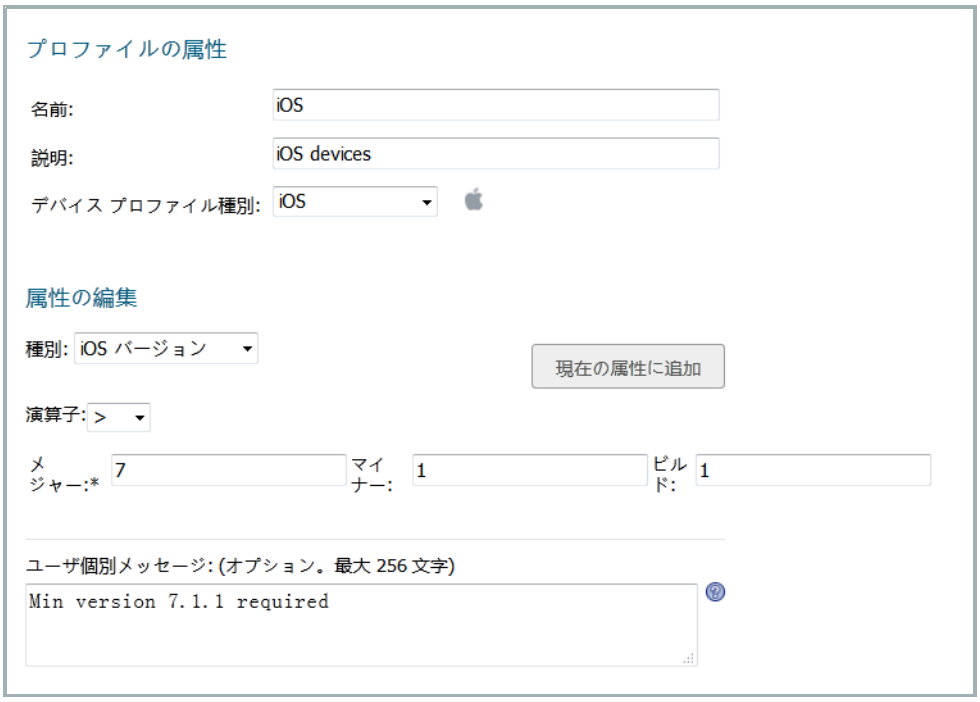
エンド ポイント制御 > デバイス プロファイル

「**エンド ポイント制御 > デバイス プロファイル**」ページは、すべてのデバイス プロファイルを一覧表示し、プロファイルを使用することができるプラットフォームを識別します。このページには、プロファイルを追加、編集、または削除するためのボタンがあります。見分けるには、アイコンまたはボタンにマウス カーソルを合わせます。

デバイス プロファイルを作成するには、以下の手順を実行します。

1 「**エンド ポイント制御 > デバイス プロファイル**」ページで、「**デバイス プロファイルの追加**」を選択します。

「デバイス プロファイルの追加」ページが表示されます。



2 「**名前**」フィールドに、プロファイルを識別するために使用する名前を入力します。

3 「**説明**」フィールドに、オプションでプロファイルを識別するのに役立つプロファイルの簡単な説明を入力します。

4 **Windows**、**Mac**、**Linux**、**iOS**、または **Windows Phone** クライアントのいずれに対してプロファイルを作成するかを選択します。

5 「**種別**」ドロップダウン リストで、ユーザの選択に使用する属性を選択します。このページの残りのフィールドはあなたの選択によって異なります。

6 「**現在の属性に追加**」を選択します。

7 それぞれのプロファイルに含まれるべきの属性に対し、5 と 6 を繰り返します。

8 必要に応じて、EPC の確認に失敗したことをユーザに通知するカスタム メッセージを入力できます。管理者は、問題の解決方法やポリシー エラーになった理由を説明するテキストを入力できます。

9 プロファイルを完了するには、ページ右上の「**適用**」を選択します。

ユーザ > ローカル グループ > EPC 設定の編集

デバイス プロファイルを作成した後で、ユーザを認証するためにそれらを使用するローカル グループに割り当てます。デバイス プロファイルには**許可**プロファイルと**禁止**プロファイルがあります。**許可**プロファイルはユーザが認証される前に提示する必要があるクライアント ネットワークの属性を確認し、**禁止**プロファイルは提示 *できない* ネットワークの属性を確認します。あるグループに対して複数のプロファイルが定義されている場合、SMA/SRA 装置への接続は、クライアント環境がグループに対するすべての**許可**プロファイルを満たし、かつ、どの**禁止**プロファイルも満たさない場合のみ許可されます。「**ユーザ > ローカル グループ > 編集**」ページの「**EPC**」ページを使用して、デバイス プロファイルをグループに割り当てます。

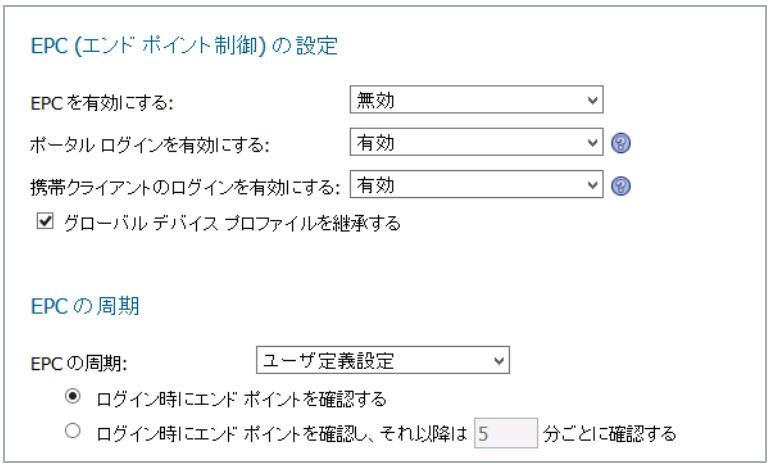
EPC が有効のプラットフォーム上で NetExtender ログインを無効にできます。

EPC ポータル確認では、NetExtender ブラウザ プラグインを使用します。EPC は、ユーザがウェブ ブラウザからウェブ ポータルにログインする際に確認され、信頼されていないサイトからのプライベート ネットワークへのアクセスをすべて遮断します。

ローカル グループ内のユーザを認証するときに使用するデバイス プロファイルを設定するには、以下の手順を実行します。

1 「**ユーザ > ローカル グループ**」ページに移動して、グローバル グループまたは EPC を設定するローカル グループに対する「**編集**」 を選択します。

2 「ローカル グループの編集」ページが表示されたら、「EPC 設定」セクションに移動します。**EPC** ページを使用して、ユーザに対する EPC の有効化または無効化を行います。また、サポートされないクライアントからの認証要求の処理方法、およびデバイス プロファイルの追加または削除の方法を選択します。



3 「**EPC を有効にする**」フィールドで、グループの EPC を有効にするには「**有効**」を選択し、グループの EPC を無効にするには「**無効**」を選択します。あるいは、「**ユーザ > ローカル ユーザ > グローバル ポリシーの編集**」または「**ユーザ > ローカル グループ > グローバル ポリシーの編集**」ページの EPC が有効かどうかに基づいて EPC を有効または無効にするには「**グローバル設定を使用する**」を選択します。

4 EPC が有効なときにこれらのポータルからのログインを許可する場合には「**ポータル ログインを有効にする**」フィールドで既定の動作を**有効**に、遮断する場合は**無効**に設定します。

5 iOS と Android の携帯クライアントで EPC がサポートされています。ECP が有効なときにこれらのクライアントからのログインを許可する場合には「**携帯クライアントのログインを有効にする**」フィールドで既定の動作を有効に、遮断する場合は無効に設定します。

6 「**EPC の周期**」セクションのフィールドは、グローバル グループまたはローカル グループどちらの EPC を設定しているかによって変化します。グローバル グループの EPC を設定する場合は、ユーザがログインするときのみ EPC チェックを実行するように「**ログイン時にエンド ポイントを確認する**」を選択するか、設定した間隔でも EPC チェックを実行するように「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」を選択します。例えば、ユーザがログインしたときと、ログイン中に *x* 分ごとに EPC チェックを実行するには、「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」を選択し、EPC のチェックの周期を分単位で入力します。

   OR

   ローカル グループの EPC を設定する場合は、「**EPC の周期**」ドロップダウン リストから「**グローバル設定を使用する**」または「**ユーザ定義設定**」を選択します。「**グローバル設定を使用する**」を選択した場合は、ローカル グループはグローバル グループから EPC 設定を継承します。「**ユーザ定義設定**」を選択した場合は、「**ログイン時にエンド ポイントを確認する**」と「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」が表示され、グローバル グループに対して説明したように EPC を設定できます。

7 グループに対して定義されたすべての許可と禁止デバイス プロファイルを使用するには「**グローバル デバイス プロファイルを継承する**」をオンにします。

   OR

   「EPC の編集」ページを使用してプロファイルを追加または削除します。

   a グループのため**許可**プロファイルを追加または削除するには、「**許可プロファイルの追加**」を選択します。

   b 「EPC の編集」ページで、「**すべてのプロファイル**」リストからグループに追加するプロファイルを選択し、「**選択されたプロファイルの追加**」を選択します。すると選択されたプロファイルは、グループに対して使用されるすべてのデバイス プロファイルが一覧表示される、ページ上の「**使用中のプロファイル**」リストに移動されます。

   c プロファイルを削除せずに無効にするには、プロファイルの横にある「**有効**」をオフにします。プロファイルを有効にするには、「**有効**」をオンにします。これにより、都合に合わせて定期的に使用されるプロファイルを有効または無効にすることができます。

   d グループから許可プロファイルを削除するには、「**使用中のプロファイル**」リストからプロファイルを選択して「**選択されたプロファイルの削除**」を選択します。

   e グループに対する禁止プロファイルを追加または削除するには、「**禁止プロファイルの追加**」を選択してから上記 b と d と同様の手順を実行します。

8 「**適用**」を選択して変更を保存します。

ユーザ > ローカル ユーザ > EPC 設定の編集

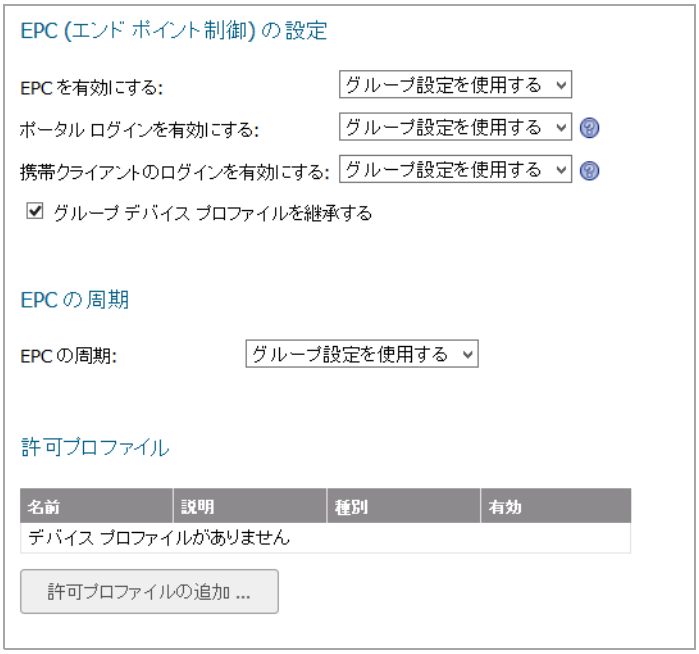
デバイス プロファイルを作成した後で、それらをローカル ユーザに割り当てます。デバイス プロファイルには**許可**プロファイルと**禁止**プロファイルがあります。**許可**プロファイルはユーザが認証される前に提示する必要があるクライアント ネットワークの属性を確認し、**禁止**プロファイルは提示 *できない* ネットワークの属性を確認します。あるユーザに対して複数のプロファイルが定義されている場合、SMA/SRA 装置への接続は、クライアント環境がユーザに対するすべての**許可**プロファイルを満たし、かつ、どの**禁止**プロファイルも満たさない場合のみ許可されます。「**ユーザ > ローカル ユーザ > 編集**」ページの「**EPC**」ページを使用して、デバイス プロファイルをユーザに割り当てます。

EPC が有効のプラットフォーム上で NetExtender ログインを無効にできます。

ローカル ユーザを認証するときに使用するデバイス プロファイルを設定するには、以下の手順を実行します。

1 「**ユーザ > ローカル ユーザ**」ページに移動して、EPC を設定するユーザに対する「**編集**」を選択します。

2 「ローカル ユーザの編集」ページが表示されたら、「**EPC**」ページを選択します。**EPC** ページを使用して、ユーザに対する EPC の有効化または無効化を行います。また、サポートされないクライアントからの認証要求の処理方法、およびデバイス プロファイルの追加または削除の方法を選択します。



3 「**EPC を有効にする**」フィールドで、ユーザの EPC を有効にするには「**有効**」を選択し、ユーザの EPC を無効にするには「**無効**」を選択します。あるいは、「**エンド ポイント制御 > 設定**」ページの EPC が有効かどうかに基づいて EPC を有効または無効にするには「**グループ設定を使用する**」を選択します。

4 EPC が有効なときにこれらのクライアントからのログインを許可する場合には「**ポータル ログインを有効にする**」フィールドで既定の動作を**有効**に、遮断する場合は**無効**に設定します。

5 iOS と Android の携帯クライアントで EPC がサポートされています。「**携帯クライアントのログインを有効にする**」フィールドで、EPC が有効なときにこれらのクライアントからのログインを、既定で許可する場合は「**有効**」を、禁止する場合は「**無効**」を選択します。または、「**グループ設定を使用する**」を既定の動作として選択することもできます。この場合は、「**エンド ポイント制御 > 設定**」ページで EPC が有効になっているかどうかによって、EPC が有効または無効になります。

6 「**EPC の周期**」セクションで、EPC チェックがいつ行われるべきかを設定します。ユーザがログインするときのみ EPC チェックを実行するように「**ログイン時にエンド ポイントを確認する**」を選択するか、設定した間隔でも EPC チェックを実行するように「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」を選択します。例えば、ユーザがログインしたときと、ログイン中に *x* 分ごとに EPC チェックを実行するには、「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」を選択し、EPC のチェックの周期を分単位で入力します。

7 「**EPC の周期**」セクションのフィールドは、グローバル グループまたはローカル ユーザどちらの EPC を設定しているかによって変化します。グローバル グループの EPC を設定する場合は、ユーザがログインするときのみ EPC チェックを実行するように「**ログイン時にエンド ポイントを確認する**」を選択するか、設定した間隔でも EPC チェックを実行するように「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」を選択します。例えば、ユーザがログインしたときと、ログイン中に *x* 分ごとに EPC チェックを実行するには、「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」を選択し、EPC のチェックの周期を分単位で入力します。

OR

ローカル ユーザの EPC を設定する場合は、「**EPC の周期**」ドロップダウン リストから「**グローバル設定を使用する**」または「**ユーザ定義設定**」を選択します。「**グローバル設定を使用する**」を選択した場合は、ローカル ユーザはグローバル グループから EPC 設定を継承します。「**ユーザ定義設定**」を選択した場合は、「**ログイン時にエンド ポイントを確認する**」と「**ログイン時にエンド ポイントを確認し、それ以降は *x* 分ごとに確認する**」が表示され、グローバル グループに対して説明したように EPC を設定できます。

8 ユーザに対して定義されたすべての許可と禁止デバイス プロファイルを使用するには「**グループ デバイス プロファイルを継承する**」をオンにします。

OR

「**EPC の編集**」ページを使用してプロファイルを追加または削除します。

a ユーザのため**許可**プロファイルを追加または削除するには、「**許可プロファイルの追加**」を選択します。

b 「EPC の編集」ページで、「**すべてのプロファイル**」リストからユーザに追加したいプロファイルを選択し、「**選択されたプロファイルの追加**」を選択します。すると選択されたプロファイルは、ユーザに対して使用されるすべてのデバイス プロファイルが一覧表示される、ページ上の「**使用中のプロファイル**」リストに移動されます。

c ユーザの許可プロファイルを削除するには、「**使用中のプロファイル**」リストからプロファイルを選択して「**選択されたプロファイルの削除**」を選択します。

d ユーザに対する禁止プロファイルを追加または削除するには、「**禁止プロファイルの追加**」を選択してから上記 b と d と同様の手順を実行します。

9 「**適用**」を選択して変更を保存します。

エンド ポイント制御 > 状況

「**エンド ポイント制御 > 状況**」ページを使用して、自動アップデートの設定、使用されている現在の EPC バージョンの表示、EPC バージョンの更新、およびサービスの失効期日の表示を行うことができます。

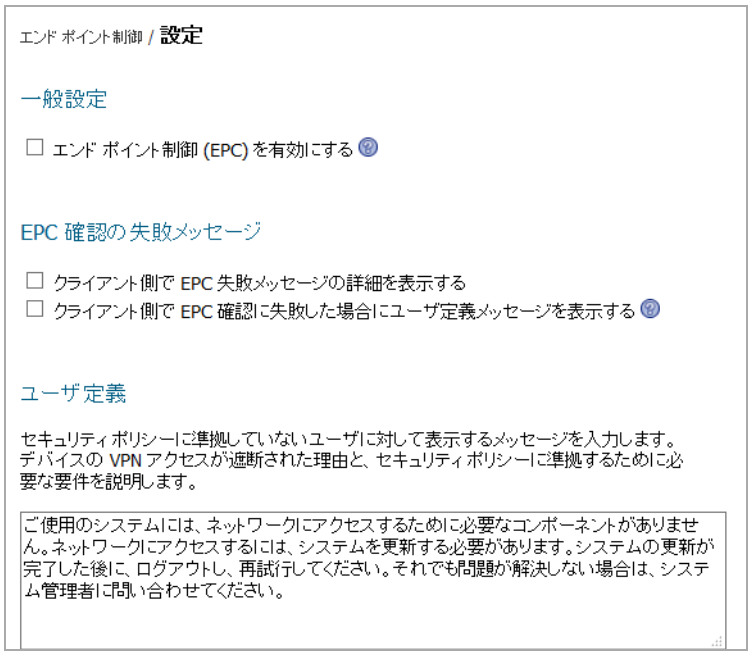
エンド ポイント制御 > 状況

1. 「**自動アップデートを許可**」をオンにして、OPSWAT の自動アップデートを有効にします。
2. 「インストール バージョン」には、使用されている現在のバージョンが表示されます。
3. 「**アップデートの確認**」を選択して、利用可能なアップデートがあるかどうかただちに問い合わせます。利用可能な新しいアップデートがある場合、ボタンが「**アップデートを適用**」に変化します。
4. 「サービスの失効期日」には、現在のサービスがいつ失効するかが表示されます。
5. 「**戻す**」を選択して、サービスの前バージョンを適用します。

エンド ポイント制御 > 設定

EPC は「**エンド ポイント制御 > 設定**」ページ上で全体的に有効または無効にします。EPC が無効の場合、グローバル、グループ、そしてユーザ レベルで無効です。この設定ページは、NetExtender クライアントのログインが EPC セキュリティ確認で失敗した場合に表示するメッセージをカスタマイズするためにも使われます。

エンド ポイント制御 > 設定



エンド ポイント制御 > ログ

「**エンド ポイント制御 > ログ**」ページには、EPC によって遮断されたすべてのクライアント ログインがリストされます。このログは検索、フィルタ、電子メール送信、そしてエクスポートすることができます。

エンド ポイント制御 > ログ

このページを使用して以下の機能を実行します。

- 「**エクスポート**」を選択して、すべてのログ セッションのすべてのテキストを含む zip ファイルを保存します。
- すべてのログ メッセージを削除するには「**ログの消去**」を選択します。
- 「**ログ > 設定**」ページで設定された電子メール アドレスにログを送信するには「**ログのメール送信**」を選択します。

- ログ メッセージをフィルタするには「**検索**」オプションを使用します。検索は大文字と小文字を区別することに注意してください。ドロップダウン メニューで、検索に使用するフィールドを選択します。「**検索**」を選択すると、検索文字列に一致するメッセージだけが表示されます。検索文字列に一致するメッセージを非表示にするには、「**除外**」を選択します。すべてのメッセージを表示するには「**リセット**」を選択します。
- 1 ページに表示されるログ メッセージを増やしたり減らしたりするには、「**1 ページあたりの項目**」フィールドの値を変更します。ログ メッセージのページをスクロールするには前方または後方矢印を選択します。
- 見出しを選択すると、ログ メッセージは見出しのアルファベット順に並べ替えられます。

10

セキュア仮想アシストの設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**セキュア仮想アシスト**」ページと、このページで行う設定タスクについて説明します。

Secure Mobile Access ユーザがリモートの場所から顧客をサポートするために顧客の使用しているコンピュータの制御を取得できる、使いやすいツールがセキュア仮想アシストです。顧客サポートは、昔から費用と時間がかかるビジネス分野でした。仮想アシストは、簡単に展開できる、使いやすいリモート サポート ソリューションを実現します。この機能は、現在 Windows と MacOS でサポートされています。

セキュア仮想アシストの概念の詳細については、セキュア仮想アシストの概要 (57 ページ) を参照してください。詳細については、『*Secure Mobile Access セキュア仮想ミーティングおよびセキュア仮想アシスト機能モジュール*』も参照できます。

トピック:

セキュア仮想アシスト > 状況

このセクションでは、「**セキュア仮想アシスト > 状況**」ページの概要と、このページで行える設定タスクについて説明します。

「**セキュア仮想アシスト** > 状況」ページには、現在アクティブな要求の要約 (顧客の名前、顧客から提供された問題の要約、仮想アシスト セッションの状況、顧客をアシストしている技術者) が表示されます。技術者に対しては、このページにポータル、ドメイン、状況が表示されます。

仮想アシスト > 状況

画面右側の「**ストリーミング更新**」は顧客状況の変化が動的に更新されることを示します。「**オン/オフ**」を選択すると、それぞれストリーミング更新が有効/無効になります。

「**ログアウト**」を選択すると、顧客がキューから削除されます。現在セッション中の顧客の場合は顧客と技術者の両方が切断されます。

技術者の立場から仮想アシストを使うときの情報については、次のセクションを参照してください。

- セキュア仮想アシストの技術者セッションの開始 (60 ページ)
- セキュア仮想アシストの技術者タスクの実行 (62 ページ)

セキュア仮想アシスト > 設定

このセクションでは、「**セキュア仮想アシスト** > 設定」ページと、このページで使用できる設定タスクについて説明します。仮想アシストのオプションは次のページに分かれています。

- 一般設定 (292 ページ)
- 要求の設定 (293 ページ)
- 通知設定 (294 ページ)
- 制限の設定 (295 ページ)

一般設定

仮想アシストの一般設定を行うには:

1 「**セキュア仮想アシスト** > 設定」ページを表示します。

2 仮想アシストへのアクセスを許可する前に顧客にパスワードの入力を求める場合は、「**アシスト コード**」ウィンドウにパスワードを入力します。

3 (オプション)「**招待なしでのサポートを有効にする**」がオンのとき、顧客は招待の電子メールを受け取っていなくてもアシストを要求できます。これがオフのときは、技術者によって明示的に招待された顧客だけがアシストを受けることができます。

4 (オプション)「**技術者による LAN 上のクライアントの起動を有効にする**」を選択すると、仮想アシストを実行する LAN 上のクライアントを起動できます。ただし、両者が同じサブネットに属する場合に限ります。クライアント PC は、電源がオフの場合も、スリープ状態の場合も、休止状態の場合も起動できます。この機能は、グローバルでも、ポータル単位でも、クライアントからでも有効にできます。

> ⓘ **メモ**：クライアント起動を可能にするには、この機能をポータル上でも有効にする必要があります。「**ポータル > ポータル**」ページと、クライアント マシンの BIOS において、これを行います。

5 (オプション) 仮想アシストを、ローカル マシンにインストールすることなくウェブから起動するには、「**セキュア仮想アシストをインストールせずに起動する**」を選択します。この機能はグローバルまたはポータルごとに有効化できます。

6 (オプション) 顧客が仮想アシスト クライアントをダウンロードできるようにする場合は、「**顧客ポータル ページで仮想アシストのダウンロードを許可する**」をオンにします。

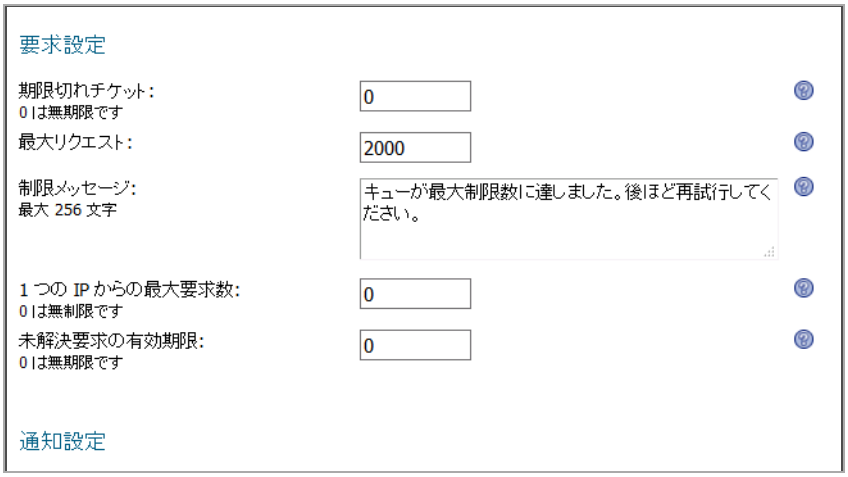
7 (オプション) 仮想アシストを受ける顧客に法的な免責事項、指示、またはその他の追加情報を示すには、「**免責事項**」フィールドにその内容を入力します。このフィールドでは HTML コードを使用できます。免責事項が表示されたら、顧客は仮想アシスト セッションを開始する前に「承諾」を選択する必要があります。

8 ポータル ログイン ページに仮想アシストへのリンクを表示するには、「**ポータル ログイン ページに仮想アシスト リンクを表示**」をオンにします。顧客はリンクを選択すると、仮想アシスト ポータル ログイン ページに直接移動でき、仮想オフィスにログオンする必要はありません。

要求の設定

仮想アシストの要求設定を行うには:

1 「**セキュア仮想アシスト** > **設定**」ページの下部にある「要求の設定」タブを選択します。



2 一定の時間が経過したとき仮想アシスト要求をタイムアウトさせるには、「**期限切れチケット**」フィールドに値を入力します。既定値は **0** で、期限が終了しないことを意味します。タイムアウト時間が経過すると、顧客は仮想アシスト要求を再び出す必要があります。

3 仮想アシスト キューに含めることができる顧客の数を制限するには、「**最大リクエスト**」フィールドに値を入力します。

4 「**制限メッセージ**」フィールドでは、必要に応じて、キューが一杯になったとき顧客に表示するメッセージをカスタマイズできます。メッセージは最大 256 文字です。

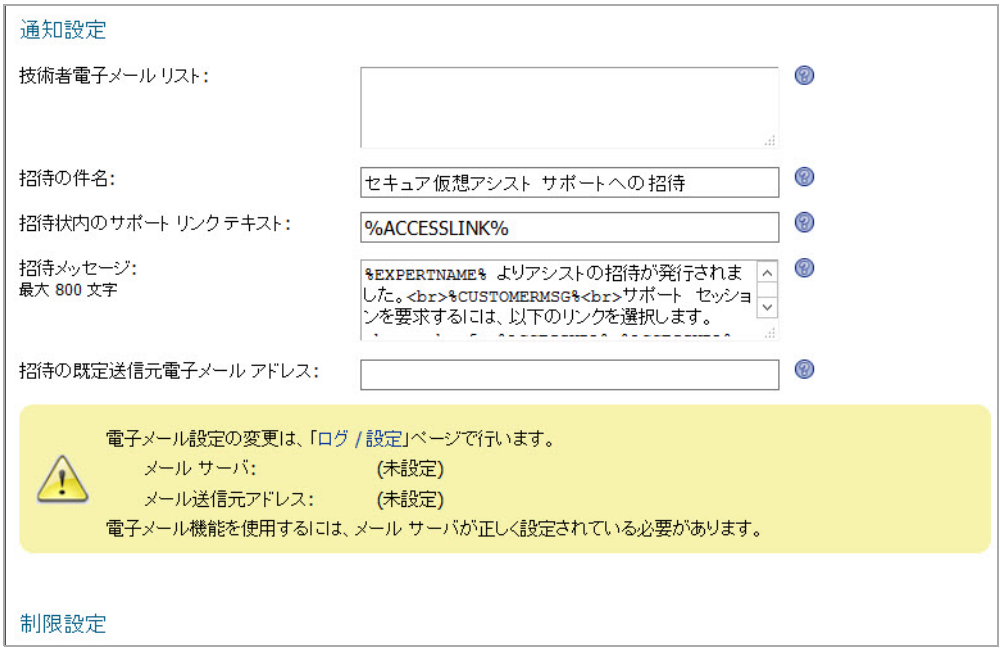
5 「**1 つの IP からの最大要求数**」フィールドに値を入力すると、特定の顧客が繰り返し支援を求めるような状況で制限を課すことができます。ただし、これは顧客が単一の IP アドレスの背後で DHCP を使用している場合に問題を起こすことがあります。既定値の **0** は、特定の IP アドレスの要求を制限しないことを意味します。

6 「**未解決要求の有効期限**」フィールドに値を入力すると、所定の時間 (分単位) 内にアシストされなかった顧客がキューから自動的に削除されます。既定値の **0** は、アシストされなかった顧客を削除しないことを意味します。

通知設定

仮想アシストの通知設定を行うには:

1 「**セキュア仮想アシスト** > **設定**」ページの下部にある「通知設定」タブを選択します。



2 顧客が仮想アシスト キューにログインしたときサポート技術者に自動的に電子メールが送信されるようにするには、技術者の電子メール アドレスを「**技術者電子メール リスト**」に入力します。複数のメール アドレスを入力する場合は、セミコロン (;) で区切って入力します。

3 次の 3 つのフィールドで招待の電子メールをカスタマイズできます。

- 「**招待の件名**」- 電子メールの件名
- 「**招待状内のサポート リンク テキスト**」- 仮想アシストにアクセスする URL へのリンクの説明文
- 「**招待メッセージ**」- 招待の電子メールの本文
- 「**招待の既定送信元電子メール アドレス**」- 既定の電子メールの送信元

これらの 3 つのフィールドでは次の変数を使用して招待をカスタマイズしたり特定の個人に合わせたりすることができます。

- %EXPERTNAME% - 招待の電子メールを送信する技術者の名前
- %CUSTOMERMSG% -「**一般設定**」ページで設定した免責事項
- %SUPPORTLINK% - 仮想アシストにアクセスするための URL

- %ACCESSLINK% - Secure Mobile Access 仮想オフィスにアクセスするための URL

メモ：現在設定されているメール サーバと電子メール返信先アドレスが「**セキュア仮想アシスト** > 設定」ページの下部にリストされます。技術者が通知の電子メールを受け取ったり、仮想アシストの招待を顧客にメールしたりできるようにするには、「**ログ** > 設定」ページでメール サーバを設定する必要があります。技術者の電子メール アドレスが正確なら、顧客に送信された電子メールがサードパーティの電子メール フィルタで遮断された場合に仮想アシスト クライアントにエラーを返さず、遮断された電子メール通知をシステム内の技術者に送ることもできます。

ログ > 設定

制限の設定

仮想アシストの制限設定を行うには:

1 「**セキュア仮想アシスト** > **設定**」ページの下部にある「制限の設定」タブを選択します。

2 特定の IP アドレスまたはネットワークの仮想アシスト要求を拒否するには、「**定義済みアドレスからの要求**」ドロップダウン メニューから「**拒否**」を選択します。

3 特定の IP アドレスまたはネットワークの仮想アシスト要求だけを許可するには、「**定義済みアドレスからの要求**」ドロップダウン メニューから「**許可**」を選択します。

4 IP アドレスまたはネットワークを「拒否」または「許可」リストに追加するには、「**追加 ...**」を選択します。「**管理者のアドレス**」ウィンドウが表示されます。制限の設定にアドレスを追加する (296 ページ) を参照してください。

5 設定済みの制限を削除するには、「**アドレス**」フィールド内の削除したいアドレスを選択して、「**削除**」を選択します。フィールドからアドレスが削除されます。

制限の設定にアドレスを追加する

IP アドレスまたはネットワークを仮想アシストの制限設定の「拒否」または「許可」リストに追加するには:

1 「**セキュア仮想アシスト** > **設定**」ページの下部にある「制限の設定」タブを選択します。

2 「**追加...**」を選択します。「**管理者のアドレス**」ウィンドウが表示されます。

3 「**送信元アドレス種別**」プルダウン メニューで以下の中から指定したいものを選択します。

- IP アドレス
- IP ネットワーク
- IPv6 アドレス
- IPv6 ネットワーク

4 アドレスまたはネットワークを定義する情報を入力し、「**適用**」を選択します。

セキュア仮想アシスト > ログ

「**セキュア仮想アシスト** > ログ」ページでは、以前の仮想アシスト セッションに関する詳細な情報にアクセスできます。「**ログ**」ページには、最近のセッションの要約が表示されます。

顧客に対応する技術者の活動 (技術者の ID、接客時間、顧客と技術者のコンピュータに関する情報、チャット ダイアログ、顧客要求の登録情報、サービス作業に先立って顧客が終了したかどうか、セッション終了後の技術者の意見など) がログに詳細に記録されるようになりました。

仮想アシスト > ログ

「**チケット**」を選択すると、セッション (チケットとも呼ばれる)の詳細が表示されます。「**セキュア仮想アシスト > ログ > <チケット番号>**」ページが表示されます。「**ログの保存**」を選択してページ上の情報を保存します。「**セキュア仮想アシスト > ログ**」要約ページに戻るには、「戻る」を選択します。

「**エクスポート**」を選択して、すべてのログ セッションのすべてのテキストを含む zip ファイルを保存します。このログは要約ファイルと各セッションの詳細ファイルで構成されます。これらのファイルの内容は、Microsoft Word で表示できます。

すべてのログ メッセージを削除するには「**ログの消去**」を選択します。

「**電子メールログ**」を選択して、「**ログ** > 設定」ページで設定した電子メール アドレスにログを送信します。

「**検索**」オプションは、ログ メッセージをフィルタすることができます。検索は大文字と小文字を区別することに注意してください。ドロップダウン メニューで、検索に使用するフィールドを選択します。「**検索**」を選択すると、検索文字列に一致するメッセージだけが表示されます。検索文字列に一致するメッセージを非表示にするには、「**除外**」を選択します。すべてのメッセージを表示するには「**リセット**」を選択します。

1 ページに表示されるログ メッセージを増やしたり減らしたりするには、「**1 ページあたりの項目**」フィールドの値を変更します。ログ メッセージのページをスクロールするには前方または後方矢印を選択します。

見出しを選択すると、ログ メッセージは見出しのアルファベット順に並べ替えられます。

セキュア仮想アシスト > ライセンス

このセクションでは、「**セキュア仮想アシスト > ライセンス**」ページの概要と、このページで行える設定タスクについて説明します。

- 「セキュア仮想アシスト > ライセンス」ページの概要 (298 ページ)
- セキュア仮想アシストの有効化 (298 ページ)

「セキュア仮想アシスト > ライセンス」ページの概要

セキュア仮想アシストは、ライセンス サービスです。

セキュア仮想アシストの有効化

仮想アシストがライセンスされた後で作成されたポータル上では、既定で仮想アシストが有効になっています。セキュア仮想アシスト ライセンスが購入される前に作成されたすべてのポータル上では、既定で仮想アシストが無効になっています。

基本的な画面共有サポートのためには、ユーザは管理者権限が不要です。クライアントの完全インストールに対しては、管理者権限が必要になることもありますが、サービスを使うために完全インストールする必要はありません。セキュア仮想アクセスおよび不在モードは管理者権限を必要とします。

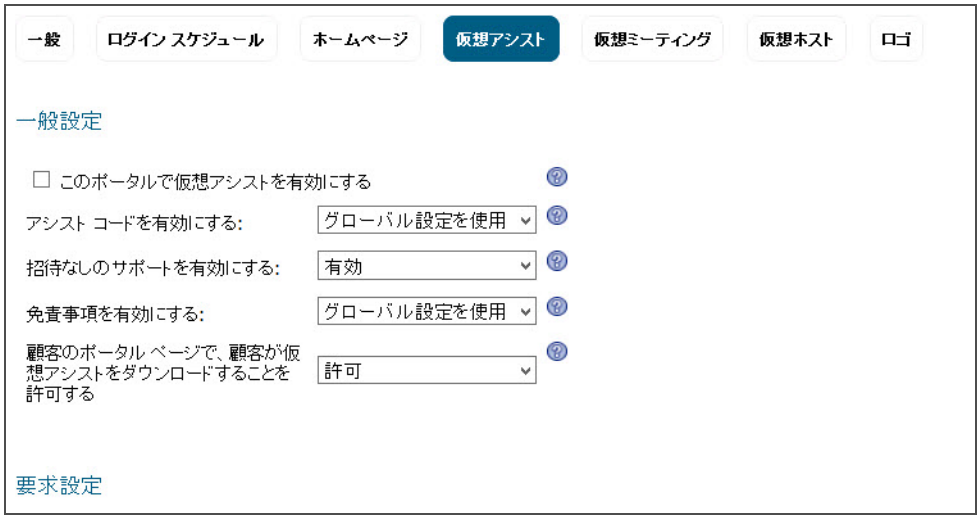
仮想アシストを設定するには

1 セキュア仮想アシストのライセンスを購入して有効化するには、「**システム > ライセンス**」に移動し、「**サービスの購読、アップグレード、及び更新**」へのリンクを選択します。

詳細については、システム > ライセンス (102 ページ) を参照してください。

2 ポータルに対して仮想アシストを有効にするには、「**ポータル > ポータル**」ページに進み、必要なポータルの「**設定**」アイコンを選択します。新しいポータルを作成するには、「**ポータル > ポータル**」ページに進み、「**ポータルの追加**」を選択します。ポータル > ポータル (148 ページ) を参照してください。

3 「**ポータルの編集**」ウィンドウの「**仮想アシスト**」ページを選択します。



4 「**このポータルで仮想アシストを有効にする**」をオンにし、「**適用**」を選択します。これで、仮想アシストが有効になり、すぐに使用できます。Secure Mobile Access ユーザの「仮想オフィス」ページに仮想アシスト アイコンが表示されます。

5 仮想オフィス ウィンドウ上の技術者ボタンを隠して、技術者にクライアントを通した直接ログインを要求するには、「**技術者ボタンを表示する**」をオフにします。

6 仮想オフィス上に、ユーザが仮想アシストを起動するための支援ボタンを表示するには、「**「サポートの要求」ボタンを表示する**」をオンにします。

7 このポータルへのセキュア仮想アクセス接続を許可するには、「**仮想アクセス モードを有効にする**」をオンにします。このポータル上で仮想アシストを機能させるためには、これは必須です。

8 仮想オフィス上に、セキュア仮想アクセス設定リンクを表示するには、「**仮想アクセス設定リンクを表示する**」をオンにします。

9 (オプション) 仮想アシストを、ローカル マシンにインストールすることなくウェブから起動するには、「**セキュア仮想アシストをインストールせずに起動する**」を選択します。この機能はグローバルまたはポータルごとに有効化できます。

10 「**LAN 上の顧客の PC を起動する**」機能を使用すると、技術者は仮想アシストを実行する LAN 上のクライアントを起動できます。クライアント PC は、電源がオフの場合も、スリープ状態の場合も、休止状態の場合も起動できます。この機能はグローバルまたはポータルごとに有効化できます。

- このポータルにグローバル設定を適用するには、「**グローバル設定を使用**」を選択します。
- グローバル設定に関係なく、この機能を有効にするには、「**有効**」を選択します。
- グローバル設定に関係なく、この機能を無効にするには、「**無効**」を選択します。

ⓘ **メモ**：クライアント起動を使用するには、この機能をクライアント マシン上で設定する必要があります。『*Secure Mobile Access ユーザ ガイド*』を参照してください。

11 「**サポート セッション数の制限**」フィールドに、このポータルで許可するアクティブなサポート セッションの数を入力します。制限を設けない場合は、0 を入力します。

12 「**アシスト コードを有効にする**」をオンにすると、アシストを要求する前に指定されたコードを入力することがユーザに求められます。このチェックボックスをオンにすると、「**アシスト コード**」フィールドが表示されるので、そこにユーザが入力するコードを指定します。

13 (オプション)「**招待なしでのサポートを有効にする**」がオンのとき、顧客は招待の電子メールを受け取っていなくてもアシストを要求できます。これがオフのときは、技術者によって明示的に招待された顧客だけがアシストを受けることができます。

14 「**免責事項を有効にする**」を有効にした場合、顧客はサポートを要求するときにコードを提供する必要があります。このオプションを無効にした場合、コードは不要です。

15 (オプション) 顧客が仮想アシスト クライアントをダウンロードできるようにする場合は、「**顧客ポータル ページで仮想アシストのダウンロードを許可する**」をオンにします。

16 必要に応じて、このウィンドウのタブを使用し、この個別のポータルの仮想アシストのすべての設定をカスタマイズできます。

これで、仮想アシストが有効になり、すぐに使用できます。Secure Mobile Access ユーザの「仮想オフィス」ページに**仮想アシスト** アイコンが表示されます。

11

セキュア仮想ミーティング

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**セキュア仮想ミーティング**」ページに関する情報と設定タスクおよび、仮想ミーティングに対して使用できる設定タスクについて説明します。

トピック:

仮想ミーティングの使用方法については、『*Secure Mobile Access ユーザ ガイド*』を参照してください。詳細については、『*Secure Mobile Access セキュア仮想ミーティングおよびセキュア仮想アシスト機能モジュール*』も参照できます。

セキュア仮想ミーティング > 状況

「**セキュア仮想ミーティング > 状況**」ページには、現在アクティブなミーティングと出席者の要約に加えて今後のミーティングが表示されます。

仮想ミーティング > 状況

画面右側の「**ストリーミング更新**」は顧客状況の変化が動的に更新されることを示します。「**オン/オフ**」を選択すると、それぞれストリーミング更新が有効/無効になります。

今後のミーティングを削除するには、「ミーティング情報」セクション内のミーティングの横にある「**ログアウト**」を選択します。

セキュア仮想ミーティング > 設定

セキュア仮想ミーティング > 設定このセクションでは「**セキュア仮想ミーティング > 設定**」ページおよび仮想ミーティングに対して使用できる設定タスクについて説明します。仮想ミーティングの設定は以下のページに分かれています。

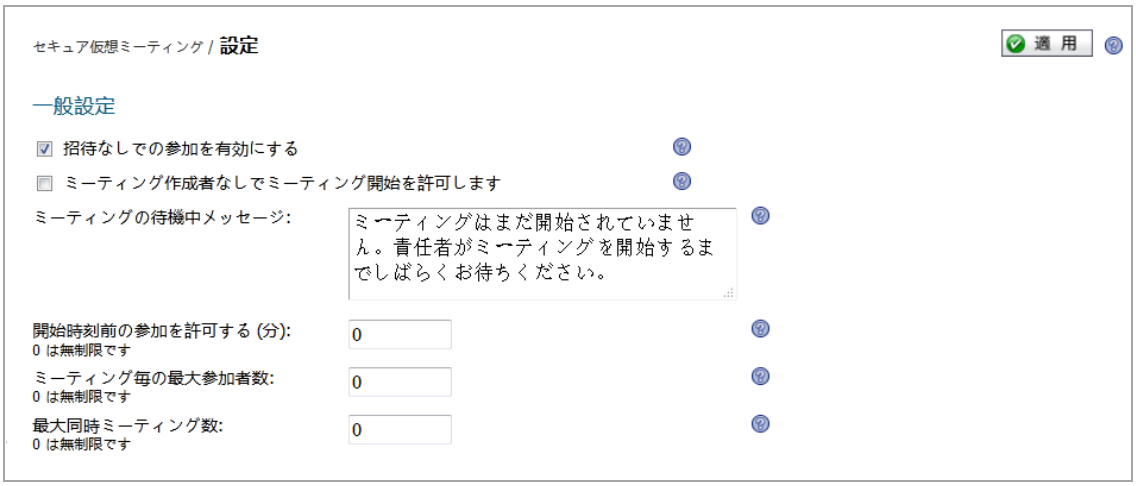
- 一般設定 (302 ページ)
- 通知設定 (303 ページ)

一般設定

仮想ミーティングの一般設定をするには「一般設定」ページを使用します。

仮想ミーティングの一般設定を行うには:

1 「**セキュア仮想ミーティング > 設定**」ページに移動します。



2 参加者が電子メールの招待リンクをたどる必要なしにミーティングに参加することを許可するには、「**招待なしでの参加を有効にする**」をオンにします。参加者は仮想ミーティング クライアントを実行し、主催者によって設定されたミーティング コードを使って直接ミーティングに参加します。

3 責任者不在でミーティングを開始することを許可するには、「**ミーティング作成者なしでミーティング開始を許可します**」をオンにします。このオプションが有効になっていて、スケジュールされた開始時刻にミーティング ルームに責任者が不在のミーティングは、1 参加者が責任者になるように選択されてミーティングが開始されます。このチェックボックスが選択されていない状態で開始時刻に主催者が不在の場合は、ミーティングは終了します。

4 「**ミーティングの待機中メッセージ**」フィールドに、ミーティングの開始をロビーで待っている参加者に表示されるメッセージを設定します。ロビーはチャットや電子メール招待といった仮想ミーティング機能を開始可能な待合室兼ミーティング ルームです。

5 「**開始時刻前の参加を許可する**」フィールドで、参加者がミーティングの開始何分前から参加できるかを示す数値を選択します。参加者が任意の時刻にミーティングに参加することを許可する場合は 0 を選択しますが、参加者がロビーに入った時からライセンスが使用中になるとい

うことを考慮する必要があります。追加のライセンス情報のついては ライセンス概要 (305 ページ) を参照してください。

6 「**ミーティング毎の最大参加者数**」フィールドで、作成されたミーティングに参加できる出席者の最大数を選択します。ミーティング出席者数が無制限の場合は、0 を選択します。

> **メモ**: セキュア仮想ミーティングはセキュア仮想アシストのライセンスを使用し、3 つのアクティブな仮想ミーティング出席者ごとに 1 つのセキュア仮想アシスト技術者ライセンスが必要です。

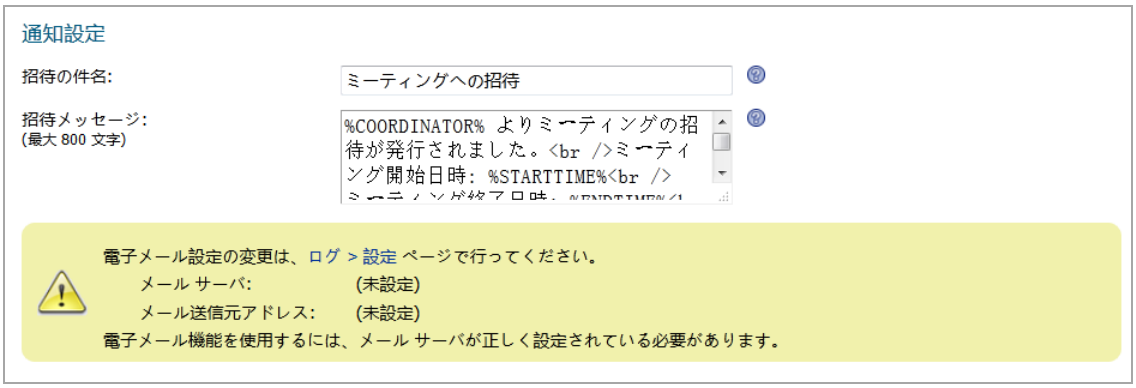
7 「**最大同時ミーティング数**」フィールドで、装置で同時に実行可能な最大ミーティング数を設定します。

例えば、会社が 5 つのセキュア仮想アシスト技術者ライセンスを所有していて、そのうち 2 つが仮想アシスト技術者に対して使用中であるとします。同時にいくつでも仮想ミーティングを行えますが、ロビー内の同時ユーザ数は 9 に制限されます (5 - 2 = 3 が利用可能なライセンス数で、3 x 3 = 9 ライセンスがミーティング ユーザに利用可能)。

通知設定

仮想ミーティングの通知設定を行うには:

1 「**セキュア仮想ミーティング > 設定**」ページで、ページの下部にある「**通知設定**」を選択します。



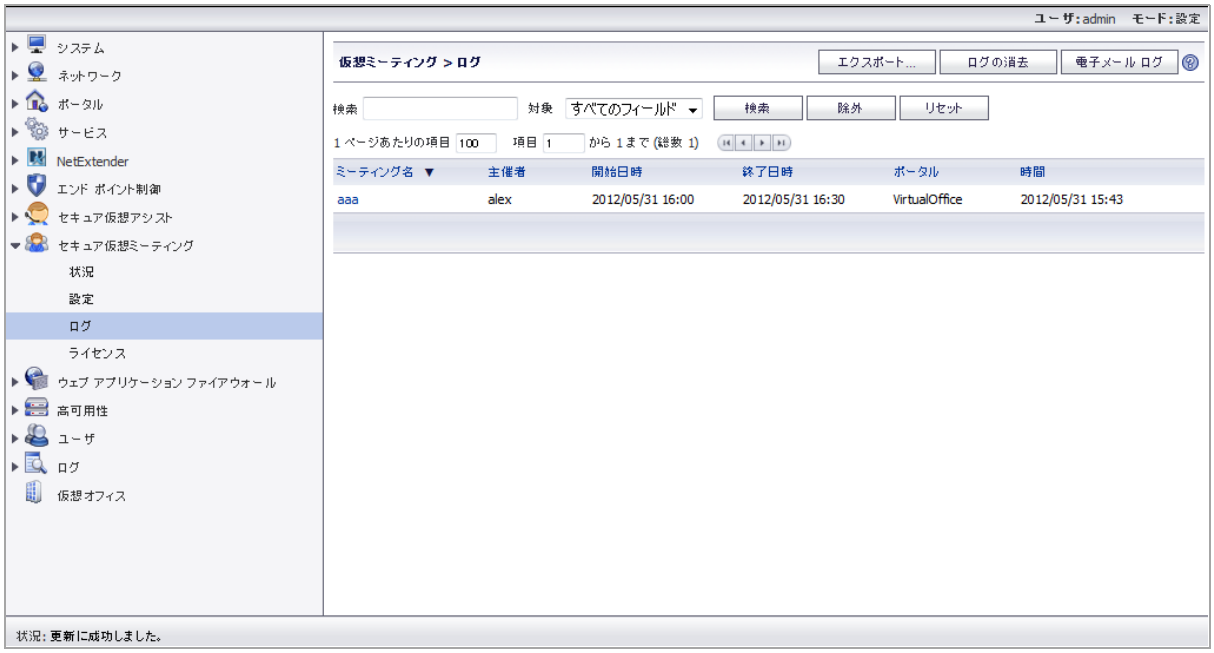
2 「**招待の件名**」フィールドに、参加者に送信する仮想ミーティング招待電子メールで使う件名を入力します。件名には、%MEETINGNAME% などの変数を含めることができます。可能な変数を表示するには、このフィールドの右にあるアイコン上にマウス ポインタを移動します。

3 「**招待メッセージ**」フィールドに、仮想ミーティング招待電子メールの本文に含めるテキストを入力します。本文には変数を含めることができます。可能な変数を表示するには、このフィールドの右にあるアイコン上にマウス ポインタを移動します。

セキュア仮想ミーティング > ログ

「**セキュア仮想ミーティング > ログ**」ページは、最近のミーティングについての詳細情報へのアクセスを提供します。

このログには、ミーティング名、主催者、ミーティングの開始と終了日時、ポータル名、およびミーティング作成日時が表示されます。



特定のミーティングに関する追加情報を表示するには、ミーティング名を選択します。「**セキュア仮想ミーティング > ログ**」ページに戻るには、ブラウザの戻るボタンを選択します。

すべてのログされたミーティングに対するテキスト全体を含む zip ファイルを作成するには、「**エクスポート**」を選択します。この zip ファイルには、ミーティング毎の要約ログ ファイルと詳細ログ ファイルが含まれ、それぞれ Microsoft Word で表示できます。

すべてのログ メッセージを削除するには「**ログの消去**」を選択します。

「**ログ > 設定**」ページで設定された電子メール アドレスにログを送信するには「**電子メール ログ**」を選択します。

「**検索**」オプションは、ログ メッセージをフィルタすることができます。検索は大文字と小文字を区別することに注意してください。ドロップダウン メニューで、検索したいフィールドを選択し、検索文字列に一致するメッセージのみを表示するには、「**検索**」を選択します。検索文字列に一致するメッセージを非表示にするには、「**除外**」を選択します。すべてのメッセージを表示するには「**リセット**」を選択します。

1 ページに表示されるログ メッセージを増やしたり減らしたりするには、「**1 ページあたりの項目**」フィールドの値を変更します。ログ メッセージのページをスクロールするには前方または後方矢印を選択します。

見出しによって表示されるログ メッセージをソートするには、見出しのいずれかを選択します。

セキュア仮想ミーティング > ライセンス

このセクションでは、「**セキュア仮想ミーティング > ライセンス**」ページの概要およびこのページ上で使用できる設定タスクについて説明します。

ライセンス概要

セキュア仮想ミーティングは、セキュア仮想アシスト パッケージの一部です。複数仮想ミーティングと仮想アシスト セッションは同時に行うことができます。しかし、これらのアクティブな仮想ミーティング ユーザ毎に仮想アシスト技術者ライセンスが必要です。例えば、会社が 5 つの仮想アシスト技術者ライセンスを所有していて、そのうち 2 つが仮想アシスト技術者に対して使用中であるとします。同時にいくつでも仮想ミーティングを行えますが、ロビー内の同時ユーザ数は 9 に制限されます (5 - 2 = 3 が利用可能なライセンス数で、3 x 3 = 9 ライセンスがミーティング ユーザに利用可能)。

ライセンスは先着順に割り当てられます。セキュア仮想ミーティング ライセンスは、参加者がロビーにいるときに使用中とみなされます。セキュア仮想アシスト/アクセス ライセンスは、接続がアクティブになって画面共有が行われているときに使用中とみなされます。

ライセンス情報

「**セキュア仮想ミーティング > ライセンス**」ページには、セキュア仮想アシストのライセンス状況が表示されます。これは「**システム > ライセンス**」ページにも表示されます。セキュア仮想アシスト ライセンスがどのようにセキュア仮想ミーティングに使用されるのかの説明については ライセンス概要 (305 ページ) を参照してください。このライセンス ページには、ライセンスを取得可能な「**システム > ライセンス**」ページへのリンクも含まれています。

セキュア仮想ミーティング ライセンス

12

ウェブ アプリケーションファイアウォールの設定

このセクションでは、Secure Mobile Access (ウェブベースの管理インターフェース) の「**ウェブ アプリケーション ファイアウォール**」ページに固有の情報と設定タスクについて説明します。

ウェブ アプリケーション ファイアウォールは購読ベースのソフトウェアです。このソフトウェアは、SMA/SRA 装置で実行され、SMA/SRA の背後のサーバ上で実行されているウェブ アプリケーションを保護します。また、ウェブ アプリケーション ファイアウォールは、SMA/SRA 装置本体で実行される HTTP(S) ブックマーク、Citrix ブックマーク、オフロードされたウェブ アプリケーション、Secure Mobile Access 管理インターフェースやユーザ ポータルなどのリソースをリアルタイムで保護します。

ウェブ アプリケーション ファイアウォールの概念の詳細については、ウェブ アプリケーション ファイアウォールの概要 (73 ページ) を参照してください。

トピック:

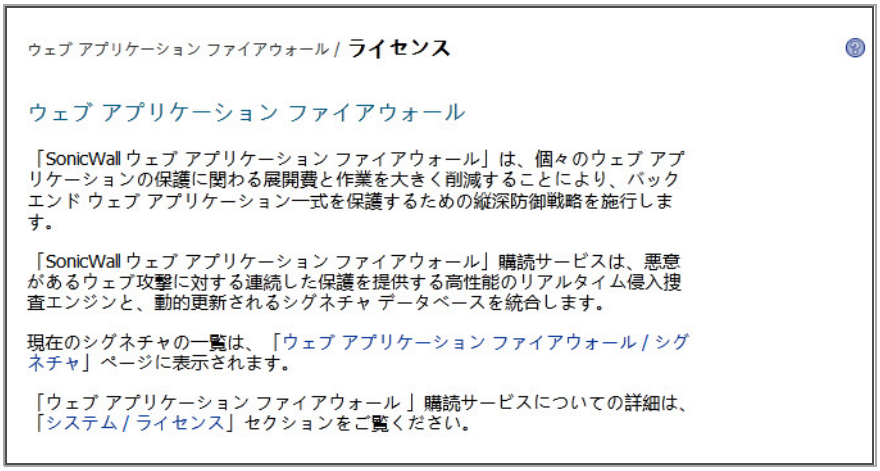
ウェブ アプリケーション ファイアウォールのライセンス

Secure Mobile Access ウェブ アプリケーション ファイアウォールを使用するには、ライセンスが必要です。Secure Mobile Access 管理インターフェースから mySonicWall ウェブ サイトに直接アクセスしてライセンスを取得できます。

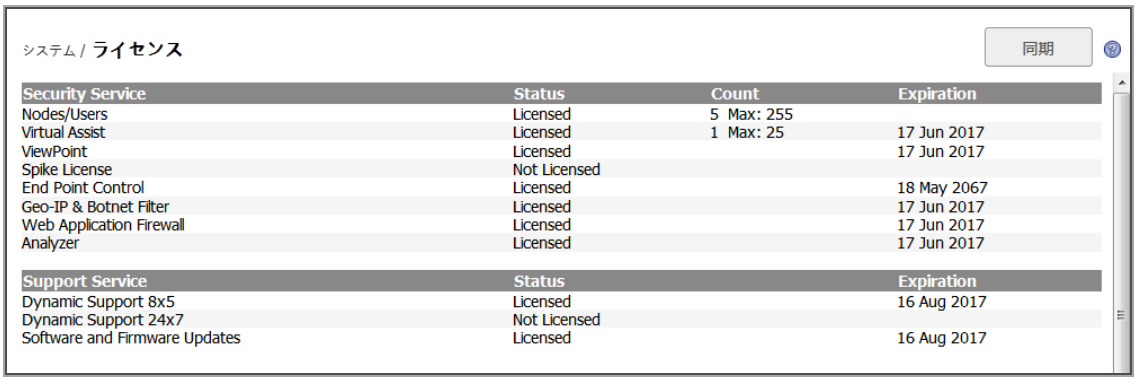
Secure Mobile Access 管理インターフェースの「**ウェブ アプリケーション ファイアウォール > ライセンス**」ページには、「**システム > ライセンス**」ページへのリンクがあります。このページから mySonicWall に接続してライセンスを購入するか、無料トライアルを開始できます。Secure Mobile Access 管理インターフェースの「**システム > ライセンス**」ページでは、すべてのシステム ライセンスを表示できます。

mySonicWall でウェブ アプリケーション ファイアウォールのライセンス情報を表示し、ライセンスを取得するには:

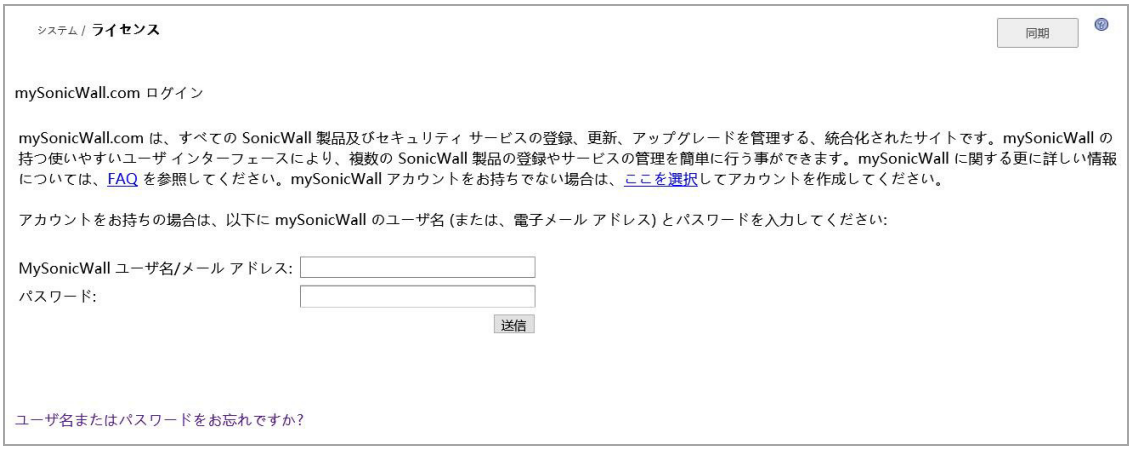
1 SMA/SRA 装置にログインし、「**ウェブ アプリケーション ファイアウォール > ライセンス**」を開きます。



2 ライセンスが未取得の場合は、「**システム** > ライセンス」リンクを選択します。「**システム** > **ライセンス**」ページが表示されます。



3 「セキュリティ サービスのオンライン管理」で「**サービスの購読、アップグレード、及び更新**」を選択します。「MySonicWall.com ログイン」ページが表示されます。



4 mySonicWall 資格情報を各フィールドに入力し、「**送信**」を選択します。

5 「**システム > ライセンス**」ページが表示されます。

6 「**試行**」を選択して 30 日間の無料トライアルを開始するか、「**有効化**」を選択して 1 年間のサービスを購読します。無料トライアルを選択すると、次の画面が表示されます。

7 「**同期**」を選択して「**システム > ライセンス**」ページにライセンスを表示します。

ウェブ アプリケーション ファイアウォールのライセンスが SMA/SRA 装置に取得されました。「**ウェブ アプリケーション ファイアウォール > 設定**」を開いてファイアウォールを有効化してから、装置を再起動して、ウェブ アプリケーション ファイアウォールを完全に有効化します。

ウェブ アプリケーション ファイアウォールの設定

メモ：ウェブ アプリケーション ファイアウォールを使用するには、ライセンスを追加で購入する必要があります。

トピック:

ウェブ アプリケーション ファイアウォールのステータス情報を表示および更新する

「**ウェブ アプリケーション ファイアウォール > 状況**」ページには、ウェブ アプリケーション ファイアウォールのサービスとシグネチャ データベースのステータス情報が提供され、ライセンス状況と有効期限が表示されます。「**同期**」を選択すると、最新のシグネチャ情報を SonicWall Inc. オンライン データベースからダウンロードできます。「**ダウンロード**」を使って PCI 準拠レポート ファイルを生成してダウンロードできます。

状況の表示とシグネチャの同期

シグネチャ データベースやウェブ アプリケーション ファイアウォールのサービス ライセンスの状況を表示したり、シグネチャ データベースを同期するには、Secure Mobile Access 管理インターフェースで以下の手順を実行します。

1 「**ウェブ アプリケーション ファイアウォール > 状況**」を開きます。「WAF 状況」セクションには、以下の情報が表示されます。

- シグネチャ データベースの更新ステータス
- シグネチャ データベースのタイムスタンプ
- シグネチャ データベースの最新の更新を前回チェックした時刻
- サービス購読の有効期限
- ライセンスのステータス

2 シグネチャ データベースの更新があれば、「**適用**」が表示されます。「**適用**」を選択して更新をダウンロードします。

「**ウェブ アプリケーション ファイアウォール > 設定**」ページ上で、新しいシグネチャを自動的に更新して適用するようオプションを選択できます。この自動更新オプションが有効の場合、新しいシグネチャが自動的に適用されるとすぐに「**ウェブ アプリケーション ファイアウォール > 状況**」ページから「**適用**」は消えます。

3 シグネチャ データベースを SonicWall Inc. オンライン データベース サーバーに同期するには、「**同期**」を選択します。タイムスタンプが更新されます。

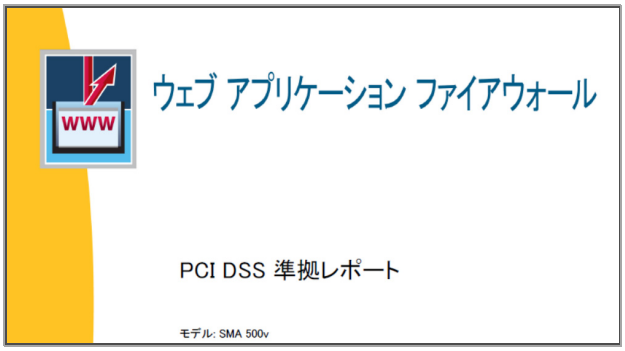
PCI 準拠レポートのダウンロード

PCI DSS 6.5/6.6 準拠レポートをダウンロードするには:

1 「**ウェブ アプリケーション ファイアウォール > 状況**」を開きます。

2 「**ダウンロード**」をクリックします。

3 ダウンロードのダイアログ ボックスで、PCI レポートを生成して一時ファイルとして開いて Adobe Acrobat で参照するか、レポートを PDF ファイルとして保存します。



ウェブ アプリケーション ファイアウォールの設定を行う

「**ウェブ アプリケーション ファイアウォール > 設定**」ページでは、SMA/SRA 装置のウェブ アプリケーション ファイアウォールをグローバルおよび攻撃危険度ごとに有効化/無効化できます。検知または阻止を、高、中、低の 3 つの攻撃クラスについて個別に指定できます。また、このページには特定のホストを検査対象から除外する設定オプションもあります。

このページではまた、その他のウェブ アプリケーション ファイアウォール設定も提供します。以下のセクションでは、ウェブ アプリケーション ファイアウォールを有効化し、設定する手順を説明します。

- ウェブ アプリケーション ファイアウォールを有効化して一般設定をする (312 ページ)
- グローバル除外の設定 (313 ページ)

- 侵入防御エラー ページの設定 (314 ページ)
- クロスサイト リクエスト フォージェリ防御の設定 (315 ページ)
- Cookie 改竄防御の設定 (316 ページ)
- ウェブ サイト隠蔽の設定 (318 ページ)
- 情報暴露防御の設定 (319 ページ)
- セッション管理の設定 (320 ページ)

ウェブ アプリケーション ファイアウォールを有効化して一般設定をする

ウェブアプリケーション ファイアウォールを有効化するには、チェックボックスを選択してグローバルに有効化し、少なくとも 1 つのチェックボックスを「シグネチャ グループ」テーブルで選択します。このページの「一般設定」セクションでは、高、中、低のいずれかの危険度の攻撃に対する保護レベルを選択して、ネットワーク保護をグローバルに管理できます。また、**グローバルの「ウェブ アプリケーション ファイアウォールを有効にする」**をオフにすると、ユーザ定義の設定を維持したまま、一時的にウェブ アプリケーション ファイアウォールを無効化できます。

このページの「**一般設定**」セクションで自動的なシグネチャの更新を有効にしておくと、新しいシグネチャが利用可能になったときにそのダウンロードと適用が自動的に行われます。自動的なシグネチャの更新のそれぞれについてログ エントリが生成されます。シグネチャが自動更新時に削除された場合は、関連する除外リストも削除されます。その削除を記録するためにログ エントリが生成されます。ログ エントリは「**ウェブ アプリケーション ファイアウォール > ログ**」ページで表示できます。

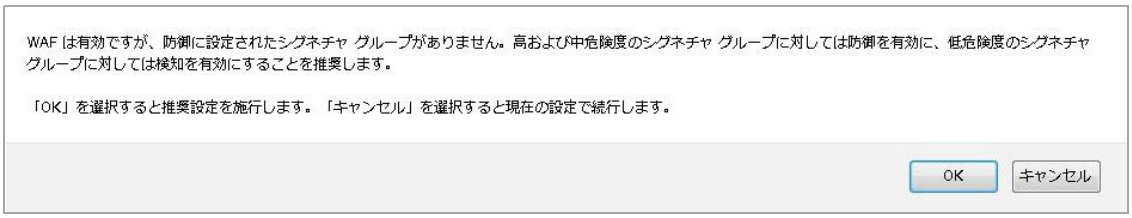
このページでは、クロスサイト要求偽装 (CSRF) に対する保護の設定も行えます。CSRF 攻撃が検知されると、「**ウェブ アプリケーション ファイアウォール > ログ**」と「ログ > 表示」ページの両方にログ エントリが作成されます。CSRF/XSRF 攻撃の詳細については、クロスサイトリクエストフォージェリを阻止する方法 (79 ページ) を参照してください。

ウェブ アプリケーション ファイアウォールのグローバル設定を構成するには:

1 「**ウェブ アプリケーション ファイアウォール > 設定**」ページで、「**一般設定**」セクションを展開します。

2 「**ウェブ アプリケーション ファイアウォールを有効にする**」をオンにします。

3 「**すべて防御**」が選択されたシグネチャ グループが 1 つもない場合は、警告ダイアログ ボックスが表示されます。ダイアログ ボックスの「**OK**」を選択してすべてのシグネチャ グループを「**すべて防御**」に設定します。または、「**キャンセル**」を選択して、設定を元のままにするか手動で設定を続行します。



4 新しいシグネチャが利用可能になった場合にそのダウンロードと適用を自動的に行うには、「**自動シグネチャ更新を適用する**」をオンにします。そうすると、「**ウェブ アプリケーション ファイアウォール > 状況**」ページの「**適用**」を選択しなくても新しいシグネチャを適用できます。

5 「シグネチャ グループ」テーブルの「**高危険度の攻撃**」で、必要な保護レベルを選択します。以下のいずれかのオプションを選択します。

- 攻撃が検知されたときにリソースへのアクセスを遮断するには、「**すべて防御**」をオンにします。「**すべて防御**」をオンにすると、自動的に「**すべて検知**」がオンになり、ログ機能が有効になります。
- 「**すべて防御**」をオフにし、「**すべて検知**」をオンにすると、攻撃がログに記録されますが、リソースへのアクセスは許可されます。
- 特定の攻撃危険度のログと阻止をグローバルに無効化するには、両方のチェックボックスをオフにします。

6 「シグネチャ グループ」テーブルの「**中危険度の攻撃**」で、必要な保護レベルを選択します。

7 「シグネチャ グループ」テーブルの「**低危険度の攻撃**」で、必要な保護レベルを選択します。

8 終了したら、「**適用**」を選択します。

グローバル除外の設定

現在のグローバルな設定から特定のホストを除外する方法が 3つあります。特定のホストについてを完全に無効化するか、特定のホストへのアクション レベルを「禁止」から「検知」に下げるか、ウェブ アプリケーション ファイアウォールがアクションを起こさないように設定することができます。

対象となるホストは、HTTP (S) ブックマークや Citrix ブックマークで使用されるホスト名と同一であり、オフロード ウェブ アプリケーション用に設定された仮想ホスト ドメイン名である必要があります。

グローバル除外を設定するには:

1 「**ウェブ アプリケーション ファイアウォール > 設定**」ページで、「**一般設定**」セクションを展開します。

2 「**グローバル除外**」を選択します。

3 「グローバル除外の編集」ページで、これらのホスト ページ上で設定されたリソースに対するシグネチャ グループ設定に優先する動作を設定します。「**動作**」ドロップダウン リストから以下のいずれか 1 つを選択します。

- **無効** - このホストの検査を無効にする
- **検知** - ホストのアクション レベルを「禁止」から「検知」および「ログのみ」に下げる
- **動作なし** - ウェブ アプリケーション ファイアウォールはホスト トラフィックを検査するが、アクションを起こさない

4 「**ホスト**」フィールドに、ホスト エントリをブックマークまたはオフロード アプリケーションに表示される表記形式で入力します。この表記形式は、ホスト名または IP アドレスです。最大 32 文字まで許可されます。除外されるホスト エントリを正確に確認する方法については、除外されるホスト エントリの確認 (324 ページ) を参照してください。

特定のフォルダまたはファイルへのパスをホストと共に設定できます。URL に含まれるプロトコル、ポート、および要求パラメータは無視されます。パスを設定すると、除外の設定はすべてのサブフォルダとファイルにも適用されます。例えば、「**ホスト**」に **webmail.company.com/exchange** と入力した場合は、**exchange** 下のすべてのファイルとフォルダも除外されます。

5 「**追加**」を選択してホスト名をリスト ボックスに移動します。

6 ステップ 4 とステップ 5 を繰り返して、別のホストを除外対象に追加します。

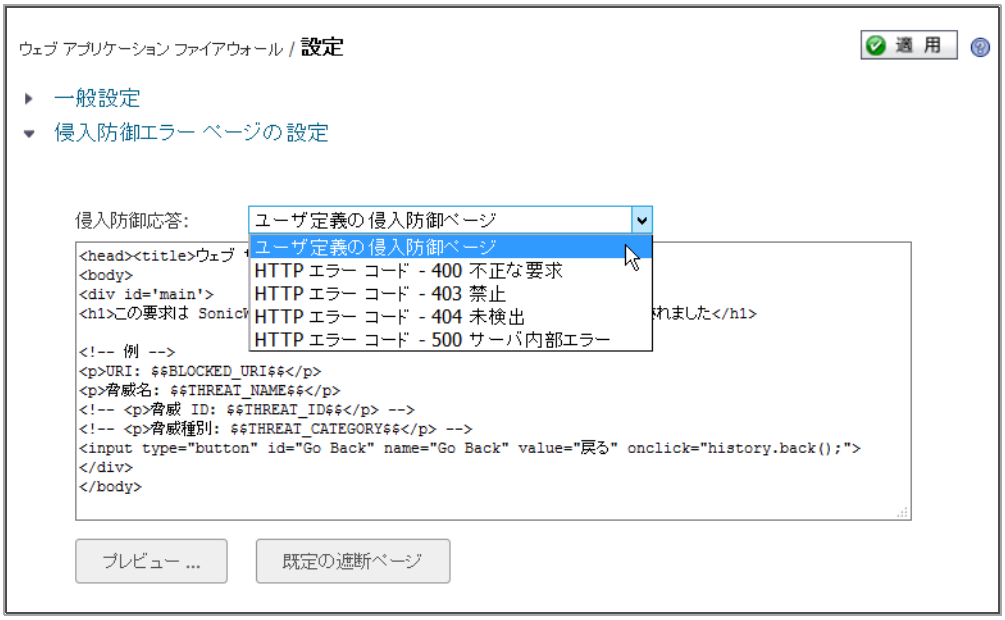
7 終了したら、「**適用**」を選択します。

侵入防御エラー ページの設定

侵入が検知されたときに使用するエラー ページを設定するには:

1 「**侵入防御エラー ページの設定**」セクションを展開します。

2 「**侵入防御応答**」ドロップダウン リストから、侵入試行の遮断時に表示されるエラー ページの種類を選択します。



3 個別ページを作成するには、「**ユーザ定義の侵入防御ページ**」を選択して、テキスト ボックスのサンプル HTML を変更します。

4 結果のページを表示するには、「**プレビュー**」を選択します。

5 現在のカスタマイズされたエラー ページをリセットして既定のエラー ページに戻すには、「**既定の遮断ページ**」を選択し、確認用ダイアログ ボックスで「**OK**」を選択します。

6 個別のエラーページを使わない場合は、エラー ページに対して以下から 1 つ選択します。

- HTTP エラー コード 400 不正な要求
- HTTP エラー コード 403 禁止
- HTTP エラー コード 404 未検出
- HTTP エラー コード 500 サーバ内部エラー

7 終了したら、「**適用**」を選択します。

クロスサイト リクエスト フォージェリ防御の設定

クロスサイト リクエスト フォージェリ (CSRF) は、各アプリケーション オフロード ポータルに対して独立して設定されます。このリリースでは新たに、フォームベースの防御方法が追加されました。シームレスなソリューションによって、誤検知を減らします。これ以外に、オリジナルの防御手法である URL 書き換えベースの防御手法が選択できます。

CSRF 攻撃が検知されると、「**ウェブ アプリケーション ファイアウォール > ログ**」と「**ログ > 表示**」ページの両方にログ エントリが作成されます。CSRF/XSRF 攻撃の詳細については、クロスサイトリクエストフォージェリを阻止する方法 (79 ページ) を参照してください。

URL 書き換えベースの防御手法で CSRF 防御を設定するには:

1 「**クロスサイト リクエスト フォージェリ (サイト横断要求の偽装/CSRF/XSRF) 防御**」セクションを展開します。

2 「**ポータル**」ドロップダウン リストから、これらの CSRF 防御設定を適用するポータルを選択します。これらの CSRF 防御設定をすべてのポータルに対する既定にする場合は、「**グローバル**」を選択します。

3 「**防御方法**」ドロップダウン リストから、「**URL 書き換えベースの防御**」を選択します。

4 「**防御モード**」から、CSRF 攻撃に対する防御に望むレベルを選択します。これらの攻撃をログするには「**検知のみ**」を、ログして遮断するには「**防御**」を、グローバル設定を継承するには「グローバルを継承」を選択します。ポータルでの CSRF 防御を無効にするには、「**無効**」を選択します。

5 終了したら、「**適用**」を選択します。

フォームベースの防御手法で CSRF 防御を設定するには:

1 「**クロスサイト リクエスト フォージェリ (サイト横断要求の偽装/CSRF/XSRF) 防御**」セクションを展開します。

2 「**ポータル**」ドロップダウン リストから、これらの CSRF 防御設定を適用するポータルを選択します。これらの CSRF 防御設定をすべてのポータルに対する既定にする場合は、「**グローバル**」を選択します。

3 「**防御方法**」ドロップダウン リストから、「**フォームベースの防御**」を選択します。

4 「**コンテンツ種別**」で、CSRF でプロファイルするコンテンツの種別を選択します。「**すべて**」、「**HTML/XML**」、「**JavaScript**」、または「**CSS**」が選択できます。

5 「**プロファイリングの開始**」を選択すると、CSRF フォームベース防御が開始されます。ファイリングを停止するには、「**プロファイリングの停止**」を選択します。

6 終了したら、「**適用**」を選択します。

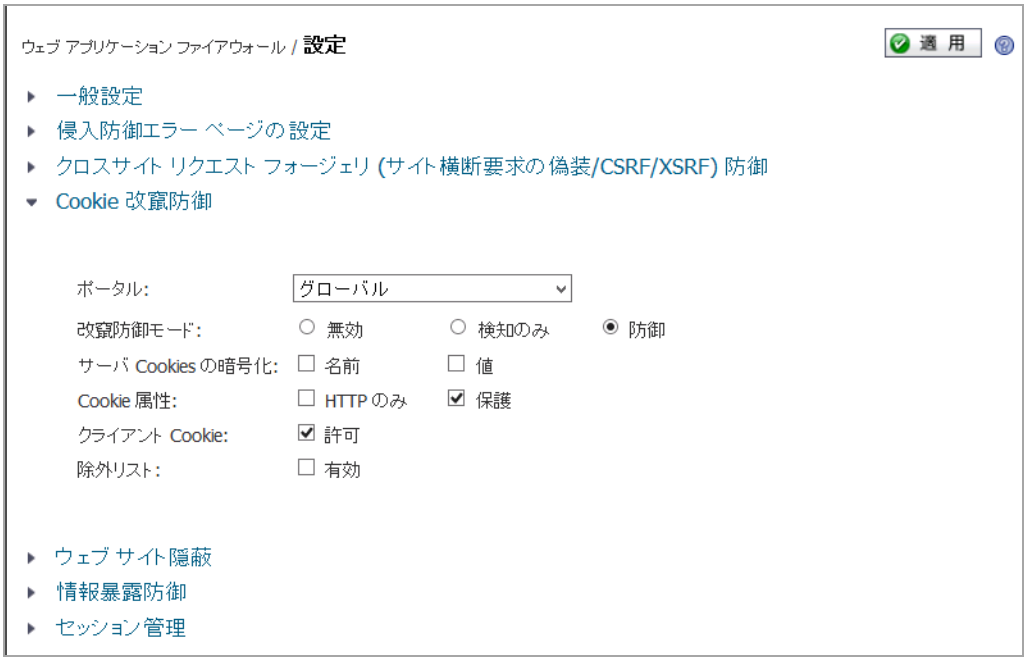
メモ：以前のバージョンからファームウェアをアップグレードし、防御方法を**フォームベースの防御**に変更した場合は、コントロールがグレー表示されて使用できない場合があります。「**適用**」を選択すると、コントロールが使用可能になります。

Cookie 改竄防御の設定

Cookie 改竄防御は、各アプリケーション オフロード ポータルに対して独立して設定されます。

Cookie 改竄防御を設定するには:

1 「**Cookie 改竄防御**」セクションを展開します。



2 「**ポータル**」ドロップダウン リストから、これらの Cookie 改竄防御設定を適用するアプリケーション オフローダ ポータルを選択します。これらの Cookie 改竄防御設定をすべてのポータルに対する既定にする場合は、「**グローバル**」を選択します。

3 「**改竄防御モード**」から、Cookie 改竄に対する防御に望むレベルを選択します。これらの攻撃をログするには「**検知のみ**」を、ログして遮断するには「**防御**」を、グローバル設定を継承するには「グローバル」を選択します。ポータルでの Cookie 改竄防御を無効にするには、「**無効**」を選択します。

4 「**サーバ Cookies の暗号化**」に対して、Cookie 名を暗号化するには「**名前**」をオンにし、Cookie 値を暗号化するには「**値**」をオンにします。両方をオンにすることもできます。これは Cookie 名または値を読めなくするので、クライアント側スクリプトの振舞いに影響します。これらのオプションによって、サーバ側 Cookie のみが暗号化されます

5 「**Cookie 属性**」に対して、サーバ側 Cookie に *HttpOnly* 属性を追加するには「**HTTP のみ**」をオンにし、*Secure* 属性をサーバ側 Cookie に追加するには「**保護**」をオンにします。両方をオンにすることもできます。*HttpOnly* 属性は、クライアント側スクリプトが Cookie にアクセスすることを防ぎます。これはクロスサイト スクリプティングやセッション ハイジャックといった攻撃を軽減するときに重要です。*Secure* 属性は、Cookie が HTTPS 接続のみで送信されることを確かにします。両方協力して、サーバ側 Cookie に対して強固なレイヤのセキュリティを追加します。

6 「**クライアント Cookie**」に対して、ポータル上のアプリケーションがクライアント Cookie すべてを必要とする場合は、「**許可**」をオンにします。無効の場合、クライアント側 Cookie はバックエンド システムに送信されることが許可されません。このオプションはサーバ側 Cookie には影響しません。

7 「**除外リスト**」に対して、「**有効**」をオンにすると、設定するための追加のフィールドが表示されます。

8 「**除外リスト**」に個別の Cookie 名とパスを入力するには、「**Cookie 名**」フィールドに Cookie の名前を入力して、「**Cookie パス**」フィールドにパスを入力します。「**追加-->**」をクリックします。

9 1 つ以上の検知済み Cookie を「**除外リスト**」に追加するには、「**検知された Cookie**」リストから追加したい Cookie を選択し (複数の Cookie を選択するときは **Ctrl** キーを押しながら選択)、「**<--追加**」ボタンを選択して「**除外リスト**」に追加します。

10 「**除外リスト**」から Cookie を削除するには、削除したい Cookie を選択して「**削除**」を選択します。

11 「**検知された Cookie**」リストをクリアするには、「**消去**」を選択します。

12 終了したら、「**適用**」を選択します。

ウェブ サイト隠蔽の設定

「**ウェブ サイト隠蔽**」セクションで、クライアントにバックエンド ウェブ サーバに関する情報を提供して場合によっては脆弱性の発見に使われる可能性のある、応答メッセージ内のヘッダをフィルタ除去できます。

ウェブ サイト隠蔽を設定するには、以下の手順に従います。

1 「**ウェブ サイト隠蔽**」セクションを展開します。

2 「**応答ヘッダの遮断**」フィールドで「**手動**」を選択し、1 つ目のフィールドにサーバ ホスト名、2 つ目のフィールドにヘッダ名を入力したら、「**追加**」を選択します。

例えば、ホスト名に "webmail.xyz.com"、そしてヘッダ名に "X-OWA-Version" を設定した場合は、ホスト "webmail.xyz.com" からの "X-OWA-Version" の名前を持つヘッダは遮断されます。通常、HTTP/HTTPS ブックマークまたはオフロードされたアプリケーションが、リストされたウェブ サーバへのアクセスに使われている場合は、リストされたヘッダはクライアントに送信されません。

すべてのホストからのあるヘッダを遮断するには、ホスト名にアスタリスク(*)を設定します。最大 64 組のホスト/ヘッダを追加できます。HTTP プロトコルでは、応答ヘッダは大文字小文字を判別しません。

ⓘ **メモ**: HTTP プロトコルで重要な Content-Type などのヘッダに対しては遮断は発生しません。

3 ホスト/ヘッダのペアを遮断リストから削除するには、テキスト　ボックス内のペアを選択してから「**削除**」を選択します。

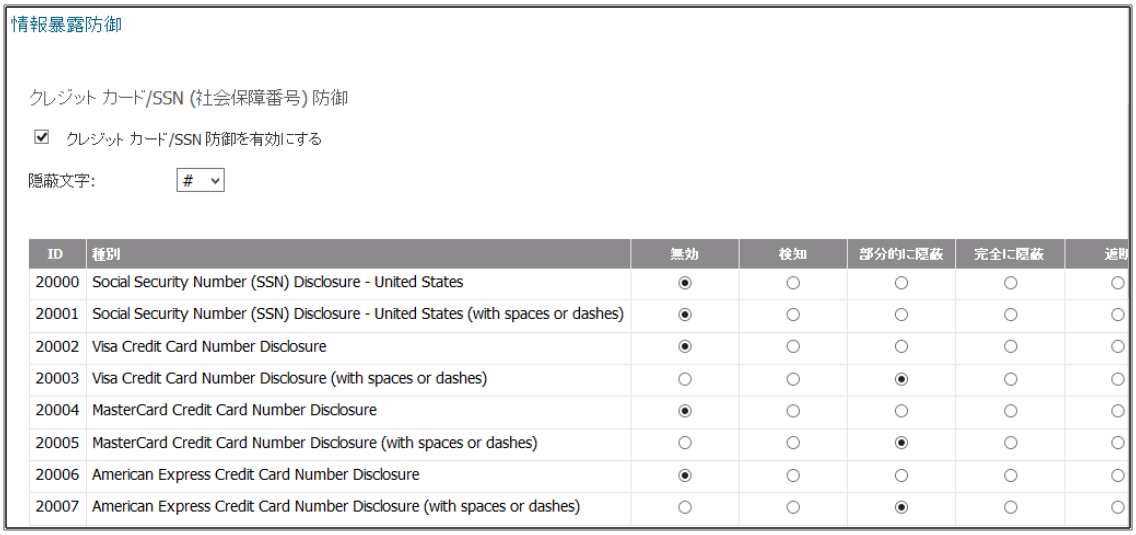
4 終了したら、「**適用**」を選択します。

情報暴露防御の設定

「**情報暴露防御**」セクションで、HTML ウェブ ページ内でのクレジット カードまたは社会保障番号 (SSN) の不慮の開示に対して保護できます。ウェブ アプリケーション ファイアウォールによって保護されているどのようなウェブ サイト上でも見られるべきでない、機密性の高いテキスト文字列を入力することもできます。

情報暴露防御を設定するには、以下の手順に従います。

1 「**情報暴露防御**」セクションを展開します。テーブルには、ウェブ　アプリケーション　ファイアウォールが HTML 応答内で検知可能な社会保障番号やクレジット カード番号の起こりうるパターンや形式それぞれに対する行があります。



ID	種別	無効	検知	部分的に隠蔽	完全に隠蔽	追加
20000	Social Security Number (SSN) Disclosure - United States	◉	○	○	○	○
20001	Social Security Number (SSN) Disclosure - United States (with spaces or dashes)	◉	○	○	○	○
20002	Visa Credit Card Number Disclosure	◉	○	○	○	○
20003	Visa Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○
20004	MasterCard Credit Card Number Disclosure	◉	○	○	○	○
20005	MasterCard Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○
20006	American Express Credit Card Number Disclosure	◉	○	○	○	○
20007	American Express Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○

2 「**クレジット カード/SSN 防御を有効にする**」をオンにします。

3 「**隠蔽文字**」ドロップダウン リストから、SSN またはクレジット カード番号を隠蔽する際に代用する文字を選択します。

4 テーブル内で、SSN またはクレジット カード番号の各表現に対して希望する防御レベルを選択します。それぞれの行に対して、以下のうち 1 つを選択できます。

- **無効** - この形式の番号は照合をしません。ログや隠蔽は実行されません。
- **検知** - この形式の番号を検知して、検知した場合はログ エントリを作成します。
- **部分的に隠蔽** - 番号の秘密性を維持できるように最後の数桁を除いたすべての桁を隠蔽文字に置換します。
- **完全に隠蔽** - 番号のすべての桁を隠蔽文字に置換します。

- **遮断** - 完全に (隠蔽された形式であっても) 番号の送信や表示をしません。

5 テーブルの下で、「**HTML ページ内の機密性の高い情報を遮断します**」テキスト ボックスに、ウェブ アプリケーション ファイアウォールによって保護されているどのようなウェブ サイト上でも見られるべきでない、機密性の高いテキスト文字列を入力することもできます。このテキストは大文字と小文字を区別せず、単語間に任意の数の空白を含めることができますが、ワイルドカード文字を含めることはできません。新しい語句は別の行に追加します。HTML 応答内では行ごとにパターンマッチングが行われます。

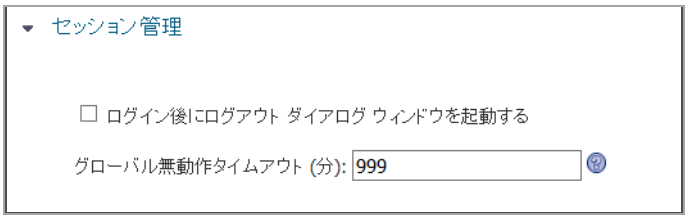
6 終了したら、「**適用**」を選択します。

セッション管理の設定

「**セッション管理**」セクションで、ユーザがユーザ ポータルやアプリケーション オフロード ポータルにログインした際に、ログアウト ダイアログ ウィンドウを表示するかどうかを制御できます。ユーザに対する無動作タイムアウトもこのセクションで設定できます。

ユーザに対する無動作タイムアウトもこのセクションで設定できます。

1 「**セッション管理**」セクションを展開します。



2 ユーザ ポータルの起動時やユーザがアプリケーション オフロード ポータルにログインした際に、セッション ログアウト ポップアップ ダイアログボックスを表示するには、「**ログイン後にログアウト ダイアログ ウィンドウを起動する**」をオンにします。

3 「**グローバル無動作タイムアウト**」フィールドに、ユーザをログアウトさせるまでの無動作時間を分単位で入力します。この設定は、グループまたはユーザ設定により優先されます。

> **メモ :** CSRF 攻撃を緩和するには、ユーザ セッションの無動作時タイムアウト値を小さくしておく (例えば 10 分) ことが重要です。

4 終了したら、「**適用**」を選択します。

ウェブ アプリケーション ファイアウォールのシグネチャ アクションの設定

「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページでは、特定のホストにのみ適用する処理や除外をシグネチャごとに設定できます。シグネチャ ベースの除外を使用して、すべてのホストを対象とした除外をシグネチャごとに適用できます。

また、指定済みの既存の除外設定を維持したままで、そのシグネチャが属するシグネチャ グループのグローバル設定に戻すこともできます。

ID ▼	シグネチャ	脅威分類	深刻度	設定
1000	Blind SQL Injection Attack Variant 4	コマンド実行--SQL インジェクション	高	
1001	Blind SQL Injection Attack Variant 5	コマンド実行--SQL インジェクション	中	
1002	Blind SQL Injection Attack Variant 6	コマンド実行--SQL インジェクション	中	
1003	Blind SQL Injection Attack Variant 7	コマンド実行--SQL インジェクション	中	
1004	Blind SQL Injection Attack Variant 8	コマンド実行--SQL インジェクション	中	
1005	Blind SQL Injection Attack Variant 9	コマンド実行--SQL インジェクション	中	
1008	AnyInventory environment.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	
1009	WebED viewitem.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	
1010	absolute_path Remote File Inclusion	コマンド実行--SSI インジェクション	低	
1011	iziContents search.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	
1012	php wcms XT config_PHPLM.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	
1013	Trionic Cite CMS custom.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	
1014	WebDesktop apps.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	
1015	Pindorama client.php Remote File Inclusion	コマンド実行--SSI インジェクション	高	

シグネチャのリストは、列の見出しを選択することによって、その列の内容の昇順または降順に並べ替えることができます。また、シグネチャを複数のページに分割したり、キーワード検索によってフィルタリングすることもできます。あるキーワードをすべてのフィールドまたは特定のフィールドに含むシグネチャだけを表示するには、「**検索**」フィールドにキーワードを入力し、検索対象として「**すべてのフィールド**」、または特定のフィールドを選択して、「検索」を選択します。「**除外**」を選択すると、キーワードを含まないシグネチャのみが表示されます。「**リセット**」を選択すると、すべてのシグネチャが表示されます。一致する箇所はすべて強調表示されます。既定では 1 ページに 50 個のシグネチャが表示されます。

「**ウェブ アプリケーション ファイアウォール > 設定**」ページでは、当該のシグネチャが属するシグネチャ グループのグローバル設定が「すべて防御」または「すべて検知」に設定されている必要があります。どちらにも設定されていない場合、シグネチャ グループはグローバルに無効であり、シグネチャごとに設定を変更することはできません。ウェブ アプリケーション ファイアウォールを有効化して一般設定をする (312 ページ) を参照してください。

シグネチャ グループ	すべて防御	すべて検知
高危険度の攻撃	☑	☑
中危険度の攻撃	☑	☑
低危険度の攻撃	☐	☑

以下のセクションを参照してください。

- パフォーマンス最適化を有効にする (322 ページ)
- シグネチャ ベースの個別処理および除外の設定 (322 ページ)
- シグネチャをグローバル設定に戻す (324 ページ)
- シグネチャごとの除外対象からホストを削除する (324 ページ)

パフォーマンス最適化を有効にする

パフォーマンス最適化オプションにより、比較的危険度が低く、多くのウェブ アプリケーションのパフォーマンスに著しく影響するシグネチャを無効にできます。これらのシグネチャは SonicWall Inc. シグネチャ チームによって確認され、そのリストは SMA/SRA 装置に配信されます。「**パフォーマンス最適化を有効にする**」をオンにすると、これらのシグネチャはウェブ アプリケーション ファイアウォールに対して無効になります。

「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページでは、パフォーマンス最適化を有効にする のように灰色で表示することによって無効化されたシグネチャを指し示します。

パフォーマンス最適化を有効にする

シグネチャ ベースの個別処理および除外の設定

個々のホストまたはすべてのホストへのトラフィックについてシグネチャの検査を無効にできます。また、個々のホストまたはすべてのホストについて検知された脅威の処理を変更できます。シグネチャが属するシグネチャ グループがグローバルに「すべて検知」に設定されている場合は、特定のホストの保護レベルを「禁止」に上げることができます。ホストが一切設定されていない場合は、動作がシグネチャそのものに適用され、すべてのホストに対するグローバル設定として機能します。こうした変更によって、その攻撃シグネチャが検知されたときにホストへのアクセスを遮断できます。同様に、所属先のシグネチャ グループがグローバルに「すべて禁止」に設定されている場合は、保護レベルを「検知」に下げることもできます。

メモ: シグネチャ ベースのカスタマイズを適用するには、変更されたシグネチャが属するシグネチャ グループが「**ウェブ アプリケーション ファイアウォール > 設定**」ページで防御または検知のどちらかについてグローバルに有効化されている必要があります。

1 つまたは複数のホストをシグネチャ検査から除外するか、ウェブ アプリケーション ファイアウォールによって1 つまたは複数のホストに特定のシグネチャが検知されたときに固有の処理を行うには、以下の手順に従います。

1 「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページで、設定を変更するシグネチャの「**設定**」 を選択します。「**WAF 署名ベースの除外の編集**」画面が表示されます。

2 「WAF 署名ベースの除外の編集」画面で、「**動作**」ドロップダウン リストから以下のいずれか 1 つを選択します。

- **無効** - このシグネチャに対するの検査を、この除外対象に含まれるホストからのトラフィックに行いません
- **検知** - この除外対象に含まれるホストからのトラフィックについて、このシグネチャに一致する脅威を検知し、ログに記録しますが、ホストへのアクセスは遮断しません
- **禁止** - この除外対象に含まれるホストからのトラフィックについて、このシグネチャに一致する脅威をログに記録し、ホスト アクセスを遮断します

3 この動作をすべてのホストに対してグローバルに適用するには、「**ホスト**」フィールドを空白にしておきます。この動作を個々のホストに適用するには、ホスト エントリをブックマークまたはオフロード アプリケーションでの表記形式で「**ホスト**」フィールドに入力します。この表記形式は、ホスト名または IP アドレスです。除外されるホスト エントリを正確に確認する方法については、除外されるホスト エントリの確認 (324 ページ) を参照してください。

特定のフォルダまたはファイルへのパスをホストと共に設定できます。URL に含まれるプロトコル、ポート、および要求パラメータは無視されます。パスを設定すると、除外の設定はすべてのサブフォルダとファイルにも適用されます。例えば、「**ホスト**」に **webmail.yourcompany.com/exchange**と入力した場合は、**exchange**下のすべてのファイルとフォルダも除外されます。

4 ホストを指定した場合は、「**追加**」を選択してホスト名をリスト ボックスに移動します。

5 この動作を別のホストにも適用する場合は、ホストごとにステップ 3 とステップ 4 を繰り返して、除外対象に追加します。

6 「**適用**」を選択します。ホストのリストにホスト エントリが含まれている場合、Secure Mobile Access はそれぞれのホスト エントリが有効であることを確認します。ホストが指定されなかった場合は、この動作がグローバル設定としてシグネチャそのものに適用されることを確認するダイアログ ボックスが表示されます。

7 確認のダイアログ ボックスで、「**OK**」を選択します。

8 「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページで「**適用**」を選択して、更新された設定を適用します。新しい設定が新しい HTTP 接続および要求のすべてに適用されます。既存の HTTP 接続および要求では、それらが終了するまで古い設定が引き続き使用されます。

シグネチャをグローバル設定に戻す

除外の設定が行われたシグネチャについて、その設定を維持したままで、シグネチャ グループのグローバル設定に戻すことができます。除外を再度有効にするときのために、ホスト名を残しておくことができます。

シグネチャをシグネチャ グループのグローバル設定に戻すには:

1. 「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページで、設定を変更するシグネチャの「**設定**」 を選択します。
2. 「WAF 署名ベースの除外の編集」画面で、「**動作**」ドロップダウン リストから「**グローバルを継承**」を選択します。
3. グローバル設定が以前にこのシグネチャに適用されていた場合、「**ホスト**」フィールドは空白になっている可能性があります。すべてのホストを対象としたグローバルなシグネチャの設定に戻すには、「**ホスト**」フィールドを空白にしておきます。この動作を 1 つ以上の個々のホストに適用するには、それらのホスト エントリを「**ホスト**」フィールド内に残し、設定を戻さないホストのエントリはすべて削除します。
4. 「**適用**」を選択します。Secure Mobile Access によって、各ホスト エントリが有効であることが確認されます。
5. 確認のダイアログ ボックスで、「**OK**」を選択します。
6. 「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページで「**適用**」を選択して、更新された設定を適用します。新しい設定が新しい HTTP 接続および要求のすべてに適用されます。既存の HTTP 接続および要求では、それらが終了するまで古い設定が引き続き使用されます。

シグネチャごとの除外対象からホストを削除する

シグネチャに設定した除外対象からホストを削除するには、以下の手順に従います。

1. 「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページで、設定を変更するシグネチャの「**設定**」 を選択します。
2. 「ホスト」フィールドの下にあるリストボックスでホスト エントリを選択し、「**除去**」を選択します。
3. 必要に応じて、ステップ 2 を繰り返してリスト内のホストをさらに削除します。
4. 「**適用**」を選択します。Secure Mobile Access によって、各ホスト エントリが有効であることが確認されます。
5. 確認のダイアログ ボックスで、「**OK**」を選択します。
6. 「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページで「**適用**」を選択して、更新された設定を適用します。新しい設定が新しい HTTP 接続および要求のすべてに適用されます。既存の HTTP 接続および要求では、それらが終了するまで古い設定が引き続き使用されます。

除外されるホスト エントリの確認

グローバルまたはシグネチャごとに除外設定を行う際には、ホスト名または IP アドレスを指定する必要があります。対象となるホストは、HTTP (S) ブックマークや Citrix ブックマークで使用されるホス

ト名と同一であり、オフロード ウェブ アプリケーション用に設定された仮想ホスト ドメイン名である必要があります。

正確なホスト名を確認する方法については、以下のセクションを参照してください。

- ブックマーク内のホスト エントリを表示する (325 ページ)
- オフロード アプリケーション内のホスト エントリを表示する (326 ページ)

ブックマーク内のホスト エントリを表示する

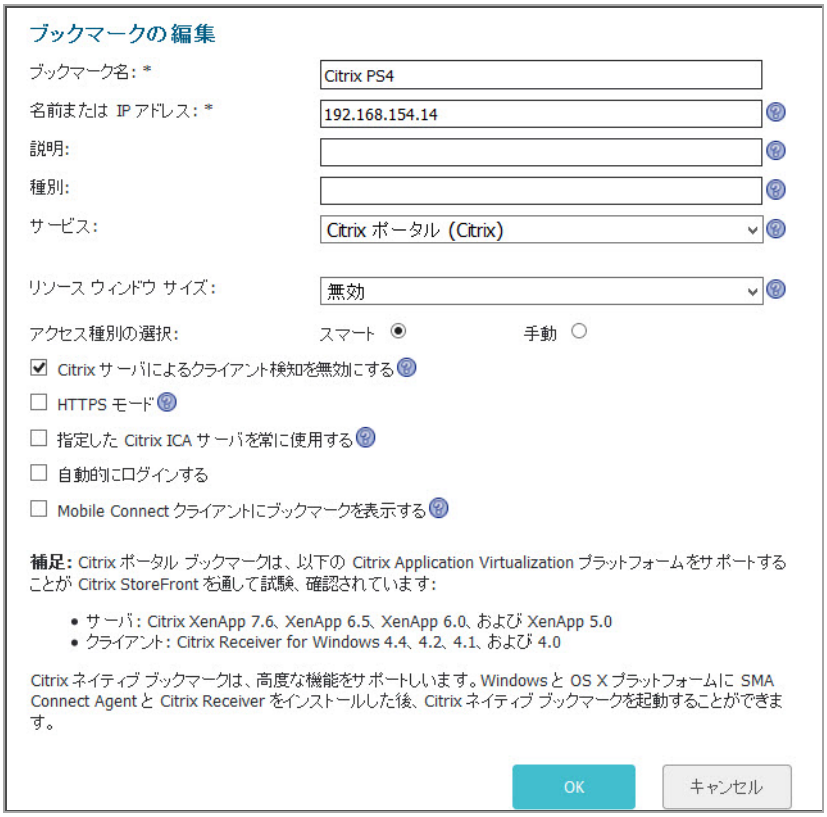
除外するホストの正確な名前は、ブックマークの詳細な設定情報を参照すると確認できます。

ブックマーク内のホスト エントリを表示するには:

1 「仮想オフィス」ページを開き、ブックマークのリストの上にある「**編集コントロールを表示する**」を選択します。

2 ブックマークの「**編集**」を選択します。

3 「ブックマークの編集」画面で、「**名前または IP アドレス**」フィールドに表示されるホスト エントリを確認します。



4 「**キャンセル**」を選択します。

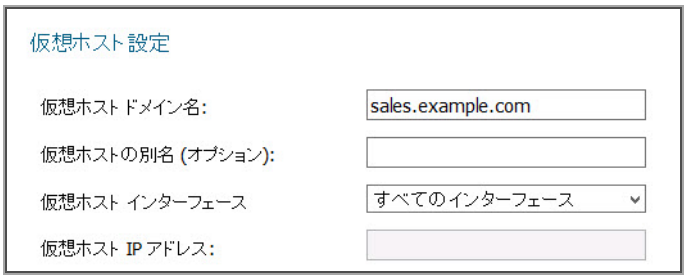
オフロード アプリケーション内のホスト エントリを表示する

除外するホストの正確な名前は、オフロード アプリケーションの詳細な設定情報を参照すると確認できます。オフロード アプリケーションでは、仮想ホスト ドメイン名を使用します。

オフロード アプリケーション内の仮想ホスト ドメイン名を表示するには:

1 「**ポータル > ポータル**」ページを開き、オフロード アプリケーションの横にある「**設定**」を選択します。

2 「ポータルの編集」画面で、「**仮想ホスト**」ページを選択します。



3 除外するホスト エントリを「**仮想ホスト ドメイン名**」フィールドで確認します。

4 「**キャンセル**」を選択します。

個別ルールとアプリケーション プロファイリングの設定

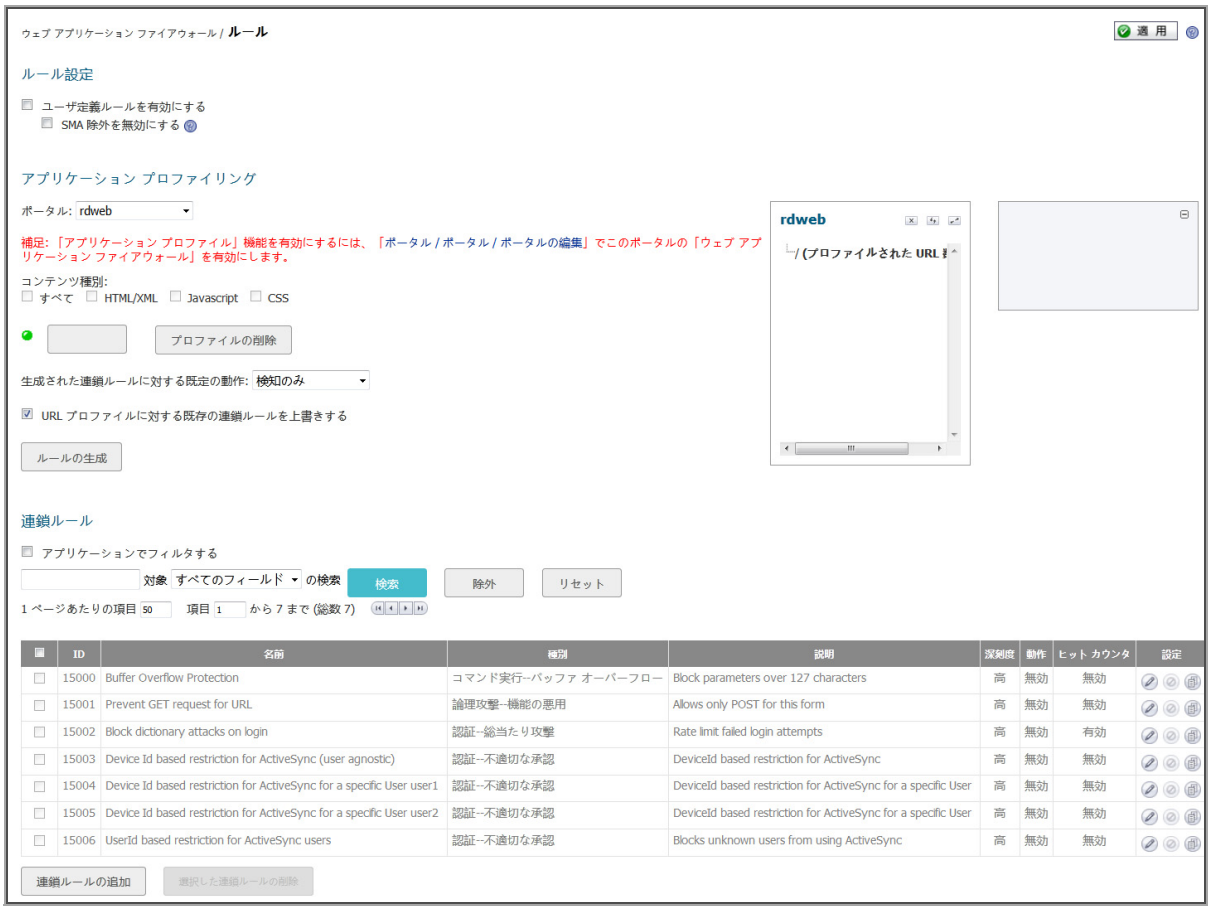
「**ウェブ アプリケーション ファイアウォール > ルール**」ページでは、個別ルールとアプリケーション プロファイリングを設定できます。

アプリケーション プロファイリングにより、どの入力がアプリケーションによって受諾しうるかのプロファイルを展開するために使われる、入力の信頼されるセットに基づいて自動化された方法で個別ルールを生成できます。その他の入力は拒否され、肯定的セキュリティ拡張が提供されます。SMA/SRA 装置を学習モードで準備環境に配備すると、装置は信頼されたユーザによってアクセスされた各 URL に対する正しい入力を学習します。学習プロセス中または後のどのタイミングでも、"学習した" プロファイルに基づいてユーザ定義ルールを生成できます。アプリケーション プロファイリングの詳細については、ウェブ アプリケーション ファイアウォールの仕組み (77 ページ) を参照してください。

メモ：アプリケーション プロファイリングは SMA 400、SRA 4600、および SMA 500v Virtual Appliance 上でのみサポートされます。

このページ上で作成した個別ルールは、SonicWall Inc. がウェブ アプリケーションが有効な装置に向けて配信するシグネチャと同じプロパティをすべて持ちます。「ウェブ アプリケーション ファイアウォール > ルール」ページ は、ルールのページです。

「ウェブ アプリケーション ファイアウォール > ルール」ページ



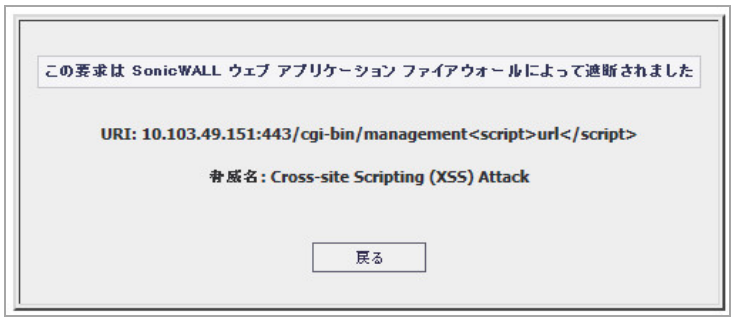
ルールを手動で追加するには、「**連鎖ルール**」を作成して、そこにルールを追加します。連鎖ルールはルールの集合であり、深刻度の評価、名前、説明、速度制限に対するヒット カウンタ、およびトラフィックに連鎖ルールが一致した場合に取る動作といった追加の属性を持ちます。連鎖ルールは、連鎖ルールのすべてのフィールドを表示しています。

「**ウェブ アプリケーション ファイアウォール > ルール**」ページのルールは、複数のページに分割したり、キーワード検索によってフィルタリングすることができます。あるキーワードをすべてのフィールドまたは特定のフィールドに含むルールだけを表示するには、「**検索**」フィールドにキーワードを入力し、検索対象として「**すべてのフィールド**」、または特定のフィールドを選択して、「検索」を選択します。「**除外**」を選択すると、キーワードを含まないルールのみが表示されます。「**リセット**」を選択すると、すべてのルールが表示されます。一致する箇所はすべて強調表示されます。既定では 1 ページに 50 個のルールが表示されます。

連鎖ルール

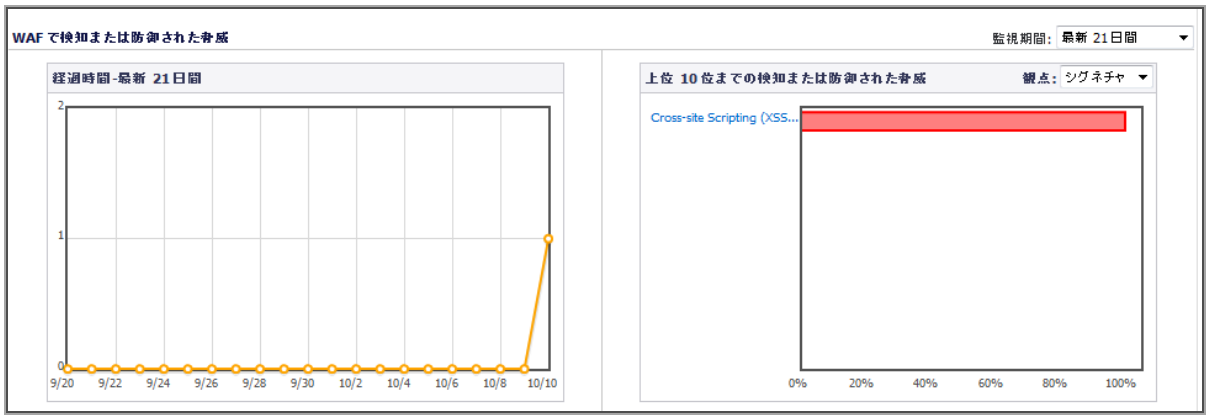
ユーザ定義ルールと連鎖ルールは、ある URI を使用するか、または、あるポータル上で実行しているウェブ アプリケーションによる定義に従って、トラフィックが正当か不当かを区別するために使用できます。連鎖内の 1 つのルールは、URL またはポータル ホスト名に一致するように設定され、一方もう 1 つのルールは HTTP(S) トラフィックの別の要素に対する望ましくない値に一致するように作成されます。この連鎖ルール (両方のルール) がトラフィックに一致した際には、その URI またはポータルからの不正なトラフィックを遮断またはログ記録するように、設定した動作が実行されます。要求が遮断された際には、ユーザに遮断ページ のような個別遮断ページが表示されます。

遮断ページ



また、「**ウェブ アプリケーション ファイアウォール > 監視**」ページにはアクティビティがグラフで表示されます。遮断後の監視ページ は、12 時間の間に検知して防御したいくつかの脅威を示しています。監視ページの詳細については、ウェブ アプリケーション ファイアウォール監視の使用 (343 ページ) を参照してください。

遮断後の監視ページ



ルールは、着信と発信両方の HTTP(S) トラフィックに対して照合されます。連鎖ルール内のすべてのルールが一致した場合、連鎖ルールに定義された動作が実行されます。連鎖ルール内で速度制限を有効にして、ある期間内に一致した攻撃数がしきい値を超過した後でのみ動作を開始することもできます。トラフィックを遮断して一致をログするか、単にログするように動作を設定できます。動作を「**無効**」に設定して、連鎖ルールを動作状態から外して、それらのルールとトラフィックの比較を停止することもできます。

個別ルール機能は、「**ユーザ定義ルールを有効にする**」グローバル設定を使って有効または無効にできます。

メモ：連鎖ルールは、連鎖ルールが追加された順序で強制されます。この順序は、連鎖ルールを削除して再作成することで変更できます。

同様に、連鎖ルール内のルールは、ルールが追加された順序で強制されます。この順序は、ルールを削除して再作成することで変更できます。

アプリケーション プロファイリングの設定

信頼されたユーザによってアプリケーションが使用されている間に SMA/SRA 装置を学習モードにすることで、URL プロファイルを作成して、それらの URL プロファイルを使用して、そのアプリケーションの故意の悪用を防ぐ連鎖ルールを生成できます。

メモ：アプリケーション プロファイリングは SMA 400、SRA 4600、および SMA 500v Virtual Appliance 上でのみサポートされます。

アプリケーション プロファイリングを設定してルールを自動生成するには、以下の手順に従います。

1 「**ウェブ アプリケーション ファイアウォール > ルール**」ページに移動します。

2 「**アプリケーション プロファイリング**」の下で、アプリケーションをプロファイルする 1 つ以上のポータルを「**ポータル**」ドロップダウン リストから選択します。Shift または Ctrl キーを押しながら選択すると、複数のポータルを選択できます。

3 「**コンテンツ種別**」に対して、プロファイルするコンテンツの種別を選択します。

- **すべて** - 画像、HTML、CSS といったすべてのコンテンツ種別を含みます。
- **HTML/XML** - 既定で選択されていて、一般的により繊細なウェブ トランザクションをカバーしているために、セキュリティの見地から最も重要です。
- **Javascript** - Javascript で記述されたアプリケーションに対して使用します。
- **CSS** - HTML、XHTML、または XML の変形で記述されたウェブ ページのフォーマットを制御するために使用されるカスケード スタイル シート コンテンツをプロファイルするには、CSS を選択します。

4 「**プロファイリングの開始**」ボタンを選択すると “学習” プロセスが開始されます。アクティブ プロファイリング期間中に、信頼されたユーザは適切なアプリケーションを選択されたポータル上で使用する必要があります。「**プロファイリングの開始**」が「**プロファイリングの停止**」に変わります。プロファイリングは「**プロファイリングの停止**」を選択するまで継続されます。

プロファイリングの間、Secure Mobile Access は入力を記録してそれらを URL プロファイルとして保存します。URL プロファイルは、「**ウェブ アプリケーション ファイアウォール > ルール**」ページの「アプリケーション プロファイリング」セクションにツリー構造でリストされます。

5 通常のアプリケーション使用から入力を記録するために十分な期間を取った後で、「**プロファイリングの停止**」を選択してプロファイリング プロセスを停止します。

6 必要に応じて、URL プロファイル ツリー内の任意のリンクを選択して、学習済みの値を編集できます。 を選択すると、ツリー内のそのレベルのすべての URL が展開されます。 を選択してリストのすべての URL を再表示したり、 を選択して選択した URL を削除することもできます。

選択した URL に対する編集ページが表示されます。

7 値を追加するには、パラメータの隣にあるフィールド内に値を入力してから、プラス ボタンを選択します。値を削除するには、リスト内の値を選択してから、マイナス ボタンを選択します。

8 編集が終了したら「**適用**」を選択します。その他の URL に対して必要に応じて繰り返します。

9 URL プロファイルからルールを生成する前に、「**生成された連鎖ルールに対する既定の動作**」ドロップダウン リストから、以下の動作の 1 つを選択します。

- **無効** - 生成されたルールは、アクティブではなく無効になります。
- **検知のみ** - 生成されたルールを起動するコンテンツは、検知されてログ記録されます。
- **防御** - 生成されたルールを起動するコンテンツは、遮断されてログ記録されます。

10 既に URL プロファイルから生成済みの連鎖ルールを上書きするには、「**URL プロファイルに対する既存の連鎖ルールを上書きする**」をオンにします。

11 「**ルールの生成**」を選択して、URL プロファイルからルールを生成します。URL プロファイルが編集された場合は、それらの変更は組み入れられます。

連鎖ルールが正しく生成されると、ステータス バーが何個の連鎖ルールが生成されたかを、上書きされたものも含めて表示します。

12 生成された連鎖ルールを受け入れたくない場合は、連鎖ルール リストの下にある「**選択した連鎖ルールの削除**」を選択します。グループの容易な削除のために、生成後すぐに自動的に追加された連鎖ルールすべてが事前に選択されています。

13 「**適用**」を選択して、生成された連鎖ルールを Secure Mobile Access 構成に適用します。

連鎖ルールの設定

連鎖ルールは追加、編集、削除、そして複製が可能です。連鎖ルールの例 (連鎖ルール ID が 15000 より大きいもの) は、Secure Mobile Access 管理インターフェースにあり、管理者が参照用として使用できます。これらは編集または削除できません。連鎖ルールに関連付けられているルールは、「**設定**」列の**連鎖ルールの編集**アイコンを選択することにより参照できます。

設定の簡略化のために、連鎖ルール例は通常の連鎖ルールを複製できます。連鎖ルールの複製は、その連鎖に関連付けられているルールをすべて複製します。連鎖ルールの複製後は、設定列の連鎖ルールの編集アイコンを選択することにより編集できます。

連鎖ルールの追加と編集

連鎖ルールを追加または編集するには:

1 新しい連鎖ルールを追加するには、「**ウェブ アプリケーション ファイアウォール > ルール**」ページで、「**連鎖ルールの追加**」を選択します。

既存の連鎖ルールを編集するには、「**設定**」列の**連鎖ルールの編集**アイコン を選択します。

新規連鎖ルールの画面または、既存の連鎖ルールの画面が表示されます。どちらの画面にも「**連鎖ルール**」セクション内に同じ設定可能フィールドがあります。

2 新規連鎖ルールの画面で、「**名前**」フィールドにこの連鎖ルールを説明する名前を入力します。

3 「**深刻度**」ドロップダウン リストから、脅威のレベルを選択します。「**高**」、「**中**」、「**低**」が選択できます。

4 「**動作**」ドロップダウンリストから「**無効**」、「**検知のみ**」、または「**防御**」を選択します。

- **無効** - 連鎖ルールは、効果を現しません。
- **検知のみ** - トラフィックを許可しますが、ログします。

- **防御** - ルールと一致したトラフィックを遮断してログします。

この「**無効**」オプションにより、連鎖ルールの設定を削除せずに一時的に連鎖ルールを無効にすることが可能です。

5 「**説明**」フィールドに、この連鎖ルールが何を照合するのか、またはその他の情報などの短い説明を入力します。

6 「**種別**」ドロップダウンリストから、この脅威の種別を選択します。このフィールドは情報目的であり、連鎖ルールが適用される方法は変更しません。

7 「**カウンタの設定**」で、連鎖ルールに一致している速度の追跡を有効にし、速度制限を設定するには「**ヒット カウンタを有効にする**」をオンにします。追加のフィールドが表示されます。

8 「**最大許可ヒット数**」フィールドに、この連鎖ルールに対する、選択された動作が起動されるまでに発生する必要がある一致数を入力します。

9 「**ヒット カウンタのリセット周期**」フィールドに、「最大許可ヒット数」への到達を許可する秒数を入力します。この時間内に「最大許可ヒット数」に到達しない場合は、選択された動作は起動されずに、ヒット カウンタはゼロにリセットされます。

10 同じ IP アドレスから来ている連鎖ルールの一致に対して速度制限を強制するには、「**リモート アドレス毎に監視する**」をオンにします。リモート アドレス毎の監視は、SMA/SRA 装置によって確認されたようにリモート アドレスを使います。これは、NAT が有効なファイアウォールの背後に複数のクライアントがある場合をカバーし、それらが実質的には同じ送信元 IP を持つパケットを送信しているようにします。

11 「**セッション毎に監視する**」をオンにして、攻撃者のブラウザ セッションに基づいた速度制限を有効にします。この方式は各ブラウザ セッションに対して Cookie を設定します。攻撃者が各攻撃に対して新しいユーザ セッションを開始する場合は、ユーザ セッションによる追跡はリモート IP による追跡ほど効果的ではありません。

12 「**適用**」を選択して、連鎖ルールを保存します。「**連鎖ルール ID**」が自動的に生成されます。

13 次は、連鎖ルールに 1 つ以上のルールを追加します。詳細については、連鎖ルール内のルールの設定 (333 ページ) を参照してください。

連鎖ルールの複製

連鎖ルールを複製するには、以下の手順に従います。

1 「**ウェブ アプリケーション ファイアウォール > ルール**」ページで、「**設定**」列の連鎖ルールの複製アイコン を選択します。

2 確認のダイアログ ボックスで、「**OK**」を選択します。

これで、連鎖ルールを編集してカスタマイズできるようになりました。連鎖ルールの追加と編集 (331 ページ) を参照してください。

連鎖ルールの削除

メモ：連鎖ルールを削除すると、関連付けられているルールもすべて削除されます。

連鎖ルールを削除するには、以下の手順に従います。

1 「**ウェブ アプリケーション ファイアウォール > ルール**」ページで、削除したい連鎖ルールの「**設定**」列の連鎖ルールの削除アイコン を選択します。

2 確認のダイアログ ボックスで、「**OK**」を選択します。

3 「**適用**」を選択します。

誤設定された連鎖ルールの修正

誤設定された連鎖ルールは、設定時に自動検出されません。誤設定してしまった場合は、管理者がログインして不正なルールを修正するか、削除する必要があります。

メモ：ルールや連鎖ルールが誤設定されている場合は、装置はどの個別ルールや連鎖ルールも強制しません。

誤設定された連鎖ルールから誤検知を見つけることは、ユーザがそれに遭遇して管理者に報告しない限り、困難です。連鎖ルールが「防御」するように設定されている場合は、ユーザにウェブ アプリケーション ファイアウォールの遮断ページが表示 (「**ウェブ アプリケーション ファイアウォール > 設定**」ページで設定したように表示) されます。そうでない場合は、"脅威" が検知されたことを示すログ メッセージが発生します。

管理者が不注意で、SMA/SRA 装置のすべてのポータルへのアクセスを遮断する個別連鎖ルールを作成するというシナリオを考えてみます。例えば、管理者がアプリケーション オフローダ ポータルに対してルールの強制を望んでいたとします。しかし、そのポータル、ホストまたは URL に対する要求と照合させる基準を絞るための別のルールを追加することを忘れました。もし 1 番目のルールが広範ならば、これは装置に対するサービス停止を意味します。具体的に説明するため、POST 要求が想定されている特定の URL に対して、管理者が、GET HTTP メソッドの使用を拒否する連鎖ルールを作成するとします。

このためには、管理者は2 つのルールを作成する必要があります。

1 1 番目のルールは、GET 要求と一致させるため。

2 2 番目のルールは、特定の URL と一致させるため。

管理者が 2 番目のルールの作成を忘れると、ウェブベースの Secure Mobile Access 管理インターフェースは GET メソッドに依存しているため、SMA/SRA 装置へのアクセスが拒否されます。

誤設定した連鎖ルールを修正するには、以下の手順を実行します。

1 ブラウザで、https://<SMA IP>/cgi-bin/welcome をポイントします。

https://<SMA IP>/ の URL を使ってウェルカム ページに移動する場合は、通常の https://<SMA IP>/cgi-bin/welcome へのリダイレクトは機能しません。誤設定したルールを修正するには、https://<SMA IP>/cgi-bin/welcome に明示的に移動する必要があります。ここで、<SMA IP> は、SMA/SRA 装置のホスト名または IP アドレスです。

2 **admin** としてログインします。

3 「**ウェブ アプリケーション ファイアウォール > ルール**」ページに移動します。

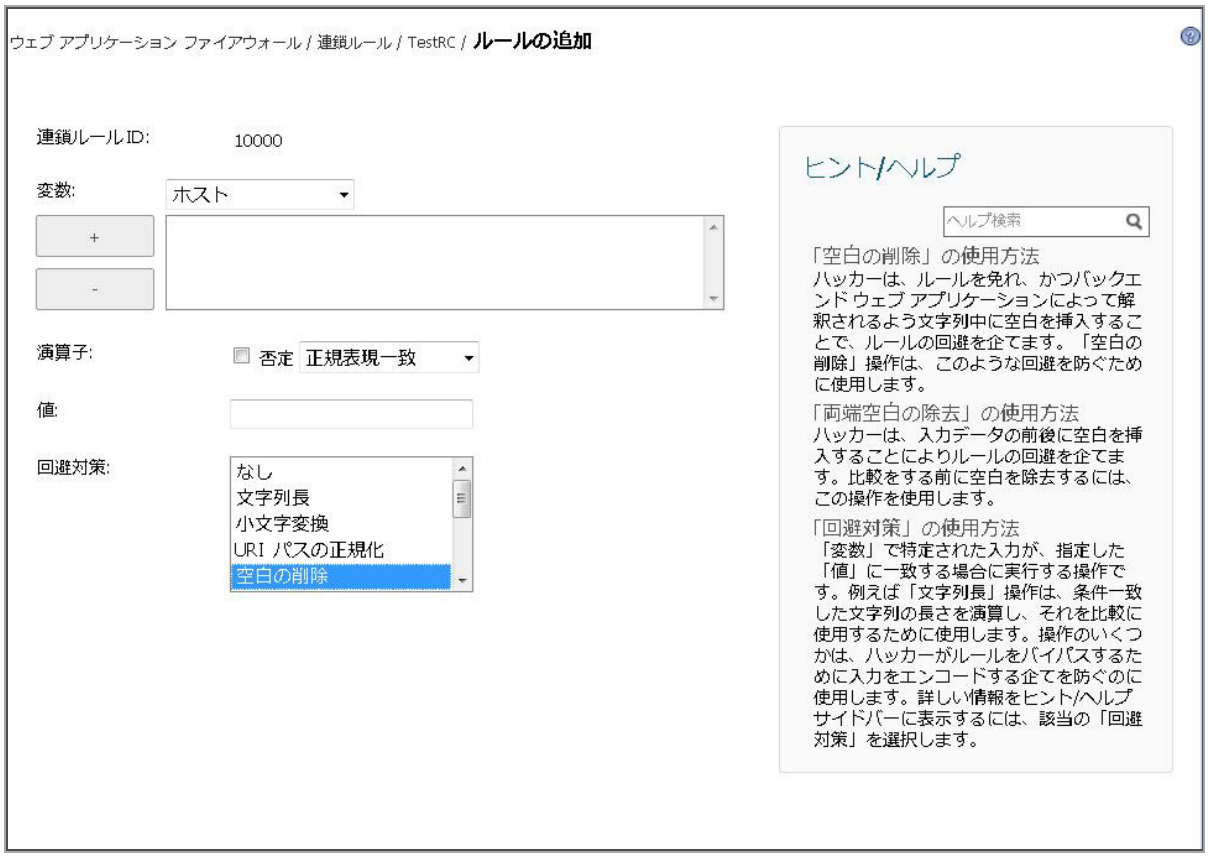
4 不正なルールを編集または削除します。

5 「**適用**」を選択します。

連鎖ルール内のルールの設定

鎖ルールは追加、編集、削除、そして複製が可能です。ルールとは、着信または発信 HTTP(S) トラフィックに対して確認される条件です。それぞれの連鎖ルールは、1 つ以上の設定されたルールを持つことができます。使用するには最低 1 つのルールが必要です。ルールの追加ページ に、「ルール追加」ページを示します。

ルールの追加ページ



ルールにより、管理者は肯定セキュリティ モデルと否定セキュリティ モデルの両方を利用できます。肯定セキュリティ モデルでは、ポリシーは許可する既知のトラフィックのみで記述され、それ以外すべてを遮断します。

ルールには、いくつかの構成要素があります。

- **変数** - これらは、正当または不正なトラフィックを区別する支援をする、ウェブ アプリケーション ファイアウォールによって走査される HTTP プロトコルのエンティティです。複数の変数を「**値**」フィールド内に設定された値に対して照合することができます。'+' と'-' ボタンにより、「**変数**」ドロップダウン リストから変数を追加する、また、それらを選択済み変数のリストから削除することができます。指定した値と照合することを要求するために、複数の変数を結合させることができます。複数の変数が設定された場合は、ルールは設定した変数のうちのどれか 1 つが対象の値に一致するかどうか照合されます。変数の詳細情報については、変数について (335 ページ) を参照してください。
- **演算子** - これらは、計算および文字列演算子です。「**否定**」チェックボックスは、設定した条件を除いたどんな値にも一致させるために使われる、逆演算子です。演算子の詳細情報については、演算子について (337 ページ) を参照してください。
- **値** - このエンティティには数字、リテラル文字列、または正規表現が使用可能で、走査される対象と比較されます。これは、指定された演算子に従って、設定された変数の値と比較されます。

  2 つ以上の値と変数を比較するために、複数の値を「**値**」フィールドに空白で区切って入力して、「**キーワード一致**」演算子を選択できます。「**キーワード一致**」演算子を選択した場合は、空白区切りのみ動作します。
- **回避対策** - このフィールドにより、特に回避対策の強化を目的とした、「**演算子**」フィールドによってサポートされている以上の対策を適用できます。これらの対策の詳細については、回避対策について (338 ページ) を参照してください。

以下のセクションで、ルールについての詳細情報を提供します。

ヒント/ヘルプ サイドバーについて

「**変数**」ドロップダウン リストで変数を選択することで、その変数に関する詳細情報を、「**ヒント/ヘルプ**」サイドバーに表示することができます。このサイドバーは、それぞれの変数がいつ使用されて、HTTP プロトコルのどこで見つけられるかを説明します。変数ごとに使用事例が提供されます。

「**回避対策**」ドロップダウン リストの項目も、選択すると詳細情報が「**ヒント / ヘルプ**」サイドバーに表示されます。

このサイドバーはまた、状況感知検索を提供します。変数を選択してから、特定のキーワードを検索すると、検索結果は変数に関連するものだけになります。

変数について

変数は、正当または不正なトラフィックを区別する支援をする、ウェブ アプリケーション ファイアウォールによって走査される HTTP プロトコルのエンティティです。複数の変数を「**値**」フィールド内に設定された値に対して照合することができます。'+' と'-' ボタンにより、「**変数**」ドロップダウン リストから変数を追加する、また、それらを選択済み変数のリストから削除することができます。

指定した値と照合することを要求するために、複数の変数を結合させることができます。複数の変数が設定された場合は、ルールは設定した変数のうちのどれか 1 つが対象の値に一致するかどうか照合されます。

変数は、単一の値または集合で表現できます。変数を「**パラメータ値**」のような集合で表現した場合は、集合内の特定の変数を、その名前を選択用テキストボックスに入力して コロン(:)の右側に付加することによって設定できます。例えば、「**URI**」または「**ホスト**」変数に対する値は各 HTTP(S) 要求内で一意です。そのような変数に対しては、選択用テキストボックスは表示されません。「**要求ヘッダ値**」や「**応答ヘッダ名**」といったその他の変数は、集合を表現します。

集合自身を入力に対して試験する必要がある場合は、選択用テキストボックスを空のままにします。しかしながら、集合内の特定項目の値を検索する必要がある場合は、選択用テキストボックスにその項目を指定します。例えば、HTTP(S) 要求内に **password** パラメータが存在するかどうかを試験する必要がある場合は、「**パラメータ名**」変数を設定して、選択用テキストボックスを空のままにします。「**演算子**」を「**文字列一致**」に、そして「**値**」を **password** に設定します。しかし、この password パラメータの値が特定の文字列 (例えば "foo") と一致しているかどうかを確認したい場合は、「**パラメータ値**」変数を選択して、選択用テキストボックスに **password** を設定します。そして「**値**」フィールドに **foo** を設定します。

ルール内で使用される変数 表に、使用可能な変数を示します。

ルール内で使用される変数

変数名	集合	説明
ホスト	いいえ	HTTP 要求のホスト ヘッダ内のホスト名または IP アドレスを指します。一般的には、ブラウザのアドレス バー内の URL のホスト部分を指します。
URI	いいえ	URL 内のパスとクエリ引数の組み合わせを指します。
HTTP メソッド	いいえ	ブラウザがウェブ サーバのリソースを要求するために使用する GET や POST などのメソッドを指します。
HTTP 状況コード	いいえ	ウェブ サーバからの応答の状況を指します。ウェブ サーバからの様々なエラー コードに対する動作を設定するために、これを使用できます。
パラメータ値	はい	すべてのクエリ引数と現在の要求の一部であるフォーム パラメータの値を含む、すべての要求パラメータ値の集合を指します。 パラメータ値の個数のような、パラメータ値のリスト全体の状況に対して照合するには、選択フィールドを空のままにします。 特定のパラメータの値に対して照合するには、パラメータの名前を選択フィールドに指定してコロンの右側に付加します。
パラメータ名	はい	すべてのクエリ引数と現在の要求の一部であるフォーム パラメータの値を含む、すべての要求パラメータ名の集合を指します。 パラメータ名のリスト全体の状況に対して照合するには、選択フィールドを空のままにします。 特定のパラメータの名前に対して照合するには、パラメータの名前を選択フィールドに指定してコロンの右側に付加します。
リモート アドレス	いいえ	クライアントの IP アドレスを指します。この値により、特定の IP アドレスからのアクセスを許可または遮断することができます。
要求ヘッダ値	はい	現在の要求に対するすべての HTTP(S) 要求ヘッダ値の集合を指します。 要求ヘッダ値のリスト全体の状況に対して照合するには、選択フィールドを空のままにします。 特定のヘッダ値に対して照合するには、ヘッダの名前を選択フィールドに指定してコロンの右側に付加します。 例えば、Ajax 要求を遮断するには、**「変数」**として**「要求ヘッダ値」**を選択し、選択テキスト ボックスに**「X-Request-With」**を指定し、**「値」**フィールドに「ajax」と入力します。
要求ヘッダ名	はい	現在の要求に対するすべての HTTP(S) 要求ヘッダ名の集合を指します。 要求ヘッダ名のリスト全体の状況に対して照合するには、選択フィールドを空のままにします。 特定のヘッダ名に対して照合するには、ヘッダの名前を選択フィールドに指定してコロンの右側に付加します。 例えば、信頼済みホストから参照されたものではない要求を遮断するには、「**変数**」として「**要求ヘッダ名**」を選択し、選択テキスト ボックスに「**Referer**」を指定し、「**値**」フィールドに信頼済みホストのホスト名または IP アドレスを入力し、「**否定**」チェックボックスをオンにして、「**キーワード一致**」演算子を選択します。

ルール内で使用される変数 (続き)

変数名	集合	説明
応答ヘッダ値	はい	現在の要求に対するすべての HTTP(S) 応答ヘッダ値の集合を指します。 応答ヘッダ値のリスト全体の状況に対して照合するには、選択フィールドを空のままにします。 特定のヘッダ値に対して照合するには、ヘッダの名前を選択フィールドに指定してコロンの右側に付加します。
応答ヘッダ名	はい	現在の要求に対するすべての HTTP(S) 応答ヘッダ名の集合を指します。 応答ヘッダ名のリスト全体の状況に対して照合するには、選択フィールドを空のままにします。 特定のヘッダ名に対して照合するには、ヘッダの名前を選択フィールドに指定してコロンの右側に付加します。
応答コンテンツ長	いいえ	応答ペイロードのサイズを指します。
応答ペイロード	いいえ	ユーザに表示されるウェブ ページの内容を指します。
ポータル ホスト名	いいえ	クライアントからの要求を受け付ける Secure Mobile Access ポータルの仮想ホスト名を指します。 特定の仮想ホストに適用する連鎖ルールを作成するには、1 つのルールはホストと一致するようにして、もう 1 つに照合するための別の条件を指定します。
ポータル アドレス	いいえ	クライアントからの要求を受け付ける Secure Mobile Access ポータルの IP アドレスまたは仮想 IP アドレスを指します。
要求パス	いいえ	ウェブ サイトの特定のリソースにアクセスするための相対パスを指します。

演算子について

多くの計算および文字列演算子があります。「**否定**」チェックボックスは、設定した条件を除いたどんな値にも一致させるために使われる、逆演算子です。

これらの演算子は、**「回避対策」**と組み合わせて使用できます。例えば、**「文字列一致」**演算子を、**「回避対策」**内の**「小文字変換」**または「**URI パスの正規化**」とともに使うことができます。

ルールの演算子 表 で、ルールで使用することができる演算子を説明します。

ルールの演算子

演算子	種別	説明
部分一致	文字列	走査した変数の 1 つ以上が「**値**」フィールドの内容を含みます。
文字列一致	文字列	走査した変数が「**値**」フィールド内の英数字文字列と完全一致します。
=	計算	走査した変数が「**値**」フィールドの内容と同値です。
>	計算	走査した変数が「**値**」フィールドの内容を超えます。
>=	計算	走査した変数が「**値**」フィールドの内容以上です。
<	計算	走査した変数が「**値**」フィールドの内容未満です。
<=	計算	走査した変数が「**値**」フィールドの内容以下です。

ルールの演算子 (続き)

演算子	種別	説明
キーワード一致	文字列	走査した変数の 1 つ以上が「**値**」フィールド内のキーワードの 1 つに一致します。複数のキーワードを指定する場合は、空白で区切る必要があります。
正規表現一致	文字列	走査した変数の 1 つ以上が「**値**」フィールド内の正規表現に一致します。例えば、4 文字の十進数を照合する正規表現は、**\d{4}** です。

回避対策について

回避対策は、入力が指定された値に対して照合される前に、選択された変数によって特定された入力に適用されます。例えば、「**文字列長**」の対策を使用すると、一致した入力の長さを計算して、それを比較に使うことができます。ウェブ アプリケーション ファイアウォールのルールをバイパスするために入力をエンコードしようとする、ハッカーの企てを阻止するために使われる回避対策もあります。リストの中の回避対策を選択すると、その対策に関する詳細情報が「**ヒント / ヘルプ**」サイドバーに表示されます。

回避対策は、通常の演算子と組み合わせて使用できます。「**回避対策**」フィールドでは、入力をそのままにする「**なし**」の対策を含む、10 種類の対策が選択できます。

複数の回避対策を同時に選択して個々に適用することができます。**Ctrl** キーを押しながら次の対策を選択することで、複数の対策が選択できます。ルール内で「**なし**」の対策をその他の対策と同時に選択した場合は、入力はそのままの状態で比較され、また、別の対策によってデコードまたは変換された後にも比較されます。ルールで使用できる回避対策 表に、ルールで使用できる回避対策の説明を示します。

ルールで使用できる回避対策

対策	説明
なし	スキャンした入力を変更せずに、設定した変数や値と比較したい場合に、**「なし」**を使います。
文字列長	選択した変数が文字列で、かつ選択した演算子の適用前に文字列の長さを計算したい場合に、**「文字列長」**を使います。
小文字変換	比較の前に入力をすべて小文字に変換することにより、大文字小文字を区別しない比較をしたい場合に、**「小文字変換」**を使います。この対策を使用する場合は、「**値**」フィールドに必ずすべて小文字の文字列を入力してください。 これは、ハッカーが大文字と小文字の変換によって、ルールをバイパスすることを防ぐ回避対策です。
URI パスの正規化	URI 内の後方参照 (URI の先頭は除く)、連続するスラッシュや自己参照といった、不正な参照を削除する場合に、「**URI パスの正規化**」を使います。例えば、www.eshop.com/././//login.aspx という URI は www.eshop.com/login.aspx に変換されます。 これは、ハッカーが不正な参照の追加によって、ルールをバイパスすることを防ぐ回避対策です。
空白の削除	比較の前に入力文字列内の空白を削除する場合に、**「空白の削除」**を使います。余分な空白によって入力がルールに一致しなくなることがありますが、バックエンドのウェブ アプリケーションはこれを解釈します。 これは、ハッカーが文字列に空白を追加することで、ルールをバイパスすることを防ぐ回避対策です。

ルールで使用できる回避対策 (続き)

対策	説明
Base64 デコード	ルールに基づく比較の前に **base64 エンコード** されたデータをデコードする場合に、「Base64 デコード」を使います。 一部のアプリケーションはバイナリ データを、URL やフォーム フィールドに含めるのに都合の良い方法でエンコードします。Base64 エンコードは、このようなデータをコンパクトにするために使用されます。バックエンド アプリケーションがこのデータをデコードします。 これは、ハッカーが入力に base64 エンコードを使用することで、ルールをバイパスすることを防ぐ回避対策です。
16 進数デコード	ルールに基づく比較の前に 16 進数エンコード されたデータをデコードする場合に、**「16 進数デコード」** を使います。 これは、ハッカーが入力に 16 進数エンコードを使用することで、ルールをバイパスすることを防ぐ回避対策です。
URL デコード URL デコード (ユニコード)	入力内の URL エンコード された文字列をデコードする場合に、**「URL デコード」** を使います。**%%uXXXX** エンコーディングを処理するには、**「URL デコード (ユニコード)」** を使います。URL エンコードは、URL に ASCII 文字セット以外の文字が含まれている場合に、インターネット上でデータを安全に送信するために使用されます。 **メモ**: すでにデコード されている入力に対しては、この対策を使用しないでください。 これは、バックエンド ウェブ サーバが悪意のある入力をデコード後に解釈できることを知るハッカーが、URL エンコードの使用によってルールをバイパスすることを防ぐ回避対策です。 例えば、www.eshop.com/hack+URL%3B という URI は、この対策によって比較の前に www.eshop.com/hack URL に変換されます。
両端空白の除去	比較の前に入力データの前後の空白を削除する場合に、**「両端空白の除去」** を使います。余分な空白によって入力がルールに一致しなくなることがありますが、バックエンドのウェブ アプリケーションはこれを解釈します。 これは、ハッカーが入力データの前後に空白を追加することで、ルールをバイパスすることを防ぐ回避対策です。

ルールのユースケース例

このセクションでは、対回避手法をさらに深く理解できるように、ポジティブおよびネガティブのセキュリティ モデルの例と、回避対策の使用方法を示すいくつかの例を紹介します。

例 - 肯定セキュリティ モデル: 不正ログインの遮断

パスワードの長さが 8 文字未満だった場合に、アプリケーション オフロード されたウェブ サイトへのログインを防ぐには、以下の 2 つのルールを持つ連鎖ルールを作成します。

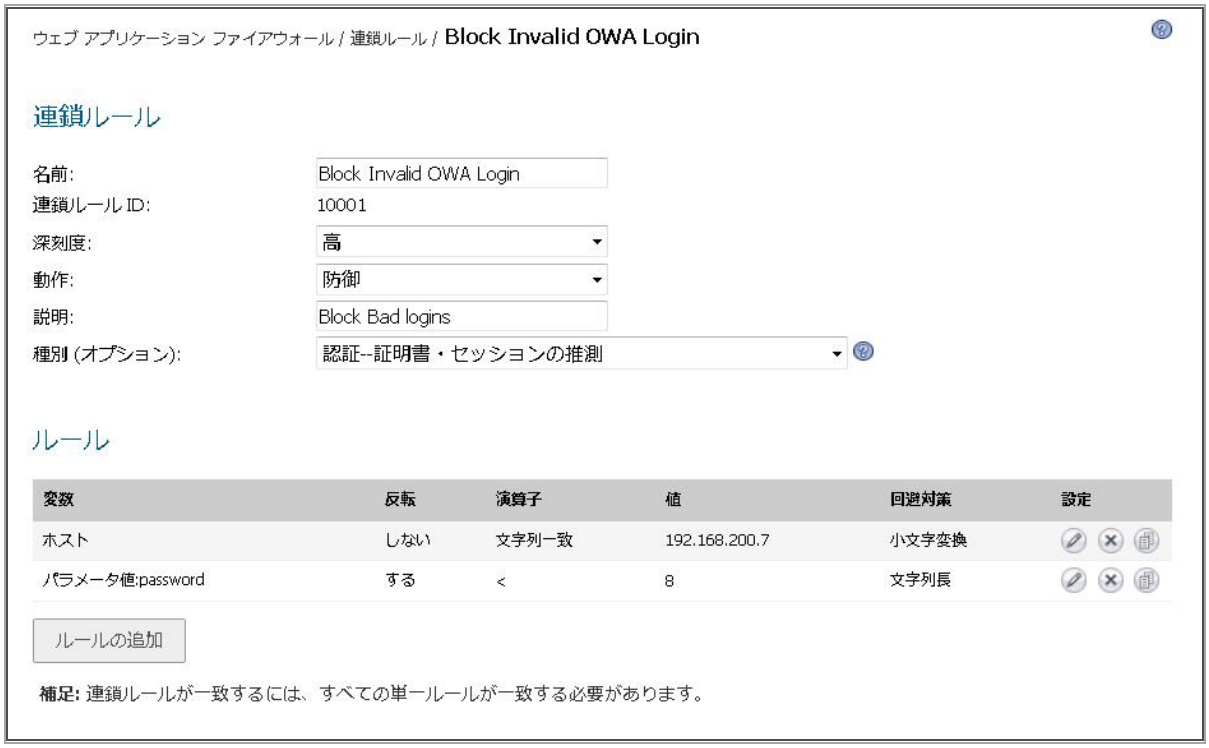
1 「**変数**」として「**ホスト**」を選択し、「+」を選択してこれを追加します。「**演算子**」として「**文字列一致**」を設定し、「**値**」にポータルの仮想ホスト名を設定します。これは、ログイン要求のホスト ヘッダが防御しようとしているサイトに一致することを確認します。この場合、連鎖ルールは 1 サイトにのみ適用されます。

2 「**変数**」として「**パラメータ値**」を選択し、選択用フィールドに **password** を入力して、「+」を選択してこの変数と選択した項目をルールに追加します。「**演算子**」として「**< (未満)**」を設

定し、「**値**」に 8 を設定します。パスワード フォーム パラメータの長さを計算するために、「**回避対策**」リストで「**文字列長**」を選択します。

この連鎖ルールの動作は「**防御**」に設定します。連鎖ルールの例 - 不正ログインの遮断は、この例の連鎖ルールを示します。

連鎖ルールの例 - 不正ログインの遮断

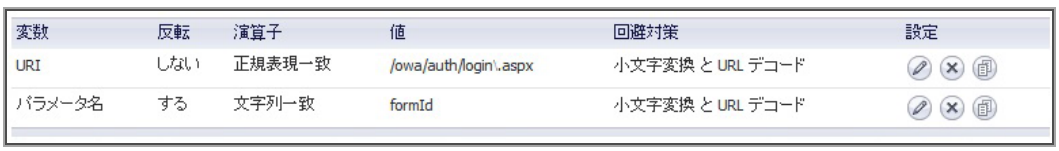


例 - 肯定セキュリティ モデル: 好ましくないパラメータを持つフォーム提出の遮断

この連鎖ルールは、フォームが**formId** 以外の要求パラメータを持つ場合と、**formId** の値が 4 文字を超える数字を含む場合にフォーム提出を遮断します。これを完了するには、以下の 2 つの連鎖ルールを作成する必要があります。

1 1 つ目の連鎖ルールは、以下の 2 つのルールを持ちます。

- 1 つ目のルールは、フォームが提出された URL を確認します。
- 2 つ目のルールは、「**パラメータ名**」が正しいパラメータの名前である **formId** と一致していないかを確認します。これは、「**文字列一致**」演算子を、逆転の「**否定**」チェックボックスを選択して使います。



2 2 つ目の連鎖ルールは、以下の 2 つのルールを持ちます。

- 1 つ目のルールは、フォームが提出された URL を確認します。
- 2 つ目のルールは、「**パラメータ値:formId**」変数に含まれる値が、1 文字から 4 文字の数字のどれかを含むものと照合するため、正規表現の **^\d{1,4}$** と一致するかどうかを確認

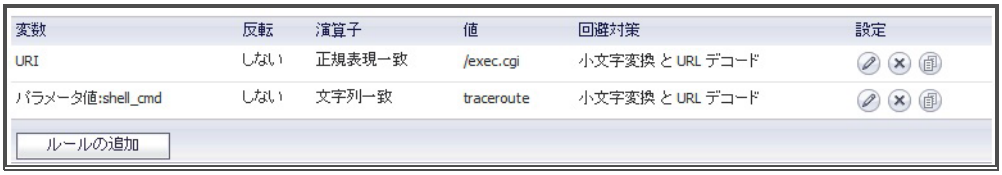
します。ルールが 1 文字から 4 文字の数字を含まないものすべてに一致するように、逆転の「**否定**」チェックボックスを選択して使います

例 - 否定セキュリティ モデル: フォームへの悪意のある入力の遮断

フォームへの悪意のある入力を遮断するには、以下の 2 つのルールを持つ連鎖ルールを作成します。

1 1 つ目のルールは、フォームの URL を確認します。

2 2 つ目のルールは、フォーム パラメータの **shell_cmd** と、不正な入力の **traceroute** を確認します。



例 - URL デコード と なし の使用

もしもハッカーが、要求 URI が CR と LF 文字 (キャリッジ リターンとライン フィード) に対して走査されていることを知ると、このハッカーはそれらの文字を、要求に追加する前に URL エンコードを実行することで、要求内に巧妙に挿入しようと試行するかもしれません。そうすると、この URI は HTTP 応答スプリッティング攻撃の開始に使われる可能性がある、**%0D** と **%0A** 文字を含みます。「**URL デコード**」と「**URL デコード (ユニコード)**」の対策は、スキャンした入力を、照合対象として設定した値と比較する前にデコードすることで、この種の攻撃を阻止するために使用できます。

具体的には、要求が http://www.host.com/foo%20bar/ という URI に対して行われ、「**URL デコード**」の対策が選択されている場合、スキャンされた URI はデコード後、http://www.host.com/foo bar/ となり、安全に照合できます。エンコードしていない要求に加えてエンコードした要求を送信するハッカーを阻止するために、管理者はルールに「**なし**」と「**URL デコード**」オプションを選択できます。

例 - パラメータ値で小文字変換と URL デコードの使用

管理者が、「**パラメータ値**」変数の内容が、値 **foo bar** と一致しているかどうかの確認を、そのような要求を遮断するために望んでいます。バックエンド アプリケーションが大文字小文字を区別する入力 (foo bar と FOO BAR) を受け入れるので、ハッカーは要求内の **foo BAR** を通過させ、ルールを回避することができます。この回避行為を阻止するために、管理者は「**小文字変換**」の対策を指定して、値を「**foo bar**」のようにすべて小文字で設定します。これにより、すべての要求パラメータ値は小文字に変換されて、大文字小文字の区別が無い確認のために、値と比較されます。

同様に、ハッカーは一般的にブラウザにより使用される URL エンコードされた形である、**foo%20BAR** を通過させることができます。この回避行為を阻止するために、管理者は「**URL デコード**」の対策を指定して要求エンティティに適用します。入力の **foo%20BAR** は、**foo BAR** に URL デコードされます。入力が既に **foo BAR** の場合は、URL デコードは適用されません。

例 - パラメータ値:ID で文字列長と URL デコードの使用

デコードされた入力に対して比較することで、管理者は「**文字列長**」の対策を使用して、入力の長さを対応する変数と比較することができます。例えば、ウェブ アプリケーションの「ID」パラメータが 4 文字以下でなければならない場合、管理者はまず、「**変数**」フィールドで「**パラメータ値**」を選択し、選択フィールドに「**ID**」と入力して、「**+**」を選択して変数と選択した項目をルールに追加します。続いて、「**値**」フィールドに **4** と入力し、「**演算子**」リストで「**>**」を選択して、「**回避対策**」リストで「**URL デコード**」と「**文字列長**」の両方を選択します。

ルールの削除

連鎖ルールからルールを削除するには、以下の手順に従います。

1. 「**ウェブ アプリケーション ファイアウォール > ルール**」ページで、削除したいルールがある連鎖ルールの「**設定**」列の連鎖ルールの編集アイコン を選択します。連鎖ルールのページが開きます。
2. 削除したいルールの「**設定**」列の削除アイコン を選択します。
3. 確認のダイアログ ボックスで、「**OK**」を選択します。
4. 「**適用**」を選択します。

ルールの複製

ルールを複製するには、以下の手順に従います。

1. 「**ウェブ アプリケーション ファイアウォール > ルール**」ページで、複製したいルールがある連鎖ルールの「**設定**」列の連鎖ルールの編集アイコン を選択します。連鎖ルールのページが開きます。
2. 複製したいルールの「**設定**」列の複製アイコン を選択します。
3. 確認のダイアログ ボックスで、「**OK**」を選択します。

これで、ルールを編集してカスタマイズできるようになりました。ルールの追加と編集 (342 ページ) を参照してください。

ルールの追加と編集

連鎖ルールのルールを追加または編集するには:

1. 「ウェブ アプリケーション ファイアウォール > ルール」ページで、ルールを追加または編集したい連鎖ルールの「**設定**」列の連鎖ルールの編集アイコン を選択します。連鎖ルールのページが開きます。
2. 新しいルールを追加するには「**ルールの追加**」を選択、ルールを編集するには、編集したいルールの「**設定**」列の編集アイコンを選択します。
3. ルールの追加ページまたは、ルールを編集するためのページで、「**変数**」ドロップダウン リストから変数を選択します。利用可能な変数の情報については、変数について (335 ページ) を参照してください。

4 選択した変数が変数の集合の場合は、「**変数**」フィールドの右側に選択用フィールドが表示されます。集合の特定のメンバに対して比較したい場合は、その項目の名前を選択用フィールドに入力します。

集合自身を入力に対して試験する必要がある場合は、選択用テキストボックスを空のままにします。例えば、要求内に特定のパラメータが存在するかどうか試験するには、「**パラメータ名**」変数を選択して、「**値**」フィールド (変数の選択用フィールドではない) にその特定のパラメータ名を入力します。

5 **プラス** [+] を選択して、変数をルールに追加します。さらに変数を追加するには、ステップ 2 からステップ 5 を繰り返します。

また、変数を削除するには、大きいテキストボックス内で対象を選択してから、**マイナス** [-] を選択します。

6 「**演算子**」ドロップダウン リストから、文字列または計算の演算子を選択します。逆演算を行うには、「**否定**」をオンにします。

7 「**値**」フィールドに、走査される HTTP(S) 入力内の選択した変数と比較する値を入力します。「**キーワード一致**」演算子を選択する場合は、複数の値それぞれを空白で区切って入力することで、入力を複数の値と比較することができます。それぞれの値が個別に比較されます。

8 **「回避対策」**リストから、1 つ以上の対策を選択します。複数の対策を選択するには、キーボードの **Ctrl** キーを押しながら選択します。

9 編集が終了したら「**適用**」を選択します。

ウェブ アプリケーション ファイアウォール監視の使用

「**ウェブ アプリケーション ファイアウォール > 監視**」には、「**ローカル**」と「**グローバル**」の 2 つのタブがあります。両方のページに、単位時間あたりに検知/防御された脅威および上位 10 位の脅威に関する統計とグラフが表示されます。「ローカル」ページにはまた、ウェブ サーバの状況統計と選択した監視期間の要求数とトラフィック量のグラフも表示されます。

それぞれのページに対する監視機能は、以下のセクションで説明されています。

- ローカル ページでの監視 (343 ページ)
- グローバル ページでの監視 (348 ページ)

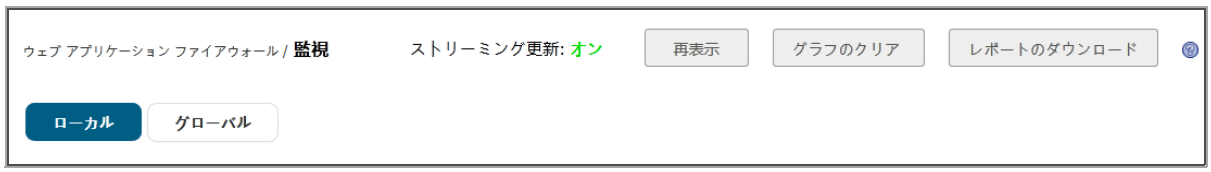
ローカル ページでの監視

「ローカル」ページにはローカル装置に対する統計とグラフが表示されます。グラフは「ウェブ サーバ状況」と「WAF で検知または防御された脅威」に対して表示されます。後者に対しては、「観点」オプションを使用して、シグネチャ、深刻度、サーバの中から表示を変更可能で、グラフではなくリスト形式で統計を表示可能です。

制御ボタンの使用

制御ボタンはページ上部に表示されます。それらは、このページ上に表示される統計を制御します。ローカル ページ上で制御ボタンを使って、ストリーミング更新のオンとオフ、ページ上のデータの再表示、グラフのクリア、およびレポートのダウンロードができます。ストリーミングがオンになってい

る場合、ウェブ アプリケーション ファイアウォールの統計情報は定期的に収集されて、グラフと脅威リストに表示されます。ストリーミングがオフになっていると、新しい情報は表示できません。



制御ボタンを使用するには、以下の手順を実行します。

1 「**ローカル**」ページを選択します。アクティブなページの名前は赤色またはピンク色で表示され、非アクティブなページの名前は青色で表示されます。制御ボタンは現在表示されているページに対して機能します。

2 ストリーミングのオン・オフを切り替えるには、「**ストリーミング更新**」の隣の「**オン**」または「**オフ**」インジケータを選択します。

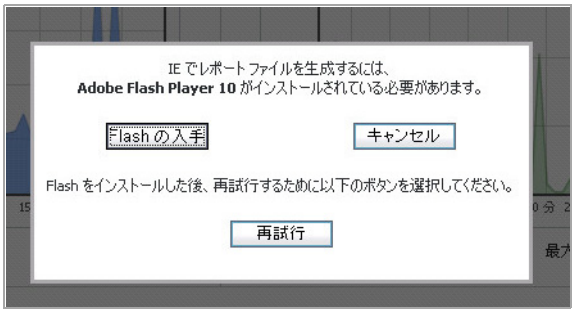
3 表示を更新するには、「**再表示**」を選択します。

4 グラフとリストから、ウェブ アプリケーション ファイアウォールの統計すべてをクリアするには、「**グラフのクリア**」を選択します。

5 ウェブ アプリケーション ファイアウォールの統計を含む PDF レポートを生成するには、「**レポートのダウンロード**」を選択します。

> **メモ**：インターネット エクスプローラは、レポートを生成するために Adobe Flash Player バージョン 10 以上が必要です。

6 Adobe Flash Player のインストールが要求された場合は、「**Flash の入手**」を選択して、インストール後に「**再試行**」を選択して、インターネット エクスプローラから PDF レポートを生成します。



ウェブ サーバ状況の監視

「**ローカル**」ページの制御ボタンの下には、ウェブ サーバ状況のグラフが表示されます。グラフの 1 つは、時間内に検知されたウェブ要求の数を表示し、もう 1 つのグラフはトラフィック量をキロバイト (KB) で表示します。

トラックされるウェブ サーバは、HTTP/HTTPS ブックマーク、オフロードされたアプリケーション、およびその他のウェブ サービスを提供する SMA/SRA 装置のローカル ネットワーク内のサーバです。トラフィック グラフは、クライアントのブラウザに送信された HTTP/HTTPS ペイロード データを示します。

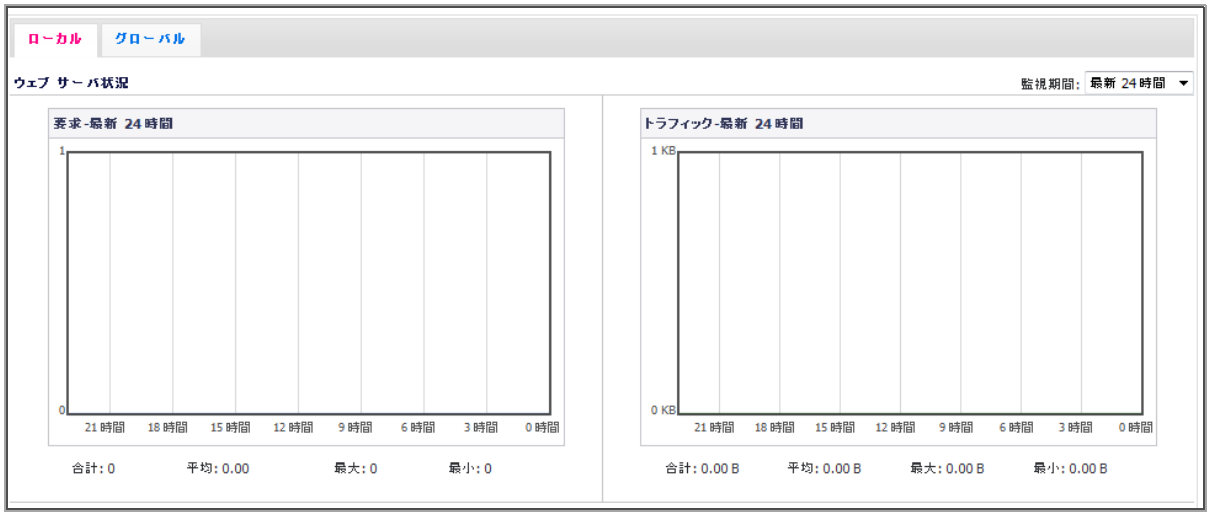
「**監視期間**」ドロップダウン リストから、以下のオプションの 1 つを選択することで、異なる期間のウェブ サーバ アクティビティを「**ローカル**」ページ上で参照できます。

- 過去 60 秒間
- 最新 60 分間

- 最新 24 時間
- 最新 30 日間

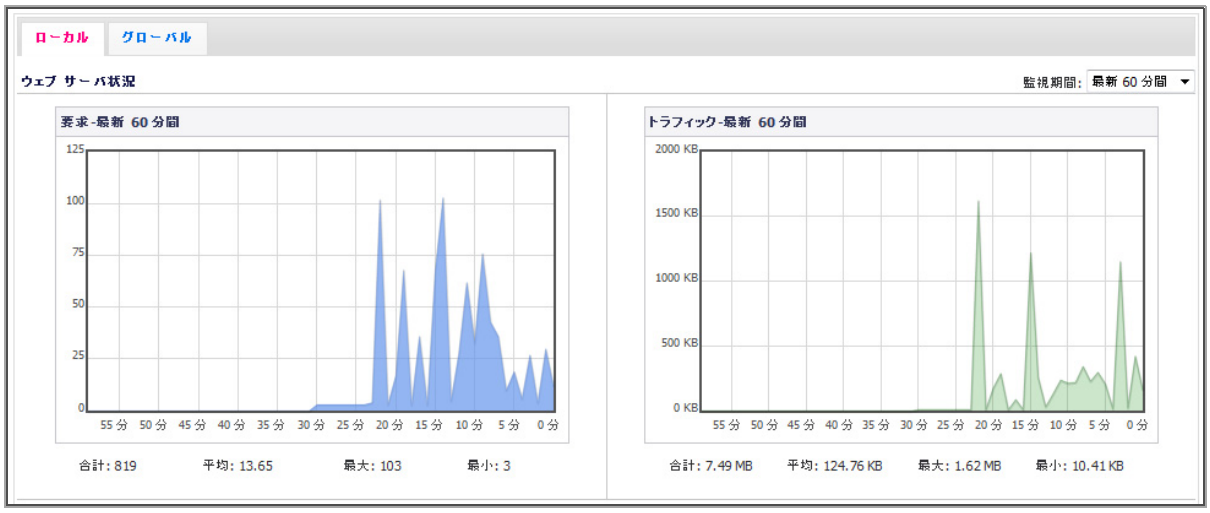
最新 24 時間のウェブ サーバ状況 は 24 時間のウェブ サーバ アクティビティを示します。

最新 24 時間のウェブ サーバ状況



最新 60 分のウェブ サーバ状況 は 60 分間のウェブ サーバ アクティビティを示します。

最新 60 分のウェブ サーバ状況



検知および防御された脅威の監視

「**ウェブ アプリケーション ファイアウォール > 監視**」ページでは、「**ローカル**」ページのウェブ サーバ状況グラフの下に、検知および防御された脅威の数を示すグラフが表示されます。グラフは 2 つあり、1 つは、時間内の脅威数を表示し、もう 1 つは時間内に検知および防御された上位 10 位までの脅威を表示します。

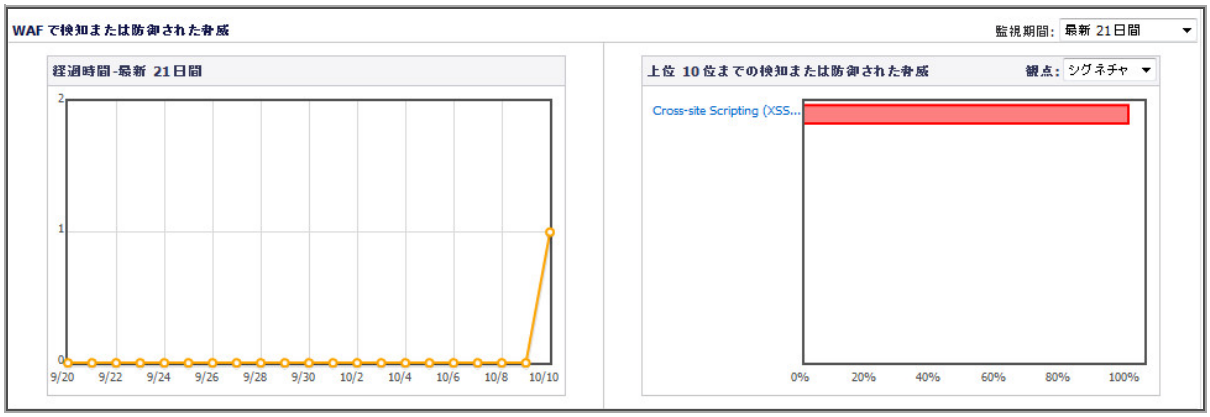
「**監視期間**」ドロップダウン リストから、以下のオプションの 1 つを選択することで、両方のグラフに表示される期間を変更する、またはリスト形式ですべての脅威を表示するように表示を変更することができます。

- 最新 12 時間

- 最新 14 日間
- 最新 21 日間
- 最新 6 か月間
- すべてを一覧表示

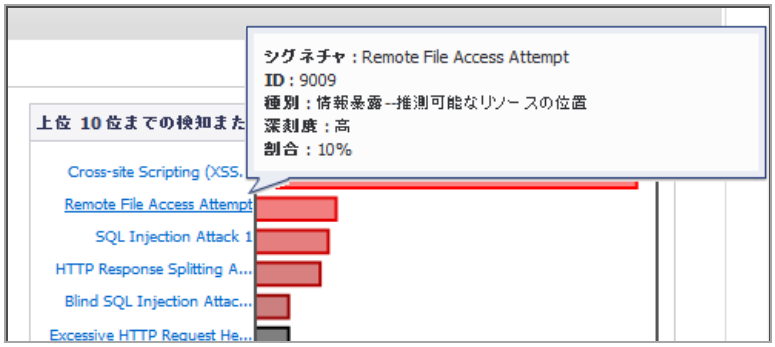
最新 21 日間の脅威 は、最新 21 日間で検知および防御された脅威の数と深刻度を示します。

最新 21 日間の脅威



「**観点**」を「**シグネチャ**」に設定して上位 10 位の脅威グラフを表示する場合、マウス ポインタをシグネチャ ID にあわせると、その脅威に関する詳細を持つツールチップが表示されます。

脅威の詳細ツールチップ



脅威をリスト形式で参照する

脅威をグラフとしてではなく、リスト形式で参照するには、「**監視期間**」ドロップダウン リストから「**すべてを一覧表示**」を選択します。リスト形式の脅威 に、このリスト形式を示します。

この脅威リストの深刻度は、素早く参照するために以下のように色分けされています。

- 高深刻度の脅威 - 赤
- 中深刻度の脅威 - オレンジ
- 低深刻度の脅威 - 黒

はじめは、既定の並び順では深刻度が高く頻度が一番高いものからリストされます。列の見出しを選択することでリストされた脅威の並びを ID、シグネチャの名前、脅威分類、または頻度順に変更できます。再度選択すると、昇順と降順を変更します。アクティブな並び順の列は、昇順に対しては上向きの矢じり、降順に対しては下向きの矢じりによってマークされます。

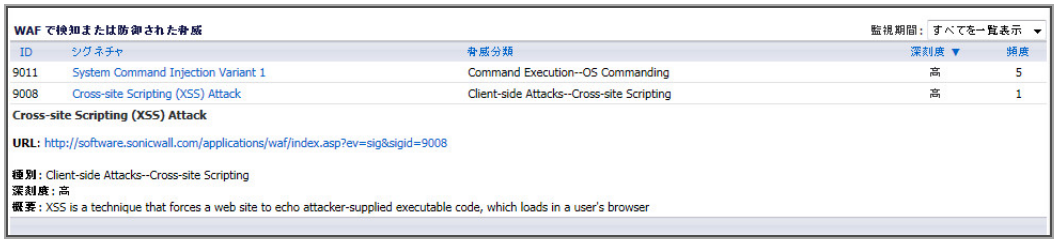
リスト形式の脅威

脅威の詳細を表示および非表示にするには:

1 「**ウェブ アプリケーション ファイアウォール > 監視**」ページで、「**監視期間**」ドロップダウン リストから「すべてを一覧表示」を選択します。「**WAF で検知または防御された脅威**」テーブルに、検知または防御された脅威のリストが表示されます。

2 脅威についての詳細を表示するには、脅威を選択します。詳細は、以下を含みます。

- **URL** - この脅威に対する SonicWall Inc. ナレッジベースの URL です。
- **種別** - この脅威の種別です。
- **深刻度** - この脅威の深刻度で、高、中、または、低です。
- **概要** - この脅威がどのように動作するかの、短い説明です。

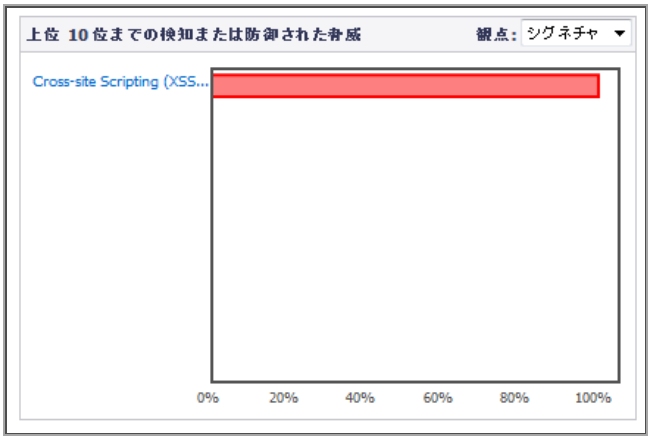


3 脅威の詳細を隠すには、脅威のリンクを再度選択します。

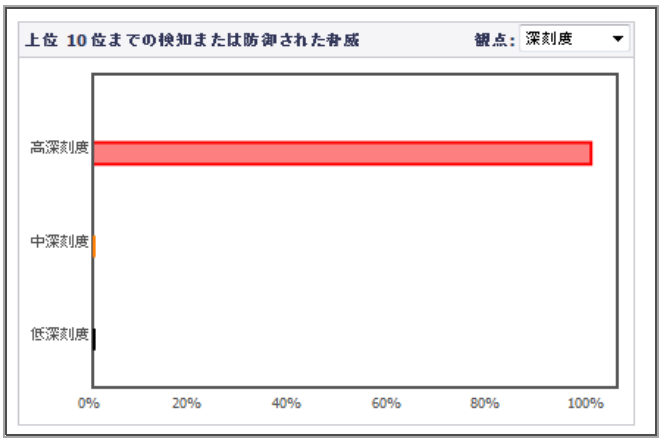
観点を変更する

上位 10 位までの脅威のグラフに対しては、「**観点**」ドロップダウン リストから、以下の表示オプションが選択できます。

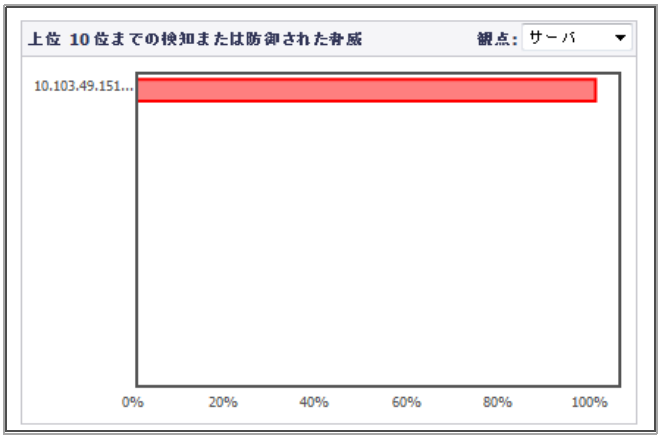
- シグネチャ - グラフの左側に、表示された各脅威の名前がリストされます。



- 深刻度 - 高、中、低の深刻度の脅威が色分けされて表示されます。



- サーバ - グラフの左側に、サーバ名がリストされます。

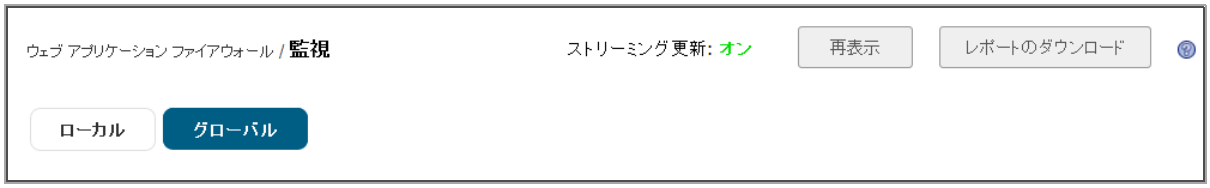


グローバル ページでの監視

「**グローバル**」ページにはウェブ アプリケーション ファイアウォールが有効になっているすべての SMA/SRA 装置によって報告された脅威に対する統計とグラフが表示されます。グラフは「WAF で検知または防御された脅威」に対して表示されます。

制御ボタンの使用

制御ボタンはページ上部に表示されます。それらは、このページ上に表示される統計を制御します。**グローバル** ページ上で制御ボタンを使って、ストリーミング更新のオンとオフ、ページ上のデータの再表示、およびレポートのダウンロードができます。ストリーミングがオンになっている場合、ウェブ アプリケーション ファイアウォールの統計情報は定期的に収集されて、グラフと脅威リストに表示されます。ストリーミングがオフになっていると、新しい情報は表示できません。



制御ボタンを使用するには、以下の手順を実行します。

1 「**グローバル**」ページを選択します。アクティブなページの名前は赤色またはピンク色で表示され、非アクティブなページの名前は青色で表示されます。制御ボタンは現在表示されているページに対して機能します。

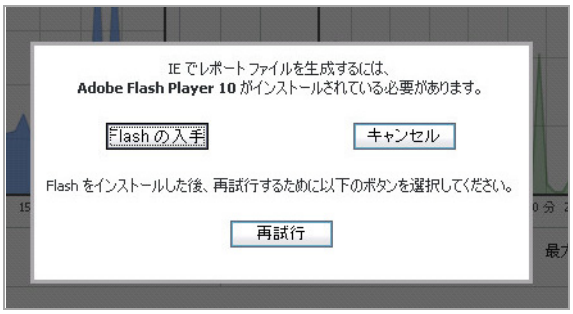
2 ストリーミングのオン・オフを切り替えるには、「**ストリーミング更新**」の隣の「**オン**」または「**オフ**」インジケータを選択します。

3 表示を更新するには、「**再表示**」を選択します。

4 ウェブ アプリケーション ファイアウォールの統計を含む PDF レポートを生成するには、「**レポートのダウンロード**」を選択します。

> **メモ**：インターネット エクスプローラは、レポートを生成するために Adobe Flash Player バージョン 10 以上が必要です。

5 Adobe Flash Player のインストールが要求された場合は、「**Flash の入手**」を選択して、インストール後に「**再試行**」を選択して、インターネット エクスプローラから PDF レポートを生成します。



検知および防御された脅威の監視

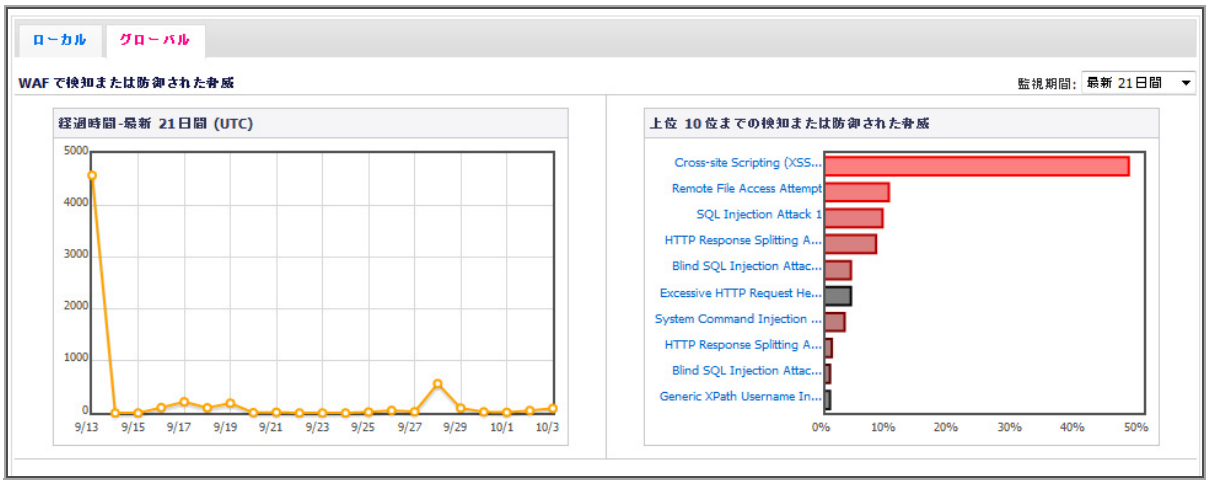
「**ウェブ アプリケーション ファイアウォール > 監視**」ページでは、「**グローバル**」ページの最上部に、検知および防御された脅威の数を示すグラフが表示されます。グラフは 2 つあり、1 つは、時間内の脅威数を表示し、もう 1 つは時間内に検知および防御された上位 10 位までの脅威を表示します。

「**監視期間**」ドロップダウン リストから、以下のオプションの 1 つを選択することで、両方のグラフに表示される期間を変更することができます。

- 最新 12 時間
- 最新 14 日間
- 最新 21 日間
- 最新 6 か月間

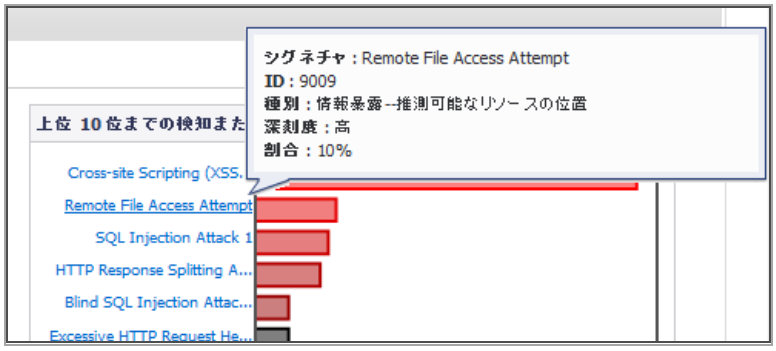
最新 21 日間の脅威 は、最新 21 日間で検知および防御された脅威の数と深刻度を示します。

最新 21 日間の脅威



マウス ポインタをシグネチャ ID にあわせると、その脅威に関する詳細を持つツールチップが表示されます。

脅威の詳細ツールチップ



詳細な脅威情報を得るために、装置上のローカル シグネチャ データベースにアクセスしますが、データベースが最新でない場合は、上位 10 位の脅威に対するいくつかの詳細情報は利用できません。この場合、グラフ内のその脅威の色は明るい灰色で表示され、その脅威のためのツールチップ内に「深刻度」が「不明」として表示されます。グラフの下に以下のメッセージも表示されます。

警告: この装置用のウェブ アプリケーション ファイアウォール シグネチャ データベースは現在利用できません。「**ウェブ アプリケーション ファイアウォール > 状況**」ページ でデータベースを同期してください。

ウェブ アプリケーション ファイアウォールのログの使用

「**ウェブ アプリケーション ファイアウォール > ログ**」ページでは、便利なログ検索機能やログをファイルにエクスポートする機能、メールで送信する機能など、さまざまなログ機能を利用できます。また、ログを消去することもできます。ログ エントリを選択すると、イベントの詳細な情報が表示されます。

以下のセクションを参照してください。

- ログを検索する (351 ページ)
- ログのページ付けを調整する (351 ページ)
- ログ エントリの詳細な情報を表示する (352 ページ)
- ログ ファイルのエクスポートとメール送信 (352 ページ)
- ログを消去する (353 ページ)

ログを検索する

ログ テーブルの特定の列に含まれる値を検索したり、指定の値を**含まない**ログ エントリを検索できます。

ウェブ アプリケーション ファイアウォールのログ ファイルを表示、検索するには:

1. 「**ウェブ アプリケーション ファイアウォール > ログ**」ページで、検索する値を「**検索**」フィールドに入力します。
2. 「検索」フィールドの右側にあるドロップダウン リストから検索の対象とする列を選択します。
3. 以下のいずれかを実行します。
   - 検索値を含むログ エントリの検索を開始するには、**「検索」**ボタンを選択します。
   - 検索値を含まないログ エントリの検索を開始するには、**「除外」**ボタンを選択します。
   - 「検索」フィールドの内容を消去し、ドロップダウン リストを既定値 (時刻) に設定し、ログ エントリの最初のページを表示するには、「**リセット**」ボタンを選択します。

ログのページ付けを調整する

1 ページに表示するログ エントリ数を調整し、エントリの表示範囲を変更するには、以下の手順に従います。

1. 「**ウェブ アプリケーション ファイアウォール > ログ**」ページで、1 ページに表示するログ エントリ数を「**1 ページあたりの項目**」フィールドに入力します。「ログ」ページの表示が新しいエントリ数に変更されます。
2. 特定の番号以降のログ エントリを表示するには、開始番号を**「項目」**フィールドに入力し、**Enter** キーを押します。

3 ログ エントリの最初のページを表示するには、矢印コントロール パッドの左端のボタン を選択します。

4 ログ エントリの前のページを表示するには、矢印コントロール パッドの左向き矢印 を選択します。

5 ログ エントリの次のページを表示するには、矢印コントロール パッドの右向き矢印 を選択します。

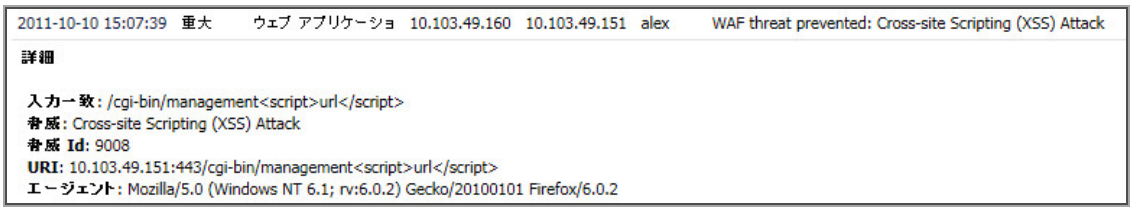
6 ログ エントリの最後のページを表示するには、矢印コントロール パッドの右端のボタン を選択します。

ログ エントリの詳細な情報を表示する

ログ エントリの詳細な情報は、ログの種類によって異なります。URI (Uniform Resource Indicator) が、脅威が検知されたコマンドと共に表示されます。また、イベントの原因となったエージェントに関する情報も表示されます。暗号のようなエージェント文字列の意味については、次の Wikipedia ページを参照してください。ユーザ エージェントに関する説明と、ユーザ エージェント文字列を解析できる外部サイトへのリンクがあります。http://en.wikipedia.org/wiki/User_agent

個別のログ エントリの詳細情報を表示するには:

1 「**ウェブ アプリケーション ファイアウォール > ログ**」ページで、詳細情報を表示するログ エントリを選択します。そのエントリの直後に詳細情報が表示されます。



2 詳細情報を非表示にするには、ログ エントリをもう一度選択します。

ログ ファイルのエクスポートとメール送信

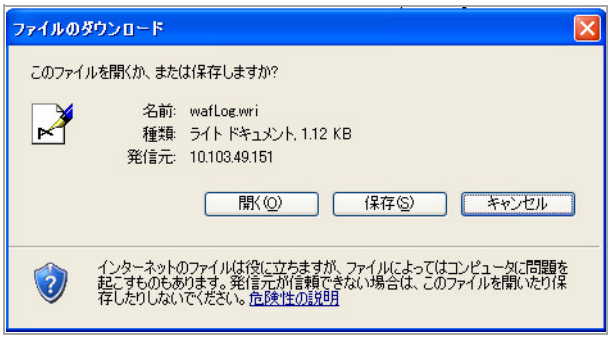
「**ウェブ アプリケーション ファイアウォール > ログ**」ページの右上隅にあるボタンを使って、現在のウェブ アプリケーション ファイアウォールのログの内容をファイルにエクスポートしたり、メールで送信することができます。

エクスポートしたファイルは **.wri** ファイル名拡張子を付けて保存され、既定でワードパッドで開かれます。

メールでファイルを送信すると、Secure Mobile Access 管理インターフェースの「**ログ > 設定**」ページで設定されたアドレスに宛てて送信されます。アドレスが未設定の場合は、「**ウェブ アプリケーション ファイアウォール > ログ**」ページで「**ログのメール送信**」を選択したときにエラー メッセージがブラウザ下部のステータス行に表示されます。

ログをエクスポートまたは送信するには:

1 ログの内容をエクスポートするには、「**ウェブ アプリケーション ファイアウォール > ログ**」ページの右上隅にある「**エクスポート**」を選択します。「ファイルのダウンロード」ダイアログ ボックスが表示されます。



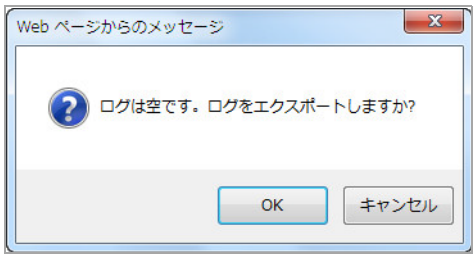
2 「ファイルのダウンロード」ダイアログ ボックスで、以下のいずれかの操作を行います。

- ファイルを開くには、「**開く**」を選択します。
- ファイルを保存するには、「**保存**」を選択してからファイルを保存するフォルダに移動し、「**保存**」を選択します。

3 ログの内容を送信するには、「**ウェブ アプリケーション ファイアウォール > ログ**」ページの右上隅にある「**ログのメール送信**」を選択します。ログの内容が、「**ログ > 設定**」ページで指定されたアドレスにメールで送信されます。

ログを消去する

「**ウェブ アプリケーション ファイアウォール > ログ**」ページでは、ウェブ アプリケーション ファイアウォールのログからすべてのエントリを削除できます。ページに表示されていたエントリが削除され、その後でログ エントリがまだ追加されない状態でログ ファイルのエクスポートやメール送信を行おうとすると、確認のダイアログ ボックスが表示されます。



ウェブ アプリケーション ファイアウォール ログを消去するには:

1 「**ウェブ アプリケーション ファイアウォール > ログ**」ページの右上隅にある「**ログの消去**」を選択します。

2 確認のダイアログ ボックスで、「**OK**」を選択します。

ウェブ アプリケーション ファイアウォールの検証とトラブルシューティング

ウェブ アプリケーション ファイアウォールの正しい設定を確認する一つの方法は、「**ウェブ アプリケーション ファイアウォール > 監視**」ページを参照することです。このページには、検知/防御された脅威に対する期間あたりの、および、上位 10 脅威の統計とグラフが表示されます。「**ローカル**」ページにはまた、ウェブ サーバの状況統計と選択した監視期間の要求数とトラフィック量のグラフも表示されます。インターネットを通常どおりに使っていれば、1 日以内に統計の表示が開始されます。

また、「**ログ > 表示**」ページと「**ウェブ アプリケーション ファイアウォール > ログ**」ページにも役に立つ情報があります。このセクションでは、主なログ メッセージについて説明し、それが表示された場合の対処方法を示します。

「ログ > 表示」のメッセージ

次のメッセージが「**ログ > 表示**」ページに表示されることがあります。

- ライセンス マネージャ SSL 接続障害 - 装置の再起動が必要です

  「**システム > 診断**」ページで **Ping** や **DNS ルックアップ**診断ユーティリティを使って **licensemanager.sonicwall.com** への接続をテストし、バックエンド サーバに接続できることを確認してください。

- ライセンス マネージャはホストを解決できませんでした。DNS をチェックしてください。

  「**システム > 診断**」ページで **Ping** や **DNS ルックアップ**診断ユーティリティを使って **licensemanager.sonicwall.com** への接続をテストし、バックエンド サーバに接続できることを確認してください。

- ライセンス マネージャ ピア識別障害 - 証明書と時刻をチェックしてください。

  ライセンス マネージャ サーバまたはシグネチャ データベース サーバが有効な SSL 証明書を保持していない可能性があります。

- ライセンス マネージャのリセットが呼び出されました

  デバイス ライセンスがリセットされました。「**システム > ライセンス**」ページを開いて、ライセンスの有効化、アップグレード、または更新を行ってください。

「ウェブ アプリケーション ファイアウォール > ログ」および「ログ > 表示」のメッセージ

次のメッセージが「**ウェブ アプリケーション ファイアウォール > ログ**」ページや「**ログ > 表示**」ページに表示されることがあります。

- WAF シグネチャ データベースの更新障害: シグネチャが更新に見つかりませんでした

  データベース更新のダウンロードは完了しましたが、適切なシグネチャがデータベースに見つかりませんでした。

- WAF シグネチャ データベースの更新障害: 更新内のシグネチャのタイムスタンプが新しくありません

  ライセンス マネージャから取得したデータベース更新内のタイムスタンプは、更新のダウンロードを開始する前に通知されたタイムスタンプよりも古い値です。

- WAF シグネチャ データベースの更新障害: 更新の処理中にエラーが発生しました

データベース更新のダウンロードと処理を行っているときに一般的なエラーが発生しました。更新内のデータがシグネチャ解析スキーマに従っていない可能性があります。

- WAF シグネチャ データベースの更新障害: WAF シグネチャ データベース更新のダウンロード中にエラーが発生しました

  データベース更新のダウンロードと処理を行っているときに一般的なエラーが発生しました。更新内のデータがシグネチャ解析スキーマに従っていない可能性があります。

- WAF シグネチャ データベースの更新がダウンロードされました。新しいデータベースには<数字>件のルールが含まれます

  シグネチャ データベースがダウンロードされました。新しいデータベースには<数字>件のルールが含まれます。ルールとは、ダウンロードされたシグネチャの数を確認するために SonicWall Inc. で使われる内部プロパティです。

  メモ：「**ウェブ アプリケーション ファイアウォール > 設定**」ページの「**自動シグネチャ更新を適用する**」オプションを選択して、新しいシグネチャを自動的に適用できます。このオプションが選択されていない場合は、ダウンロードが正常に完了した後、「**ウェブ アプリケーション ファイアウォール > 状況**」ページに表示される「**適用**」を選択する必要があります。データベースが正常に適用された後で、新しいデータベースに含まれるすべてのシグネチャが「**ウェブ アプリケーション ファイアウォール > シグネチャ**」ページに表示されます。

- WAF シグネチャ データベースが更新されました

  管理者が「**ウェブ アプリケーション ファイアウォール > 状況**」ページの「**適用**」を選択した後で、シグネチャ データベースの更新が適用されました。

- WAF エンジンが出荷時の既定のシグネチャ データベースで起動されました

  ウェブ アプリケーション ファイアウォール エンジンは、出荷時の既定のシグネチャ データベースを使ってトラフィックを検査しています。これは、ファームウェアが更新されてから新しいシグネチャが見つかっていないことを意味します。過去にダウンロードを試みたことがログからわかる場合、このメッセージは、データベース エラーが原因で更新が正しく処理されず、対処として出荷時の既定のデータベースが使用されていることも意味します。

13

キャプチャ ATP

このセクションでは、Secure Mobile Access ウェブベース管理インターフェースの「**キャプチャ ATP**」ページに固有の情報と設定タスクについて説明します。キャプチャ ATP (Capture Advanced Threat Protection) は、さまざまな種類のコンテンツを分析して有害な動作を見つけるクラウドベースのサービスです。

メモ：キャプチャ ATP は SMA 200、SMA 400、SMA 500v 装置でのみサポートされています。

キャプチャ ATP の概念の詳細については、キャプチャ ATP 統合の概要 (22 ページ) を参照してください。

トピック:

キャプチャ ATP > 設定

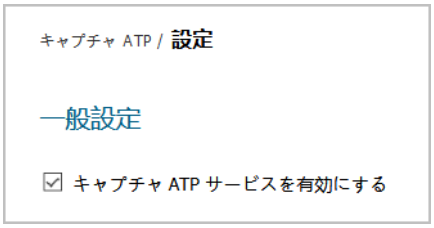
このセクションでは、「**キャプチャ ATP > 設定**」ページの概要と、このページで利用できる設定タスクについて説明します。キャプチャ ATP の設定は、以下のセクションに分かれています。

- 一般設定
- ファイル種別の設定
- ファイル サイズの設定
- ユーザ定義の遮断動作

一般設定

キャプチャ ATP の一般設定を構成するには:

1 「**キャプチャ ATP > 設定**」ページに移動します。

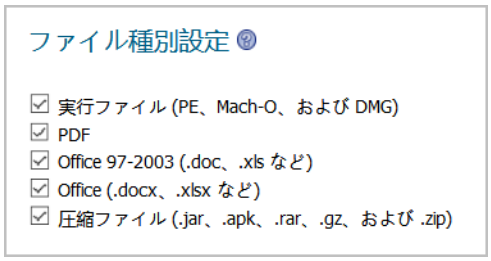


2 「**キャプチャ ATP サービスを有効にする**」を選択してキャプチャ ATP サービスを有効化します。

ファイル種別の設定

ファイル種別の設定を構成するには:

1 「**キャプチャ ATP > 設定**」ページに移動します。



2 キャプチャ ATP サービスに転送して分析するファイルの種別を選択します。使用可能なファイル種別は次のとおりです。

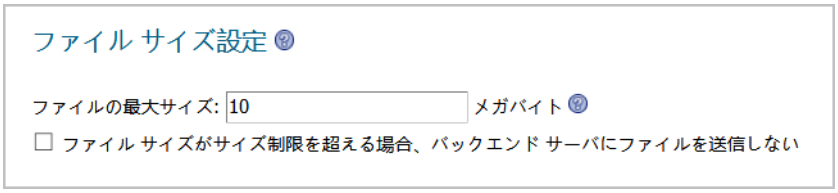
- 実行ファイル (PE、Mach-O、および DMG)
- PDF
- Office 97-2003 (.doc、.xls など)
- Office (.docx、.xlsx など)
- 圧縮ファイル (.jar、.apk、.rar、.gz、および .zip)

メモ：選択されたファイル種別のリストにないファイル種別は、キャプチャ ATP サービスに送信して分析されません。

ファイル サイズの設定

ファイル サイズの設定を構成するには:

1 「**キャプチャ ATP > 設定**」ページに移動します。



2 キャプチャ ATP サービスに送信されるファイルの最大サイズを指定するには、「**ファイルの最大サイズ**」ウィンドウに値を入力します。有効な最大サイズは、ユーザ レベルとグループ レベルで 0 - 10 MB、グローバル レベルで 1 - 10 MB です。

- ユーザ レベルで値を 0 に設定すると、SMA はグループ設定の最大ファイル サイズを使用します。
- グループ レベルで値を 0 に設定すると、SMA はグローバル設定の最大ファイル サイズを使用します。
- ファイル サイズが最大値より小さいファイルがキャプチャ ATP サービスに送信されてチェックされます。

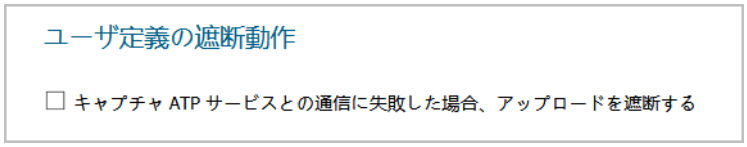
3 サイズ制限を超えたファイルをバックエンド サーバに送信したくない場合は、「**ファイル サイズがサイズ制限を超えた場合はバックエンド サーバにファイルを送信しない**」を選択します。

> **メモ**：ファイル サイズが最大値を超え、「**ファイル サイズがサイズ制限を超えた場合はバックエンド サーバにファイルを送信しない**」オプションが有効化されていれば、ファイルはバックエンド サーバに送信されません。ファイル サイズが最大値を超え、このオプションが無効化されていれば、ファイルはバックエンド サーバに送信されます。

ユーザ定義の遮断動作

ユーザ定義の遮断動作を構成するには:

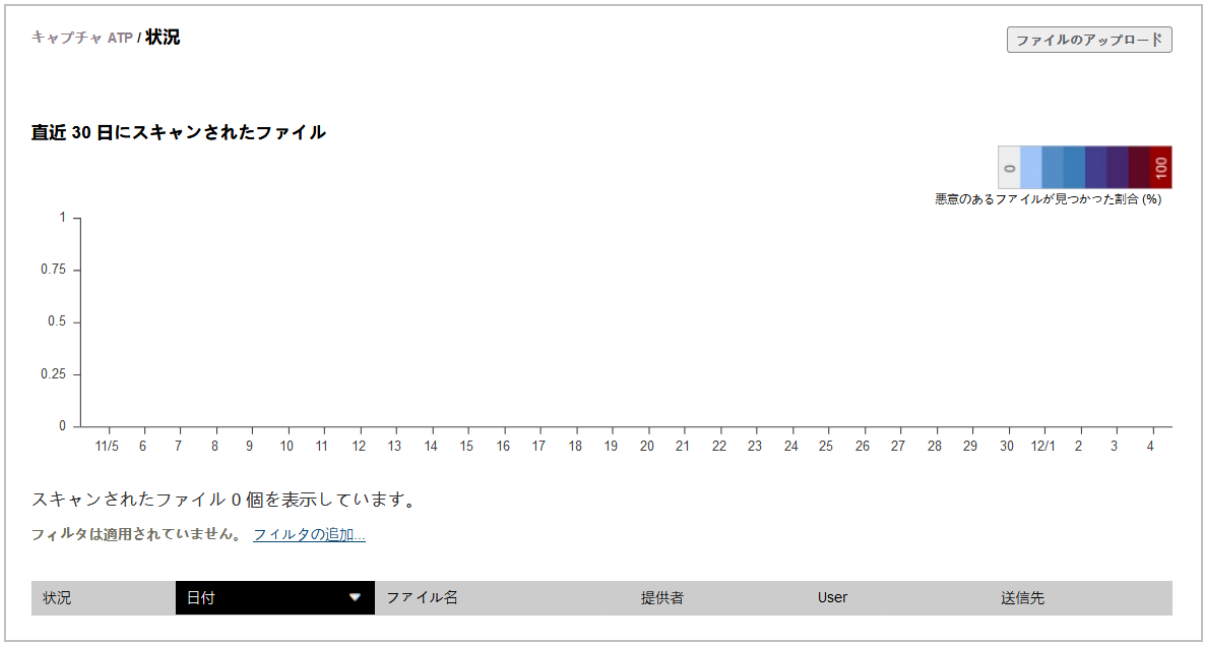
1 「**キャプチャ ATP > 設定**」ページに移動します。



2 キャプチャ ATP サービスとの通信が失敗するときは「**キャプチャ ATP サービスとの通信に失敗した場合、アップロードを遮断する**」を選択してバックエンド サーバへのファイルのアップロードを許可または遮断します。

キャプチャ ATP > レポート

このセクションでは、「**キャプチャ ATP > レポート**」ページの概要と、このページで使用できる設定タスクについて説明します。信頼できるファイルや悪意のあるファイルがアップロードされると、キャプチャ ATP はそのイベントを「**キャプチャ ATP > レポート**」ページに記録して報告します。



「**キャプチャ ATP > レポート**」ページは、以下のセクションに分かれています。

- 過去 30 日間にスキャンされたファイル
- スキャンされたファイルの表示
- 新しいフィルタの追加

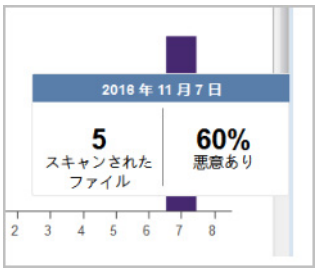
- ファイルのアップロード

過去 30 日間にスキャンされたファイル

「**過去 30 日間にスキャンされたファイル**」棒グラフは、過去 30 日間にスキャンされたファイルの数を視覚的に表したものです。Y 軸は、スキャンされたファイルの総数を示します。

特定の日付の情報を表示するには:

1 「**キャプチャ ATP > レポート**」画面で特定の日付に対応するバーの上にマウスを置くと、次の情報が表示されます。
   - 日付
   - スキャンされたファイル数
   - 悪意のあるファイルの割合



スキャンされたファイルの表示

「**スキャンされたファイルの表示**」セクションでは、過去 30 日間にスキャンされたファイルに関する以下の詳細情報が提供されます。

- **状況** - クリーンなファイルか悪意のあるファイル
- **日付** - ファイル スキャンの日付
- **ファイル名** - ファイルの名前
- **提供者** - 送信方法
   - 「レポート」ページからアップロードによって送信されたファイルは「**(アップロード済み)**」と表示されます
   - CIFS ブックマークによって送信されたファイルは SMA 装置名で表示されます
- **ユーザ**
- **宛先** - ファイルの送信先 IP アドレス

ファイルのフィルタ

スキャンされたファイルを種別でフィルタするには:

1 テーブルの上部にある種別見出しをクリックして、ファイルを降順でソートします。
2 種別をもう一度クリックすると、ファイルが昇順でフィルタされます。

新しいフィルタの追加

新しいフィルタを追加するには:

1 「**フィルタの追加**」をクリックします。「フィルタの追加」ウィンドウが表示されます。

2 ドロップダウン リストをクリックし、以下のいずれかを選択します。

- 種別
  - 状況
  - 日付
  - ファイル名
  - 提供者
  - ユーザ
  - 送信先
- 分析
  - 一致
  - 不一致
- 状況
  - 悪意あり
  - クリーン
  - スキャン待機中
  - スキャン失敗

3 「**追加**」をクリックして新しいフィルタを作成します。

ファイルのアップロード

スキャンするファイルをアップロードするには:

1 「**ファイルのアップロード**」を選択します。「スキャンするファイルのアップロード」ウィンドウが表示されます。

2 「**ファイルの選択 ...**」ウィンドウにファイル名を入力するか、「**参照**」を選択してファイルを検索します。

メモ：サポートされているファイル種別は EXE、MSI、ZIP、APK アプリケーション、PE などです。最大ファイル サイズは 100 MB です。

3 「**アップロード**」をクリックしてファイルをインポートします。

キャプチャ ATP > ライセンス

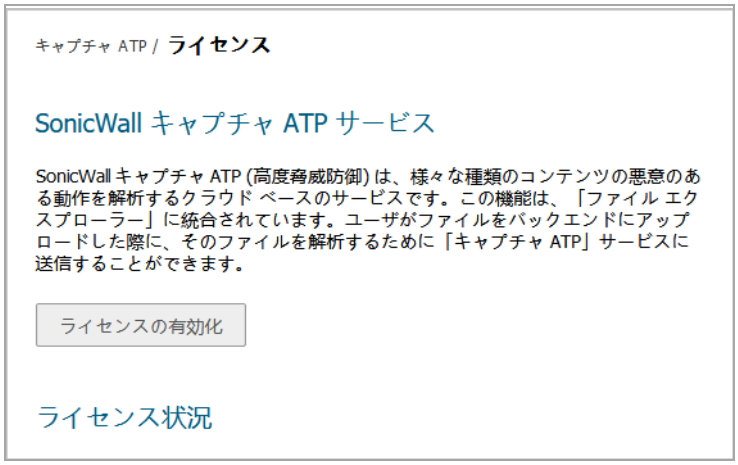
このセクションでは、「**キャプチャ > ライセンス**」ページの概要と、このページで使用できる設定タスクについて説明します。「**キャプチャ ATP > ライセンス**」ページは、以下のセクションに分かれています。

- SonicWall キャプチャ ATP サービス
- ライセンス状況

SonicWall キャプチャ ATP サービス

キャプチャ ATP (Capture Advanced Threat Protection) はファイアウォールに対するアドオン セキュリティ サービスです。ファイアウォールで有害ファイルを識別するために利用されます。キャプチャ ATP を有効化する前に、まずライセンスを取得する必要があります。

メモ：キャプチャ ATP ライセンスを有効化していない場合は、エラーメッセージが表示されます。



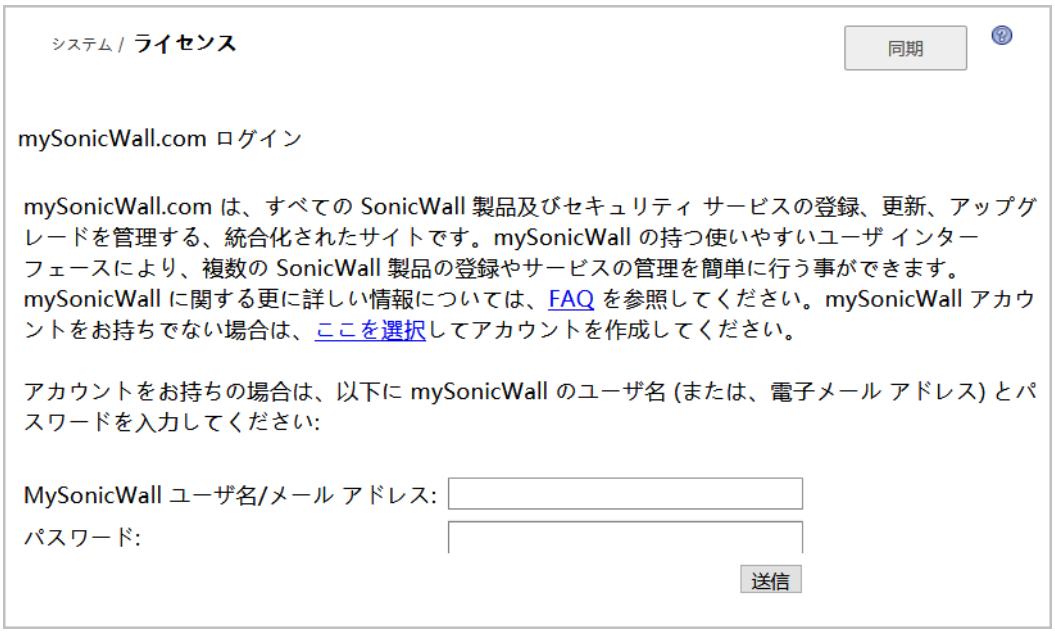
「**キャプチャ ATP > ライセンス**」ページまたは MySonicWall.com からキャプチャ ATP サービスを登録して有効化します。キャプチャ ATP のライセンスを取得すると、MySonicWall アカウントでキャプチャ ATP の状況を確認でき、警告と通知を設定して受け取ることができるようになります。

キャプチャ ATP とそのライセンス方法、および MySonicWall アカウントを使って警告と通知を設定および受け取る方法については、『*SonicOS 6.5 キャプチャ ATP 機能ガイド*』を参照してください。

ライセンスを有効化するには:

1 「**キャプチャ ATP > ライセンス**」に移動し、「**ライセンスの有効化**」をクリックします。「**システム > ライセンス**」ページが表示されます。

2 「**サービスの購読、アップグレード、及び更新**」リンクを選択します。「MySonicWall ログイン」ページが表示されます。



3 MySonicWall 資格情報を入力し、「**送信**」をクリックします。「**ライセンス > ライセンス管理** 」ページが表示されます。

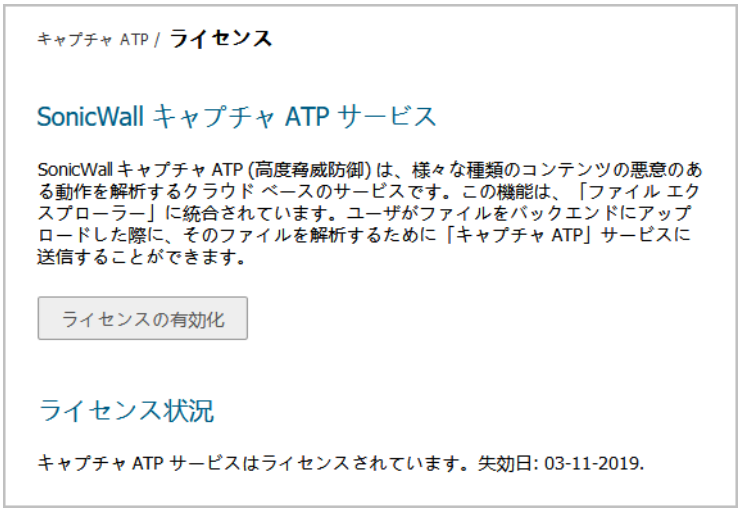
4 「**キャプチャ ATP**」を見つけます。

5 「**有効化**」をクリックします。

6 「**続行**」を選択します。キャプチャ ATP の「状態」表示が「**購読済**」になります。

ライセンス状況

「ライセンス状況」セクションには、現在のライセンス状況と失効期日が表示されます。



14

地域 IP とボットネット フィルタ

このセクションでは、Secure Mobile Access 管理インターフェースの「地域 IP とボットネット フィルタ」ページと、このページで行う設定タスクについて説明します。「地域 IP」機能により管理者は、リモート ユーザの地理的な場所に基づく監視およびポリシーの適用を効果的に行うことができます。「ボットネット フィルタ」機能は、SonicWall Inc. が管理する動的更新データベースを使用することで、ボットネットからの不正な活動に対抗するための、強固な対回避防御を行います。ボットネットは、サービス妨害 (DoS) 攻撃やデータ漏洩などの多大なセキュリティ上の危険性をもたらします。ボットネットは、発生源が一時的であるというその性質のために、識別と制御が困難です。これらの機能は既定では無効になっています。

トピック:

状況

「地域 IP とボットネット フィルタ > 状況」には、「一般状況」と「ボットネット状況」という 2 つのタブがあります。

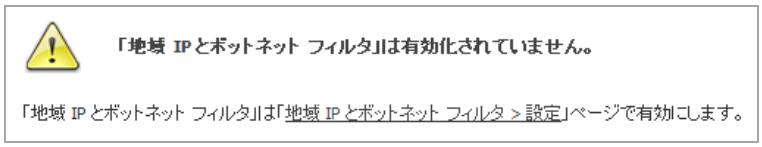
次を参照してください。

一般状況

「**一般状況**」ページには、地域 IP とボットネット フィルタに関する一般的な情報が表示されます。また、データベースを同期することができます。地域 IP とボットネット フィルタを有効にすると、「一般状況」ページには次の情報が表示されます。

- 「**データベース**」には更新状況が表示され、更新を手動で同期するための「**同期**」があります。「**同期**」をクリックすると、サーバは直ちに、バックエンド サーバ上の新しい更新を確認します。
- 「**保護状況**」は、バックエンド サーバが接続されているかどうかを示します。「オフライン」になっている場合は、ネットワーク設定の変更が必要な可能性があります。
- 「**キャッシュサイズ**」は、地域 IP とボットネットのキャッシュの総数を示します。キャッシュはすべて、サーバによって自動的に管理されます。
- 「**最終確認**」は、キャッシュの最新タイムスタンプを表示します。
- 「**サービスの失効期日**」は、地域 IP とボットネット フィルタ サービスのライセンス失効期日を示します。
- 「**ライセンス状況**」は、地域 IP とボットネット フィルタ サービスが購読済みであるかどうかを示します。地域 IP とボットネット フィルタは、無料トライアルを含む購読サービスです。

地域 IP とボットネット フィルタがライセンスされているが無効になっている場合には、この機能を有効にできる「設定」ページへのリンクを含む警告が「状況」ページに表示されます。



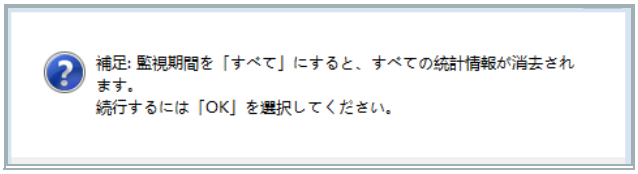
ボットネット状況

「**ボットネット状況**」ページには、現在のレポート期間におけるボットネット IP アドレスのトラフィック統計が表示されます。ボットネット フィルタが選択期間に検知した IP アドレス上位 10 件に対する統計が表示されます。

メモ：IP アドレスの場所が変化する場合は、各場所が異なる IP アドレスとして表示され、統計は分割されることに注意してください。

「**監視周期**」ドロップダウン リストを使用して、レポート期間を選択します。「最新 12 時間」、「最新 14 日間」、「最新 21 日間」、「最新 6 か月間」、「すべて」の記録済みトラフィック データが選択できます。

「**消去**」をクリックすると、選択されている「監視期間」以外の期間の統計が消去されます。消去する前に、消去操作を確認するポップアップ ウィンドウが表示されます。



ヒント：「**消去**」は「監視期間」と組み合わせて使用する必要があります。例えば、「監視周期」として「**最新 12 時間**」が選択されている状態で「**消去**」をクリックすると、「最新 12 時間」の履歴を残して、それ以外の履歴がすべて消去されます。

設定

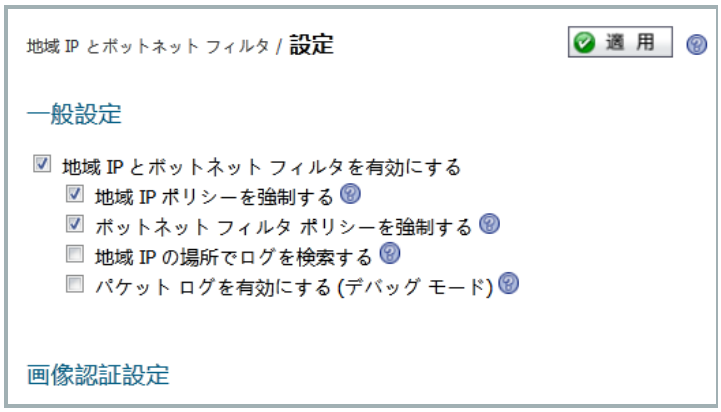
「**地域 IP とボットネット フィルタ > 設定**」ページでは、地域 IP とボットネット フィルタの有効化/無効化と、修復設定を行います。「**地域 IP とボットネット フィルタ > 設定**」ページには、次のページがあります。

- 一般設定 (366 ページ)
- 修復設定 (367 ページ)

一般設定

「**地域 IP とボットネット フィルタ > 設定**」ページの「一般設定」セクションでは、地域 IP とボットネット フィルタをグローバルに有効または無効にできます。既定では無効になっています。

メモ：「**システム > 診断**」ページからアクセス可能な「**ボットネットのテスト**」診断ツールを使用することによって、IP アドレスを手動でボットネット IP アドレスとして特定することができます。



地域 IP とボットネット フィルタを有効にするには、以下の手順に従います。

1 「**地域 IP とボットネット フィルタを有効にする**」をオンにして、この機能を全体的に有効にします。この機能を有効にすると、ユーザの送信元 IP アドレスの場所を識別する「**NetExtender > 状況**」、「**仮想アシスト > 状況**」、「**仮想ミーティング > 状況**」、「**ユーザ > 状況**」の各ページに「場所」列が追加されます。「場所」列のアイコン上にマウスを移動させると、送信元 IP の「都市」(該当する場合)、「地域」、「国」が表示されます。

2 「**適用**」を選択します。

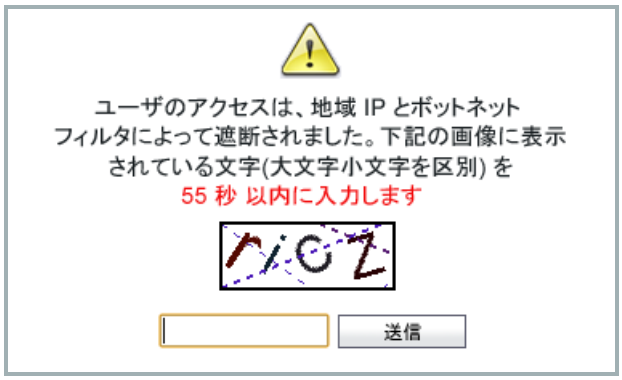
この機能を有効にすると、「一般設定」セクションには、個別に有効または無効にすることのできる次の 4 つのサブ機能が表示されます。

- **地域 IP ポリシーを適用する** - 地域 IP ポリシーを適用します。
- **ボットネット フィルタ ポリシーを適用する** - SonicWall ボットネット データベース内の IP アドレスの遮断を有効にして (定義済みのポリシーは不要)、ボットネット フィルタ ポリシーを適用します。このオプションを無効にした場合、ボットネット IP アドレスは遮断はされませんが検知され、ボットネット フィルタ統計に含められます。
- **地域 IP の場所でログを検索する** - このオプションを選択すると、送信元 IP の場所を示す列が、「**エンド ポイント制御 > ログ**」、「**ウェブ アプリケーション ファイアウォール > ログ**」、「**地域 IP とボットネット フィルタ > ログ**」、「**ログ > 表示**」の画面に追加されます。
- **パケット ログを有効にする (デバッグ モード)** - 許可または拒否されたパケットのログを生成します。このオプションはデバッグ目的にのみ使用します。パケット ログを有効にすると、ログ レベルが「デバッグ」に設定されている場合、ログ数は急速に増加します。

修復設定

地域 IP とボットネット フィルタが有効な場合、アグレッシブな IP アドレスから SMA/SRA 装置によって保護されたリソースへのアクセスは拒否されます。修復は、正当なユーザに自身が「ボット」ではなく実在のユーザであることを証明する機会を与え、アクセスを許可するための仕組みです。

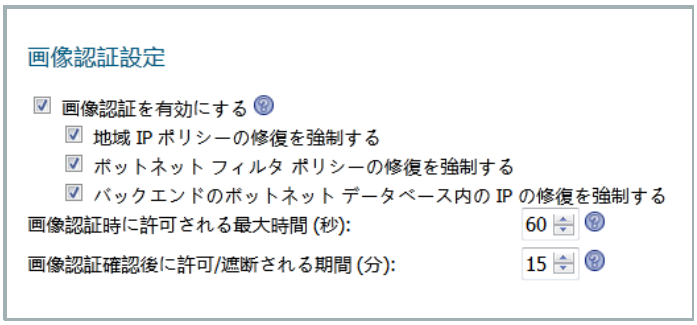
ウェブ アクセスの場合、ユーザは次の図に示す CAPTCHA ページにリダイレクトされます。カウントダウン タイマーは、ユーザが修復を完了するまでの残り時間を示します。ユーザは制限時間内に修復を完了する必要があります。制限時間を過ぎると、ユーザの IP アドレスは遮断リストに追加され、その IP アドレスからのすべてのアクセスが一定期間にわたって遮断されます。



検証時間内に修復に成功すると、ユーザが要求したページが表示されます。続いて修復状況を記録するために、CAPTCHA セッションが作成されます。有効期間の間、その IP アドレスからのすべてのアクセスが許可されます。有効期間を過ぎると、CAPTCHA セッションは期限切れになります。ユーザがまだログインしている場合は、アクセスは遮断されませんが、ユーザのログイン セッションの期限が切れると、CAPTCHA セッションは削除され、再度修復が要求されます。

修復を有効にして設定するには:

1 「**修復設定**」を選択します。



2 「**画像認証を有効にする**」をオンにします。拒否されたユーザは、CAPTCHA ベースの修復がないと装置によって保護されたリソースにアクセスできません。修復は、地域 IP ポリシー、ボットネット フィルタ ポリシー、またはバックエンドのボットネット データベースで定義された IP アドレスに対して個別に適用できます。必要に応じて、さらにオプションを選択します。

3 「**画像認証時に許可される最大時間 (秒)**」フィールドに、ユーザが修復を完了するための制限時間 (秒) を入力します。30 ～ 300 秒の範囲内で設定します。既定値は 60 秒です。

4 「**画像認証確認後に許可/遮断される期間 (分)**」フィールドに、CAPTCHA 検証後にユーザを許可/遮断する期間 (分) を入力します。5 ～ 30 分の範囲内で設定します。既定値は 15 分です。

アクセス ポリシー

「**地域 IP とボットネット フィルタ > ポリシー**」ページでは、地域 IP とボットネット フィルタのアクセス ポリシーを表示、追加、編集、削除できます。地域 IP とボットネット フィルタに対し、最大で合計 64 件のアクセス ポリシーを作成できます。各ポリシーには、異なる優先度が自動的に割り当てられます。

最も高い優先度は 1 です。ポリシーの優先度によって、適用順序が決まります。「設定」ページには、この優先度の順序でポリシーが表示されます。

- ボットネット フィルタのポリシーは、地域 IP のポリシーよりも優先度が高くなります。地域 IP のポリシーは、作成された時間によって優先度が割り当てられ、先に作成されたものほど優先度が高くなります。
- ボットネット フィルタのポリシーは、1 つの IP アドレスに対して定義されたものの方が、サブネットに対して定義されたものよりも優先度が高く、それぞれの種別の中では、作成された時間によって優先度が割り当てられ、先に作成されたものほど優先度が高くなります。

- 個別に作成されたポリシーは先に適用されます。つまり、ある IP アドレスが SonicWall ボットネット フィルタ データベースに登録されていても、管理者がこの IP に対して許可ポリシーを定義している場合は、この IP からのアクセスが許可されます。

ポリシーは、編集 ボタンを選択することによって変更できますが、ポリシー名を変更することはできません。

削除 ボタンを選択すると、ポリシーを削除できます。

新しいアクセス ポリシーを作成するには、「**ポリシーの追加...**」ボタンを選択します。次の 2 種類のポリシーを追加できます。

- 「**地域 IP ポリシー**」タブ

  地域 IP ポリシーは、指定された国からのトラフィックを許可または拒否します。「**ポリシー名**」を入力し、許可または拒否する国を選択します。国を大陸別に並べ替えることができます。ドロップダウンをクリックして目的の大陸を選択するだけで、その大陸内のすべての国が「**ポリシーの適用先**」リストに表示されます。地図から国を直接選択することもできます。

  地図には、選択されている国と選択されていない国が色分けされて表示されます。選択されていない国はグレーで、選択されている国は色付きで表示されます。「**ポリシーの適用先**」リストの中の国にマウスを合わせると、その国が地図上で点滅します。ズーム ツールで地図を拡大/縮小します。地図を使用しない場合は、地図の左側にある**地図**アイコンを選択して非表示にします。

- **ボットネット ポリシー**

  ボットネット ポリシーは、指定された IPv4 IP アドレスまたは IP アドレス範囲からのアクセスを許可または拒否します。最大で 64 件のポリシーが作成できます。「**ポリシー名**」を入力し、「動作」ドロップダウンでの選択に基づいて許可または拒否する「**IP アドレスまたは IP 範囲**」を選択します。

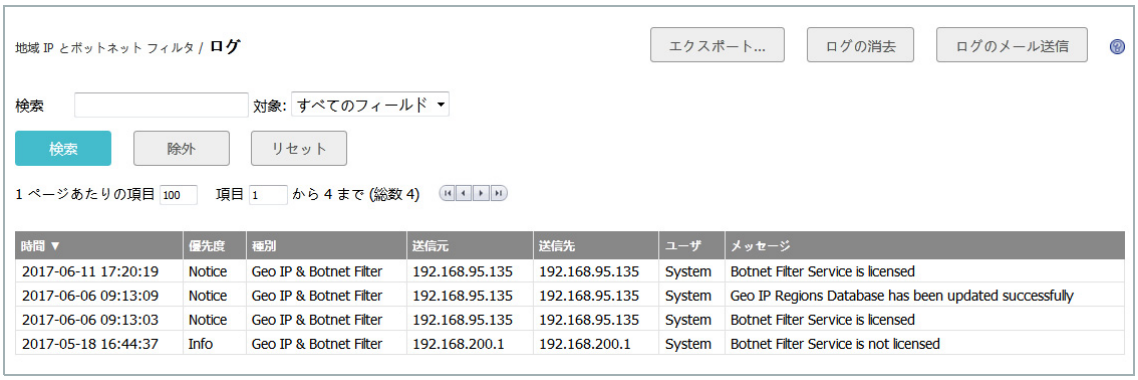
ログ

「**地域 IP とボットネット フィルタ > ログ**」ページには、地域 IP とボットネット フィルタによって検出された以下の情報が一覧表示されます。

- 地域 IP によって生成された各イベント ログ メッセージの送信元 IP の地理的な場所を識別する場所情報。場所情報は、該当する Secure Mobile Access ログと状況のページにも表示されます。地域 IP のログ記録が無効である場合は、記録されていないことを表すアイコン がこの列に表示されます。場所または国の旗がない場合は、不明を表すアイコン がこの列に表示されます。

  「場所」フィールドのアイコン上にマウスを移動させると、送信元 IP の「都市」(該当する場合)、「地域」、「国」が表示されます。

- ボットネット フィルタによって検知されたトラフィック。各 IP からのトラフィックは、拒否されたか許可されたかに関わらず、1 秒に一度だけログ記録されます。



このページでは、便利なログ検索機能やログをファイルにエクスポートする機能、メールで送信する機能など、さまざまなログ機能が利用できます。

- ログ エントリを選択すると、イベントの詳細な情報が (存在する場合は) 表示されます。
- 見出しを選択すると、ログ メッセージが見出しのアルファベット順に並べ替えられます。

ログを検索する

ログ テーブルの特定の列に含まれる値を検索したり、指定の値を**含まない**ログ エントリを検索できます。

ログを表示および検索するには:

1 「**地域 IP とボットネット フィルタ > ログ**」ページで、検索する値を「**検索**」フィールドに入力します。検索値は大文字と小文字が区別されます。

2 「検索」フィールドの右側にあるドロップダウン リストから検索の対象とする列を選択します。

3 以下のいずれかを実行します。

- 検索値を含むログ エントリの検索を開始するには、**「検索」**ボタンを選択します。
- 検索値を含まないログ エントリの検索を開始するには、**「除外」**ボタンを選択します。
- 「検索」フィールドの内容を消去し、ログ エントリの最初のページを表示するには、**「リセット」**ボタンを選択します。

ログのページ付けを調整する

1 ページに表示するログ エントリ数を調整し、エントリの表示範囲を変更するには:

1 「**地域 IP とボットネット フィルタ > ログ**」ページで、1 ページに表示するログ エントリ数を「**1 ページあたりの項目**」フィールドに入力します。「ログ」ページの表示が新しいエントリ数に変更されます。

2 特定の番号以降のログ エントリを表示するには、開始番号を**「項目」**フィールドに入力し、**Enter** キーを押します。

3 ログ エントリの最初のページを表示するには、矢印コントロール パッドの左端のボタン  を選択します。

4 ログ エントリの前のページを表示するには、矢印コントロール パッドの左向き矢印  を選択します。

5 ログ エントリの次のページを表示するには、矢印コントロール パッドの右向き矢印  を選択します。

6 ログ エントリの最後のページを表示するには、矢印コントロール パッドの右端のボタン  を選択します。

ログ ファイルのエクスポートとメール送信

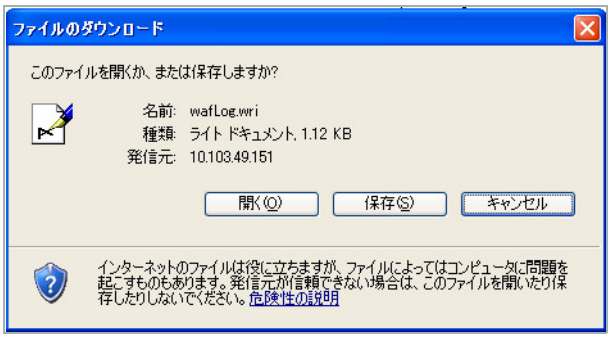
「**地域 IP とボットネット フィルタ > ログ**」ページの右上隅にあるボタンを使って、現在のログの内容をファイルにエクスポートしたり、メールで送信することができます。

エクスポートしたファイルは **.wri** ファイル名拡張子を付けて保存され、既定でワードパッドで開かれます。

メールでファイルを送信すると、Secure Mobile Access 管理インターフェースの「**ログ > 設定**」ページで設定されたアドレスに宛てて送信されます。アドレスが未設定の場合は、「**電子メール ログ**」を選択したときにエラー メッセージがブラウザ下部のステータス行に表示されます。

ログをエクスポートまたは送信するには:

1 ログの内容をエクスポートするには、「**地域 IP とボットネット フィルタ > ログ**」ページの右上隅にある「**エクスポート**」を選択します。「ファイルのダウンロード」ダイアログ ボックスが表示されます。



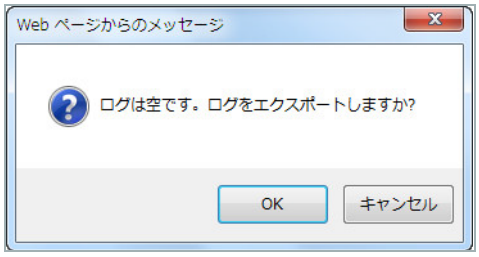
2 「ファイルのダウンロード」ダイアログ ボックスで、以下のいずれかの操作を行います。

- ファイルを開くには、「**開く**」を選択します。
- ファイルを保存するには、「**保存**」を選択してからファイルを保存するフォルダに移動し、「**保存**」を選択します。

3 ログの内容をメールで送信するには、「**地域 IP とボットネット フィルタ > ログ**」ページの右上隅にある「**電子メール ログ**」を選択します。ログの内容が、「**ログ > 設定**」ページで指定されたアドレスにメールで送信されます。

ログを消去する

「**地域 IP とボットネット フィルタ > ログ**」ページでは、ログからすべてのエントリを削除できます。ページに表示されていたエントリが削除され、その後でログ エントリがまだ追加されない状態でログ ファイルのエクスポートやメール送信を行おうとすると、確認のダイアログ ボックスが表示されます。



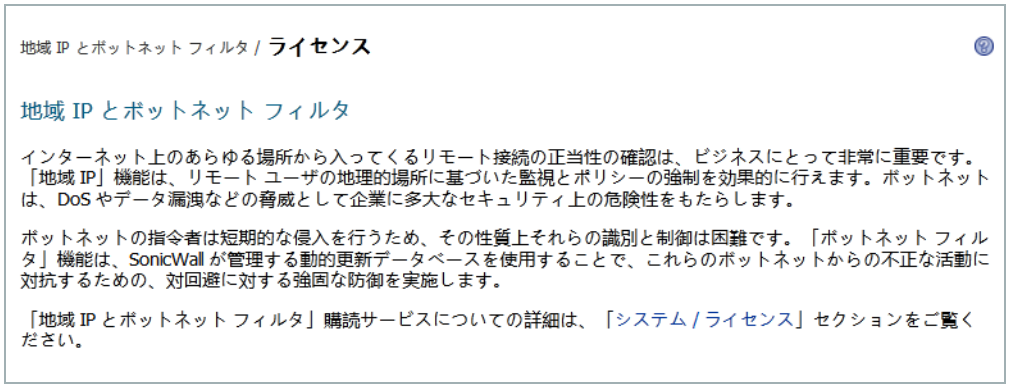
ログを消去するには、以下の手順に従います。

1 「**地域 IP とボットネット フィルタ > ログ**」ページの右上隅にある「**ログの消去**」ボタンを選択します。

2 確認のダイアログ ボックスで、「**OK**」を選択します。

ライセンス

地域 IP とボットネット フィルタは購読サービスで、リリース日の 1 年後に失効する無料トライアルが含まれています。「**地域 IP とボットネット フィルタ > ライセンス**」ページには、地域 IP とボットネット フィルタ購読サービスのライセンス状況が表示されます。



「ライセンス」ページには、この機能の簡単な説明と、ライセンスを有効化、アップグレード、更新できる「**システム > ライセンス**」ページへのリンクもあります。

15

高可用性の設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**高可用性**」ページと、このページで行う設定タスクについて説明します。

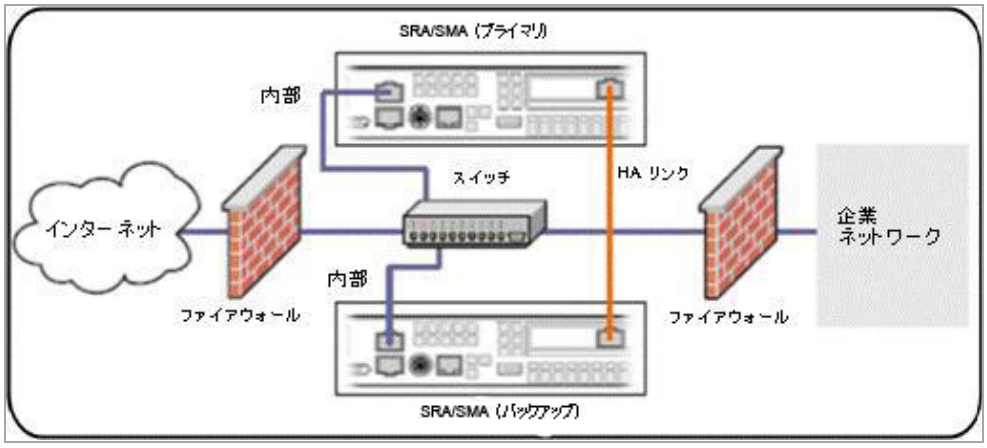
高可用性 (HA) とは、2 台の同一の SMA/SRA 装置または SMA 500v Virtual Appliance が、パブリック インターネットに対して信頼性の高い連続した接続を提供できるようにする機能です。この 2 台の SMA/SRA 装置は、同時に配備され、互いに接続されており、高可用性ペア (HA ペア) と呼ばれます。

トピック:

高可用性機能の概要

高可用性には、プライマリ装置として設定された 1 台の SMA/SRA 装置と、バックアップ装置として設定された同等の SMA/SRA が必要です。

高可用性の設定



通常運転中は、プライマリ装置がアクティブ状態で、すべての接続を提供します。バックアップ装置はアイドル状態です。プライマリ装置が接続性を失うと、バックアップがアクティブ状態に移行して、外部接続の提供を開始します。設定データとセッション データを含む、必要なデータはプライマリとバックアップの間で同期されます。

フェイルオーバーは、プライマリ装置上の機能性やネットワーク レイヤの接続の障害に適用されます。バックアップ装置へのフェイルオーバーは、重要なサービスが影響を受けた、物理(または論理)リンクの障害が検知された、またはプライマリ装置への電源供給が失われた際に発生します。

サポート対象プラットフォーム

高可用性は、SMA 400、SRA 4600、および SMA 500v Virtual Appliance でサポートされます。

高可用性の設定

高可用性 (HA) には、プライマリ装置として設定された 1 台の SMA 400、SRA 4600 または SMA 500v Virtual Appliance と、バックアップ装置として設定された同等の SMA/SRA 装置が必要です。2 台の SMA/SRA 装置間の HA 接続は、アクティブ / パッシブ状態です。セッション情報は HA ペア間で同期され、バックアップ装置へのフェイルオーバー発生時にユーザを再認証する必要がなくなります。

設定に関する情報については、以下のセクションを参照してください。

物理接続

HA 制御トラフィックのために使われるインターフェースを選択できます。HA リンクは、プライマリ装置の X3 とバックアップ装置の X3 など、SMA/SRA HA ペアの同一ポートを接続する必要があります。

通常運転中は、プライマリ装置がアクティブ状態で、すべての接続を提供する一方、バックアップ装置はアイドル状態です。プライマリ装置が接続性を失うと、バックアップがアクティブ状態に移行して、外部接続の提供を開始します。

高可用性の準備

「**高可用性 > 設定**」ページでオプションを構成する前に、高可用性のために機器を以下の手順で準備します。

1 サブネット上の独立した IP アドレスを使用して、2 つの SMA/SRA 装置を個別の機器として設定します。

ⓘ **メモ**：HA ペアの SMA/SRA 装置をプロキシを介して配備することはできません。

2 両方の機器に最新の Secure Mobile Access ファームウェアをアップロードします。HA は、両方の機器に同じファームウェア バージョンがインストールされていないと、正しく機能しません。

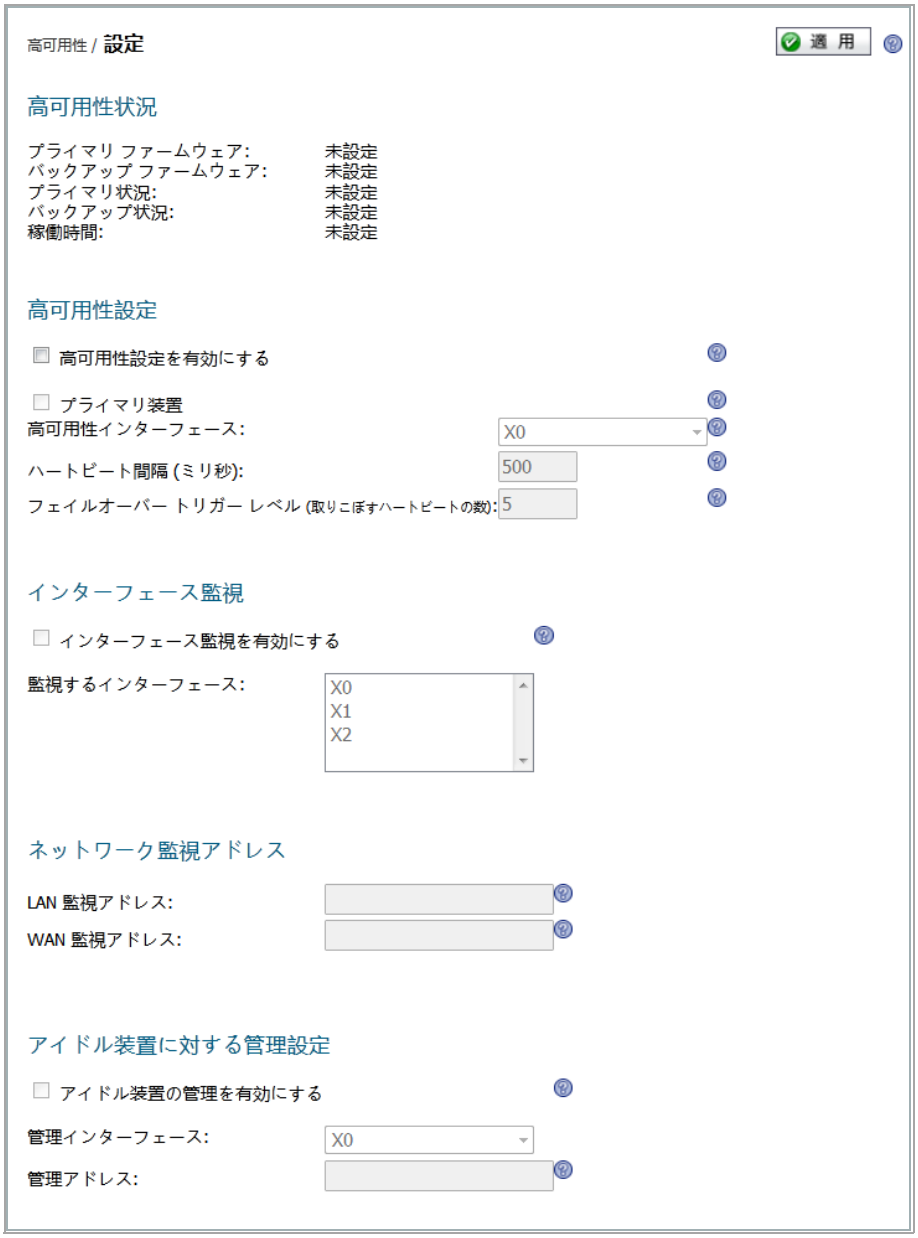
3 両方の機器の X3 インターフェースを、ギガビットの接続を確保するためにカテゴリ 5E またはより高性能なケーブルを使って接続します。

メモ：SonicWall Inc. は、この段階で両方の SMA/SRA 装置の設定をバックアップしてダウンロードしておくことを推奨します。

4 ブラウザでプライマリ装置にログインして、「**ネットワーク > インターフェース**」ページに移動します。「**状況**」を見ることで、X3 ポートがアクティブであることを確認します。「**1000 Mbps - 全二重**」と表示されているはずです。

ハードウェア装置上での高可用性の設定

「**高可用性 > 設定**」ページでは、高可用性を構成するための設定が可能です。



メモ：仮想装置に対しては、このページの内容が少し異なります。仮想装置上での高可用性の設定 (378 ページ) を参照してください。

「高可用性設定」セクションで高可用性を有効にし、オプションを設定するには:

1 ブラウザでプライマリ装置にログインして、「**高可用性 > 設定**」ページに移動します。

2 「**高可用性設定を有効にする**」をオンにします。

HA インターフェースは、装置が HA 非接続モードにある場合のみ設定できます。両方の装置に同じインターフェースを設定する必要があります。

3 ドロップダウン リストから「**高可用性インターフェース**」を選択します。HA インターフェースは、装置が HA 非接続モードにある場合のみ設定できます。両方の装置で同じインターフェースを設定する必要があります。

4 「**ハートビート間隔**」をミリ秒で入力します。ハートビートは、プライマリとバックアップ装置の間の接続性の試験に使用されます。ハートビート間隔は、2 台の装置の間の通信頻度を制御します。最小値は 500 ミリ秒 (0.5 秒) で、最大値は 300,000 ミリ秒 (5 分) です。

5 「**フェイルオーバー トリガーレベル**」の値を入力します。これは、フェイルオーバーが発生するまでに取りこぼすハートビートの数です。最小値は 4 で、最大値は 99 です。

6 「**プライマリ シリアル番号**」フィールドに、プライマリ装置のシリアル番号を入力します。最長 12 文字です。

7 「**バックアップ シリアル番号**」フィールドに、バックアップ装置のシリアル番号を入力します。最長 12 文字です。

8 「**適用**」を選択します。

9 ブラウザで、新しいページを開いてバックアップ装置の IP アドレスをポイントします。バックアップ装置にログインします。

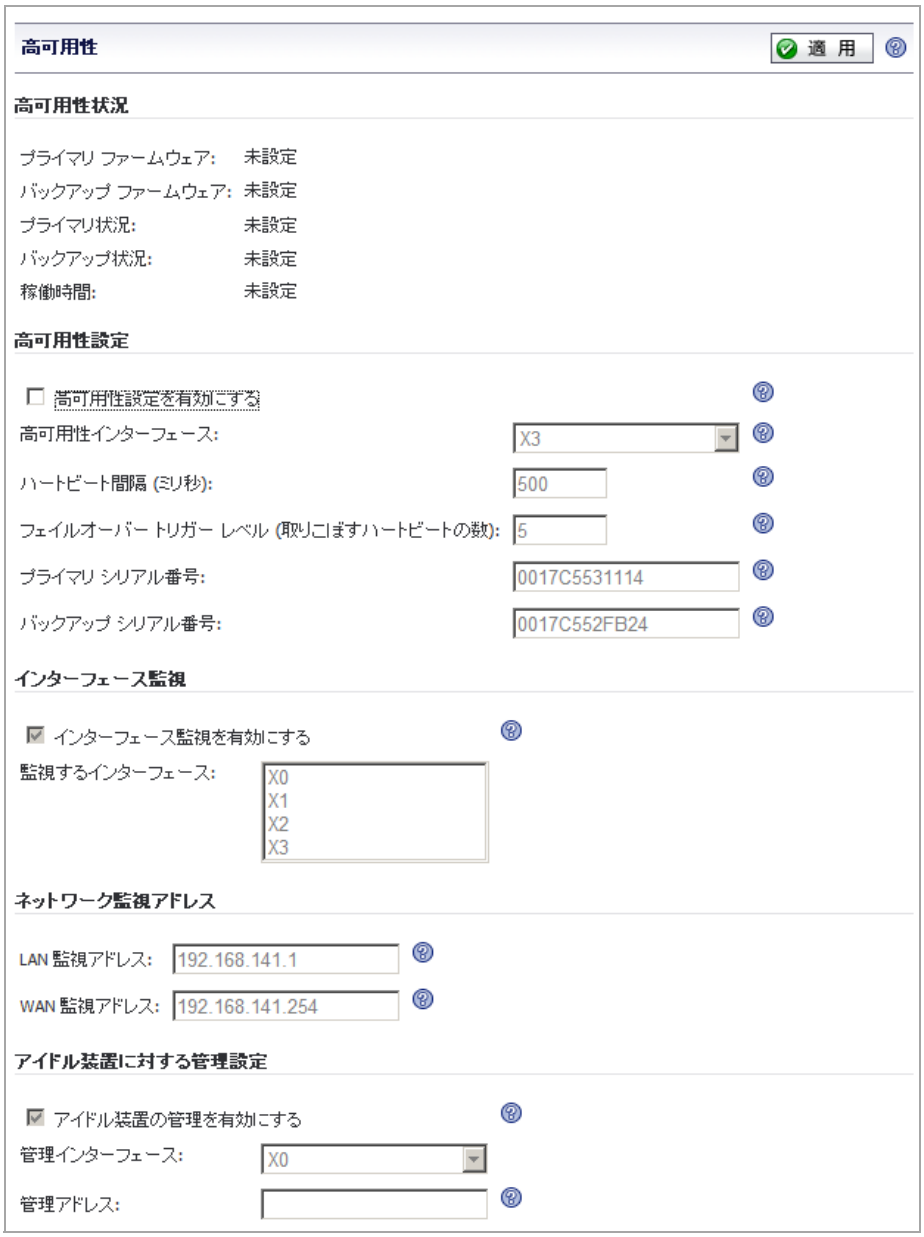
10 バックアップ装置で 1 から 8 を繰り返します。

「**適用**」を選択すると、バックアップ装置はアイドルになり、その IP アドレスを使ってアクセスできなくなります。このときプライマリ装置が HA 設定の前と同じ設定でアクティブになります。

HA ペアの装置は、すぐにプライマリからバックアップ装置へのデータの同期を開始します。フェイルオーバーが発生してプライマリがダウンした場合、バックアップ装置がプライマリと同じ設定でアクティブになります。

仮想装置上での高可用性の設定

「**高可用性 > 設定**」ページでは、高可用性を構成するための設定が可能です。



「高可用性設定」セクションで仮想装置に対して高可用性を有効にし、オプションを設定するには:

1 ブラウザでプライマリ装置にログインして、「**高可用性 > 設定**」ページに移動します。

2 「**高可用性設定を有効にする**」をオンにします。

HA インターフェースは、装置が HA 非接続モードにある場合のみ設定できます。両方の装置に同じインターフェースを設定する必要があります。

3 この仮想装置が HA ペアのプライマリ装置である場合は、「**プライマリ装置**」をオンにします。

4 ドロップダウン リストから「**高可用性インターフェース**」を選択します。HA インターフェースは、装置が HA 非接続モードにある場合のみ設定できます。両方の装置で同じインターフェースを設定する必要があります。

5 「**ハートビート間隔**」をミリ秒で入力します。ハートビートは、プライマリとバックアップ装置の間の接続性の試験に使用されます。ハートビート間隔は、2 台の装置の間の通信頻度を制御します。最小値は 500 ミリ秒 (0.5 秒) で、最大値は 300,000 ミリ秒 (5 分) です。

6 「**フェイルオーバー トリガーレベル**」の値を入力します。これは、フェイルオーバーが発生するまでに取りこぼすハートビートの数です。最小値は 4 で、最大値は 99 です。

7 「**適用**」を選択します。

8 ブラウザで、新しいページを開いてバックアップ装置の IP アドレスをポイントします。バックアップ装置にログインします。

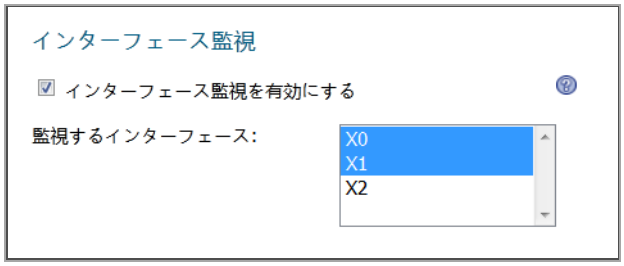
9 バックアップ装置上で高可用性を設定します。

「**適用**」を選択すると、バックアップ装置はアイドルになり、その IP アドレスを使ってアクセスできなくなります。このときプライマリ装置が HA 設定の前と同じ設定でアクティブになります。

HA ペアの装置は、すぐにプライマリからバックアップ装置へのデータの同期を開始します。フェイルオーバーが発生してプライマリがダウンした場合、バックアップ装置がプライマリと同じ設定でアクティブになります。

インターフェース監視の有効化

「高可用性 > 設定」ページの「インターフェース監視」セクションで、インターフェースの監視を有効にして監視するインターフェースを選択できます。



選択可能な監視対象のインターフェースは、X0、X1、および X2 です。インターフェース監視が有効にされて設定されると、監視されているインターフェースのどれかがアクティブ装置で接続性を失い、かつアイドル装置で到達可能のままだった場合は、フェイルオーバーが発生します。

インターフェース監視を有効にするには、以下の手順に従います。

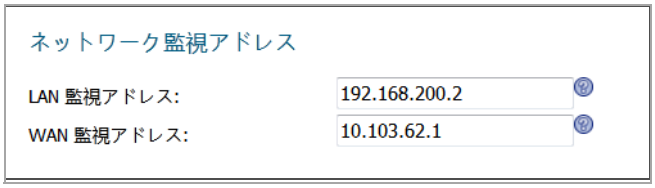
1 「**高可用性 > 設定**」ページの「インターフェース監視」の下で、「**インターフェース監視を有効にする**」をオンにします。

2 「**監視するインターフェース**」リストから、監視したいインターフェースを選択します。

3 「**適用**」を選択します。

ネットワーク監視アドレスの設定

「ネットワーク監視アドレス」セクションで、LAN および WAN IP Adoresu の監視を設定できます。ネットワーク監視が設定されると、LAN または WAN 接続がアクティブ装置で失われ、しかしアイドル装置で到達可能の場合は、フェイルオーバーが発生します。



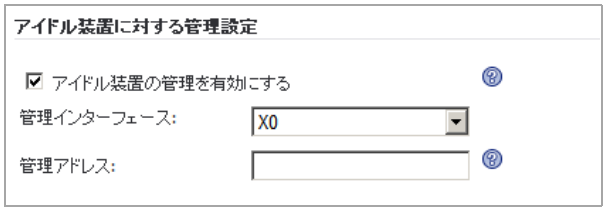
設定されると、LAN と WAN の接続状態が検出され、画面最上部の「高可用性状況」セクションに表示されます。

ネットワーク監視を設定するには、以下の手順に従います。

1. 「**高可用性 > 設定**」ページの「ネットワーク監視アドレス」の下で、「LAN 監視アドレス」フィールドに LAN IP アドレスを入力します。
2. 「WAN 監視アドレス」フィールドに WAN IP アドレスを入力します。
3. 「**適用**」を選択します。

アイドル装置に対する管理設定

「ネットワーク監視アドレス」セクションで、アイドル装置に対する管理設定ができます。



SMA 500v Virtual Appliance に対する高可用性設定には、制約があります。「**高可用性 > 設定**」ページで、SMA 500v Virtual Appliance 上の高可用性を有効にし、それをプライマリまたはセカンダリ装置として指定し、インターフェースを選択します。SMA 500v Virtual Appliance に対する管理設定を行う際には、以下の制約に注意してください。

- 高可用性は、単一ネットワーク インターフェース モードの SMA 500v Virtual Appliance 上ではサポートされません。
- ファームウェアの同期機能は、SMA 500v Virtual Appliance に対してはサポートされていません。

アイドル装置に対して管理設定を行うには、以下の手順に従います。

1 「**高可用性 > 設定**」ページの「アイドル装置に対する管理設定」の下で、「**アイドル装置の管理を有効にする**」をオンにします。

2 ドロップダウン リストを使用して**管理インターフェース**を選択します。

3 アイドル装置の管理 IP アドレスを「**管理アドレス**」フィールドに入力します。

> **メモ**：管理 IP アドレスを入力しない場合、装置の実際の状況に関係なく、「**高可用性状況 > バックアップ状況**」フィールドには "未設定" と表示されます。状況を表示したい場合は、アイドル装置の管理 IP アドレスを入力してください。

4 「**適用**」を選択します。

ファームウェアの同期

「**ファームウェアの同期**」を選択することで、HA ペアのアクティブ装置からアイドル装置にファームウェアを同期できます。

これにより、アクティブ装置を異なるバージョンにアップグレードした後で、装置間でファームウェアを同期できます。「適用」ボタンを選択してもファームウェアは同期されませんが、アクティブからアイドル装置に設定は同期されます。

> **メモ**：ファームウェアの同期は現在、SMA 500v Virtual Appliance 上ではサポートされていません。

設定の同期

「**適用**」を選択して、設定を同期します。設定を同期してもファームウェアは同期されませんが、アクティブからアイドル装置に設定が同期されます。

HA ペアの装置は、すぐにプライマリからバックアップ装置へのデータの同期を開始します。フェイルオーバーが発生してプライマリがダウンした場合、バックアップ装置がプライマリと同じ設定でアクティブになります。

ライセンスの同期

HA ペアの 2 台の SMA/SRA 装置間でライセンスを同期するには、MySonicWall.com にログインして 2 台の SMA/SRA 装置をバインドします。これによって、両方の装置でプライマリ装置のライセンス情報が共有されます。

> **メモ**：Secure Mobile Access 管理インターフェースには、HA ペアの 2 台の装置間でライセンスを同期するための機能はありません。ライセンス同期はすべて、MySonicWall を介して制御されます。

技術 FAQ

1 HA を有効にした後、アイドル装置を個別に使うことができますか?

いいえ。HA が設定されると、同時に 1 台の装置のみ使用可能です。フェイルオーバーの間は、アイドル装置がアクティブになります。HA モードの 2 台の装置は、別々の SMA/SRA 装置として使用できません。

2 HA インターフェース ケーブルを装置から抜くと、どうなりますか?

HA インターフェース ケーブルを抜くと、アイドル装置をスタンドアロンとして動作するように再設定できます。ただし、これはプライマリ装置とバックアップ装置が同じ IP 設定を有するために IP 競合を起こすことがあります。

3 HA が有効になってから HA インターフェースの設定を修正できますか?

HA が設定されると、HA インターフェースの「編集」ボタンはグレーアウトされて無効になります。したがって、装置が HA モードになった後は、HA インターフェースの設定は変更できません。

4 HA モードが設定されてから X0、X1、X2 インターフェースの設定を修正できますか?

はい。X0、X1、X2 インターフェースの設定はプライマリ装置上で修正可能で、これらの新しい設定はバックアップ装置にコピーされます。

5 装置間の同期状況は、Secure Mobile Access 管理インターフェースで確認できますか?

はい。これらは、アクティブ SMA/SRA の「**ログ > 表示**」ページで確認できます。すべてのデータの同期が終了したことを告げるログ メッセージが表示されます。

6 バックアップ装置が正しく動作していることを確認するための準備がありますか?

はい。「**ログ > 表示**」ページに、アクティブおよびアイドル装置の移行に関する多くのメッセージが表示されます。

「高可用性」ページで、装置の状況が、下図のように 1 台がアクティブでもう 1 台がアイドルになっていることを確認できます。

「ネットワーク監視アドレス」セクションで LAN および WAN 監視 IP アドレスが設定されている場合、それらのインターフェースの状況が表示されます。

「**ネットワーク > インターフェース**」ページで、X3 インターフェースの状況が、"HA Link-Connected" になっていることを確認できます。

7 ファームウェアと設定はアイドル装置に同期されますか?

はい。アクティブとアイドル ノードの間では、ファームウェアと設定の両方が同期されます。「ファームウェアの同期」ボタンにより、アクティブからアイドル装置にファームウェアを同期できます。設定が変更された場合は、「**適用**」を選択すると設定が同期されます。

8 SMA/SRA 装置の HA 設定は、SonicWall Inc. ファイアウォール機器の HA 設定と異なりますか?

はい。ファイアウォールの HA 設定は大きく異なります。他の HA 機能と協調して、ファイアウォールの HA はアクティブ/アクティブ 状態が利用可能で、仮想 IP アドレスを割り当てることができます。SMA/SRA 装置の HA は、現状はアクティブ/パッシブ モードのみ利用可能です。

9 アイドル装置に設定を適用するには、どうすれば良いですか?

HA 設定が完了するとすぐに、設定はアクティブ装置からアイドル装置にコピーされます。これの成功は、アクティブ機器のイベント ログ メッセージで確認できます。

10 バックアップ装置の設定では、何が起こりますか?

アイドル装置の設定は削除され、アクティブ機器の設定に置き換わります。バックアップ装置の設定を保持したい場合は、HA に切り替える前に設定のバックアップをダウンロードしておくことを推奨します。

11 バックアップ装置の状況はどのようにして確認しますか ?

「**高可用性 > 設定」ページの「アイドル装置に対する管理設定**」の下で、アイドル装置の管理 IP アドレスを「管理アドレス」フィールドに入力し、「**適用**」を選択します。「**高可用性状況**」に移動すると、「**バックアップ状況**」フィールドに状況が表示されます。アイドル装置の管理 IP アドレスを入力しない場合は、「バックアップ状況」に "未設定" と表示されます。

12 プロキシを介して HA ペアを配備できますか ?

いいえ。HA ペアの SMA/SRA 装置をプロキシを介して配備することはできません。HA ペアの装置は、バックエンド サーバと直接通信して、シグネチャのダウンロードなどを行います。

第 2 部

ユーザとログの設定

- ユーザの設定
- ログの設定

16

ユーザの設定

このセクションでは、ユーザとグループのアクセス ポリシーやブックマークなど、ウェブベースの Secure Mobile Access 管理インターフェースの「**ユーザ**」ページに関する情報や固有の設定タスクについて説明します。ポリシーは、SMA/SRA 装置で定義されているオブジェクトに、さまざまなレベルでアクセスできるようにするものです。

トピック:

ユーザ > 状況

「**ユーザ > 状況**」ページには、SMA/SRA 装置にログインしているユーザと管理者に関する情報が表示されます。このセクションでは、一連の階層型のポリシーを使って SMA/SRA 装置でユーザを管理する方法について、概要を説明します。

このセクションは次のサブセクションで構成されています。

「ユーザ > 状況」ページ

「**ストリーミング更新**」が「**オン**」の場合、「**ユーザ > 状況**」ページの内容は、常に最新の情報が表示されるよう自動的に更新されます。「**オン**」を押すことにより、「**オフ**」に切り替わります。

「**現在のユーザ**」テーブルには、SMA/SRA 装置にログインしている現在のユーザまたは管理者が表示されます。エントリには、ユーザの名前、ユーザが属するグループ、ユーザがログインしているポータル、ユーザの IP アドレス、ユーザがログインした時間を示すタイムスタンプ、セッションの経過時間、およびセッションの累積無動作時間が表示されます。管理者は、ユーザの右側に表示されているログアウト アイコンを選択することで、直ちにユーザ セッションを終了してユーザをログアウトさせることができます。「**現在のユーザ**」テーブルには、以下の情報が表示されます。

アクティブなユーザの情報

列	説明
名前	ユーザの ID を示す文字列
グループ	ユーザが属するグループ
ポータル	ユーザがログインしているポータル
IP アドレス	ユーザがログインしているワークステーションの IP アドレス
場所	各ユーザの送信元 IP の地理的な場所
ログイン時間	ユーザが SMA/SRA 装置との接続を最初に確立した時間 (曜日、日付、および時刻 (HH:MM:SS) の形式)
ログイン経過時間	ユーザが SMA/SRA 装置との接続を最初に確立してからの経過時間 (日数と時間数 (HH:MM:SS) の形式)
無動作時間	ユーザが SMA/SRA 装置に対してアクティブではない状態または無動作の状態だった時間
ログアウト	ユーザを装置からログアウトさせることができるアイコン

アクセス ポリシーの概念

ウェブベースの Secure Mobile Access 管理インターフェースでは、SMA/SRA 装置へのアクセスを細かく制御することができます。アクセス ポリシーは、SMA/SRA 装置を使ってアクセスできる各種のネットワーク リソースに、さまざまなレベルでアクセスできるようにするものです。アクセス ポリシーには、グローバル、グループ、ユーザの 3 つのレベルがあります。特定の IP アドレス、IP アドレス範囲、すべてのアドレス、またはネットワーク オブジェクトに対してアクセス ポリシーを作成することによって、アクセスを遮断または許可することができます。

アクセス ポリシー階層

管理者は、ユーザ、グループ、グローバルの各ポリシーを、定義済みネットワーク オブジェクト、IP アドレス、アドレス範囲、すべての IP アドレス、および各種の Secure Mobile Access サービスに対して定義することができます。ポリシーには優先度があります。

Secure Mobile Access ポリシー階層は次のように構成されています。

- ユーザ ポリシーはグループ ポリシーよりも優先される
- グループ ポリシーはグローバル ポリシーよりも優先される
- 複数のユーザ、グループ、またはグローバル ポリシーが設定されている場合は、最も限定的なポリシーが優先される

例えば、特定の IP アドレスに設定されたポリシーは、アドレス範囲に設定されたポリシーよりも優先されます。IP アドレス範囲に適用されるポリシーは、すべての IP アドレスに適用されるポリシーよりも優先されます。複数の IP アドレス範囲が設定されている場合は、最も小さいアドレス範囲が優先されます。ホスト名は個別の IP アドレスと同等に扱われます。

ネットワーク オブジェクトの優先度はアドレス範囲と似ています。ただし、ネットワーク オブジェクト全体ではなく、個別のアドレスまたはアドレス範囲で優先度が決まります。

以下に例を示します。

- ポリシー 1: IP アドレス範囲 10.0.0.0 - 10.0.0.255 へのすべてのサービスを阻止する拒否ルール
- ポリシー 2: 10.0.1.2 - 10.0.1.10 への FTP アクセスを阻止する拒否ルール
- ポリシー 3: 定義済みネットワーク オブジェクト (FTP Servers) への FTP アクセスを許可する許可ルール。FTP Servers ネットワーク オブジェクトには、アドレス範囲 10.0.0.5 - 10.0.0.20 が指定されている。さらに、ftp.company.com が指定されており、これは 10.0.1.3 に解決される。

競合するユーザ ポリシーまたはグループ ポリシーは設定されていないと仮定します。ユーザが以下のサーバへのアクセスを試みた場合、結果は次のようになります。

- FTP サーバ (10.0.0.1)。ユーザはポリシー 1 によって阻止されます。
- FTP サーバ (10.0.1.5)。ユーザはポリシー 2 によって阻止されます。
- FTP サーバ (10.0.0.10)。ユーザはポリシー 3 によってアクセスを許可されます。IP アドレス範囲 10.0.0.5 - 10.0.0.20 は、ポリシー 1 で定義されている IP アドレス範囲よりも限定的です。
- FTP サーバ (ftp.company.com)。ユーザはポリシー 3 によってアクセスを許可されます。特定のホスト名は、ポリシー 2 で設定されている IP アドレス範囲よりも限定的です。

メモ：この例では、ユーザは IP アドレス 10.0.1.3 を使って ftp.company.com にアクセスすることはできません。Secure Mobile Access のポリシー エンジンは、DNS の逆引きを行いません。

ヒント：Citrix ブックマークを使用するときには、ホストへのプロキシ アクセスを制限するために、Citrix サービスと HTTP サービスの両方に対して拒否ルールを設定する必要があります。

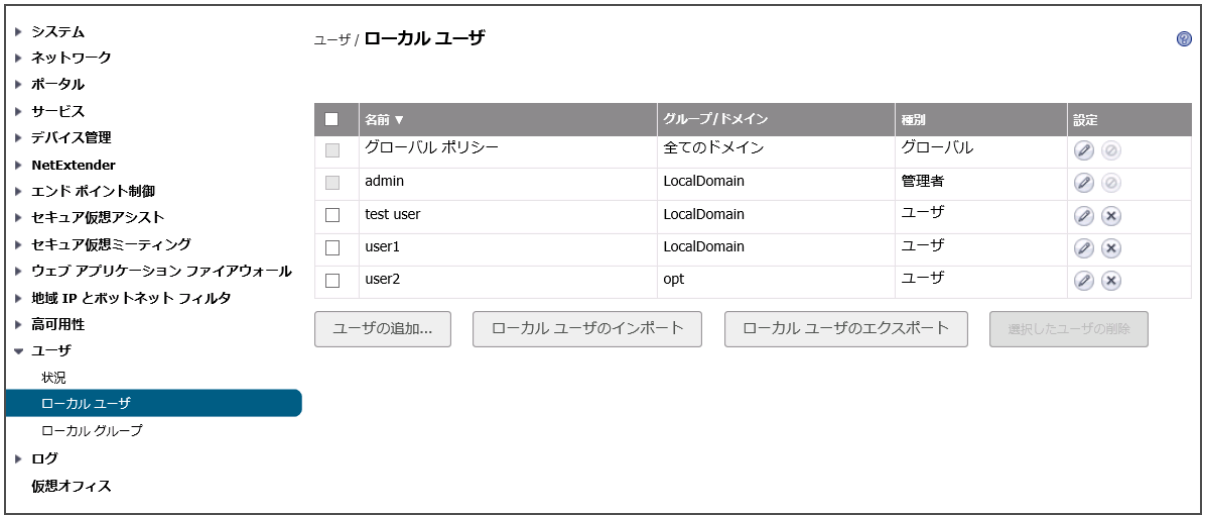
ユーザ > ローカル ユーザ

このセクションでは、「**ユーザ > ローカル ユーザ**」ページの概要と、このページで行える設定タスクについて説明します。

グローバルな設定については、「グローバル設定 (474 ページ)」を参照してください。

「ユーザ > ローカル ユーザ」の概要

ユーザ > ローカル ユーザのページで、ユーザのインポート、エクスポート、追加、設定、削除ができます。



ローカル ユーザ

「ローカル ユーザ」のページでは、ユーザ名の指定、グループとドメインの選択、パスワードの作成と確認、およびユーザ タイプ (ユーザ、管理者、または読み込み専用管理者) の選択を行うことによって、ユーザを追加および設定できます。

メモ：RADIUS、LDAP、またはアクティブ ディレクトリ認証を使うように設定されたユーザは、外部認証サーバがユーザ名とパスワードを検証するので、パスワードを必要としません。

ヒント：RADIUS およびアクティブ ディレクトリを使ってユーザが認証された場合は、ローカル ユーザ データベース内に外部ユーザが作成されます。ただし、管理者はこのユーザのグループを変更することができません。RADIUS またはアクティブ ディレクトリを使用するときに、ユーザ グループごとに異なるポリシーを指定したい場合は、ローカル ユーザ データベースにユーザを手動で作成する必要があります。

ユーザの削除

ユーザを削除するには、「**ユーザ > ローカル ユーザ**」を開いて、削除するユーザの名前の横にある削除アイコンを選択します。削除されたユーザは、「**ローカル ユーザ**」ウィンドウから消えます。

ローカル ユーザの追加

新しいローカル ユーザを作成するには:

1 「**ユーザ** > **ローカル ユーザ**」ページを開いて、「**ユーザの追加**」を選択します。「**ローカル ユーザの追加**」ウィンドウが表示されます。

2 「**ローカル ユーザの追加**」ウィンドウで、ユーザのユーザ名を「**ユーザ名**」フィールドに入力します。これは、Secure Mobile Access ユーザ ポータルにログインするためにユーザが入力する名前です。

3 ユーザが所属するドメインの名前を「**ドメイン**」ドロップダウン リストで選択します。

4 ユーザが所属するグループの名前を「**グループ**」ドロップダウン リストで選択します。

5 ユーザのパスワードを「**パスワード**」フィールドに入力します。

6 同じパスワードを「**パスワードの確認**」フィールドにもう一度入力してパスワードを確認します。

> **メモ**：ポータル ログインの際は、ユーザ名は大文字と小文字の区別はありませんが、パスワードとドメインは大文字と小文字が区別されます。

7 必要に応じて、ローカル ユーザ データベースのユーザに対し、設定された間隔で、または次回のログイン時に、必ずパスワードを変更するよう求めます。設定された間隔で必ずパスワードを変更させるには、「**パスワードを *x* 日で失効させる**」フィールドに失効間隔を入力します。

8 パスワードの失効間隔を設定する場合は、「**パスワード失効の *x* 日前に警告を表示する**」フィールドに、失効の何日前にユーザに通知を送信するかを入力します。

これを設定し、パスワードの失効が近づくと、ユーザの「仮想オフィス」ページ、または管理者の管理コンソールに、パスワード失効までの日数を示す通知が表示されます。通知とともに、パスワードを変更する画面へのリンクも表示されます。

9 必要に応じて、「**次回ログイン時にパスワードの変更を要求する**」で、「**ドメイン設定を使用**」または「**有効**」を選択して、次回のログイン時にユーザに必ずパスワードを変更させます。「**ドメイン設定を使用**」を選択すると、「**ポータル > ドメイン**」ページでの設定が適用されます。

10 「**アカウントが期限切れになる日**」の設定で、プルダウン カレンダーを使って有効期限の日付を設定できます。設定しない場合、アカウントは無期限になります。

11 「**ユーザ種別**」ドロップダウン リストで、ユーザ種別オプションを選択します。選択できるユーザ種別は「**ユーザ**」、「**管理者**」または「**読み込み専用管理者**」です。

> **ヒント**：選択したグループのドメインで、アクティブ ディレクトリ、RADIUS、LDAP などの外部認証が使われている場合は、「**ユーザの追加**」ウィンドウが閉じ、新しいユーザが「**ローカル ユーザ**」リストに追加されます。

12 「**適用**」を選択して設定を更新します。ユーザを追加すると、新しいユーザが「**ローカル ユーザ**」ウィンドウに表示されます。

> **メモ**：RADIUS、LDAP、およびアクティブ ディレクトリのユーザ名の入力が必要になるのは、ユーザごとに個別のポリシーやブックマークを定義する場合だけです。ユーザが SMA/SRA 装置で定義されていなければ、グローバルなポリシーとブックマークが、外部認証サーバの認証を受けるユーザに適用されます。外部 (非 LocalDomain) ユーザを操作するときは、ユーザ作成 (個人) のブックマークを Secure Mobile Access の設定ファイル内に保存できるように、ローカル ユーザ エンティティが存在していなければなりません。ブックマークを SMA/SRA 装置に保存する必要があるのは、LDAP および RADIUS の外部ドメインが、この情報をブックマークとして保存する仕組みを備えていないからです。個人のブックマークを使用する外部ドメイン ユーザのために、管理者がローカル ユーザを手動で作成せずに済むように、外部ドメイン ユーザが個人のブックマークを作成すると、SMA/SRA 装置は対応するローカル ユーザ エンティティを自動的に作成し、ブックマーク情報を保存できるようにします。

ローカル ユーザのインポート

「ローカル ユーザのインポート」では、JSON 形式を使用して、新規ユーザを外部ファイルからインポートできます。この形式は、新規ユーザとその属性に関する有効な情報を後で提供するために使用できます。

新しいローカル ユーザをインポートするには、以下の手順に従います。

1 「**ユーザ > ローカル ユーザ**」に移動します。

2 「**ローカル ユーザのインポート**」を選択します。「**ローカル ユーザのインポート**」ページが表示されます。

3 「**参照**」を使用して、JSON 形式のローカル ユーザ ファイルの場所に移動してそれを選択し、「**インポート**」をクリックします。

4 「**ユーザが存在する場合、ユーザ設定を保持する**」が有効の場合は、既存ユーザを保持します。無効の場合は、既存ユーザを上書きします。

ローカル ユーザのエクスポート

「ローカル ユーザのエクスポート」では、追加したすべてのユーザを含む JSON ファイルをエクスポートできます。このファイル形式は、新規ユーザとその属性に関する有効な情報を後で提供するために使用できます。

すべてのローカル ユーザを含むファイルをエクスポートするには、次の手順に従います。

1 「ユーザ > ローカル ユーザ」に移動します。

2 「**ローカル ユーザのエクスポート**」を選択します。すべてのローカル ユーザ (既定の「admin」ユーザは除く) が、ローカル ディレクトリにダウンロードされます。

ユーザ設定の編集

ユーザの属性を編集するには、「**ユーザ** > **ローカル ユーザ**」ウィンドウを開いて、設定を変更するユーザの横にある「設定」アイコンを選択します。「**ユーザ設定の編集**」ウィンドウが表示されます。

次の表に示すとおり、「**ローカル ユーザの編集**」ページにはそれぞれのページがあります。

「ローカル ユーザの編集」ページ

Tab	説明
一般	パスワードおよび無動作タイムアウトを設定し、このユーザのブックマークに自動でログインするためのシングル サインオンの設定を指定する
グループ	グループ メンバーシップの追加、プライマリ グループの設定、およびログイン時にグループを自動的に割り当てるかどうかの制御が可能
ポータル	NetExtender、ファイル共有、仮想アシスト、ブックマークの設定を有効化/無効化したり、グループ設定を使用する
クライアント	NetExtender クライアント アドレス範囲 (IPv6 の場合は「VPN 常時有効」も含む) や Mobile Connect の既定のポリシー設定を指定する。クライアントの設定を構成する。
ルート	トンネルオール モードと NetExtender クライアント ルートを指定する
ポリシー	装置のユーザ セッションからリソースへのアクセスを制御するアクセス ポリシーを作成する
ブックマーク	サービスに簡単にアクセスするためのブックマークをユーザ レベルで作成する
ログイン ポリシー	特定の送信元 IP アドレスやクライアント ブラウザに関するポリシーなど、ユーザ ログイン ポリシーを作成する。ユーザ ログインを無効化する。ワンタイム パスワードを要求する。ワンタイム パスワードの設定を編集する。クライアント証明書の強制を指定する
EPC	ローカル グループによって使用されるエンド ポイント制御プロファイルを設定する
キャプチャ	「一般設定」、「ファイル設定」、「ユーザ定義の遮断動作」を構成する

ユーザが外部認証サーバの認証を受ける場合、「**ユーザ種別**」フィールドと「**パスワード**」フィールドは表示されません。「パスワード」フィールドを設定できないのは、認証サーバがパスワードを検証するからです。「ユーザ種別」を設定できないのは、SMA/SRA 装置では、内部ユーザ データベースの認証を受けたユーザしか管理者権限を持つことができないからです。また、ユーザ種別「**External**」は、外部認証ユーザに対応して自動的に作成されるローカル ユーザ インスタンスを識別するために使用されます。

「**ユーザ設定の編集**」ウィンドウの各ページで使用できる設定オプションについては、以下のセクションを参照してください。

- 一般ユーザ設定の変更 (392 ページ)
- グループ設定の変更 (394 ページ)
- ポータル設定の変更 (394 ページ)
- クライアント設定の変更 (395 ページ)

- NetExtender クライアント ルートの変更 (402 ページ)
- ユーザ ポリシーの追加 (402 ページ)
- ユーザ ブックマークの追加または編集 (409 ページ)
- ログイン ポリシーの設定 (434 ページ)
- ユーザに対するエンド ポイント制御の設定 (437 ページ)
- キャプチャ ATP の設定 (437 ページ)

一般ユーザ設定の変更

「**一般**」ページには、ユーザのパスワード、無動作タイムアウトの値、およびブックマーク シングル サインオン (SSO) 制御の設定オプションがあります。アプリケーションのサポート 表 は、SSO、グローバル/グループ/ユーザ ポリシー、およびブックマーク ポリシーに対するアプリケーションごとのサポートの一覧表です。

アプリケーションのサポート

アプリケーション	SSO のサポート	グローバル/グループ/ユーザ ポリシー	ブックマーク ポリシー
ターミナル サービス (RDP - ActiveX)	はい	はい	はい
ターミナル サービス (RDP - Java)	はい	はい	はい
ターミナル サービス (RDP - HTML5)	はい	はい	はい
仮想ネットワーク コンピューティング (VNC - HTML5)	はい	はい	はい
ファイル転送プロトコル (FTP)	はい	はい	はい
Telnet	いいえ	はい	はい
Telnet (HTML5)	はい	はい	はい
セキュア シェル (SSH)	いいえ	はい	はい
ウェブ (HTTP)	はい	はい	はい
セキュア ウェブ (HTTPS)	はい	はい	はい
ファイル共有 (CIFS)	はい	はい	はい
Citrix Portal (Citrix)	いいえ	はい	はい

メモ：SSO は、二段階認証と併用することはできません。

一般ユーザ設定を変更するには:

1 左側の列で、「**ユーザ** > **ローカル ユーザ**」を開きます。

2 設定するユーザの横にある設定アイコンを選択します。「**ユーザ設定の編集**」ウィンドウの「**一般**」ページが表示されます。「**一般**」ページの「**ユーザ名**」、「**プライマリ グループ**」、「**所属するドメイン**」、および「**ユーザ種別**」は、設定できないフィールドです。これらのフィールドに表示される情報を変更する必要がある場合は、ユーザの削除 (388 ページ) の説明に従ってユーザを削除し、再度ユーザを追加します。

3 ユーザのパスワードを設定または変更するには、「**パスワード**」フィールドにパスワードを入力します。さらに、「**パスワードの確認**」フィールドに同じパスワードを入力します。

4 必要に応じて、ローカル ユーザ データベースのユーザに対し、設定された間隔で、または次回のログイン時に、必ずパスワードを変更するよう求めます。設定された間隔で必ずパスワードを変更させるには、「**パスワードを *x* 日で失効させる**」フィールドに失効間隔を入力します。次回のログイン時に必ずパスワードを変更させるには、「**次回ログイン時にパスワードの変更を要求する**」をオンにします。

メモ : 特定のローカル ドメインのユーザにパスワードの変更を求めることもできます。「**ユーザ > ローカル ユーザ > 編集**」ページの「**一般**」ページを使用してください。

5 パスワードの失効間隔を設定する場合は、「**パスワード失効の *x* 日前に警告を表示する**」フィールドに、失効の何日前にユーザに通知を送信するかを入力します。

これを設定し、パスワードの失効が近づくと、ユーザの「仮想オフィス」ページ、または管理者の管理コンソールに、パスワード失効までの日数を示す通知が表示されます。通知とともに、パスワードを変更する画面へのリンクも表示されます。

6 ユーザの無動作タイムアウトを設定し、指定した時間が経過したらユーザを仮想オフィスからログアウトさせるには、許容する無動作時間 (分) を「**無動作タイムアウト**」フィールドに入力します。ワンタイム パスワードが設定されているユーザの場合、タイムアウト値はワンタイム パスワードの有効な時間 (分) も制御します。

無動作タイムアウトは、ユーザ、グループ、グローバルの各レベルで設定できます。特定のユーザに複数のタイムアウトが設定されている場合は、ユーザ タイムアウトの設定がグループ タイムアウトよりも優先され、グループ タイムアウトがグローバル タイムアウトよりも優先されます。グローバル タイムアウトを 0 に設定すると、グループまたはユーザ タイムアウトが設定されていないユーザの無動作タイムアウトは無効になります。

7 このグループのユーザが自分自身のブックマークを編集または削除できるようにするには、「**ユーザのブックマークの編集/削除を許可**」ドロップダウン メニューで「**許可**」を選択します。ユーザが自分自身のブックマークを編集または削除できないようにするには、「**拒否**」を選択します。グループ ポリシーを使用するには、「**グループ アカウント ポリシーの使用**」を選択します。

メモ : ユーザはグループおよびグローバル ブックマークを編集または削除できません。

8 ユーザが新しいブックマークを追加できるようにするには、「**ユーザにブックマークの追加を許可する**」ドロップダウン メニューで「**許可**」を選択します。ユーザが新しいブックマークを追加できないようにするには、「**拒否**」を選択します。グループ ポリシーを使用するには、「**グループ アカウント ポリシーの使用**」を選択します。

ブックマークの変更を制御することにより、事前定義されたソースへの個別アクセスが可能になり、ユーザがサポートを必要としないようにすることができます。

9 「**シングル サインオン設定**」で、「**自動的にブックマークにログイン**」ドロップダウン メニューから、次のいずれかのオプションを選択します。

- **グループ設定を使用する**: グループ ポリシーの設定を使ってブックマークのシングル サインオン (SSO) を制御します。
- **ユーザ制御**: ブックマークのシングル サインオン (SSO) をユーザが有効または無効にできるようにします。
- **有効**: ブックマークのシングル サインオンを有効にします。

- **無効**: ブックマークのシングル サインオンを無効にします。

メモ：SSO の変更を制御することにより、セキュリティが強化され、異なるログイン資格情報の利用をユーザに禁止または許可することができます。SSO が有効になっている場合は、ユーザのログイン名とパスワードが多くのサービスのためにバックエンド サーバに提示されます。ファイル共有では、機器上でユーザが所属するドメイン名がサーバに渡されます。その他のサービスでは、先頭にドメイン名の付いたユーザ名をサーバが想定している場合があります。この場合、SSO は失敗し、ユーザは先頭にドメイン名の付いたユーザ名を使ってログインする必要があります。場合によっては、サーバで既定のドメイン名を設定すると SSO が成功することがあります。

10 「**適用**」を選択して設定の変更を保存します。

グループ設定の変更

「**グループ**」ページで、ユーザに対するグループ メンバーシップの追加、プライマリ グループの設定、およびユーザ ログイン時にグループを自動的に割り当てるかどうかの制御が可能です。

アクティブ ディレクトリ、LDAP、および RADIUS ドメインにログインするユーザは、外部 AD グループ メンバーシップ、LDAP 属性、または RADIUS フィルタ ID に基づいて、リアルタイムで Secure Mobile Access グループに自動的に割り当てられます。

メモ：ユーザの外部グループ メンバーシップが変更された場合は、Secure Mobile Access グループ メンバーシップが外部グループ メンバーシップに対応するように自動的に変更されます。

「グループ」ページ上の設定を行うには、以下の手順に従います。

1 グループをプライマリ グループとして設定するには、プライマリに設定したいグループに対応する、プライマリ グループ設定の星印を選択します。

2 ユーザがメンバーになるグループを追加するには、「**グループの追加**」を選択します。グループは、「**ユーザ > ローカル グループ**」で設定済みである必要があります。

3 ドロップダウン リストから希望するグループを選択します。

4 これをユーザのプライマリ グループ メンバーシップにするには、「**プライマリ グループに設定する**」をオンにします。

5 「**グループの追加**」を選択して、選択したグループを「**グループ　メンバーシップ**」のリストに追加します。

6 「**グループ設定**」の下で、「**ログイン時にグループを自動的に割り当てる**」ドロップダウン リストから以下のうち 1 つを選択します。

- **グループ設定を使用する** - グループに対して設定されている設定を使います。
- **有効** - ログイン時のユーザのグループへの自動割当を有効にします。
- **無効** - ログイン時のユーザのグループへの自動割当を無効にします。

7 「**適用**」を選択します。

ポータル設定の変更

「**ポータル**」ページには、このユーザのポータル設定用のオプションがあります。

このユーザのポータル設定を構成するには:

1 「**ポータル**」ページの「**ポータル設定**」下で、以下のいずれか 1 つのポータル設定をこのユーザに選択します。

- **グループ設定を使用する** - このユーザが属するグループに定義された設定を使用して、ポータル機能を有効にするか無効にするかを決定します。グループ設定は、「**ユーザ > ローカル ユーザ**」ページでグループを設定すると定義されます。
- **有効** - このポータル機能をこのユーザに有効にします。
- **無効** - このポータル機能をこのユーザに無効にします。

以下のポータル機能を上記の設定の 1 つに指定できます。

- **NetExtender** - Mobile Connect は装置への接続時に NetExtender クライアントとして動作するため、この設定は NetExtender と Mobile Connect の両方に適用されます。
- ログインした後、NetExtender を起動する
- ファイル共有
- 仮想アシスト技術者
- 仮想アシストのサポートの要求
- 仮想アシスト設定のリンク
- ブックマークの追加を許可する
- **ユーザのブックマークの編集/削除を許可** - ユーザ自身のブックマークにのみ適用されます。

2 「**適用**」を選択します。

クライアント設定の変更

この機能は外部ユーザ用です。外部ユーザはログイン時に、割り当てられたグループから設定を継承します。NetExtender クライアント設定はユーザに対して、またはグループ設定を使って指定できます。グループ設定の構成に関する情報については、グループ設定の編集 (442 ページ) を参照してください。

ユーザに対して NetExtender/Mobile Connect の範囲を有効にして、静的なクライアント設定を構成するには:

1 「**ユーザ > ローカル ユーザ**」に移動します。

2 設定するユーザの横にある設定アイコンを選択します。

3 「**ローカル ユーザの編集**」ページで、「**クライアント**」ページを選択します。

a 「**クライアント アドレス範囲**」の下で、ドロップダウン リストから「**静的プールを使用**」を選択します。

b 「**クライアント アドレス範囲の開始**」フィールドに、クライアント IPv4 アドレス範囲の開始アドレスを入力します。

c 「**クライアント アドレス範囲の終了**」フィールドに、クライアント IPv4 アドレス範囲の終了アドレスを入力します。

d 「**クライアント IPv6 アドレス範囲**」の下で、必要に応じて、ドロップダウン リストから「**静的プールを使用**」を選択します。

e 「**クライアント アドレス範囲の開始**」フィールドに、クライアント IPv6 アドレス範囲の開始アドレスを入力します。

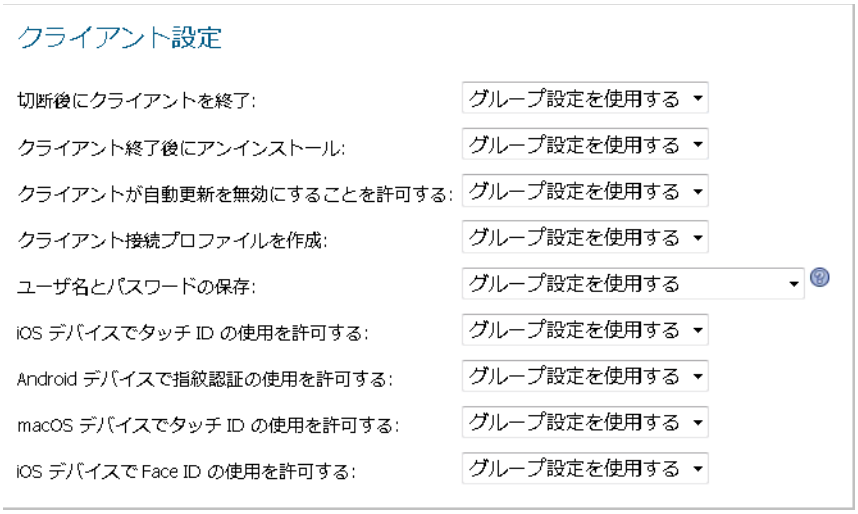
f IPv6 を使用する場合は、「**クライアント アドレス範囲の終了**」フィールドに、クライアント IPv6 アドレス範囲の終了アドレスを入力します。

4 「**DNS 設定**」で、以下の操作を行います。

以下のフィールドに入力します。

- **プライマリ DNS サーバ:**「**プライマリ DNS サーバ**」フィールドにプライマリ DNS サーバのアドレスを入力します。
- **セカンダリ DNS サーバ:** オプションで、「**セカンダリ DNS サーバ**」フィールドにセカンダリ サーバのアドレスを入力します。
- **DNS 検索リスト (検索順):** DNS ドメインの接尾辞を入力し、「**追加**」をクリックします。続いて、上下方向の矢印を使用して、複数の DNS ドメインを使用されるべき順序に並べ替えます。
    - Apple iPhone、iPad、その他の iOS 端末からの SonicWall Mobile Connect を使った接続をサポートする SMA/SRA 装置に対しては、この DNS 検索リストを使用してください。この DNS ドメインは、iPhone/iPad の VPN インターフェース上に、機器が装置との接続を確立した後で設定されます。モバイル機器のユーザがある URL にアクセスする際に、iOS はこのドメインが VPN インターフェースのドメインと一致しているかどうかを判断し、一致している場合は VPN インターフェースの DNS サーバを使ってホスト名検索を解決します。そうでない場合は、組織のイントラネット内のホストを解決できない Wi-Fi または 3G の DNS サーバが使われます。

5 「**クライアント設定**」で、以下の操作を行います。



「**切断後にクライアントを終了**」ドロップダウン リストで次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

6 「**クライアント終了後にアンインストール**」ドロップダウン リストで、次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

7 「**クライアントが自動更新を無効にすることを許可する**」ドロップダウン リストで、以下のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

8 「**クライアント接続プロファイルを作成**」ドロップダウン リストで、次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

9 「**ユーザ名とパスワードの保存**」ドロップダウン リストで、次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。

- **ユーザ名だけ保存を許可** - ユーザ名のキャッシュを許可します。NetExtender を起動するときにユーザはパスワードのみを入力する必要があります。この設定はグループ設定に優先します。
- **ユーザ名とパスワードの保存を許可** - ユーザ名とパスワードのキャッシュを許可します。NetExtender を起動すると自動的にログインします。この設定はグループ設定に優先します。
- **ユーザ名とパスワードの保存を禁止** - ユーザ名とパスワードのキャッシュを許可しません。NetExtender を起動するときにユーザはユーザ名とパスワードの両方を入力する必要があります。この設定はグループ設定に優先します。

10 このオプションが無効になっている場合、「**iOS デバイスでタッチ ID の使用を許可する**」では、iOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

11 このオプションが無効になっている場合、「**Android デバイスで指紋認証の使用を許可する**」では、Android デバイスでの指紋認証による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

12 このオプションが無効になっている場合、「**macOS デバイスでタッチ ID の使用を許可する**」では、macOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

13 「**iOS デバイスで Face ID の使用を許可する**」(iOS デバイスで Face ID 技術を使用して今後のログイン試行を遮断するコントロール) が無効化されていると、サーバはクライアントが接続を試みるまでクライアントの設定を変更する手段がありません。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

14 「**VPN 常時有効**」セクションで、次のように構成します。

- 「**VPN 常時有効を有効にする**」で、以下のいずれかを選択します。
  - **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグローバル設定に優先します。
  - **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。
- 「**ユーザに切断を許可する**」で、以下のいずれかを選択します。
  - **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグローバル設定に優先します。

- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

- 「**VPN の接続に失敗した場合にネットワーク アクセスを許可する**」で、以下のいずれかを選択します。
  - **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグローバル設定に優先します。
  - **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。
- 「**信頼済みネットワークで VPN に接続しない**」で、以下のいずれかを選択します。
  - **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグローバル設定に優先します。
  - **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

15 「**内部プロキシ設定**」セクションのドロップダウン リストで、グローバル設定を適用するか、内部プロキシ機能を有効または無効にします。詳細については、クライアント > 設定 (262 ページ) を参照してください。

16 「**適用**」を選択します。

クライアントの範囲を有効化し、特定のユーザに関して DHCP クライアントの設定を構成するには:

1 「**ユーザ > ローカル ユーザ**」に移動します。

2 設定するユーザの横にある設定アイコンを選択します。

3 「**ローカル ユーザの編集**」ページで、「**クライアント**」**ページを選択します。**

   a 「**クライアント アドレス範囲**」の下で、ドロップダウン リストから「**DHCP を使用**」を選択します。

   b 「**インターフェースの選択**」の下で、ドロップダウン リストから DHCP に使用するインターフェースを選択します。

   c **DHCP サーバ**をフィールドに入力します。

   d 「**クライアント IPv6 アドレス範囲**」セクションで、必要に応じてドロップダウン リストから「**DHCPv6 を使用する**」を選択します。

   e 「**インターフェースの選択**」の下で、ドロップダウン リストから DHCPv6 に使用するインターフェースを選択します。

   f 必要に応じて、**DHCPv6 サーバ**をフィールドに入力します。

4 「**DNS 設定**」で、以下の操作を行います。

以下のフィールドに入力します。

- **プライマリ DNS サーバ:**「**プライマリ DNS サーバ**」フィールドにプライマリ DNS サーバのアドレスを入力します。
- **セカンダリ DNS サーバ:** オプションで、「**セカンダリ DNS サーバ**」フィールドにセカンダリ サーバのアドレスを入力します。
- **DNS 検索リスト (検索順):** DNS ドメインの接尾辞を入力し、「**追加**」をクリックします。続いて、上下方向の矢印を使用して、複数の DNS ドメインを使用されるべき順序に並べ替えます。

Apple iPhone、iPad、その他の iOS 端末からの SonicWall Mobile Connect を使った接続をサポートする SMA/SRA 装置に対しては、この DNS 検索リストを使用してください。この DNS ドメインは、iPhone/iPad の VPN インターフェース上に、機器が装置との接続を確立した後で設定されます。モバイル機器のユーザがある URL にアクセスする際に、iOS はこのドメインが VPN インターフェースのドメインと一致しているかどうかを判断し、一致している場合は VPN インターフェースの DNS サーバを使ってホスト名検索を解決します。そうでない場合は、組織のイントラネット内のホストを解決できない Wi-Fi または 3G の DNS サーバが使われます。

5 「**クライアント設定**」の下で、「**切断後にクライアントを終了**」ドロップダウン リストで次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

6 「**クライアント終了後にアンインストール**」ドロップダウン リストで、次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

7 「**クライアント接続プロファイルを作成**」ドロップダウン リストで、次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

8 「**ユーザ名とパスワードの保存**」ドロップダウン リストで、次のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **ユーザ名だけ保存を許可** - ユーザ名のキャッシュを許可します。NetExtender を起動するときにユーザはパスワードのみを入力する必要があります。この設定はグループ設定に優先します。
- **ユーザ名とパスワードの保存を許可** - ユーザ名とパスワードのキャッシュを許可します。NetExtender を起動すると自動的にログインします。この設定はグループ設定に優先します。
- **ユーザ名とパスワードの保存を禁止** - ユーザ名とパスワードのキャッシュを許可しません。NetExtender を起動するときにユーザはユーザ名とパスワードの両方を入力する必要があります。この設定はグループ設定に優先します。

9 このオプションが無効になっている場合、「**iOS デバイスでタッチ ID の使用を許可する**」では、iOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

10 このオプションが無効になっている場合、「**Android デバイスで指紋認証の使用を許可する**」では、Android デバイスでの指紋認証による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

11 このオプションが無効になっている場合、「**macOS デバイスでタッチ ID の使用を許可する**」では、macOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

12 「**iOS デバイスで Face ID の使用を許可する**」(iOS デバイスで Face ID 技術を使用して今後のログイン試行を遮断するコントロール) が無効化されていると、サーバはクライアントが接続を試みるまでクライアントの設定を変更する手段がありません。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

13 「**VPN 常時有効**」セクションで、次のように構成します。

- 「**VPN 常時有効を有効にする**」で、以下のいずれかを選択します。
  - **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
  - **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。
- 「**ユーザに切断を許可する**」で、以下のいずれかを選択します。
  - **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。

- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

- 「**VPN の接続に失敗した場合にネットワーク アクセスを許可する**」で、以下のいずれかを選択します。
  - **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
  - **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。
- 「**信頼済みネットワークで VPN に接続しない**」で、以下のいずれかを選択します。
  - **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
  - **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
  - **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

14 「**内部プロキシ設定**」セクションのドロップダウン リストで、内部プロキシ機能を有効または無効にします。詳細については、クライアント > 設定 (262 ページ) を参照してください。

15 「**適用**」を選択します。

NetExtender クライアント ルートの変更

「**ルート**」ページには、NetExtender クライアントのルートを設定するオプションがあります。NetExtender のクライアント ルート設定を変更する手順については、クライアント > ルート (268 ページ) を参照してください。

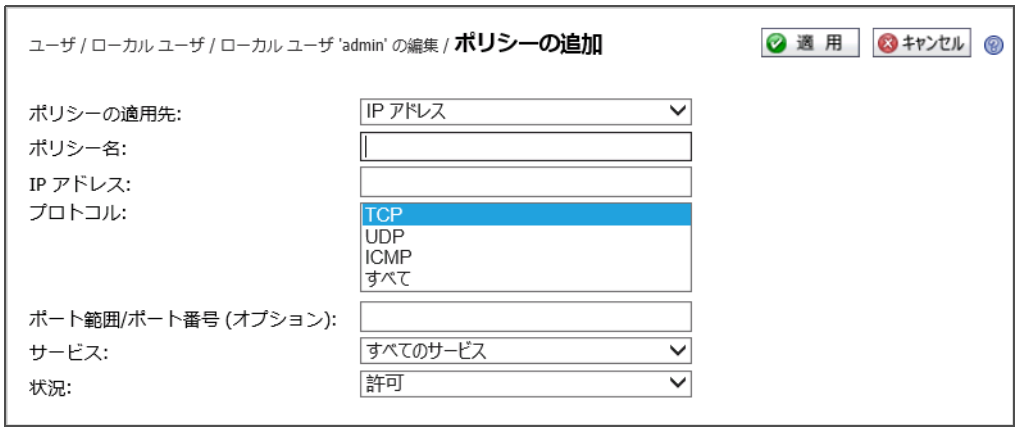
ユーザ ポリシーの追加

「**ポリシー**」ページには、ポリシーの設定オプションがあります。

メモ：ユーザのアクセス ポリシーを追加するには、以下の手順を実行します。

新しいアクセス ポリシーを追加するには:

1 「**ポリシー**」ページで「**ポリシーの追加**」を選択します。「**ポリシーの追加**」ウィンドウが表示されます。



2 「**ポリシーの適用先**」ドロップダウン リストで、ポリシーの適用先として、個別ホスト、アドレス範囲、すべてのアドレス、ネットワーク オブジェクト、サーバ パス、または URL オブジェクトのいずれかを選択します。単一の IPv6 ホスト、IPv6 アドレス範囲、またはすべての IPv6 アドレスの選択もできます。「**ポリシーの追加**」ウィンドウの内容は、「**ポリシーの適用先**」ドロップダウン リストで選択したオブジェクトの種別に応じて変化します。

> **メモ**：これらの Secure Mobile Access のポリシーは SMA/SRA 接続の送信元アドレスではなく送信先アドレスに適用されます。インターネット上の特定の IP アドレスが「**ポリシー**」ページ上で作成されたポリシーを用いて SMA/SRA ゲートウェイの認証を受けることを許可または阻止することはできません。ただし、ユーザの「**ログイン ポリシー**」ページ上で作成されたログイン ポリシーを用いて IP アドレスにより送信元ログインを制御することが可能です。詳細については、ログイン ポリシーの設定 (434 ページ) を参照してください。

- **IP アドレス** - 特定のホストにポリシーを適用する場合は、ローカル ホスト コンピュータの IP アドレスを「**IP アドレス**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IP アドレスのポリシーの追加 (404 ページ) を参照してください。
- **IP ネットワーク** - アドレス範囲にポリシーを適用する場合は、IP アドレス範囲の開始アドレスを「**IP ネットワーク アドレス**」フィールドに入力し、IP アドレス範囲を定義するサブネットを「**サブネット マスク**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IP ネットワークに対するポリシーの追加 (405 ページ) を参照してください。
- **すべてのアドレス** - ポリシーをすべての IPv4 アドレスに適用する場合は、IP アドレス情報を入力する必要はありません。すべてのアドレスのポリシーの追加 (405 ページ) を参照してください。
- **ネットワーク オブジェクト** - 定義済みネットワーク オブジェクトにポリシーを適用する場合は、「**ネットワーク オブジェクト**」ドロップダウン リストでオブジェクトの名前を選択します。ネットワーク オブジェクトを定義するときにポートまたはポート範囲を指定できます。ネットワーク オブジェクトの追加 (145 ページ) を参照してください。
- **サーバ パス** - サーバ パスにポリシーを適用する場合は、「**リソース**」フィールドで以下のラジオ ボタンの 1 つを選択します。
  - 共有 (サーバ パス) - このオプションを選択するときは、パスを「サーバ パス」フィールドに入力します。

- ネットワーク (ドメイン リスト)
- サーバ (コンピュータ リスト)

ファイル共有アクセス ポリシーの設定 (406 ページ) を参照してください。

- **URL オブジェクト** - 定義済みの URL オブジェクトにポリシーを適用する場合は、URL を「**URL**」フィールドに入力します。URL オブジェクトのポリシーの追加 (407 ページ) を参照してください。
- **すべての IPv6 アドレス** - すべての IPv6 アドレスにポリシーを適用する場合は、IP アドレス情報を入力する必要はありません。ユーザ ブックマークの追加または編集 (409 ページ) を参照してください。
- **IPv6 アドレス** - 特定のホストにポリシーを適用する場合は、ローカル ホスト マシンの IPv6 アドレスを「**IPv6 アドレス**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IPv6 アドレスに対するポリシーの追加 (408 ページ) を参照してください。
- **IPv6 ネットワーク** - アドレス範囲にポリシーを適用する場合は、先頭の IPv6 アドレスを「**IPv6 ネットワーク アドレス**」フィールドに入力して、この IPv6 アドレス範囲を定義する接頭辞を「**IPv6 接頭辞**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。IPv6 ネットワークに対するポリシーの追加 (409 ページ) を参照してください。

3 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

メモ：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

4 サービスの種類を「**サービス**」ドロップダウン リストで選択します。ポリシーの適用先がネットワーク オブジェクトの場合は、そのネットワーク オブジェクトで定義されたサービスが使用されます。

5 「**状況**」ドロップダウン リストから「**許可**」または「**拒否**」を選択し、指定したサービスおよびホスト コンピュータの SMA/SRA 接続を許可または拒否します。

ヒント：Citrix ブックマークを使用するときには、ホストへのプロキシ アクセスを制限するために、Citrix サービスと HTTP サービスの両方に対して**拒否**ルールを設定する必要があります。

6 「**適用**」を選択して設定を更新します。設定を更新すると、新しいポリシーが「**ローカル ユーザの編集**」ページに表示されます。

ユーザ ポリシーは、「**現在のユーザ ポリシー**」テーブルに、優先度の高いものから順番に表示されます。

IP アドレスのポリシーの追加

1 「**ユーザ > ローカル ユーザ**」に移動します。

2 設定するユーザの横にある設定アイコンを選択します。

3 「**ポリシー**」ページを選択します。

4 「**ポリシーの追加**」を選択します。

5 「**ポリシーの適用先**」フィールドで、「IP アドレス」オプションを選択します。

6 ポリシーの名前を「**ポリシー名**」フィールドに指定します。

7 IP アドレスを「IP**アドレス**」フィールドに入力します。

8 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

ⓘ **メモ**：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

9 オプションとして「**ポート範囲/ポート番号**」フィールドにポート範囲または特定のポート番号を入力します。

10 「**サービス**」ドロップダウン リストで、サービス オブジェクトを選択します。

11 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。

12 「**適用**」を選択します。

IP ネットワークに対するポリシーの追加

1 「**ポリシーの適用先**」フィールドで、「**IP ネットワーク** 」オプションを選択します。

2 ポリシーの名前を「**ポリシー名**」フィールドに指定します。

3 開始 IP アドレスを「IP**ネットワーク アドレス**」フィールドに入力します。

4 サブネット マスク値を「**サブネット マスク**」フィールドに“255.255.255.0”形式で入力します。

5 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

ⓘ **メモ**：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

6 オプションとして「**ポート範囲/ポート番号**」フィールドにポート範囲または特定のポート番号を入力します。

7 「**サービス**」ドロップダウン リストで、サービス オプションを選択します。

8 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。

9 「**適用**」を選択します。

すべてのアドレスのポリシーの追加

1 「**ポリシーの適用先**」フィールドで、「**すべてのアドレス**」オプションを選択します。

2 ポリシーの名前を「**ポリシー名**」フィールドに指定します。

3 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

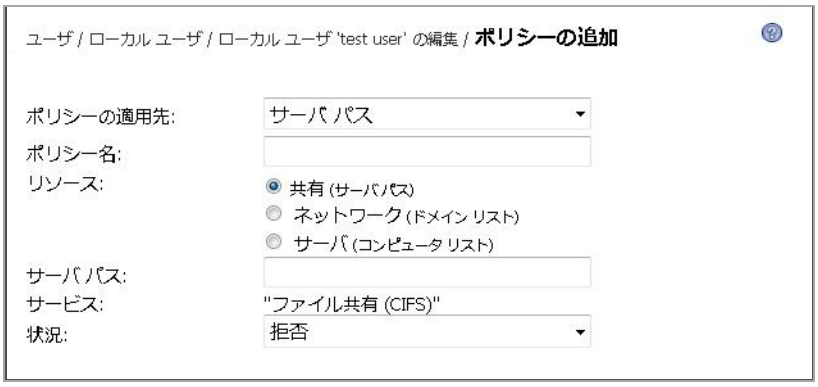
ⓘ **メモ**：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

4 「**IP アドレス範囲**」フィールドは読み取り専用になり、「すべての IP アドレス」が指定されます。
5 「**サービス**」ドロップダウン リストで、サービス オプションを選択します。
6 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。
7 「**適用**」を選択します。

ファイル共有アクセス ポリシーの設定

ファイル共有アクセス ポリシーを設定するには:

1 「**ユーザ > ローカル ユーザ**」に移動します。
2 設定するユーザの横にある設定アイコンを選択します。
3 「**ポリシー**」ページを選択します。
4 「**ポリシーの追加**」を選択します。
5 「**ポリシーの適用先**」ドロップダウン リストで「**サーバ パス**」を選択します。



6 ポリシーの名前を「**ポリシー名**」フィールドに入力します。
7 「**リソース**」フィールドで「**共有**」を選択します。
8 サーバ パスを「**サーバ パス**」フィールドに入力します。
9 「**状況**」ドロップダウン リストで「**許可**」または「**拒否**」を選択します。

> **メモ**：サーバ パスのアクセスの制限など、ファイル共有のポリシーの編集については、ファイル共有のポリシーの追加 (406 ページ) を参照してください。

10 「**適用**」を選択します。

ファイル共有のポリシーの追加

ファイル共有アクセス ポリシーを追加するには:

1 「**ユーザ > ローカル ユーザ**」に移動します。
2 設定するユーザの横にある設定アイコンを選択します。
3 「**ポリシー**」ページを選択します。
4 「**ポリシーの追加**」を選択します。
5 「**ポリシーの適用先**」ドロップダウン リストで「**サーバ パス**」を選択します。
6 ポリシーの名前を「**ポリシー名**」フィールドに入力します。

7 「**サーバ パス**」フィールドに、サーバ パスを *servername/share/path* または *servername\share\path* の形式で入力します。使用できる接頭辞は \\、//、\、および / です。

ⓘ **メモ：**共有とパスによって、ポリシーをより細かく管理できるようになります。どちらの設定もオプションです。

8 「**状況**」ドロップダウン リストで「**許可**」または「**拒否**」を選択します。

9 「**適用**」を選択します。

URL オブジェクトのポリシーの追加

オブジェクトベースの HTTP または HTTPS ユーザ ポリシーを作成するには:

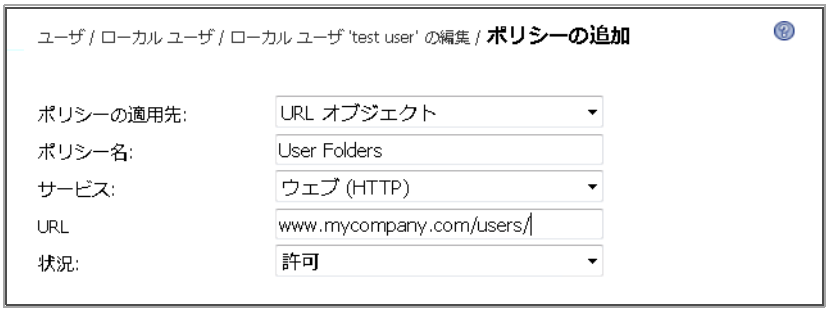
1 「**ユーザ > ローカル ユーザ**」に移動します。

2 設定するユーザの横にある設定アイコンを選択します。

3 「**ポリシー**」ページを選択します。

4 「**ポリシーの追加**」を選択します。

5 「**ポリシーの適用先**」ドロップダウン メニューで「**URL オブジェクト**」オプションを選択します。



6 ポリシーの名前を「**ポリシー名**」フィールドに指定します。

7 「**サービス**」ドロップダウン リストで、「**ウェブ (HTTP)**」または「**セキュア ウェブ (HTTPS)**」を選択します。

8 「**URL**」フィールドで、このポリシーで適用する URL 文字列を追加します。

ⓘ **メモ：**「URL」フィールドでは、標準の URL 要素に加えて、ポート、パス、およびワイルドカード要素を入力できます。これらの追加的要素の詳細については、「ポリシー URL オブジェクト フィールドの要素 (407 ページ)」を参照してください。

パスを指定した場合、URL ポリシーはすべてのサブディレクトリについても適用されます。例えば、www.mycompany.com/users/* を指定した場合、ユーザは www.mycompany.com/users/ フォルダの下にあるすべてのフォルダやファイルにアクセスできます。

9 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。

10 「**適用**」を選択します。

ポリシー URL オブジェクト フィールドの要素

HTTP/HTTPS ポリシーを作成するときに、有効なホスト URL を「URL」フィールドに入力する必要があります。「URL」フィールドでは、ポート、パス、およびワイルドカード要素を指定できます。以下に、「URL」フィールドの標準要素の概要を示します。

標準の URL フィールド要素

要素	使用法
ホスト	IP アドレスに解決されるホスト名。ホスト情報が存在する必要があります。
ポート	ポートを指定しない場合、ホストに一致するすべてのポートが使用されます。特定のポートまたはポート範囲を数値 (0-9) またはワイルドカード要素を使って指定します。ゼロ (0) をこのフィールドの 1 文字目に使用することはできません。ワイルドカード式に一致する最小の数値が、有効なポート番号の範囲 (1 ～ 65535 など) に含まれる必要があります。
パス	これは、URL に問い合わせ文字列を連結したファイル パスです。URL パスは、ファイル パス区切り文字 (/) で区切られた部分から構成されます。各部分にはワイルドカード文字を使用できます。ワイルドカード文字の効力は、ファイル パス区切り文字で前後を区切られた部分の内部に限定されます。
ユーザ名	%USERNAME% は、有効なセッション中に要求された URL に含まれるユーザ名に一致する変数です。グループやグループ ポリシーの場合にこの変数は便利です。
ワイルドカード文字	ポートまたはパスを指定するために、以下のワイルドカード文字を 1 つまたは複数の文字に一致する文字として使用できます。 * - その位置にある 1 つまたは複数の任意の文字に一致します。 ^ - その位置にある 1 つの任意の文字に一致します。 **[!<文字セット>]** - その位置にある、文字セットに含まれない任意の 1 つの文字に一致します。例: **[!acd]**、**[!8a0]** **[<範囲>]** - 指定した ASCII 範囲に含まれる任意の 1 文字に一致します。英数字を指定できます。例: **[a-d]**、**[3-5]**、**[H-X]**

メモ：「URL」フィールドに "http://" 要素や "https://" 要素を入力することはできません。また、# などのフラグメント区切り文字を含めることもできません。

すべての IPv6 アドレスのポリシーの追加

すべての IPv6 アドレスに対するポリシーを追加するには:

1. 「**ポリシーの適用先**」フィールドで、「**すべての IPv6 アドレス**」オプションを選択します。
2. ポリシーの名前を「**ポリシー名**」フィールドに指定します。
3. 「**IPv6 アドレス範囲**」フィールドは読み取り専用になり、「すべての IPv6 アドレス」が指定されます。
4. 「**サービス**」ドロップダウン リストで、サービス オプションを選択します。
5. 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。
6. 「**適用**」を選択します。

IPv6 アドレスに対するポリシーの追加

IPv6 アドレスに対するポリシーを追加するには:

1. 「**ユーザ > ローカル ユーザ**」に移動します。

2 設定するユーザの横にある設定アイコンを選択します。
3 「**ポリシー**」ページを選択します。
4 「**ポリシーの追加**」を選択します。
5 「**ポリシーの適用先**」フィールドで、「**IPv6 アドレス範囲**」オプションを選択します。
6 ポリシーの名前を「**ポリシー名**」フィールドに指定します。
7 IPv6 アドレスを「**IPv6 アドレス**」フィールドに 2001::1:2:3:4 形式で入力します。
8 オプションとして「**ポート範囲/ポート番号**」フィールドにポート範囲または特定のポート番号を入力します。
9 「**サービス**」ドロップダウン リストで、サービス オブジェクトを選択します。
10 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。
11 「**適用**」を選択します。

IPv6 ネットワークに対するポリシーの追加

IPv6 ネットワークに対するポリシーを追加するには:

1 「**ポリシーの適用先**」フィールドで、「**IPv6 ネットワーク**」オプションを選択します。
2 ポリシーの名前を「**ポリシー名**」フィールドに指定します。
3 開始 IPv6 アドレスを「IPv6**ネットワーク アドレス**」フィールドに入力します。
4 64 や 112 などのプレフィックス値を「**IPv6 プレフィックス**」に入力します。
5 オプションとして「**ポート範囲/ポート番号**」フィールドにポート範囲または特定のポート番号を入力します。
6 「**サービス**」ドロップダウン リストで、サービス オプションを選択します。
7 「**状況**」ドロップダウン リストで、アクセス動作として「**許可**」または「**拒否**」を選択します。
8 「**適用**」を選択します。

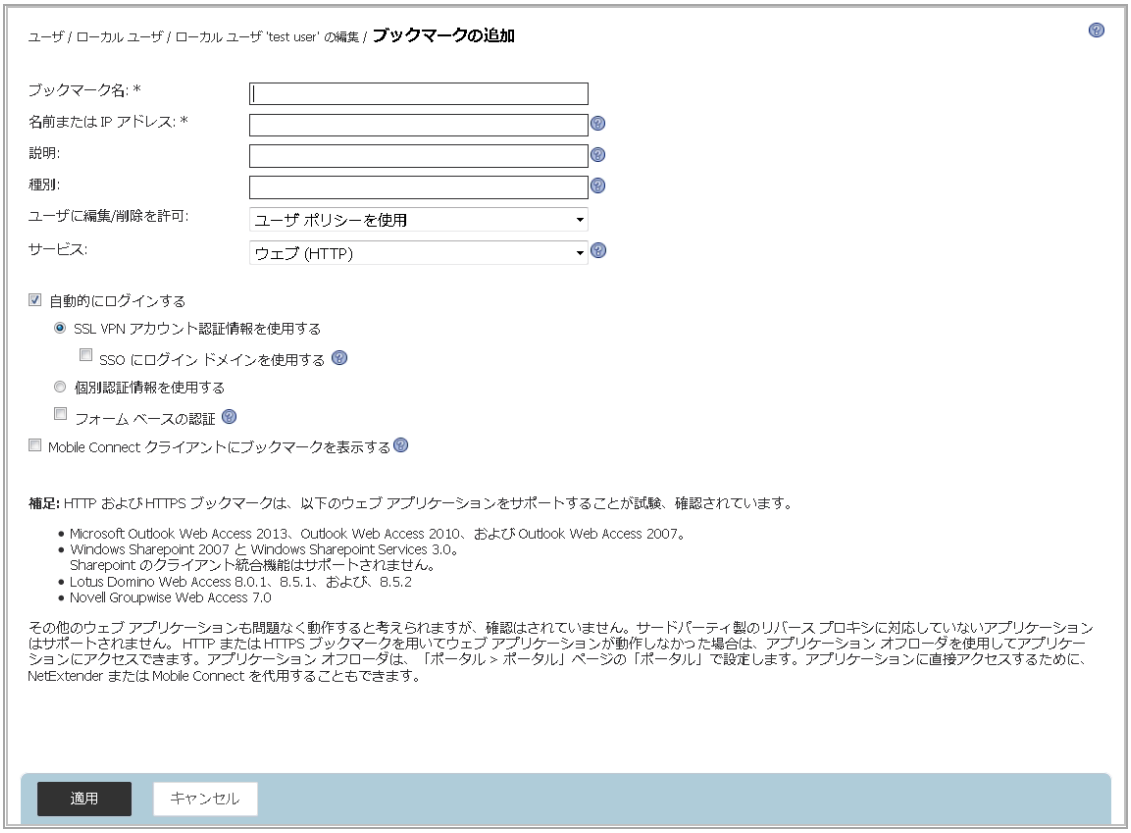
ユーザ ブックマークの追加または編集

「**ブックマーク**」ページには、ユーザ ブックマークを追加および編集するための設定オプションがあります。以下に説明するメインの手順に加えて、以下のセクションを参照してください。

- ローカル ユーザの Citrix ブックマークの作成 (430 ページ)
- 個別 SSO 資格情報によるブックマークの作成 (432 ページ)

ユーザ ブックマークを定義するには:

1 「**ユーザ設定の編集**」ウィンドウで、「**ブックマーク**」ページを選択します。
2 「**ブックマークの追加**」を選択します。「**ブックマークの追加**」ウィンドウが表示されます。



ユーザ ブックマークを定義すると、ユーザは Secure Mobile Access 仮想オフィス ホーム ページで定義済みのブックマークを見ることができます。

1 わかりやすいブックマーク名を「**ブックマーク名**」フィールドに入力します。

2 LAN 上のホスト コンピュータの完全修飾ドメイン名 (FQDN) または IPv4/IPv6 アドレスを「**名前または IP アドレス**」フィールドに入力します。Windows ローカル ネットワークで VNC ブックマークを作成する場合など、環境によってはホスト名のみを入力できます。

「**名前または IP アドレス**」フィールド内でポート番号が IPv6 アドレスに含まれる場合は、IPv6 アドレスを角かっこで囲む必要があります。入力例:**[2008::1:2:3:4]:6818**。

メモ：IPv6 は、ActiveX、およびファイル共有ではサポートされません。

サービスによっては、非標準ポートで動作し、接続時にパスを要求することがあります。「サービス」フィールドで選択したオプションによって、サービス種別に対するブックマーク名または IP アドレスの形式 表に示した例のいずれかの形式で「**ホスト名または IP アドレス**」フィールドに入力します。

サービス種別に対するブックマーク名または IP アドレスの形式

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
RDP - HTML5 RDP - ネイティブ	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
VNC VNC - HTML5	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (セッションへ割り当て済み)	10.20.30.4:5901 (セッション 1 へ割り当て済み)
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
	メモ：ポートの代わりにセッション番号または表示番号を使用しないでください。	**メモ**：10.20.30.4:1 を使用しないでください。 **ヒント**：Linux サーバへのブックマークについては、この表の下にヒントがあります。
Citrix (Citrix ウェブインターフェース) Citrix - HTML5 Citrix - ネイティブ Citrix - ActiveX	IP アドレス	172.55.44.3
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート	172.55.44.3:8080 または [2008::1:2:3:4]:8080
	IP:パスまたはファイル	172.55.44.3/フォルダ/file.html
	IP:ポート:パスまたはファイル	172.55.44.3:8080/report.pdf
	FQDN	www.citrixhost.company.net
	URL:パスまたはファイル	www.citrixhost.net/フォルダ/
	URL:ポート	www.citrixhost.company.net:8080
	URL:ポート:パスまたはファイル	www.citrixhost.com:8080/フォルダ/index.html
	メモ: *ポート*は、Citrix クライアント ポートではなく、Citrix ウェブ インターフェースの HTTP(S) ポートです。	
HTTP HTTPS	URL	www.sonicwall.com
	URL の IP アドレス	204.212.170.11
	IPv6 アドレス	2008::1:2:3:4
	URL:パスまたはファイル	www.sonicwall.com/index.html
	IP:パスまたはファイル	204.212.170.11/フォルダ/
	URL:ポート	www.sonicwall.com:8080
	IP:ポート	204.212.170.11:8080 または [2008::1:2:3:4]:8080
	URL:ポート:パスまたはファイル	www.sonicwall.com:8080/フォルダ/index.html
	IP:ポート:パスまたはファイル	www.sonicwall.com:8080/index.html

サービス種別に対するブックマーク名または IP アドレスの形式 (続き)

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
ファイル共有 (CIFS)	ホスト\フォルダ\	server-3\共有フォルダ\
	ホスト\フォルダ	server-3\inventory.xls
	完全修飾名\フォルダ	server-3.company.net\共有フォルダ\
	完全修飾名\ファイル	server-3.company.net\inventory.xls
	IP\フォルダ\	10.20.30.4\共有フォルダ\
	IP\ファイル	10.20.30.4\status.doc
		メモ：Linux や Mac コンピュータでもファイル共有に Windows API が使用されるため、\ 記号を使用してください。
FTP	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818 または [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
Telnet Telnet - HTML5	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818 または [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
SSHv2	IP アドレス	10.20.30.4
	IPv6 アドレス	2008::1:2:3:4
	IP:ポート (非標準)	10.20.30.4:6818 または [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC

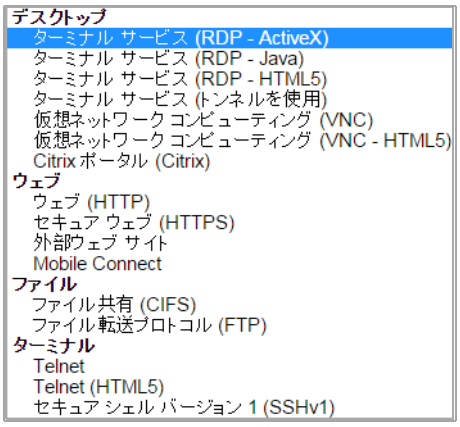
ヒント：Linux サーバへの **Virtual Network Computing (VNC)** ブックマークを作成するときは、「**ホスト名または IP アドレス**」フィールドで、Linux サーバの IP アドレスとともにポート番号とサーバ番号を**ipaddress:port:server**の形式で指定する必要があります。例えば、Linux サーバの IP アドレスが 192.168.2.2、ポート番号が 5901、サーバ番号が 1 の場合は、「**ホスト名または IP アドレス**」フィールドに**192.168.2.2:5901:1**を指定します。

3 オプションで、ブックマーク テーブル内に表示される、わかりやすい説明を「**説明**」フィールドに入力することができます。

4 必要に応じて、このブックマークを表示する種別を「**種別**」フィールドにコンマで区切って列挙することができます。以下に例を示します。お気に入り, タブ 1, タブ 2デスクトップ、ウェブ、ターミナル、モバイルなど標準のタブは指定する必要がありません。

5 仮想オフィス ポータルからユーザがブックマークを編集または削除できるかどうかを、「**ユーザに編集/削除を許可**」の選択により設定します。「**許可**」、「**拒否**」または、「**ユーザ ポリシーを使用**」を選択できます。

6 「**サービス**」ドロップダウン リストから、サービス タイプを 1 つ選択します。



「**サービス**」ドロップダウン リストで選択するサービスに応じて、追加のフィールドが表示されることがあります。選択したサービスに対する以下の情報を使ってブックマークを完成させます。

ターミナル サービス (RDP) またはターミナル サービス (RDP - HTML5)

メモ：HTML5 RDP ブックマークは、ターミナル サーバ接続上の「ユーザ毎」のライセンスでのみサポートされます。ターミナル サーバのライセンス モードが「装置ごと」の場合、これらのブックマークは機能しません。

- 「**画面サイズ**」ドロップダウン リストで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。*(すべてのターミナル サービスで使用できます)*

  画面サイズはコンピュータによって異なるので、リモート デスクトップ アプリケーションを使用するときは、リモート デスクトップ セッションの実行元のコンピュータ画面のサイズを選択する必要があります。また、場合によっては「**アプリケーション パス**」フィールドでリモート コンピュータ上のアプリケーションのパスを指定する必要があります。
- 「**カラー**」ドロップダウン リストで、このブックマークの実行時に使用されるターミナル サービス画面の既定の色深度を選択します。*(すべてのターミナル サービスで使用できます)*
- 「**アクセス タイプの選択**」を選びます。「**スマート**」または「**手動**」のどちらかです。
  - 「**スマート**」: ファームウェアにクライアントを起動するモードを決定させます。

    新しい統合ブックマークを作成する場合は、「**スマート**」がデフォルトで選択されています。ブックマークの起動時には、ブックマーク固有の既定モードを使用して自動検出の処理が行われます。
  - 「**手動**」: モードや優先順位を設定し、方法を選択するオプションを提供します。選択ボックスで、少なくとも 1 つのモードが有効になっている必要があります。

起動シーケンスは、「**HTML5**」と「**Native**」です。「手動」を選択すると、起動方法を変更、有効化、または無効化できます。「**Native**」を選択して RDP ブックマークを起動した場合は、SMA Connect Agent によって RDP クライアントがローカルマシン上で起動され、RDP 接続が行われます。

「**上**」と「**下**」の矢印を使って起動順序を調整します。バツとチェックのアイコンを使ってモードの有効と無効を切り替えます。無効にしたモードはリストの下に移動し、グレー表示されます。

「**手動**」モードでは、デフォルトで「**起動中に選択**」オプションは有効ではありません。この設定では、ブックマークの起動時に、設定済みリストの先頭にある使用可能なモードが自動検出後に実行されます。

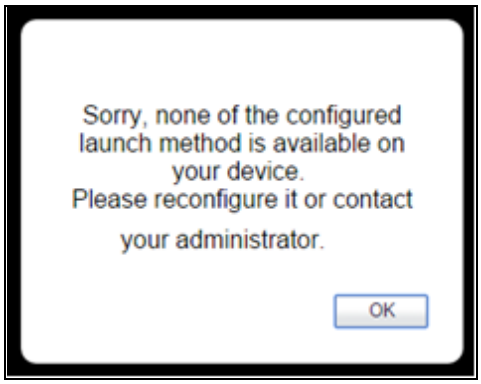
「**起動時に選択する**」オプションが有効になっていて、複数のモードがクライアントで使用可能な場合は、統合ブックマークの起動時にメニューが表示されます。このメニューでは、5 秒のカウントダウンが行われている間にモードを選択できます。使用可能なモードが 1 つしかない場合、ブックマークはただちに実行されます。

起動時に「**この選択を記憶する**」オプションが有効になっている場合は、選択されたモードが Cookie によって記憶されます。

その場合、次にブックマークを起動すると、記憶したモードが 2 秒以内に直接実行されます。HTML のどこかをクリックすると、記憶したモードを「忘れる」ので、再選択を行うことができます。

同じブラウザでブックマークの編集や削除しても、記憶したモードがリセットされます。

設定されたクライアントでどのモードも実行できない場合、次の通知が表示されます。



- 「**Wake on LAN を有効にする**」をオンにすると、ネットワーク接続を介してコンピュータの電源を投入できます。このチェックボックスをオンにした場合、以下の新しいフィールドが表示されます。*(すべてのターミナル サービスで使用できます)*
  - **MAC/イーサネット アドレス** - 電源を投入するホストの 1 つ以上の MAC アドレスをスペースで区切って入力します。
  - **起動待ち時間 (秒)** - WoL 操作を中止するまでターゲット ホストの起動完了を待機する時間を秒単位で入力します。
  - **WOL パケットをホスト名または IP アドレスに送信する** - WOL パケットをこのブックマークのホスト名または IP アドレスに送信するには、「**WOL パケットをホスト名または IP アドレスに送信する**」をオンにします。この設定は、WOL で電源を投入する別のコンピュータの MAC アドレスと併用して適用できます。
- オプションで、このアプリケーションのローカル パスを「**アプリケーションおよびパス**」フィールドに入力し、フォルダを「**次のフォルダから開始」フィールドに指定します。リモート アプリケーション機能は、単一のアプリケーションをユーザに対して表示します。 値はリモート アプリケーションのエイリアスにすることもできます。**
- RemoteApp 用 の「**コマンドライン引数**」を入力します。*(ActiveX でのみ使用できます)*
- 「**次のフォルダから開始**」フィールドに、アプリケーション コマンドを実行するローカル フォルダをオプションで入力します。*(ActiveX でのみ使用できます)*
- 「**コンソール / 管理者セッションとしてログインする**」をオンにすると、コンソールまたは管理者としてログインできます。RDC 6.1 以降では、admin セッションへのログインは、コンソール セッションへのログインに置き換わります。*(すべてのターミナル サービスで使用できます)*
- TS ファームまたは負荷分散サーバに接続する場合は、「**サーバは TS ファーム**」をオンにします。

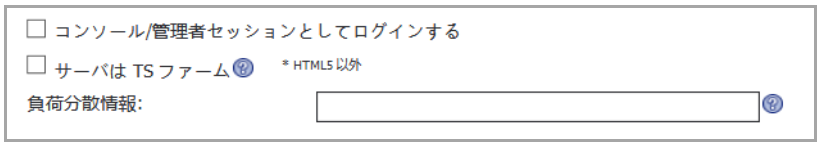
  Windows 2012 には、リダイレクト (負荷分散) を行う新しい方法があります。RDP クライアントはブローカ サーバに直接接続し、ブローカ サーバがリダイレクト情報をクライアントに返します。RDP クライアントは「コレクション」内の RDP ホストに接続できます。

  Windows 2012 RD Web にアクセスしたら、ページ上のアイテムをクリックして RDP ファイルをダウンロードします。RDP ファイルには、次の文字列を含む行があります。

  “loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.<CollectionName>”

  <CollectionName> はユーザのファーム内のコレクション名です。この行が「負荷分散情報」です。ブローカ サーバはこの情報に基づいて負荷分散 (リダイレクト) を行います。

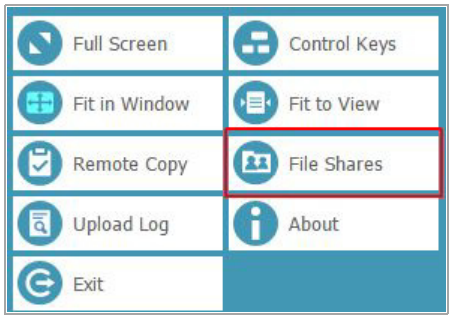
- ターミナル サービス ブローカ情報を「**負荷分散情報**」ボックスに入力します (例: `tsv://MS Terminal Services Plugin.1.SSLVPN`)。最大 1024 文字まで入力できます。複雑なオプションを持つブックマーク (RDP など) では、すべてのモードのオプションが混在していますが、「*HTML5 以外」、「*HTML5 向け」のようなヒントによってオプションの区別が行われています。



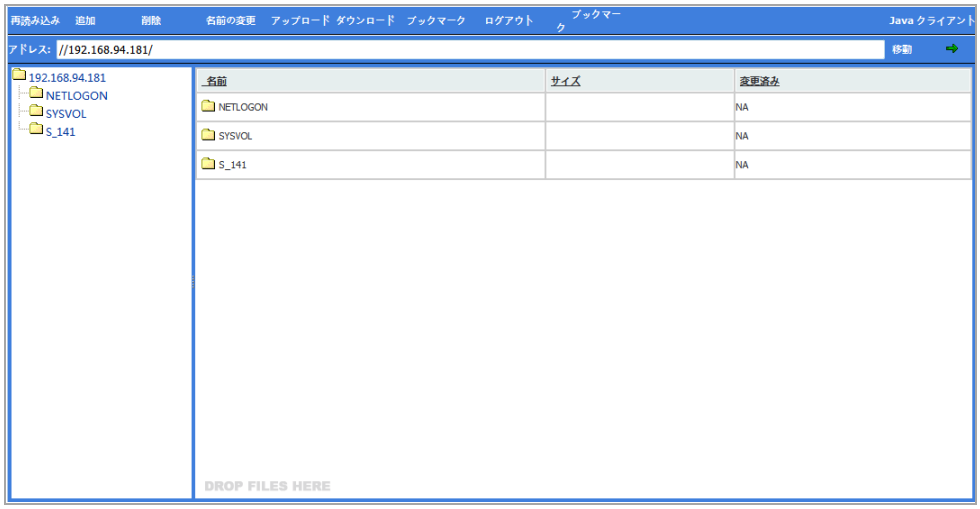
  既定では、ブックマークは提供された名前と IP アドレスのみに接続します。この機能を有効にすると、SMA/SRA 装置はリダイレクトされたアドレスを取得し、ユーザを正しいサーバに接続します。この機能が正しく動作するには、対話型ログインを無効しなければならない場合があることに注意してください。

- 「*RDP - HTML5*」の場合は、ドロップダウン メニューから「**既定の言語**」を選択します。
- Windows クライアント、または RDC をインストール済みの Mac OS X 10.5 以上の Mac クライアントでは、「**詳細な Windows オプションを表示**」を展開し、各チェックボックスをオンにすることにより、ローカル ネットワーク上の以下の機能を、このブックマークで使用するためにリダイレクトします。*RDP - HTML5 またはネイティブ*の場合、以下の詳細な Windows オプションが使用できます。
  - **デスクトップ背景**
  - **メニューとウインドウ アニメーション**
  - **ドラッグ/リサイズの間にウィンドウの内容を表示する**
  - **クリップボードをリダイレクトする**
  - **ファイル共有**

    「ファイル共有」を選択すると、**盾**アイコンをクリックしたときに HTML5 RDP メニューにこの機能の新しいボタンが表示されます。



    「**ファイル共有**」をクリックすると、「ファイル共有」ウィンドウが開きます。ウィンドウ内のフォルダとファイルを操作できます。



- **ドライブをリダイレクトする**
- **スマートカードをリダイレクトする**
- **ビットマップのキャッシュ**
- **自動再接続**
- **表示スタイル**
- **リモート コピー**
- **プリンタをリダイレクトする** - **プリンタ リダイレクトの設定の詳細については、プリンタのリダイレクト (515 ページ) を参照してください。**
- **ポートをリダイレクトする**
- **接続バーを表示する**
- ドロップダウン リストから「**リモート音声**」オプションを選択します。オーディオ リダイレクションにより、リモートまたはローカルでサーバ上のオーディオ クリップを再生できます。有効な選択肢は、「**このコンピュータで再生する**」、「**リモート コンピュータで再生する**」、または「**再生しない**」です。現在、この機能は Chrome、Firefox、および Safari でサポートされています。

メモ：一部のオプションの横にあるヘルプ アイコン の上にマウス ポインタを移動すると、要求事項がツールチップに表示されます。

- クライアント アプリケーションが RDP6 の場合はさらに、以下のいずれかのオプションを選択できます(*すべてのターミナル サービスで使用できます*)。
  - **フォント補整**
  - **スパン画面表示**
  - **デスクトップ コンポジション**
  - **デュアル モニタ**
  - **リモート アプリケーション**
- ドロップダウン リストから「**接続速度**」を選択して (低速ブロードバンドまたは高速ブロードバンド)、パフォーマンスを最適化します。(*すべてのターミナル サービスで使用できます*)

- 「**サーバ認証が失敗した場合**」に発生するアクションをドロップダウン リストから選択します。意図したリモート コンピュータに接続していることが、サーバ認証により確認されました。接続に必要な確認の強度は、システムのセキュリティ ポリシーによって決まります。(*すべてのターミナル サービスで使用できます*)
- 「**RDP オプションのインポート**」をクリックします。RDP ファイルのダウンロードが終了したら、テキスト エディタ (メモ帳など) でそのファイルを開き、ファイルの内容全体を選択します。内容をコピーして、「**RDP オプションのインポート**」のテキスト フィールドにテキストを貼り付けます。「**OK**」を選択します。ブックマークにインポートするサポート オプションが選択されます。

  次の表に、RDP オプションと RDP ファイルのオプションを示します。

ブックマークのフィールド	RDP オプション
名前または IP アドレス	full address:s:<値>
画面サイズ	desktopheight:i:<値> desktopwidth:i:<値>
画面の色	session bpp:i:<値>
負荷分散情報	loadbalanceinfo:s:<値>
デスクトップ背景	disable wallpaper:i:<値>
自動再接続	autoreconnection enabled:i:<値>
メニュー/ウィンドウ アニメーション	disable menu anims:i:<値>
表示スタイル	disable themes:i:<値>
ドラッグ/リサイズの間にウィンドウの内容を表示する	disable full window drag:i:<値>
クリップボードをリダイレクトする/リモート コピー	redirectclipboard:i:<値>
プリンタをリダイレクトする	redirectprinters:i:<値>
ドライブをリダイレクトする	redirectdrives:i:<値>
ポートをリダイレクトする	redirectcomports:i:<値>
スマートカードをリダイレクトする	redirectsmartcards:i:<値>
接続バーを表示する	displayconnectionbar:i:<値>
ビットマップのキャッシュ	bitmapcachepersistenable:i:<値>
リモート音声	audiomode:i:<値>
フォント補整	allow font smoothing:i:<値>
スパン画面表示	span monitors:i:<値>
デュアル モニタ	use multimon:i:<値>
デスクトップ コンポジション	allow desktop composition:i:<値>
リモート アプリケーション	remoteapplicationmode:i:<値>
接続スピードを選択してパフォーマンスを最適化してください	connection type:i:<値>

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプション

を有効にして、ユーザのドメインを RDP サーバに引き渡します。Windows 2008 以降のサーバでは、このオプションを有効にしなければならない可能性があります。*(すべてのターミナル サービスで使用できます)*

このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。*(すべてのターミナル サービスで使用できます)*

  メモ：RDP over HTML5 は、iOS または Android で既定および標準のブラウザを使用してサポートされます。

仮想オフィスからのターミナル サービス ブックマークに対する制限事項

ネットワーク内部にいるかのように、まず NetExtender で接続してから RDP クライアントを実行して、リモート アクセス装置外でアクセスと構成が正しくセットアップされていることを確認してください。NetExtender が正しく接続できない場合は、正しく設定する必要がある別の機器または設定がネットワーク上に存在する可能性があります。

指示された手順で設定を変更できない場合は、サーバのガイドを参照するか、ターミナル サーバの設定に関してマイクロソフトに詳しく問い合わせてください。

- インタラクティブ ログインを無効にしなければならない場合があります。Windows のログイン通知によって、プロキシが正しいリダイレクション サーバを取得できなくなります。
- gpedit.msc を実行し、「**コンピュータの構成 > Windows 設定 > ローカル ポリシー > セキュリティ オプション**」に移動して、ログオンを試みているユーザのインタラクティブ ログオン: メッセージ タイトルとログオンを試みているユーザのインタラクティブ ログオン: メッセージ テキストを探し、どちらも空白であることを確認します。
- 複数の RDP セッションを無効にしなければならない場合があります。複数の RDP セッションによって複数のリダイレクションが発生し、ブックマーク プロキシが正しいサーバに接続できなくなる場合があります。グループ ポリシーでユーザのセッションへのログオンを制限すると、このような状況を防ぐことができます。
- リモート サーバ上で gpedit.msc を実行し、「**コンピュータの構成 > 管理用テンプレート > Windows コンポーネント > リモート デスクトップ サービス > リモート デスクトップ セッション ホスト > 接続**」に移動して、「リモート デスクトップ サービスのユーザを単一のリモート デスクトップ サービス セッションに制限」を「**有効**」に設定します。
- RDP サーバに接続すると新しいセッション要求が作成され、ブックマークから古いセッションをクリアすることができません。使用可能なライセンスと、切断されたセッションの処理方法によって、サーバのセットアップに問題が生じる場合があります。
- SSO オプションが有効な場合は、SSO が正しいことを確認してください。SSO 認証情報が正しくないと、ブックマークがサーバに正しくアクセスできなくなります。問題が発生した場合は、SSO を無効にして、接続用に正しい認証情報が入力されていることを確認してください。
- ネイティブ RDP クライアントを利用できないシステムから接続するユーザには、HTML5 RDP クライアントの使用を推奨します。最新のブラウザは、接続に必要なウェブ ソケット機能をサポートします。また、ネイティブ RDP クライアントを持たないシステム上でも使用可能です。

仮想ネットワーク コンピューティング (VNC)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッション

から RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプションを有効にして、ユーザのドメインを RDP サーバに引き渡します。

- 「**エンコード**」ドロップダウン リストで、以下から 1 つを選択します。
  - **Raw** - ピクセル データは、左から右へのスキャンライン順で送信され、最初のフルスクリーンが送信された後で、変更のある長方形のみが送信されます。
  - **RRE** - ライズアンドランレングス エンコーディングは、単一の値と繰り返し数に圧縮された変換可能なピクセルの連続を使います。これは、一定の色の大きなブロックに対して能率的なエンコードです。
  - **CoRRE** - RRE の亜種で、最大で 255x255 ピクセルの長方形を使い、1 バイトの値を使用することができます。非常に大きな区域が同じ色の場合を除いて、RRE よりも能率的です。
  - **Hextile** - 長方形は最大 16x16 タイルの Raw または RRE データに分割され、あらかじめ決められた順序で送信されます。LAN 内のような、高速ネットワーク環境内の使用に最良です。
  - **Zlib** - 素のピクセル データの圧縮に zlib ライブラリを使用する簡素なエンコードで、多くの CPU 時間を消費します。Zib よりもほとんどすべての実生活環境で能率的な Tighe エンコードを理解しない VNC サーバでの互換性がサポートされます。
  - **Tight** - 既定であり、VNC をインターネット上またはその他の低帯域ネットワーク環境で使用するために最良のエンコードです。zlib ライブラリを使って、あらかじめ処理されたピクセル データを最大の圧縮率に、最小の CPU 使用率で圧縮します。
- 「**圧縮レベル**」ドロップダウン リストで、圧縮レベルを「**既定**」または「**1**」～「**9**」(**1** が最低圧縮で **9** が最高圧縮) から選択します。
- 「**JPEG イメージ品質**」オプションは変更できず、「**6**」に設定されています。
- 「**カーソル状態更新**」ドロップダウン リストで、「**有効**」、「**無視**」、または「**無効**」から選択します。既定は「**無視**」です。
- 画面上でアイテムを移動する際に効率を上げるには、「**CopyRect の使用**」を選択します。
- 色数を減らすことで能率を上げるには、「**制限された色数 (256 色)**」を選択します。
- マウスの右クリックと左クリックのボタンを入れ替えるには、「**マウス ボタン 2 と 3 を逆にする**」を選択します。
- 「**表示のみ**」を選択すると、デスクトップ ウィンドウ内のキーボードおよびマウス イベントが無効になります。
- 複数のユーザが同じ VNC デスクトップを参照して使用することを許可するには、「**デスクトップ共有**」を選択します。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、Mobile Connect クライアント上にブックマークが表示されます。このブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。

  メモ：サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

Citrix Portal (Citrix)

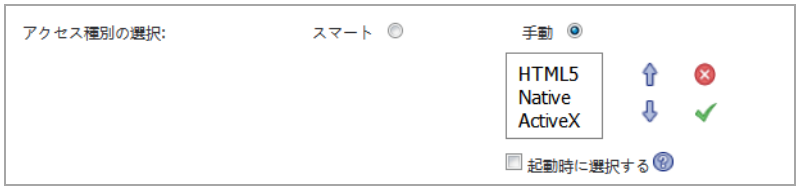
- 「**リソース ウィンドウ サイズ**」ドロップダウン リストから、ユーザがこのブックマークを実行した際に使用される既定の Citrix ポータル画面サイズを選択します。

1 「**アクセス タイプの選択**」を選びます。「**スマート**」または「**手動**」のどちらかです。

- 「**スマート**」: ファームウェアにクライアントを起動するモードを決定させます。

新しい統合ブックマークを作成する場合は、「**スマート**」がデフォルトで選択されています。ブックマークの起動時には、ブックマーク固有の既定モードを使用して自動検出の処理が行われます。

- 「**手動**」: モードや優先順位を設定し、方法を選択するオプションを提供します。選択ボックスで、少なくとも 1 つのモードが有効になっている必要があります。



起動シーケンスは、「**HTML5**」、「**Native**」、「**ActiveX**」です。「手動」を選択すると、起動方法を変更、有効化、または無効化できます。Citrix ブックマークの起動に「**Native**」を選択すると、SMA Connect Agent がローカル マシンの Citrix Receiver を起動して Citrix 接続を行います。

「**上**」と「**下**」の矢印を使って起動順序を調整します。バツとチェックのアイコンを使ってモードの有効と無効を切り替えます。無効にしたモードはリストの下に移動し、グレー表示されます。

「**手動**」モードでは、デフォルトで「**起動中に選択**」オプションは有効ではありません。この設定では、ブックマークの起動時に、設定済みリストの先頭にある使用可能なモードが自動検出後に実行されます。

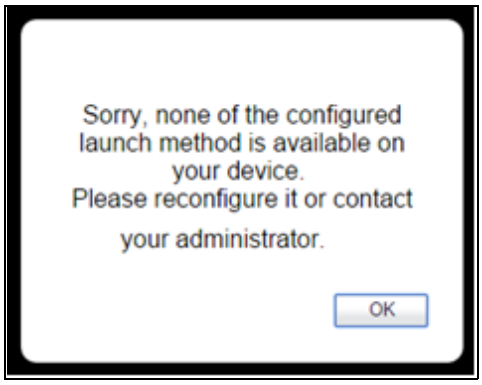
「**起動時に選択する**」オプションが有効になっていて、複数のモードがクライアントで使用可能な場合は、統合ブックマークの起動時にメニューが表示されます。このメニューでは、5 秒のカウントダウンが行われている間にモードを選択できます。使用可能なモードが 1 つしかない場合、ブックマークはただちに実行されます。

起動時に「**この選択を記憶する**」オプションが有効になっている場合は、選択されたモードが Cookie によって記憶されます。

その場合、次にブックマークを起動すると、記憶したモードが 2 秒以内に直接実行されます。HTML のどこかをクリックすると、記憶したモードを「忘れる」ので、再選択を行うことができます。

同じブラウザでブックマークの編集や削除しても、記憶したモードがリセットされます。

設定されたクライアントでどのモードも実行できない場合、次の通知が表示されます。



- HTTPS を使用して Citrix ポータルに安全にアクセスするには、オプションで「**HTTPS モード**」を選択します。
- オプションで「**指定した Citrix ICA サーバを常に使用する**」を選択して、現れた「**Citrix ICA サーバ アドレス**」フィールドに IP アドレスを指定します。この設定により、Citrix ICA セッションに対する Citrix ICA サーバのアドレスを指定することが可能です。既定では、ブックマークは Citrix サーバ上の ICA 設定内で提供される情報を使用します。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

ウェブ (HTTP)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ)を参照してください。
- シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の‘name’または‘id’属性と同じになるように設定します。例えば、<input type=text name='userid'> のようにします。「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の ‘name’ または ‘id’ 属性と同じになるように設定します。例えば、<input type=password name='PASSWORD' id='PASSWORD' maxlength=128> のようにします。

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

セキュア ウェブ (HTTPS)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の'name'または'id'属性と同じになるように設定します。例えば、<input type=text name='userid'> のようにします。「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の 'name' または 'id' 属性と同じになるように設定します。例えば、<input type=password name='PASSWORD' id='PASSWORD' maxlength=128> のようにします。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

外部ウェブ サイト

- SSL を使用してこのウェブ サイトとの通信を暗号化するには、「**HTTPS モード**」をオンにします。
- このウェブ サイトにアクセスする際にセキュリティ警告を一切表示しない場合は、「**セキュリティ警告を無効にする**」をオンにします。ブックマークがアプリケーション オフロードされたウェブ サイト以外の何かを参照しようとした場合に、通常セキュリティ警告が表示されます。
- このブックマークの仮想ホスト ドメインのシングル サインオンを有効にするには、「**自動的にログインする**」をオンにします。ブックマーク内のホストが、このポータルと同一の共有ドメインを持つポータルを参照する場合、このチェックボックスを選択すると、このポータルの認証情報で自動的にログインすることができます。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

Mobile Connect

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

  メモ：このブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

ファイル共有 (CIFS)

メモ：SMB2 および SMB3 プロトコルは現在サポートされていません。サーバは、Linux ベースのクライアントからの通信を許可するよう設定する必要があります。

- クライアント UI へのアクセスを制限するには、「**特定のファイル/フォルダにアクセスするユーザを設定する**」をオンにします。完全にアクセスを制限するには、「**サービス > ポリシー**」ページに移動して、アクセス制限のポリシーを設定します。詳細については、ユーザ ポリシーの追加 (402 ページ) を参照してください。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプションを有効にして、ユーザのドメインを RDP サーバに引き渡します。

  このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

  ファイル共有を作成するときは、DFS (Distributed File System) サーバをウィンドウズ ドメイン ルート システムに設定しないでください。ドメイン ルートはドメイン内の Windows コンピュータへのアクセスのみを提供するので、DFS サーバをドメイン ルートに設定すると、他のドメインから DFS ファイル共有にアクセスできません。SMA/SRA 装置は、ドメイン メンバではなく、このような DFS 共有に接続できません。

  スタンドアロン ルート上の DFS ファイル共有には、Microsoft の制限は適用されません。

ファイル転送プロトコル (FTP)

- 「**詳細なサーバ設定を表示**」を展開して、代替値を「**文字エンコード**」ドロップダウンリストで選択します。既定値は「**標準 (UTF-8)**」です。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから FTP サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

  ファイル共有を作成するときは、DFS (Distributed File System) サーバをウィンドウズ ドメイン ルート システムに設定しないでください。ドメイン ルートはドメイン内の Windows コンピュータへのアクセスのみを提供するので、DFS サーバをドメイン ルートに設定すると、他のドメインから DFS ファイル共有にアクセスできません。SMA/SRA 装置は、ドメイン メンバではなく、このような DFS 共有に接続できません。

  スタンドアロン ルート上の DFS ファイル共有には、Microsoft の制限は適用されません。

SSH ファイル転送プロトコル (SFTP)

- 「**詳細なサーバ設定を表示**」を展開して、代替値を「**文字エンコード**」ドロップダウンリストで選択します。既定値は「**標準 (UTF-8)**」です。

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから FTP サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

Telnet

- シングル サインオン (SSO) は Telnet ブックマークに対応しています。ブックマークは、ブックマーク設定の「**自動的にログインする**」オプションを有効にして設定しておく必要があります。適切なユーザ名とパスワードが設定されている場合、セッションへのログインは自動的に行われます。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

セキュア シェル バージョン 2 (SSHv2)

- シングル サインオンは SSH ブックマークに対応しています。ブックマークは、ブックマーク設定の「**自動的にログインする**」オプションを有効にして設定しておく必要があります。適切なユーザ名とパスワードが設定されている場合、セッションへのログインは自動的に行われます。
- SSHv2 HTML5 ブックマークの場合、SSO はユーザ名とパスワードの両方の認証でサポートされています。SSO に失敗した場合は、メニューがポップアップ表示され、資格情報の手動入力またはログインのキャンセルを選択することができます。

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

2 「**適用**」を選択して設定を更新します。設定を更新すると、新しいユーザ ブックマークが「**ローカル ユーザの編集**」ウィンドウに表示されます。

機器単位ライセンスのサポート

リモート デスクトップ セッション ホスト (RD セッション ホスト) サーバが機器単位ライセンス モードを使用するように設定されている場合、クライアント コンピュータまたはクライアント機器が RD セッション ホスト サーバに初めて接続すると、既定ではクライアント コンピュータまたは機器に対して一時的なライセンスが発行されます。リモート デスクトップ ライセンス サーバがアクティブで、十分な数のリモート デスクトップ サービス (RDS) 機器単位クライアント アクセス ライセンス (CAL) が使用可能な場合、クライアント コンピュータまたは機器が 2 回目に RD セッション ホスト サーバに接続すると、ライセンス サーバはクライアント コンピュータまたは機器に対して永続的な RDS 機器単位 CAL を発行します。ライセンス サーバがアクティブでないか、使用可能な機器単位 CAL がない場合、機器は引き続き、一時的なライセンスを使用します。一時的なライセンスは、90 日間有効です。

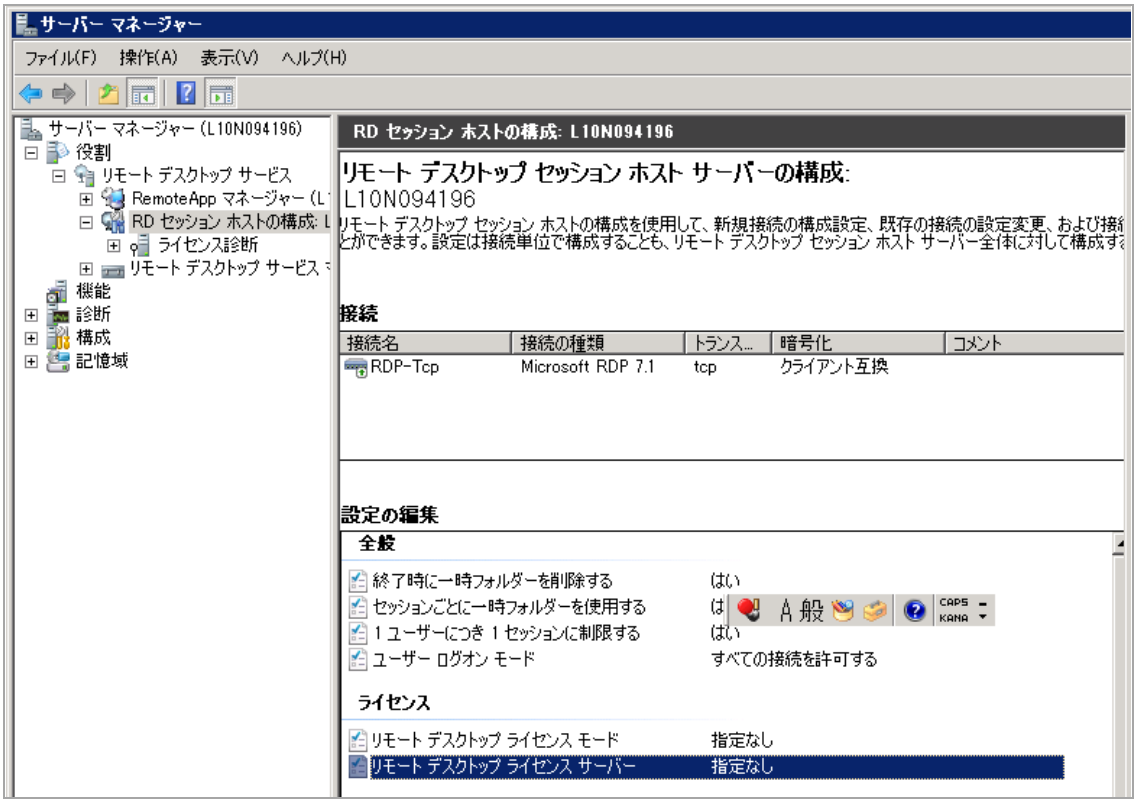
ライセンス サーバによって発行された永続的な RDS 機器単位 CAL は、52 ～ 89 日間のランダムな期間の経過後に自動的に期限が切れるように設定されており、その時点で RDS 機器単位 CAL は、ライセンス サーバ上にある使用可能な RDS 機器単位 CAL のプールに返却されます。

機器単位ライセンス サーバの設定

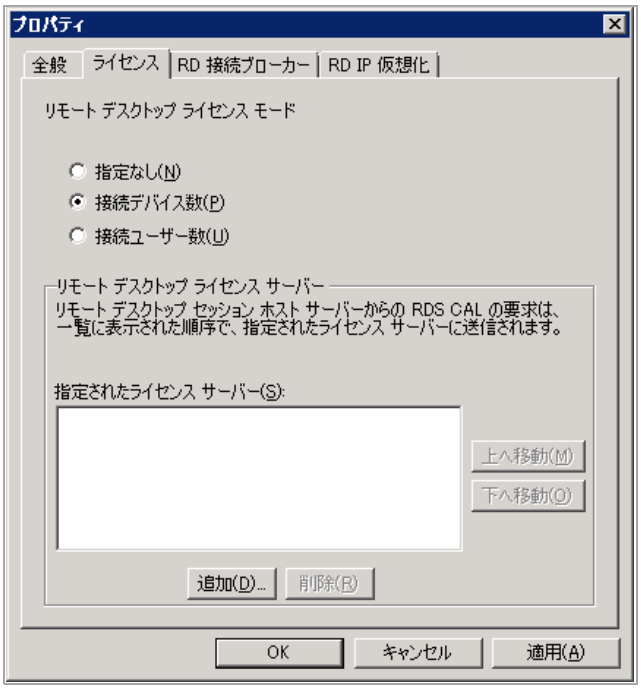
このセクションでは、Windows Server 2008 R2 での機器単位ライセンスの設定方法を説明します。ほかのバージョンのサーバでは、設定の詳細が異なる場合があります。

ライセンス サーバを追加するには、以下の手順に従います。

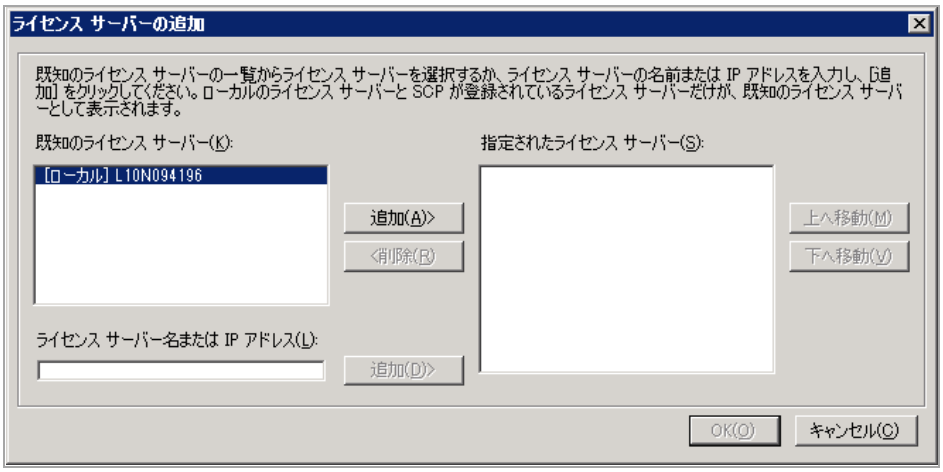
1 「サーバ マネージャ」画面の「**設定の編集**」の下にある「**リモート デスクトップ ライセンス サーバ**」をダブルクリックします。



2 表示される「プロパティ」ダイアログの「ライセンス」ページで、「**追加**」をクリックします。

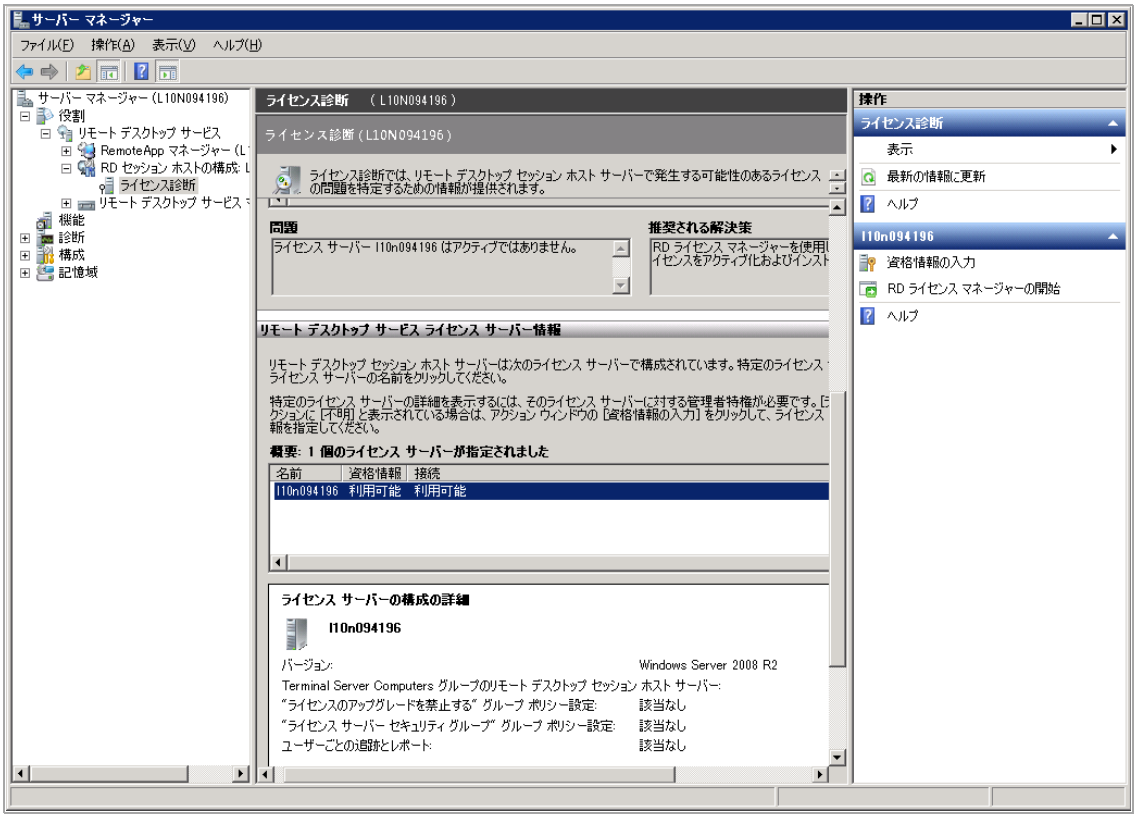


3 「**ライセンス サーバの追加**」ダイアログが表示されます。「ライセンス サーバ名または IP アドレス」フィールドを選択し、「**追加**」をクリックします。



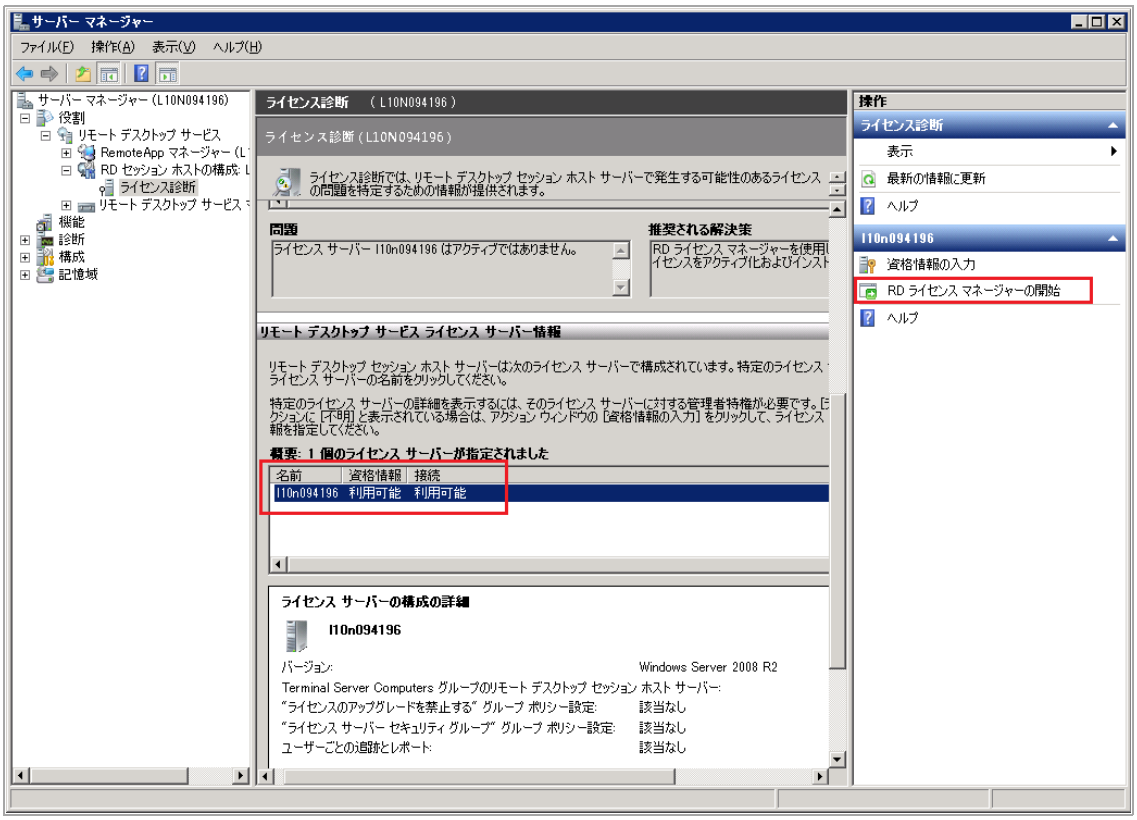
ライセンス サーバを設定するには:

1 「サーバ マネージャ」画面の左ナビゲーション ペインで、「**ライセンス診断**」を選択します。

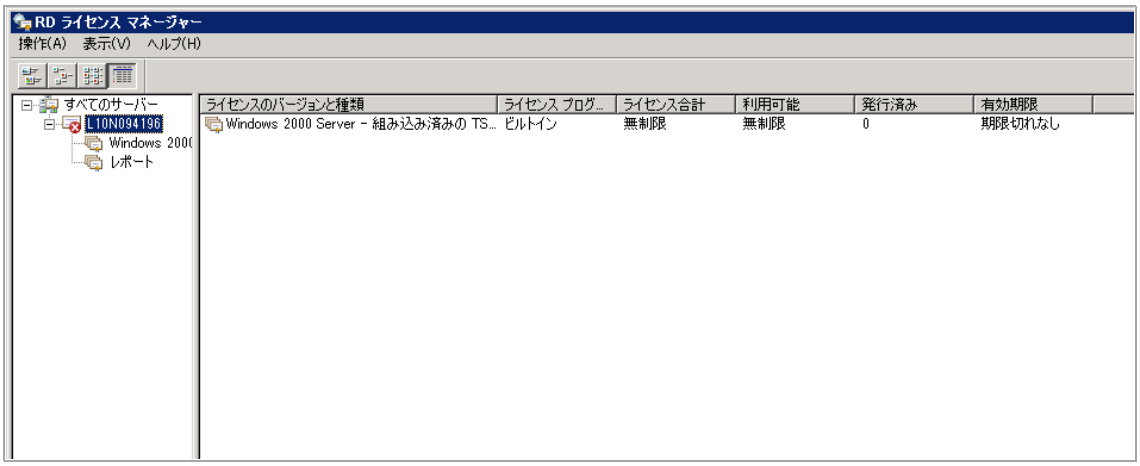


2 中央ペインの「**x 個のライセンス サーバーが指定されました**」の下で、適切なサーバ名または IP アドレスを選択します。右側のペインに追加の動作が表示されます。

3 右側のペインで、「**RD ライセンス マネージャの開始**」をクリックします。



4 次の画面には、「**一時的**」と表示された使用可能ライセンスのリストが表示されます。

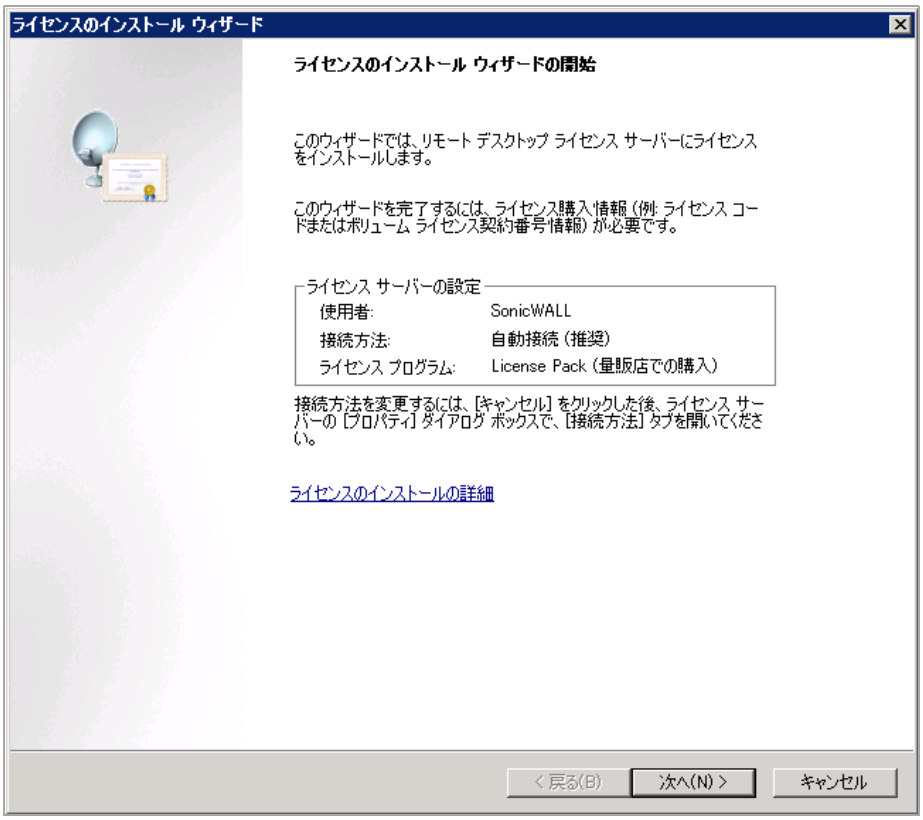


この画面で、機器単位ライセンスを管理します。

異なるウェブ ブラウザからのリモート接続ごとに機器ライセンスが 1 つ消費されます。前の画面ではライセンスを取り消すことができますが、一定の期間に取り消せる回数は限られています。

リモート デスクトップ サービスのクライアント アクセス ライセンスをインストールするには:

1 「すべてのサーバ」の下の左ペインにあるサーバを右クリックし、「ライセンスのインストール」を選択して、ウィザードによる段階的な指示に従います。ただし、インターネット接続が利用可能なことを確認しておいてください。



ローカル ユーザの Citrix ブックマークの作成

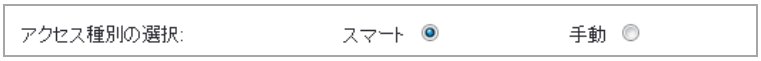
Citrix ブックマークは、Windows、MacOS、および Linux でサポートされています。Citrix サポートには、ActiveX または Java クライアントを Citrix のウェブ サイトからダウンロードするためのインターネット接続が必要です。インターネット エクスプローラでは既定で ActiveX を使用して、その他のブラウザでは Java を使用して Citrix にアクセスします。Java をインターネット エクスプローラで使用するには、ブックマーク設定でオプションを選択します。サーバはどの Citrix クライアント バージョンを使用するかを自動的に判断します。

メモ：Citrix が Java の Receiver のサポートを終了したため、SonicWall Inc. は Citrix Java ブックマークの公式サポートを終了しました。Citrix ブックマークには、HTML5、ネイティブ、または ActiveX のアクセス方法の使用を推奨します。

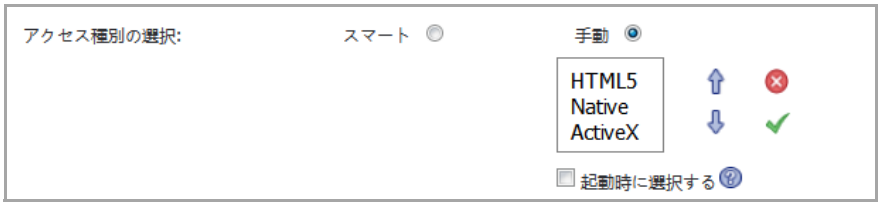
ユーザの Citrix ブックマークを設定するには:

1. 「**ユーザ** > ローカル ユーザ」を開き、設定するユーザの横にある設定アイコンを選択します。
2. 「**ローカル ユーザの編集**」ページで、「**ブックマーク**」ページを選択します。
3. 「**ブックマークの追加**」を選択します。
4. ブックマークの名前を「**ブックマーク名**」フィールドに入力します。
5. ブックマークの名前または IP アドレスを「**名前または IP アドレス**」フィールドに入力します。

   メモ：HTTPS、HTTP、Citrix、SSHv2、Telnet、および VNC では、ポート オプションの :portnum を指定できます。HTTP、HTTPS、およびファイル共有では、ディレクトリまたはファイルのパスも指定できます。
6. 「**説明**」フィールドに、ブックマーク テーブル内に表示するわかりやすい説明を必要に応じて入力します。
7. 必要に応じて、このブックマークを表示する場所に**タブ**のコンマ区切りリストを入力します。標準のタブ (デスクトップ、ウェブ、ファイル、ターミナル、モバイル) は指定する必要がありません。例えば、「お気に入り, タブ 1, タブ 2」と指定します。
8. 「**サービス**」ドロップダウン リストで、「**Citrix ポータル (Citrix)**」を選択します。表示が変更されます。
9. ドロップダウン リストから「**リソース ウィンドウ サイズ**」を選択します。
10. 「**アクセス タイプの選択**」を選びます。「**スマート**」または「**手動**」のどちらかです。
    - 「**スマート**」: ファームウェアにクライアントを起動するモードを決定させます。

      新しい統合ブックマークを作成する場合は、「**スマート**」がデフォルトで選択されています。ブックマークの起動時には、ブックマーク固有の既定モードを使用して自動検出の処理が行われます。
    - 「**手動**」: モードや優先順位を設定し、方法を選択するオプションを提供します。選択ボックスで、少なくとも 1 つのモードが有効になっている必要があります。

起動シーケンスは、「**HTML5**」、「**Native**」、「**ActiveX**」です。「手動」を選択すると、起動方法を変更、有効化、または無効化できます。Citrix ブックマークの起動に「**Native**」を選択すると、SMA Connect Agent がローカル マシンの Citrix Receiver を起動して Citrix 接続を行います。

「**上**」と「**下**」の矢印を使って起動順序を調整します。バツとチェックのアイコンを使ってモードの有効と無効を切り替えます。無効にしたモードはリストの下に移動し、グレー表示されます。

「**手動**」モードでは、デフォルトで「**起動中に選択**」オプションは有効ではありません。この設定では、ブックマークの起動時に、設定済みリストの先頭にある使用可能なモードが自動検出後に実行されます。

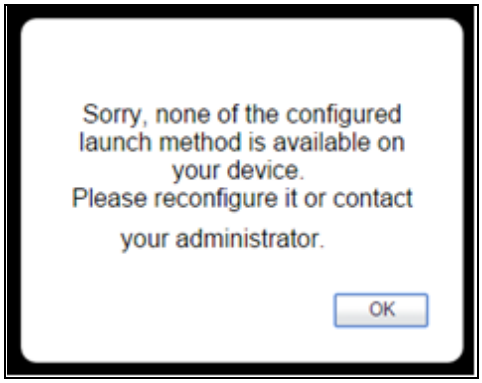
「**起動時に選択する**」オプションが有効になっていて、複数のモードがクライアントで使用可能な場合は、統合ブックマークの起動時にメニューが表示されます。このメニューでは、5 秒のカウントダウンが行われている間にモードを選択できます。使用可能なモードが 1 つしかない場合、ブックマークはただちに実行されます。

起動時に「**この選択を記憶する**」オプションが有効になっている場合は、選択されたモードが Cookie によって記憶されます。

その場合、次にブックマークを起動すると、記憶したモードが 2 秒以内に直接実行されます。HTML のどこかをクリックすると、記憶したモードを「忘れる」ので、再選択を行うことができます。

同じブラウザでブックマークの編集や削除しても、記憶したモードがリセットされます。

設定されたクライアントでどのモードも実行できない場合、次の通知が表示されます。



11 「**HTTPS モード**」の横のボックスをオンにして、Citrix ポータルにセキュアにアクセスします。

12 オプションで「**指定した Citrix ICA サーバを常に使用する**」を選択して、現れた「**Citrix ICA サーバ アドレス**」フィールドに IP アドレスを指定します。この設定により、Citrix ICA セッションに対する Citrix ICA サーバのアドレスを指定することが可能です。既定では、ブックマークは Citrix サーバ上の ICA 設定内で提供される情報を使用します。

- **Windows** - SMA Connect Agent は ICA ファイルを開いて Citrix Receiver を起動しようとします。Citrix Receiver がインストールされていない場合は、次のメッセージがポップアップ表示されます。
- **Macintosh** - SMA Connect Agent は "Citrix Receiver"を検索してこのアプリケーションがインストールされていることを確認します。SMA Connect Agent は Citrix 接続を確立するために "Citrix Receiver" を起動します。このアプリケーションをまだインストールしていない場合は、インストールを開始するための警告メッセージが SMA Connect Agent によってポップアップ表示されます。

13 「**適用**」を選択します。

個別 SSO 資格情報によるブックマークの作成

管理者は HTTP (HTTPS)、RDP (ActiveX、VNC)、ファイル共有 (CIFS)、および FTP ブックマークで個別のシングル サイン オン (SSO) 資格情報をユーザ別、グループ別、またはグローバルに設定することができます。この機能は、SSO 認証の際にドメイン接頭辞を必要とする HTTP、RDP、FTP サーバなどのリソースにアクセスするために使用されます。ユーザは SMA/SRA 装置に *username* を使ってログインし、個別のブックマークを選択して *domain\username* を使ってサーバにアクセスできます。「**ユーザ名**」と「**ドメイン**」には、テキストのパラメータまたは動的変数を使用できます。「**パスワード**」フィールドには、提示する個別パスワードを入力するか、空白のままにして現在のユーザのパスワードをブックマークに提示します。

個別の SSO 認証情報を設定して、シングル サインオンをフォーム ベースの認証 (FBA) に対して設定するには:

1 ユーザ ブックマークの追加または編集 (409 ページ) に説明した手順に従って、Citrix、HTTP (HTTPS)、RDP、ファイル共有 (CIFS)、または FTP ブックマークを作成または編集します。

2 Citrix ブックマークの場合は、「**自動的にログインする**」オプションを有効にします。Citrix SSO ブックマークでは「**フォームベース認証**」のみが使用できます。

「**ブックマーク**」ページで、「**個別認証情報を使用する**」オプションを選択します。

3 「**ユーザ名**」と「**ドメイン**」に、ブックマークに提示する個別のテキストを入力するか、以下の動的な変数を使用します。

動的変数

用途	変数	使用例
ログイン名	%USERNAME%	US\%USERNAME%
ドメイン名	%USERDOMAIN%	%USERDOMAIN%\%USERNAME%
グループ名	%USERGROUP%	%USERGROUP%\%USERNAME%
IP アドレス	%IPADDR%	%IPADDR%\%USERNAME%

4 「**パスワード**」フィールドに、提示する個別パスワードを入力するか、空白のままにして現在のユーザのパスワードをブックマークに提示します。

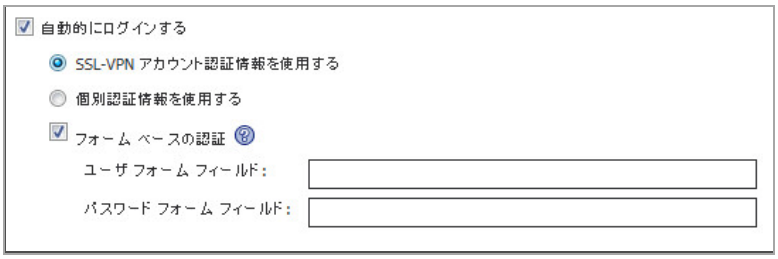
5 シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。

- **ユーザ フォーム フィールド** - ログイン フォームでユーザ名を表す HTML 要素の'name'および'id'属性と同じになるように設定します。例えば、次のようにします。

  ```
  <input type=text name='userid'>
  ```

- **パスワード フォーム フィールド** - ログイン フォームでパスワードを表す HTML 要素の'name'または'id'属性と同じになるように設定します。例えば、次のようにします。

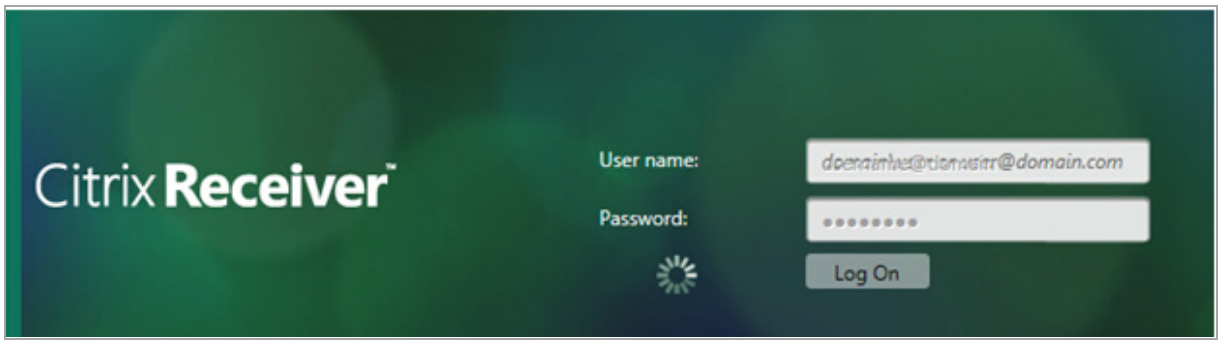
  ```
  <input type=password name=PASSWORD id=PASSWORD maxlength=128>
  ```



6 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

7 「**適用**」を選択します。

Citrix ブックマークの起動後、次の図に示すように Citrix StoreFront ポータルへの自動ログインが可能になり、**XenApp** または **XenDesktop** を使用できる状態になります。



ログイン ポリシーの設定

「**ログイン ポリシー**」ページには、SMA/SRA 装置へのログインをユーザの IP アドレスによって許可または拒否するポリシーの設定オプションがあります。

装置への特定のユーザのログインを許可または拒否するには:

1 「**ユーザ > ローカル ユーザ**」ページに移動します。

2 設定するユーザの設定アイコンを選択します。「**ローカル ユーザの編集**」ページが表示されます。

3 「**ログイン ポリシー**」ページを選択します。「**ローカル ユーザの編集 - ログイン ポリシー**」ページが表示されます。

4 指定したユーザが装置にログインするのを阻止するには、「**ログインを無効にする**」をオンにします。

5 必要に応じて、「**クライアント証明書の強制を有効にする**」ドロップダウン メニューから「**有効化**」を選択して、ログインに際してクライアント証明書を要求するようにします。このオプションをオンにするのは、クライアントにクライアント証明書を提示するよう要求して強力な相互認証を行う場合です。さらに次の 2 つのフィールドが表示されます。

- **ユーザ名がクライアント証明書の一般名 (CN) と一致していることを確認する** - ユーザのアカウント名がクライアント証明書と一致することを要件とする場合は、このチェックボックスをオンにします。
- **サブジェクト内の部分 DN を確認する** - 次の変数を使ってクライアント証明書と一致する部分 DN を設定します。
  - ユーザ名: %USERNAME%
  - ドメイン名: %USERDOMAIN%
  - アクティブ ディレクトリ ユーザ名: %ADUSERNAME%
  - ワイルドカード: %WILDCARD%

6 指定したユーザに装置へのログイン時にワンタイム パスワードの使用を要求するには、「**ワンタイム パスワードを要求する**」をオンにします。

7 「**ワンタイム パスワード**」ドロップダウン リストで、「**ドメイン設定を使用する**」、「**有効化**」、または「**無効化**」を選択します。既定値は「**ドメイン設定を使用する**」です。

8 「**ワンタイム パスワード**」ドロップダウン メニューから、以下のいずれかを選択します。

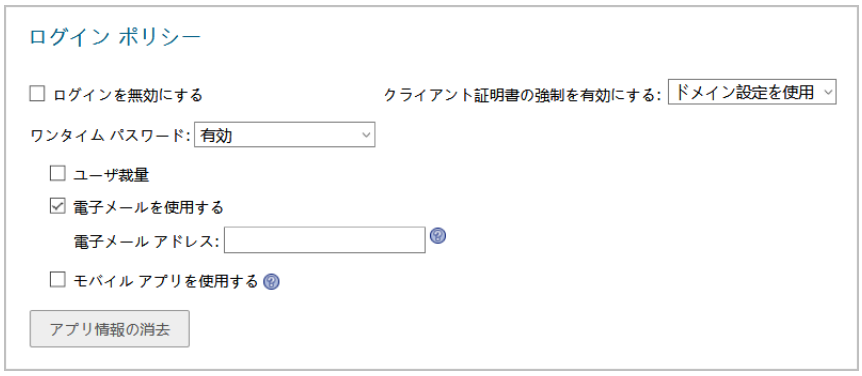
- **ドメイン設定を使用する** - ドメイン設定で指定されているアクションを実行します。このオプションの既定の設定は「ドメイン設定を使用」です。ドメインの追加と編集 (188 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。ドメイン設定を上書きします。

このオプションを選択すると、さらに次の 3 つのフィールドが表示されます。

- **ユーザ裁量** -「**ユーザ > ローカル ユーザ > ローカル ユーザの編集**」ページからワンタイム パスワード設定を編集できるようにします。ユーザは、以下のワンタイム パスワード方式のどちらか一方または両方を選択できます。
  - 「**電子メールを使用する**」は、ユーザが「**電子メールを使用する**」を選択して、このワンタイム パスワード方式を有効化できるようにします。
  - 「**モバイル アプリを使用する**」は、ユーザが「モバイル アプリを使用する」を選択してこのワンタイム パスワード方式を有効化できるようにします。

    メモ：電子メールとモバイル アプリの両方の方式を有効化した場合、ドロップダウン メニューから優先するワンタイム パスワード方式を指定します。

- **電子メールを使用する** - 必要に応じて「**電子メールを使用する**」を選択して、このワンタイム パスワード方式を有効化します。「**電子メール ドメイン:**」ウィンドウが表示されます。ここで、ワンタイム パスワードを送信する電子メール アドレスを入力できます。



- **モバイル アプリを使用する** - 必要に応じて「**モバイル アプリを使用する**」を選択します。これで、このワンタイム パスワード方式を有効化してユーザにワンタイム パスワードを強制的に使用させることができます。ユーザは Google Authenticator、Duo Mobile、またはその他の適合二段階認証サービスを利用できます。

> **メモ**:電子メールとモバイル アプリの両方の方式を有効化した場合、ドロップダウン メニューから優先するワンタイム パスワード方式を指定します。

- **無効** - この操作をユーザに対して無効にします。ドメイン設定を上書きします。

9 必要に応じて「**アプリ情報の消去**」をクリックして、モバイル アプリのバインディング情報を消去します。

10 選択したポリシーを送信元 IP アドレスに適用するには、アクセス ポリシー (「**許可**」または「**拒否**」) を、「**送信元 IP アドレスに対するログイン ポリシー**」の「**定義済みアドレスからのログイン**」ドロップダウン リストで選択し、リストボックスの下にある「**追加**」を選択します。「**アドレスの定義**」ウィンドウが表示されます。

11 「**アドレスの定義**」ウィンドウで、「**送信元アドレス種別**」ドロップダウン リストから送信元 IP アドレスの種類の 1 つを選択します。

- **IP アドレス** - 特定の IP アドレスを選択します。
- **IP ネットワーク** - IP アドレス範囲を選択します。このオプションを選択すると、「**ネットワーク アドレス**」フィールドと「**サブネット マスク**」フィールドが「**アドレスの定義**」ウィンドウに表示されます。
- **IPv6 アドレス** - これにより特定の IPv6 アドレスを選択できます。

- **IPv6 ネットワーク** - これにより IPv6 アドレス範囲を選択できます。このオプションを選択すると、「**IPv6 ネットワーク**」フィールドと「**プレフィックス**」フィールドが「**アドレスの定義**」ウィンドウに表示されます。

12 選択した送信元アドレス種別に対応する IP アドレスを指定します。

- **IP アドレス** - 単一の IP アドレスを「**IP アドレス**」フィールドに入力します。
- **IP ネットワーク** - IP アドレスを「**ネットワーク アドレス**」フィールドに入力し、アドレス範囲を指定するサブネット マスク値を「**サブネット マスク**」フィールドに入力します。
- **IPv6 アドレス** - **2007::1:2:3:4**などの IPv6 アドレスを入力します。
- **IPv6 ネットワーク** - IPv6 ネットワーク アドレスを「**IPv6 ネットワーク**」フィールドに **2007:1:2::**形式で入力します。**64** などのプレフィックスを「**プレフィックス**」フィールドに入力します。

13 「**追加**」を選択します。アドレスまたはアドレス範囲が「**ユーザ設定の編集**」ウィンドウの「**定義済みアドレス**」リストに表示されます。例えば、ネットワーク アドレス 10.202.4.32、サブネット マスク値 255.255.255.240 (28 ビット)のアドレス範囲を選択すると、「定義済みアドレス」リストに 10.202.4.32 - 10.202.4.47 と表示されます。この例では、10.202.4.47 はブロードキャスト アドレスになります。選択したログイン ポリシーが、この範囲のアドレスに適用されます。

14 選択したポリシーをクライアント ブラウザに適用するには、「**クライアント ブラウザに対するログイン ポリシー**」の「**定義済みブラウザからのログイン**」ドロップダウン リストでアクセス ポリシー (**許可**または**拒否**) を選択し、リストから「**追加**」を選択します。「**ブラウザの定義**」ウィンドウが表示されます。

15 「**ブラウザの定義**」ウィンドウで、ブラウザの定義を「**クライアント ブラウザ**」フィールドに入力し、「**追加**」を選択します。ブラウザの名前が「**定義済みブラウザ**」リストに表示されます。

> **メモ：** Firefox、および Internet Explorer のブラウザの定義は、javascript:document:writeln (navigator.userAgent) です。

16 「**適用**」を選択します。新しいログイン ポリシーが保存されます。

ユーザに対するエンド ポイント制御の設定

ローカル ユーザが使用するエンド ポイント制御プロファイルを設定するには:

1 「**ユーザ** > **ローカル ユーザ**」ページを開きます。

2 EPC を設定するユーザの設定アイコンを選択します。「**ローカル ユーザの編集**」ページが表示されます。

3 「**EPC** 」ページを選択します。「**EPC の設定**」ページが表示されます。

4 ユーザの EPC 設定を構成して、デバイス プロファイルを追加または削除します。

キャプチャ ATP の設定

「**キャプチャ ATP**」ページには、キャプチャ ATP を有効化する設定オプションがあります。キャプチャ ATP の設定は、以下のセクションに分かれています。

- 一般設定
- ファイル 種別の設定

- ファイル サイズの設定
- ユーザ定義の遮断動作

一般設定

仮想アシストの一般設定を行うには:

1 「**ユーザ > ローカル ユーザ > ローカル ユーザの編集**」ページに移動し、「**キャプチャ**」タブを選択します。「ローカル ユーザの編集」ページが表示されます。

2 「一般設定」セクションの「**キャプチャ ATP サービスを有効にする**」ドロップダウン メニューから、以下のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **有効** - この操作をユーザに対して有効にします。この設定はグループ設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

3 「**適用**」を選択して設定を保存します。

ファイル 種別の設定

ファイル 種別の設定を構成するには:

1 「**ユーザ > ローカル ユーザ > ローカル ユーザの編集**」ページに移動し、「**キャプチャ**」タブを選択します。「ローカル ユーザの編集」ページが表示されます。

2 「**ファイル 種別設定**」ドロップダウン メニューから、以下のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **個別設定を使用する** - 個別設定で指定されたアクションを実行します。

3 「**適用**」を選択して設定を保存します。

ファイル サイズの設定

ファイル サイズの設定を構成するには:

1 「**ユーザ > ローカル ユーザ > ローカル ユーザの編集**」ページに移動し、「**キャプチャ**」タブを選択します。「ローカル ユーザの編集」ページが表示されます。

2 キャプチャ ATP サービスに送信されるファイルの最大サイズを指定するには、「**ファイルの最大サイズ**」ウィンドウに値を入力します。有効な最大サイズは、ユーザ レベルとグループ レベルで 0 - 10 MB、グローバル レベルで 1 - 10 MB です。

- ユーザ レベルで値を 0 に設定すると、SMA はグループ設定の最大ファイル サイズを使用します。
- グループ レベルで値を 0 に設定すると、SMA はグローバル設定の最大ファイル サイズを使用します。

3 ファイル サイズが最大値より小さいファイルがキャプチャ ATP サービスに送信されてチェックされます。

4 「**ファイル サイズがサイズ制限を超える場合、バックエンド サーバにファイルを送信しない**」ドロップダウン メニューから、以下のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **個別設定を使用する** - 個別設定で指定されたアクションを実行します。

5 「**適用**」を選択して設定を保存します。

ユーザ定義の遮断動作

ユーザ定義の遮断動作を構成するには:

1 「**キャプチャ ATP サービスとの通信が失敗した場合、アップロードを遮断する**」ドロップダウン メニューから以下のいずれかを選択します。

- **グループ設定を使用する** - グループ設定で指定された操作を行います。グループ設定の編集 (442 ページ) を参照してください。
- **個別設定を使用する** - 個別設定で指定されたアクションを実行します。

2 「**適用**」を選択して設定を保存します。

ユーザ > ローカル グループ

このセクションでは、「**ユーザ > ローカル グループ**」ページの概要と、このページで行える設定タスクについて説明します。

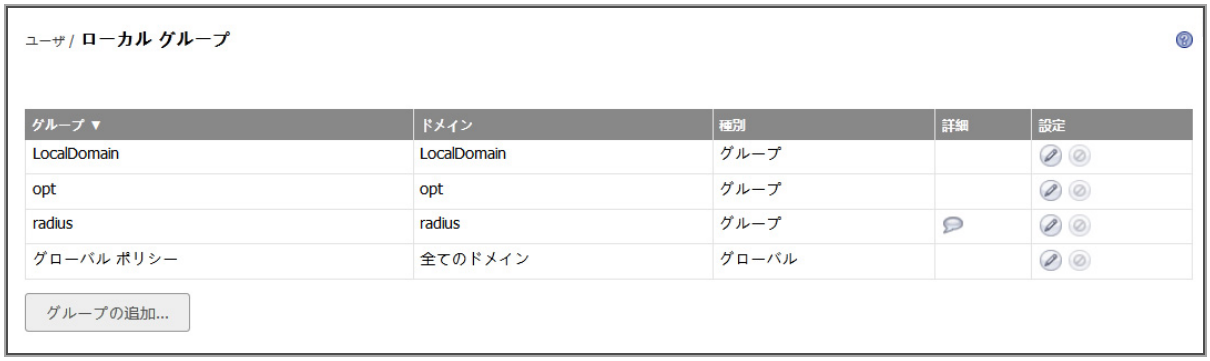
ローカル グループのグローバルな設定の詳細については、グローバル設定 (474 ページ) を参照してください。

「ユーザ > ローカル グループ」の概要

「**ユーザ > ローカル グループ**」ページでは、グループ名とドメインを指定することにより、ユーザのアクセスを正確に制御するためにグループを追加および設定できます。

ドメインを作成するとグループが自動的に作成されることに注意してください。ドメインは、「**ポータル > ドメイン**」ページで作成することができます。「**ユーザ > ローカル グループ**」ページからグループを直接作成することもできます。

「ユーザ > ローカル グループ」ページ



グループ メンバーシップは、2 つのグループ、'プライマリ' と '追加'に分けられます。

プライマリ グループ - タイムアウトやブックマークの追加/編集といった、単純なポリシーの割り当てに使用します。URL やネットワーク オブジェクト ポリシーといった、上級のポリシーには、プライマリまたは追加グループが使用できます。

追加グループ - 複数の追加グループを割り当てることができますが、ポリシーの競合がある場合はプライマリ グループがすべての追加グループより優先されます。

ユーザは、単一ドメイン内のグループにのみ所属できることを覚えておいてください。

グループの削除

グループを削除するには、「**ユーザ > ローカル グループ**」ページのローカル グループ テーブルで、削除するグループの行の削除アイコン ⊗ を選択します。削除したグループは、定義済みグループのリストに表示されなくなります。

ⓘ **メモ**：ユーザがグループに追加されたままの場合、またはグループが認証ドメインに対する既定のグループになっている場合は、グループは削除できません。認証ドメインに対する既定のグループを削除するには、対応するドメインを削除します (「**グループ設定の編集**」ウィンドウからはグループを削除できません) 。グループが認証ドメインに対する既定のグループではない場合は、最初にグループからすべてのユーザを削除します。その後、「**グループ設定の編集**」ページでグループを削除することができます。

新規グループの追加

ドメインを作成するとグループが自動的に作成されることに注意してください。ドメインは、「**ポータル > ドメイン**」ページで作成することができます。「**ユーザ > ローカル グループ**」ページからグループを直接作成することもできます。

「**ユーザ > ローカル グループ**」ウィンドウに次の 2 つの既定のオブジェクトがあります。

- **グローバル ポリシー** - 組織内のすべてのノードのアクセス ポリシーです。
- **LocalDomain** - LocalDomain グループは、既定の LocalDomain 認証ドメインに対応して自動的に作成されます。これは、特に指定がなかったときにローカル ユーザが追加される既定のグループです。

新しいグループを作成するには:

1 「**ユーザ > ローカル グループ**」ページに移動します。「ローカル グループ」ページが表示されます。

1 「**グループの追加**」をクリックします。「**ローカル グループの追加**」ウィンドウが表示されます。

2 「**ローカル グループの追加**」ウィンドウで、わかりやすいグループ名を「**グループ名**」フィールドに入力します。

3 適切なドメインを「**ドメイン**」ドロップダウン リストで選択します。ドメインがグループにマッピングされます。

4 「**適用**」を選択して設定を更新します。グループを追加すると、新しいグループが「**ローカル グループ**」ウィンドウに追加されます。

設定したすべてのグループは、「**ユーザ > ローカル グループ**」ページにアルファベット順で表示されます。

グループ設定の編集

グループを編集するには、「**ユーザ > ローカル グループ**」ページのローカル グループ テーブルで、編集するグループの行で設定アイコン を選択します。「グループ設定の編集」ウィンドウは次の 8 ページで構成されます: **一般**、**ポータル**、**クライアント**、**ルート**、**ポリシー**、**ブックマーク**、**EPC**、**キャプチャ**。

設定については、以下の各セクションを参照してください。

- ローカル グループの一般設定を編集する (442 ページ)
- グループ ポータル設定の変更 (444 ページ)
- クライアントのグループ設定を有効化する (445 ページ)
- グループ単位で ルートを有効にする (448 ページ)
- グループ ポリシーの追加 (449 ページ)
- ファイル共有のポリシーの編集 (451 ページ)
- グループ ブックマークの設定 (452 ページ)

ローカル グループの一般設定を編集する

「**一般**」**ページ**には、グループの無動作タイムアウトの値およびシングル サインオン設定の構成オプションがあります。

グループの一般設定を変更するには:

1 左側の列で、「**ユーザ > ローカル グループ**」を開きます。

2 設定するグループの横にある設定アイコンを選択します。「**グループ設定の編集**」ウィンドウの「**一般**」ページが表示されます。「**一般グループ設定**」セクションの「**グループ名**」および「**ドメイン名**」は、設定できないフィールドです。

3 グループの無動作タイムアウトを設定し、コンピュータ上の無動作が指定した時間を経過したらユーザを仮想オフィスからログアウトさせるには、許容する無動作時間 (分) を「**無動作タイムアウト**」フィールドに入力します。グローバル タイムアウトを使うには 0 に設定します。

> **メモ**：無動作タイムアウトは、ユーザ、グループ、グローバルの各レベルで設定できます。特定のユーザに複数のタイムアウトが設定されている場合は、ユーザ タイムアウトの設定がグループ タイムアウトよりも優先され、グループ タイムアウトがグローバル タイムアウトよりも優先されます。グローバル タイムアウトを 0 に設定すると、グループまたはユーザ タイムアウトが設定されていないユーザの無動作タイムアウトは無効になります。

4 グループに対してセッション制限タイムアウト (セッションが指定の時間だけアイドルだったときユーザを仮想オフィスからサインアウトさせる) を設定するには、以下のいずれかのオプションを選択します。

- **グローバル設定を使用する** このオプションは、グローバル ポリシーの設定を使用してセッション制限タイムアウトを制御する場合に選択します。デフォルト値は **0** です。

  > **メモ**：セッション制限タイムアウトは、ユーザ、グループ、グローバルの各レベルで設定できます。特定のユーザに複数のタイムアウトが設定されている場合は、ユーザ タイムアウトの設定がグループ タイムアウトよりも優先され、グループ タイムアウトがグローバル タイムアウトよりも優先されます。グローバル設定のタイムアウトを 0 に設定すると、グループまたはユーザのタイムアウトが構成されていないユーザのセッション制限タイムアウトが無効化されます。

- **ユーザ定義:** セッション制限タイムアウトの値を設定するには、このオプションを選択します。既定値は 0 です。

5 「**シングル サインオン設定**」で、「**自動的にブックマークにログイン**」ドロップダウン メニューから、次のいずれかのオプションを選択します。

- **グローバル ポリシーを使用する**: グローバル ポリシーの設定を使ってブックマークのシングル サインオン (SSO) を制御します。
- **ユーザ制御** (新しいユーザに既定で有効): ブックマークのシングル サインオン (SSO) をユーザが有効または無効にできるようにします。新規ユーザの場合は、この設定によって SSO が既定で有効になります。

  メモ: SMA/SRA 装置のシングル サインオンは、二段階認証をサポートしていません。

- **ユーザ制御 (新しいユーザに既定で無効)**: ブックマークのシングル サインオン (SSO) をユーザが有効または無効にできるようにします。新規ユーザの場合は、この設定によって SSO が既定で無効になります。
- **有効**: ブックマークのシングル サインオンを有効にします。
- **無効**: ブックマークのシングル サインオンを無効にします。

6 「**適用**」を選択して設定の変更を保存します。

グループ ポータル設定の変更

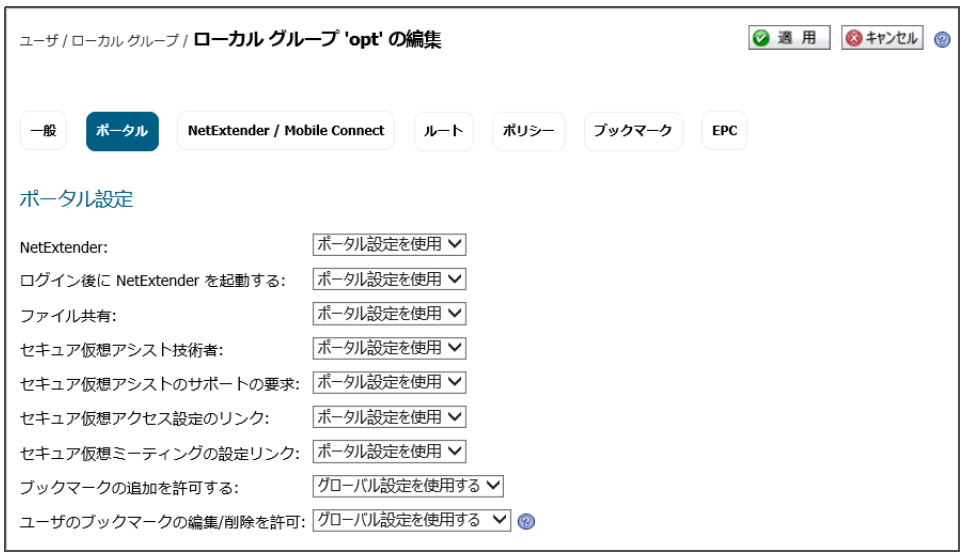
「**ポータル設定**」セクションには、このグループのポータル設定用のオプションがあります。

このグループに対してポータル設定を構成するには:

1 左側の列で、「**ユーザ** > **ローカル グループ**」を開きます。

2 設定するグループの横にある設定アイコンを選択します。

3 「**ローカル グループの編集**」ページで、「**ポータル**」をクリックします。



4 「**ポータル設定**」セクションの「**NetExtender**」、「**ログイン後に NetExtender を起動する**」、「**ファイル共有**」、「**セキュア仮想アシスト技術者**」、「**セキュア仮想アシストのサポートの**

要求」、「**セキュア仮想アクセス設定のリンク**」について、以下のいずれかのポータル設定をこのグループに対して選択します。

- **ポータル設定を使用** - メイン ポータル設定に定義された設定を使用して、ポータル機能を有効にするか無効にするかを決定します。メイン ポータル設定は、「**ポータル > ポータル**」ページの「ポータルの編集」画面の「**ホーム**」ページでポータルを設定すると定義されます。
- **有効** - このポータル機能をこのグループに有効にします。
- **無効** - このポータル機能をこのグループに無効にします。

Mobile Connect は装置への接続時に NetExtender クライアントとして動作するため、この NetExtender に対する設定は、Mobile Connect ユーザによるアクセスも制御します。

5 このグループのユーザが新しいブックマークを追加できるようにするには、「**ブックマークの追加を許可する**」ドロップダウン メニューで「**許可**」を選択します。ユーザが新しいブックマークを追加できないようにするには、「**拒否**」を選択します。グローバルで定義された設定を使うには、「**グローバル設定を使用する**」を選択します。グローバル設定については、グローバル設定の編集 (474 ページ) を参照してください。

6 このグループのユーザが自分自身のブックマークを編集または削除できるようにするには、「**ユーザのブックマークの編集/削除を許可**」ドロップダウン メニューで「**許可**」を選択します。ユーザが自分自身のブックマークを編集または削除できないようにするには、「**拒否**」を選択します。グローバルで定義された設定を使うには、「**グローバル設定を使用する**」を選択します。

7 「**適用**」を選択します。

クライアントのグループ設定を有効化する

この機能は外部ユーザ用です。外部ユーザはログイン時に、割り当てられたグループから設定を継承します。クライアント設定は、グループに対して個別にか、またはグローバルに指定できます。グローバルな設定については、グローバル設定の編集 (474 ページ)を参照してください。

クライアントの範囲を有効化し、特定のグループに関してDNS およびクライアントの設定を構成するには:

1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**ローカル グループの編集**」ページで、「**クライアント**」ページを選択します。

4 「**クライアント アドレス プールの設定**」を選択します。グローバル設定、DHCP 設定、または静的プールを使用するオプションなどがあります。

5 「**クライアント IPv6 アドレス プールの設定**」を選択します。グローバル設定、DHCPv6 設定、または静的プールを使用するオプションなどがあります。

6 「**DNS 設定**」の下で、「**プライマリ DNS サーバ**」フィールドにプライマリ DNS サーバのアドレスを入力します。

7 オプションで、「**セカンダリ DNS サーバ**」フィールドにセカンダリ サーバのアドレスを入力します。

8 「**DNS 検索リスト**」フィールドに DNS ドメインの接尾辞を入力して、「**追加**」を選択します。続いて、上下方向の矢印を使用して、複数の DNS ドメインを使用されるべき順序に並べ替えます。

Apple iPhone、iPad、その他の iOS 端末からの SonicWall Inc. Mobile Connect を使った接続をサポートする SMA/SRA 装置に対しては、この DNS 検索リストを使用してください。この DNS ドメインは、iPhone/iPad の VPN インターフェース上に、機器が装置との接続を確立した後で設定され

ます。モバイル機器のユーザがある URL にアクセスする際に、iOS はこのドメインが VPN インターフェースのドメインと一致しているかどうかを判断し、一致している場合は VPN インターフェースの DNS サーバを使ってホスト名検索を解決します。そうでない場合は、組織のイントラネット内のホストを解決できない Wi-Fi または 3G の DNS サーバが使われます。

9 **「クライアント設定」**の下で、**「切断後にクライアントを終了」**ドロップダウン リストで次のいずれかを選択します。

- **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
- **有効** - この操作をグループのすべてのメンバーに対して有効にします。この設定はグローバル設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

10 **「クライアント終了後にアンインストール」**ドロップダウン リストで、次のいずれかを選択します。

- **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
- **有効** - この操作をグループのすべてのメンバーに対して有効にします。この設定はグローバル設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

11 **「クライアント接続プロファイルを作成」**ドロップダウン リストで、次のいずれかを選択します。

- **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
- **有効** - この操作をグループのすべてのメンバーに対して有効にします。この設定はグローバル設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

12 **「ユーザ名とパスワードの保存」**ドロップダウン リストで、次のいずれかを選択します。

- **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
- **ユーザ名だけ保存を許可** - グループのメンバーのユーザ名をキャッシュします。NetExtender を起動するときにグループのメンバーはパスワードのみを入力します。この設定はグローバル設定に優先します。
- **ユーザ名とパスワードの保存を許可** - グループのメンバーのユーザ名とパスワードをキャッシュします。NetExtender を起動すると、グループのメンバーは自動的にログインします。この設定はグローバル設定に優先します。
- **ユーザ名とパスワードの保存は不可** - グループのメンバーのユーザ名とパスワードをキャッシュしません。NetExtender を起動するときにグループのメンバーはユーザ名とパスワードの両方を入力する必要があります。この設定はグローバル設定に優先します。

13 このオプションが無効になっている場合、**「iOS デバイスでタッチ ID の使用を許可する」**では、iOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

14 このオプションが無効になっている場合、「**Android デバイスで指紋認証の使用を許可する**」では、Android デバイスでの指紋認証による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

15 このオプションが無効になっている場合、「**macOS デバイスでタッチ ID の使用を許可する**」では、macOS デバイスでのフィンガープリント技術による今後のログイン試行のみが遮断されます。サーバには、クライアントが接続を試みるまではクライアント側の設定を変更する手段がないためです。場合によっては、最初の接続であるためにクライアントが以前のポリシーに従っていない可能性があります。設定はグローバルに行うことも、グループごとやユーザ単位で行うこともできます。

16 「**適用**」を選択します。

グループ単位で ルートを有効にする

「**ルート**」ページで、管理者はクライアント ルートを追加して構成できます。IPv6 クライアント ルートは SMA/SRA 装置でサポートされます。

グループに対して複数のルートを有効にするには:

1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**ローカル グループの編集**」ページで、「**クライアント ルート**」セクションに移動します。

4 「**強制トンネル方式**」ドロップダウン リストで、次のいずれかを選択します。

- **グローバル設定を使用する** - グローバル設定で指定された操作を行います。グローバル設定の編集 (474 ページ) を参照してください。
- **有効** - リモート ユーザのローカル ネットワーク宛のトラフィックを含め、このユーザに対するすべてのトラフィックは Secure Mobile Access NetExtender トンネルを通過します。この設定はグループのすべてのメンバーに適用されます。この設定はグローバル設定に優先します。
- **無効** - この操作をユーザに対して無効にします。この設定はグローバル設定に優先します。

5 グローバルに定義された **NetExtender** クライアントのルートをこのグループのメンバーに追加するには、「**グローバル クライアント ルートを追加する**」を選択します。

6 このグループのメンバーに対して明確に NetExtender クライアント ルートを設定するには、「**クライアント ルートの追加**」を選択します。

7 「**クライアント ルートの追加**」画面で、送信先ネットワークを「**送信先ネットワーク**」フィールドに入力します。たとえば、IPv4 ネットワーク アドレスを 10.202.0.0、IPv6 ネットワーク アドレスを 2007::1:2:3:0 形式で入力します。

8 IPv4 の送信先ネットワークに対しては、「**サブネット マスク/接頭辞**」フィールドに、サブネット マスクを 10 進形式 (255.0.0.0、255.255.0.0、または 255.255.255.0) で入力します。IPv6 の送信先ネットワークに対しては、112 のように接頭辞を入力します。

9 「**クライアント ルートの追加**」画面で、「**適用**」を選択します。

10 「**ローカル グループの編集**」画面で、「**適用**」を選択します。

グループのクライアント ルートを有効化する

作成済みのグループに対してグローバル クライアント ルートを有効化するには:

1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**クライアント ルート**」セクションで、「**グローバル クライアント ルートを追加**」を選択します。

4 「**適用**」を選択します。

ローカル グループに対する強制トンネル方式の有効化

この機能は外部ユーザ用です。外部ユーザはログイン時に、割り当てられたグループから設定を継承します。強制トンネル方式を有効化すると、すべてのネットワーク通信が Secure Mobile Access トンネルを通じて安全にトンネリングされます。

強制トンネル方式を有効にするには:

1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**ローカル グループの編集**」セクションで、「**強制トンネル方式**」ドロップダウン リストから「**有効**」を選択します。

4 「**適用**」を選択します。

> **メモ**:「クライアント ルートの追加」ウィンドウで「送信先ネットワーク」と「サブネット マスク/接頭辞」に 0.0.0.0 を入力することで、必要に応じて、NetExtender 接続を介した Secure Mobile Access クライアント トラフィックをすべてトンネルすることができます。

グループ ポリシーの追加

グループ アクセス ポリシーでは、すべてのトラフィックが既定で許可されます。追加の許可および拒否ポリシーを、送信先アドレスまたはアドレス範囲か、サービス種別ごとに作成することができます。

ポリシーは限定的な方が優先されます。例えば、特定の IP アドレスに適用されるポリシーは、IP アドレス範囲に適用されるポリシーよりも優先されます。特定の IP アドレスに適用されるポリシーが 2 つあるときは、特定のサービス (RDP など) に関するポリシーがすべてのサービスに関するポリシーよりも優先されます。

ユーザ ポリシーはグループ ポリシーよりも優先され、グループ ポリシーはグローバル ポリシーよりも優先されます。これはポリシーの定義と関係ありません。すべての IP アドレスへのアクセスを許可するユーザ ポリシーは、特定の IP アドレスへのアクセスを拒否するグループ ポリシーよりも優先されます。

メモ：グループ ポリシーの仕組みでは、プライマリ グループ ポリシーがどの追加グループ ポリシーよりも優先され常に強制されます。

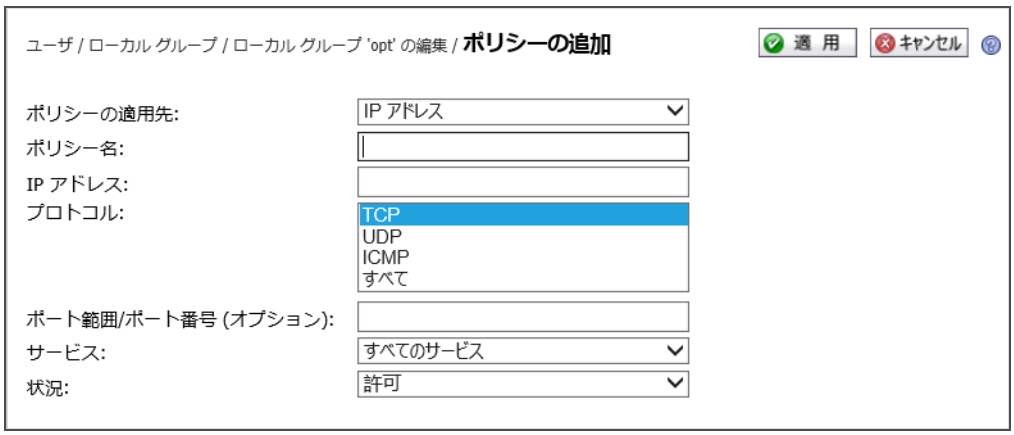
グループ アクセス ポリシーを定義するには:

1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**ローカル グループの編集**」ページで、「**ポリシー**」ページを選択します。

4 「**ポリシー**」ページで「**ポリシーの追加**」を選択します。「**ポリシーの追加**」画面が表示されます。



5 ポリシーの名前を「**ポリシー名**」フィールドに指定します。

6 「**ポリシーの適用先**」ドロップダウン リストで、ポリシーの適用先として、個別ホスト、アドレス範囲、すべてのアドレス、ネットワーク オブジェクト、サーバ パス、または URL オブジェクトのいずれかを選択します。単一の IPv6 ホスト、IPv6 アドレス範囲、またはすべての IPv6 アドレスの選択もできます。「**ポリシーの追加**」ウィンドウの内容は、「**ポリシーの適用先**」ドロップダウン リストで選択したオブジェクトの種別に応じて変化します。

メモ：Secure Mobile Access のポリシーは SMA/SRA 接続の送信元アドレスではなく送信先アドレスに適用されます。インターネット上の特定の IP アドレスがポリシー エンジンを通じて SMA/SRA ゲートウェイの認証を受けることを許可または阻止することはできません。ユーザの「**ログイン ポリシー**」ページから IP アドレスで送信元のログインを制御することが可能です。詳細については、ログイン ポリシーの設定 (434 ページ) を参照してください。

- **IP アドレス** - 特定のホストにポリシーを適用する場合は、ローカル ホスト コンピュータの IP アドレスを「**IP アドレス**」フィールドに入力します。オプションで、ポート範囲 (80-443 など) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。
- **IP ネットワーク** - アドレス範囲にポリシーを適用する場合は、IP アドレス範囲の開始アドレスを「**IP ネットワーク アドレス**」フィールドに入力し、IP アドレス範囲を定義するサブネットを「**サブネット マスク**」フィールドに入力します。オプションとして、ポート範囲 (4100-4200) または 1 つのポート番号を「**ポート範囲/ポート番号**」フィールドに入力できます。

- **ネットワーク オブジェクト** - 定義済みネットワーク オブジェクトにポリシーを適用する場合は、「**ネットワーク オブジェクト**」ドロップダウン リストでオブジェクトの名前を選択します。ネットワーク オブジェクトを定義するときにポートまたはポート範囲を指定できます。ネットワーク オブジェクトの追加 (145 ページ) を参照してください。
- **サーバ パス** - サーバ パスにポリシーを適用する場合は、「**リソース**」フィールドで以下のラジオ ボタンの 1 つを選択します。
  - 共有 (サーバ パス) - このオプションを選択するときは、パスを「サーバ パス」フィールドに入力します。
  - ネットワーク (ドメイン リスト)
  - サーバ (コンピュータ リスト)

  ファイル共有のポリシーの編集 (451 ページ) を参照してください。
- **URL オブジェクト** - 定義済みの URL オブジェクトにポリシーを適用する場合は、URL を「**URL**」フィールドに入力します。
- **すべての IPv6 アドレス** - すべての IPv6 アドレスにポリシーを適用する場合は、IP アドレス情報を入力する必要はありません。
- **IPv6 アドレス** - 特定のホストにポリシーを適用する場合は、ローカル ホスト マシンの IPv6 アドレスを「**IPv6 アドレス**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。
- **IPv6 ネットワーク** - アドレス範囲にポリシーを適用する場合は、先頭の IPv6 アドレスを「**IPv6 ネットワーク アドレス**」フィールドに入力して、この IPv6 アドレス範囲を定義する接頭辞を「**IPv6 接頭辞**」フィールドに入力します。オプションでポート範囲 (例えば 4100-4200) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。

7 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

ⓘ **メモ**：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

8 サービスの種類を「**サービス**」メニューで選択します。ポリシーの適用先がネットワーク オブジェクトの場合は、そのネットワーク オブジェクトで定義されたサービスが使用されます。

9 「**状況**」ドロップダウン リストから「**許可**」または「**拒否**」を選択し、指定したサービスおよびホスト コンピュータの SMA/SRA 接続を許可または拒否します。

10 「**適用**」を選択して設定を更新します。設定の更新後、新しいグループ ポリシーが「**ローカル グループの編集**」ウィンドウに表示されます。グループ ポリシーは、「グループ ポリシー」リストに、優先度の高いものから順番に表示されます。

ファイル共有のポリシーの編集

ファイル共有アクセス ポリシーを編集するには:

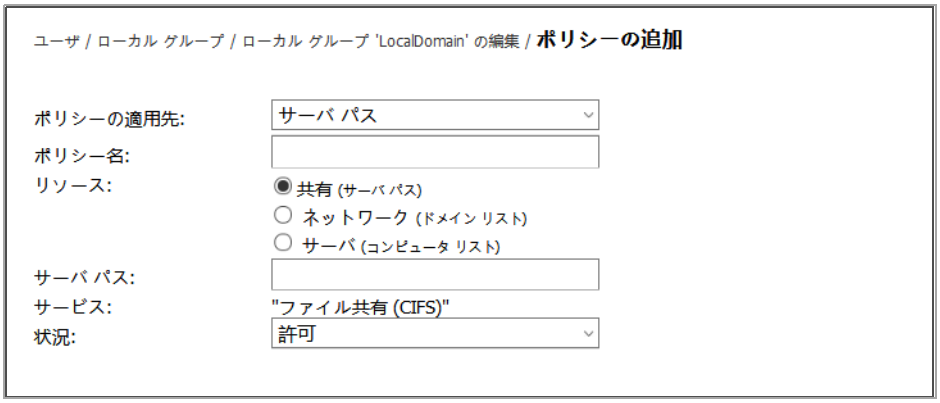
1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**ポリシー**」ページを選択します。

4 「**ポリシーの追加**」を選択します。

5 「**ポリシーの適用先**」ドロップダウン リストで「**サーバ パス**」を選択します。



6 ポリシーの名前を「**ポリシー名**」フィールドに入力します。

7 「**リソース**」に対して、「**共有 (サーバ パス)**」を選択します。

8 「**サーバ パス**」フィールドに、サーバ パスを *servername/share/path* または *servername\share\path* の形式で入力します。使用できる接頭辞は \\、//、\、および / です。

> **メモ**：共有とパスによって、ポリシーをより細かく管理できるようになります。どちらの設定もオプションです。

9 「**状況**」ドロップダウン リストで「**許可**」または「**拒否**」を選択します。

10 「**適用**」を選択します。

グループ ブックマークの設定

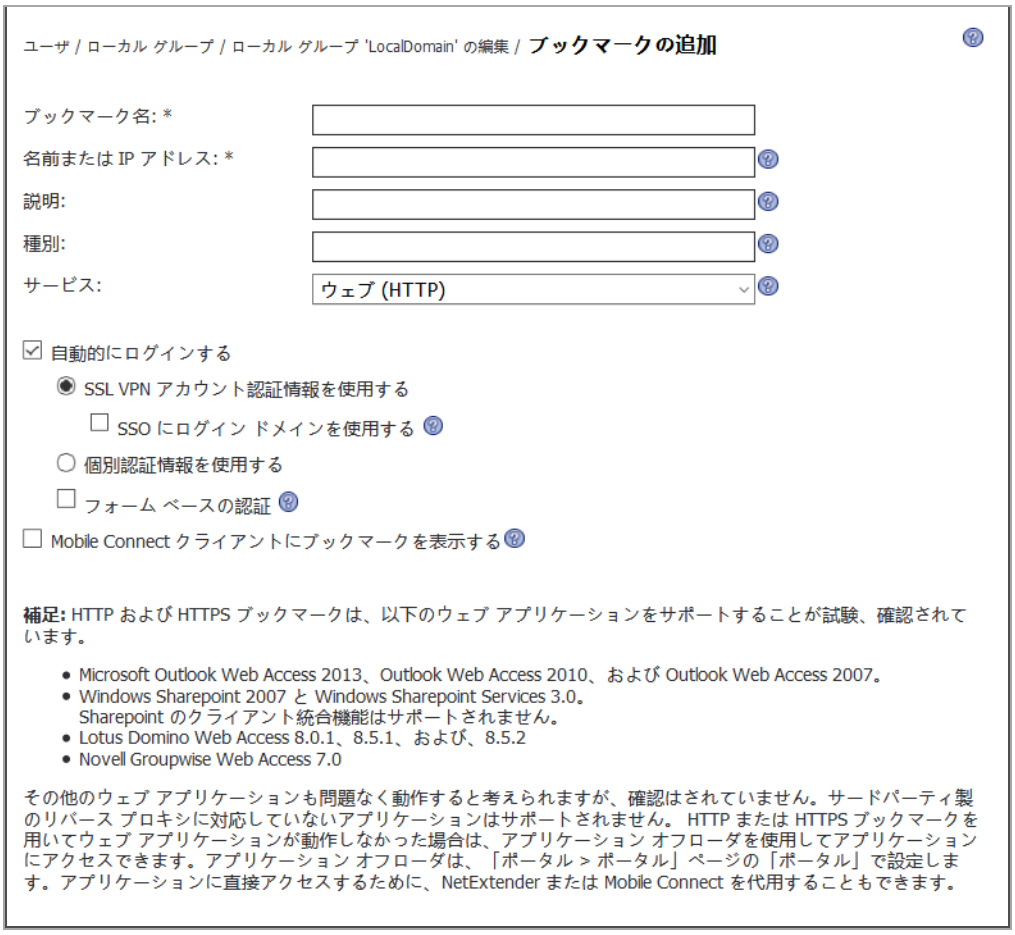
SMA/SRA 装置のブックマークは、頻繁に接続するローカル エリア ネットワーク上のコンピュータに Secure Mobile Access ユーザが簡単にアクセスできるようにする仕組みです。グループ ブックマークは、特定のグループのすべてのメンバーに適用されます。

グループ ブックマークを定義するには:

1 「**ユーザ** > **ローカル グループ**」ウィンドウを開きます。

2 ブックマークを作成するグループの設定アイコンを選択します。「**ローカル グループの編集**」ページが表示されます。

3 「**ブックマーク**」ページで、「**ブックマークの追加**」を選択します。「**ブックマークの追加**」画面が表示されます。



> **メモ**：グループ ブックマークを定義すると、グループのメンバー全員が Secure Mobile Access ユーザ ポータルで定義済みのブックマークを見ることができます。グループの個々のメンバーがグループ ブックマークを削除または変更することはできません。

4 ブックマークの名前となる文字列を「**ブックマーク名**」フィールドに入力します。

5 LAN 上のホスト コンピュータの完全修飾ドメイン名 (FQDN) または IPv4/IPv6 アドレスを「**名前または IP アドレス**」フィールドに入力します。Windows ローカル ネットワークで VNC ブックマークを作成する場合など、環境によってはホスト名のみを入力できます。

> **メモ**：「**名前または IP アドレス**」フィールド内でポート番号が IPv6 アドレスに含まれる場合は、IPv6 アドレスを角かっこで囲む必要があります。入力例: **[2008::1:2:3:4]:6818**。ファイル共有または VNC ブックマークでは IPv6 はサポートされていません。

HTTP および HTTPS の場合は、個別ポートとパスを追加できます (例:servername:port/path)。VNC、Telnet、および SSH の場合は、個別ポートを追加できます (例:servername:port)。

6 「**説明**」フィールドに、ブックマーク テーブル内に表示する、わかりやすい説明を入力します。

7 「**サービス**」ドロップダウン リストから、サービス タイプを 1 つ選択します。「**サービス**」ドロップダウン リストで選択するサービスに応じて、追加のフィールドが表示されることがあります。選択したサービスに対する以下の情報を使ってブックマークを完成させます。

ターミナル サービス (RDP)、ターミナル サービス (RDP -HTML5)、またはターミナル サービス (RDP - ネイティブ)

- 「**画面サイズ**」ドロップダウン メニューで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。

  画面サイズはコンピュータによって異なるので、リモート デスクトップ アプリケーションを使用するときは、リモート デスクトップ セッションの実行元のコンピュータ画面のサイズを選択する必要があります。また、場合によっては「**アプリケーションおよびパス**」フィールドでリモート コンピュータ上のアプリケーションのパスを指定する必要があります。
- 「**カラー**」ドロップダウン リストで、このブックマークの実行時に使用されるターミナル サービス画面の既定の色深度を選択します。

8 「**アクセス タイプの選択**」を選びます。「**スマート**」または「**手動**」のどちらかです。

- 「**スマート**」: ファームウェアにクライアントを起動するモードを決定させます。

  新しい統合ブックマークを作成する場合は、「**スマート**」がデフォルトで選択されています。ブックマークの起動時には、ブックマーク固有の既定モードを使用して自動検出の処理が行われます。
- 「**手動**」: モードや優先順位を設定し、方法を選択するオプションを提供します。選択ボックスで、少なくとも 1 つのモードが有効になっている必要があります。

  起動シーケンスは、「**HTML5**」と「**Native**」です。「手動」を選択すると、起動方法を変更、有効化、または無効化できます。「**Native**」を選択して RDP ブックマークを起動した場合は、SMA Connect Agent によって RDP Receiver がローカルマシン上で起動され、RDP 接続が行われます。

  「**上**」と「**下**」の矢印を使って起動順序を調整します。バツとチェックのアイコンを使ってモードの有効と無効を切り替えます。無効にしたモードはリストの下に移動し、グレー表示されます。

  「**手動**」モードでは、デフォルトで「**起動中に選択**」オプションは有効ではありません。この設定では、ブックマークの起動時に、設定済みリストの先頭にある使用可能なモードが自動検出後に実行されます。

  「**起動時に選択する**」オプションが有効になっていて、複数のモードがクライアントで使用可能な場合は、統合ブックマークの起動時にメニューが表示されます。このメ

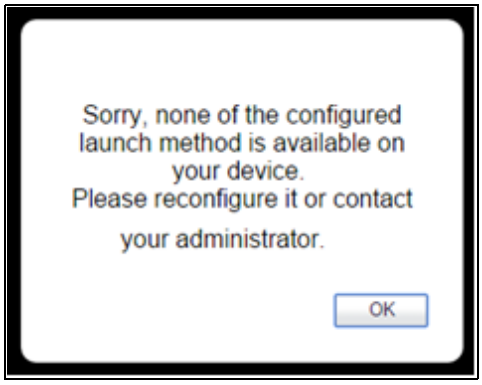
ニューでは、5 秒のカウントダウンが行われている間にモードを選択できます。使用可能なモードが 1 つしかない場合、ブックマークはただちに実行されます。

起動時に「**この選択を記憶する**」オプションが有効になっている場合は、選択されたモードが Cookie によって記憶されます。

その場合、次にブックマークを起動すると、記憶したモードが 2 秒以内に直接実行されます。HTML のどこかをクリックすると、記憶したモードを「忘れる」ので、再選択を行うことができます。

同じブラウザでブックマークの編集や削除しても、記憶したモードがリセットされます。

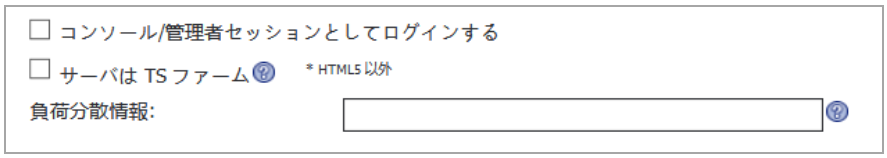
設定されたクライアントでどのモードも実行できない場合、次の通知が表示されます。



- オプションで、このアプリケーションへのローカル パスを「**アプリケーションおよびパス**」フィールドに入力します。
- 「**Wake on LAN を有効にする**」をオンにすると、ネットワーク接続を介してコンピュータの電源を投入できます。このチェックボックスをオンにした場合、以下の新しいフィールドが表示されます。

- **MAC/イーサネット アドレス** - 電源を投入するホストの 1 つ以上の MAC アドレスをスペースで区切って入力します。
- **起動待ち時間 (秒)** - WoL 操作を中止するまでターゲット ホストの起動完了を待機する時間を秒単位で入力します。
- **WOL パケットをホスト名または IP アドレスに送信する** - WOL パケットをこのブックマークのホスト名または IP アドレスに送信するには、「**WOL パケットをホスト名または IP アドレスに送信する**」をオンにします。この設定は、WOL で電源を投入する別のコンピュータの MAC アドレスと併用して適用できます。

- 「**次のフォルダから開始**」フィールドに、アプリケーション コマンドを実行するローカル フォルダをオプションで入力します。
- オプションで、このアプリケーションのローカル パスを「**アプリケーションおよびパス**」フィールドに入力し、フォルダを「**次のフォルダから開始**」フィールドに指定します。**リモート アプリケーション機能は、単一のアプリケーションをユーザに対して表示します。 値はリモート アプリケーションのエイリアスにすることもできます。**
- RemoteApp 用 の「**コマンドライン引数**」を入力します。*(ActiveX または Java でのみ使用できます)*
- 「**次のフォルダから開始**」フィールドに、アプリケーション コマンドを実行するローカル フォルダをオプションで入力します。*(ActiveX または Java でのみ使用できます)*
- 「**コンソール / 管理者セッションとしてログインする**」をオンにすると、コンソールまたは管理者としてログインできます。RDC 6.1 以降では、admin セッションへのログインは、コンソール セッションへのログインに置き換わります。*(すべてのターミナル サービスで使用できます)*
- TS ファームまたは負荷分散サーバに接続する場合は、「**サーバは TS ファーム**」をオンにします。ターミナル サービス ブローカ情報を「**負荷分散情報**」ボックスに入力します (例: tsv://MS Terminal Services Plugin.1.コレクション名)。最大 1024 文字まで入力できます。複雑なオプションを持つブックマーク (RDP など) では、すべてのモードのオプションが混在していますが、「*HTML5 以外」、「*HTML5 向け」のようなヒントによってオプションの区別が行われています。



既定では、ブックマークは提供された名前と IP アドレスのみに接続します。この機能を有効にすると、SMA/SRA 装置はリダイレクトされたアドレスを取得し、ユーザを正しいサーバに接続します。この機能が正しく動作するには、対話型ログインを無効しなければならない場合があることに注意してください。

> **メモ**：この設定を有効にする場合は、ブックマークに自動的にログインするため、正しい SSO 認証情報を設定します。この設定を有効にしない場合は、「**自動的にログインする**」をオフのままにします。

- 「*RDP - HTML5*」の場合は、ドロップダウン メニューから「**既定の言語**」を選択します。
- Windows クライアント、または RDC をインストール済みの Mac OS X 10.5 以上の Mac クライアントでは、「**詳細な Windows オプションを表示**」を展開し、各チェック ボックスをオンにすることにより、ローカル ネットワーク上の以下の機能を、このブックマークで使用するためにリダイレクトします。

- **プリンタをリダイレクトする - プリンタ リダイレクトの設定の詳細については、プリンタのリダイレクト (515 ページ) を参照してください。**
- **ポートをリダイレクトする**
- **クリップボードをリダイレクトする**
- **ドライブをリダイレクトする**
- **スマートカードをリダイレクトする**
- **プラグ アンド プレイ機器をリダイレクトする**

以下のその他の機能について、このブックマーク セッションで使用する場合はそのチェック ボックスをオンにします。

- **接続バーを表示する**
- **デスクトップ背景**
- **メニューとウインドウ アニメーション**
- **ドラッグ/リサイズの間にウィンドウの内容を表示する**
- **自動再接続**
- **ビットマップのキャッシュ**
- **表示スタイル**
- ドロップダウン リストから「**リモート音声**」オプションを選択します。オーディオ リダイレクションにより、リモートまたはローカルでサーバ上のオーディオ クリップを再生できます。有効な選択肢は、「**このコンピュータで再生する**」、「**リモート コンピュータで再生する**」、または「**再生しない**」です。現在、この機能は Chrome、Firefox、および Safari でサポートされています。

メモ：一部のオプションの横にあるヘルプ アイコン の上にマウス ポインタを移動すると、要求事項がツールチップに表示されます。

- *RDP - HTML5* の場合、以下の詳細な Windows オプションが使用できます。
  - **デスクトップ背景**
  - **メニューとウインドウ アニメーション**
  - **ドラッグ/リサイズの間にウィンドウの内容を表示する**
  - **圧縮を有効にする**
  - **表示スタイル**
  - ドロップダウン リストから「**リモート音声**」オプションを選択します。オーディオ リダイレクションにより、リモートまたはローカルでサーバ上のオーディオ クリップを再生できます。有効な選択肢は、「**このコンピュータで再生する**」、「**リモート コンピュータで再生する**」、または「**再生しない**」です。現在、この機能は Chrome、Firefox、および Safari でサポートされています。
- クライアント アプリケーションが RDP6 の場合はさらに、以下のいずれかのオプションを選択できます(*すべてのターミナル サービスで使用できます*)。
  - **フォント補整**
- ドロップダウン リストから「**接続速度**」を選択して、パフォーマンスを最適化します。(*すべてのターミナル サービスで使用できます*)

- 「**サーバ認証が失敗した場合**」に発生するアクションをドロップダウン リストから選択します。意図したリモート コンピュータに接続していることが、サーバ認証により確認されました。接続に必要な確認の強度は、システムのセキュリティ ポリシーによって決まります。(*すべてのターミナル サービスで使用できます*)
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプションを有効にして、ユーザのドメインを RDP サーバに引き渡します。Windows 2008 以降のサーバでは、このオプションを有効にしなければならない可能性があります。(*すべてのターミナル サービスで使用できます*)

  このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。(*すべてのターミナル サービスで使用できます*)

  メモ：RDP over HTML5 は、iOS または Android で既定および標準のブラウザを使用してサポートされます。

仮想ネットワーク コンピューティング (VNC)

- 「**エンコード**」ドロップダウン リストから、次のいずれかを選択します。
  - **Raw** - ピクセル データは、左から右へのスキャンライン順で送信され、最初のフル スクリーンが送信された後で、変更のある長方形のみが送信されます。
  - **RRE** - ライズアンドランレングス エンコーディングは、単一の値と繰り返し数に圧縮された変換可能なピクセルの連続を使います。これは、一定の色の大きなブロックに対して能率的なエンコードです。
  - **CoRRE** - RRE の亜種で、最大で 255x255 ピクセルの長方形を使い、1 バイトの値を使用することができます。非常に大きな区域が同じ色の場合を除いて、RRE よりも能率的です。
  - **Hextile** - 長方形は最大 16x16 タイルの Raw または RRE データに分割され、あらかじめ決められた順序で送信されます。LAN 内のような、高速ネットワーク環境内の使用に最良です。
  - **Zlib** - 素のピクセル データの圧縮に zlib ライブラリを使用する簡素なエンコードで、多くの CPU 時間を消費します。Zib よりもほとんどすべての実生活環境で能率的な Tighe エンコードを理解しない VNC サーバでの互換性がサポートされます。
  - **Tight** - 既定であり、VNC をインターネット上またはその他の低帯域ネットワーク環境で使用するために最良のエンコードです。zlib ライブラリを使って、あらかじめ処理されたピクセル データを最大の圧縮率に、最小の CPU 使用率で圧縮します。
- 「**圧縮レベル**」ドロップダウン リストで、圧縮レベルを「**既定**」または「**1**」～「**9**」(**1** が最低圧縮で **9** が最高圧縮) から選択します。
- 「**JPEG イメージ品質**」オプションは変更できず、「**6**」に設定されています。
- 「**カーソル状態更新**」ドロップダウン リストで、「**有効**」、「**無視**」、または「**無効**」から選択します。既定は「**無視**」です。
- 画面上でアイテムを移動する際に効率を上げるには、「**CopyRect の使用**」を選択します。
- 色数を減らすことで能率を上げるには、「**制限された色数 (256 色)**」を選択します。

- マウスの右クリックと左クリックのボタンを入れ替えるには、「**マウス ボタン 2 と 3 を逆にする**」を選択します。
- ユーザがリモート システム上で何も変更を行わない場合は、「**表示のみ**」を選択します。
- 複数のユーザが同じ VNC デスクトップを参照して使用することを許可するには、「**デスクトップ共有**」を選択します。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

Citrix Portal (Citrix)

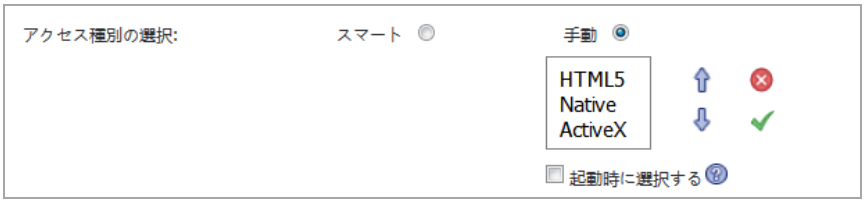
- 「**リソース ウィンドウ サイズ**」ドロップダウン リストから、ユーザがこのブックマークを実行した際に使用される既定の Citrix ポータル画面サイズを選択します。

9 「**アクセス タイプの選択**」を選びます。「**スマート**」または「**手動**」のどちらかです。

- 「**スマート**」: ファームウェアにクライアントを起動するモードを決定させます。

新しい統合ブックマークを作成する場合は、「**スマート**」がデフォルトで選択されています。ブックマークの起動時には、ブックマーク固有の既定モードを使用して自動検出の処理が行われます。

- 「**手動**」: モードや優先順位を設定し、方法を選択するオプションを提供します。選択ボックスで、少なくとも 1 つのモードが有効になっている必要があります。



起動シーケンスは、「**HTML5**」、「**Native**」、「**ActiveX**」です。「手動」を選択すると、起動方法を変更、有効化、または無効化できます。Citrix ブックマークの起動に「**Native**」を選択すると、SMA Connect Agent がローカル マシンの Citrix Receiver を起動して Citrix 接続を行います。**Native** の場合、SMA 接続エージェントおよび Citrix Receiver のインストール後にこのブックマークを Windows または OS X プラットフォームで起動すると、高度な機能を利用できます。

「**上**」と「**下**」の矢印を使って起動順序を調整します。バツとチェックのアイコンを使ってモードの有効と無効を切り替えます。無効にしたモードはリストの下に移動し、グレー表示されます。

「**手動**」モードでは、デフォルトで「**起動中に選択**」オプションは有効ではありません。この設定では、ブックマークの起動時に、設定済みリストの先頭にある使用可能なモードが自動検出後に実行されます。

「**起動時に選択する**」オプションが有効になっていて、複数のモードがクライアントで使用可能な場合は、統合ブックマークの起動時にメニューが表示されます。このメ

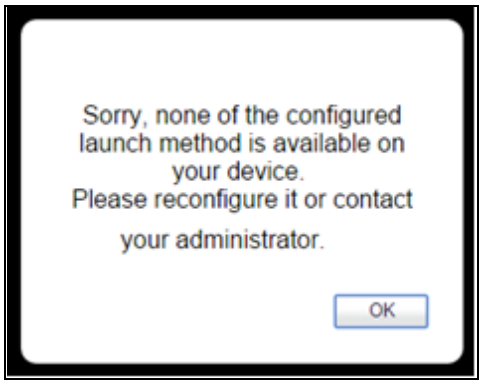
ニューでは、5 秒のカウントダウンが行われている間にモードを選択できます。使用可能なモードが 1 つしかない場合、ブックマークはただちに実行されます。

起動時に「**この選択を記憶する**」オプションが有効になっている場合は、選択されたモードが Cookie によって記憶されます。

その場合、次にブックマークを起動すると、記憶したモードが 2 秒以内に直接実行されます。HTML のどこかをクリックすると、記憶したモードを「忘れる」ので、再選択を行うことができます。

同じブラウザでブックマークの編集や削除しても、記憶したモードがリセットされます。

設定されたクライアントでどのモードも実行できない場合、次の通知が表示されます。



- HTTPS を使用して Citrix ポータルに安全にアクセスするには、オプションで「**HTTPS モード**」を選択します。
- オプションで「**指定した Citrix ICA サーバを常に使用する**」を選択して、現れた「**Citrix ICA サーバ アドレス**」フィールドに IP アドレスを指定します。この設定により、Citrix ICA

セッションに対する Citrix ICA サーバのアドレスを指定することが可能です。既定では、ブックマークは Citrix サーバ上の ICA 設定内で提供される情報を使用します。

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

ウェブ (HTTP)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプションを有効にして、ユーザのドメインを RDP サーバに引き渡します。

  このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。

- シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の‘name’または‘id’属性と同じになるように設定します。例えば、<input type=text name='userid'> のようにします。「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の ‘name’ または ‘id’ 属性と同じになるように設定します。例えば、<input type=password name='PASSWORD' id='PASSWORD' maxlength=128> のようにします。

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

セキュア ウェブ (HTTPS)

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプションを有効にして、ユーザのドメインを RDP サーバに引き渡します。

  このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。

- シングル サイン オンをフォーム ベース認証用に設定するには、「**フォーム ベースの認証**」をオンにします。「**ユーザ フォーム フィールド**」を、ログイン フォームでユーザ名を表す HTML 要素の‘name’または‘id’属性と同じになるように設定します。例えば、<input type=text name='userid'> のようにします。「**パスワード フォーム フィールド**」は、ログイン フォーム内のパスワードを表す HTML 要素の ‘name’ または ‘id’ 属性と同じになるように設定します。例えば、<input type=password name='PASSWORD' id='PASSWORD' maxlength=128> のようにします。

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

外部ウェブ サイト

- SSL を使用してこのウェブ サイトとの通信を暗号化するには、「**HTTPS モード**」をオンにします。

- このウェブ サイトにアクセスする際にセキュリティ警告を一切表示しない場合は、「**セキュリティ警告を無効にする**」をオンにします。ブックマークがアプリケーション オフロードされたウェブ サイト以外の何かを参照しようとした場合に、通常セキュリティ警告が表示されます。
- このブックマークの仮想ホスト ドメインのシングル サインオンを有効にするには、「**自動的にログインする**」をオンにします。ブックマーク内のホストが、このポータルと同一の共有ドメインを持つポータルを参照する場合、このチェックボックスを選択すると、このポータルの認証情報で自動的にログインすることができます。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

Mobile Connect

- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

  メモ：このブックマークの表示およびアクセスを行うには、Mobile Connect はバージョン 2.0 以降である必要があります。サポートは機器によって異なり、サポートされるサードパーティ アプリケーションのインストールが必要な場合があります。

ファイル共有 (CIFS)

メモ：SMB2 および SMB3 プロトコルは現在サポートされていません。サーバは、Linux ベースのクライアントからの通信を許可するよう設定する必要があります。

- クライアント UI へのアクセスを制限するには、「**特定のファイル/フォルダにアクセスするユーザを設定する**」をオンにします。完全にアクセスを制限するには、「**サービス > ポリシー**」ページに移動して、アクセス制限のポリシーを設定します。詳細については、ユーザ ポリシーの追加 (402 ページ) を参照してください。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから RDP サーバに転送されます。「**SSO にログイン ドメインを使用する**」のオプションを有効にして、ユーザのドメインを RDP サーバに引き渡します。

  このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにして、Mobile Connect クライアントにブックマーク情報を送信します。

  ファイル共有を作成するときは、DFS (Distributed File System) サーバをウィンドウズ ドメイン ルート システムに設定しないでください。ドメイン ルートはドメイン内の Windows コンピュータへのアクセスのみを提供するので、DFS サーバをドメイン ルートに設定すると、他のドメインから DFS ファイル共有にアクセスできません。SMA/SRA 装置は、ドメイン メンバではなく、このような DFS 共有に接続できません。

  スタンドアロン ルート上の DFS ファイル共有には、Microsoft の制限は適用されません。

ファイル転送プロトコル (FTP) と SSH ファイル転送プロトコル (SFTP)

- 「**詳細なサーバ設定を表示**」を展開して、代替値を「**文字エンコード**」ドロップダウンリストで選択します。既定値は「**標準 (UTF-8)**」です。

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションから FTP サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。

Telnet HTML5 設定

- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。

セキュア シェル バージョン 2 (SSHv2) HTML5 設定

- 「**既定のフォント サイズ**」を選択します。サポートされているオプションは、12 ～ 99 ポイントの範囲です。
- オプションで、「**自動的にログインする**」をオンにして、「**SSL VPN アカウント認証情報を使用する**」を選択すると、ログイン資格情報が現在の Secure Mobile Access セッションからセキュア ウェブ サーバに転送されます。このブックマーク用の個別のユーザ名、パスワード、およびドメインを入力する場合は、「**個別認証情報を使用する**」を選択します。個別資格情報の詳細については、個別 SSO 資格情報によるブックマークの作成 (432 ページ) を参照してください。

SSHv2 共通設定

- 必要に応じて、「**自動的にホスト キーを受け入れる**」をオンにします。このオプションを選択すると、ブラウザは、サーバの公開ホスト キーをローカル ストレージに自動的に保持します。
- 「**Mobile Connect クライアントにブックマークを表示する**」をオンにすると、モバイル機器上にブックマークが表示されます。
- 「**適用**」を選択して設定を更新します。設定が更新されると、新しいグループ ブックマークが「**ローカル グループの編集**」ページに表示されます。

グループ エンド ポイント制御の設定

ローカル グループが使用するエンド ポイント制御プロファイルを設定するには:

1. 「**ユーザ** > **ローカル ユーザ**」または「**ユーザ** > **ローカル グループ**」ページに移動します。
2. EPC を設定するグループの設定アイコンを選択します。「**ローカル グループの編集**」ページが表示されます。
3. 「**EPC** 」ページを選択します。「**EPC の設定**」ページが表示されます。
4. ユーザ > ローカル グループ (440 ページ) で説明されるように、グループの EPC 設定を構成して、デバイス プロファイルを追加または削除します。

LDAP 認証ドメインのグループ設定

メモ：マイクロソフト アクティブ ディレクトリ データベースでは、LDAP 組織スキーマが使われます。アクティブ ディレクトリ データベースの問い合わせには、Kerberos 認証 (標準の認証方式 - Secure Mobile Access 管理インターフェースでは「アクティブ ディレクトリ」ドメイン認証と表示)、または LDAP データベース問い合わせが使われます。Secure Mobile Access 管理インターフェースで設定された LDAP ドメインは、アクティブ ディレクトリ サーバの認証を受けることができます。

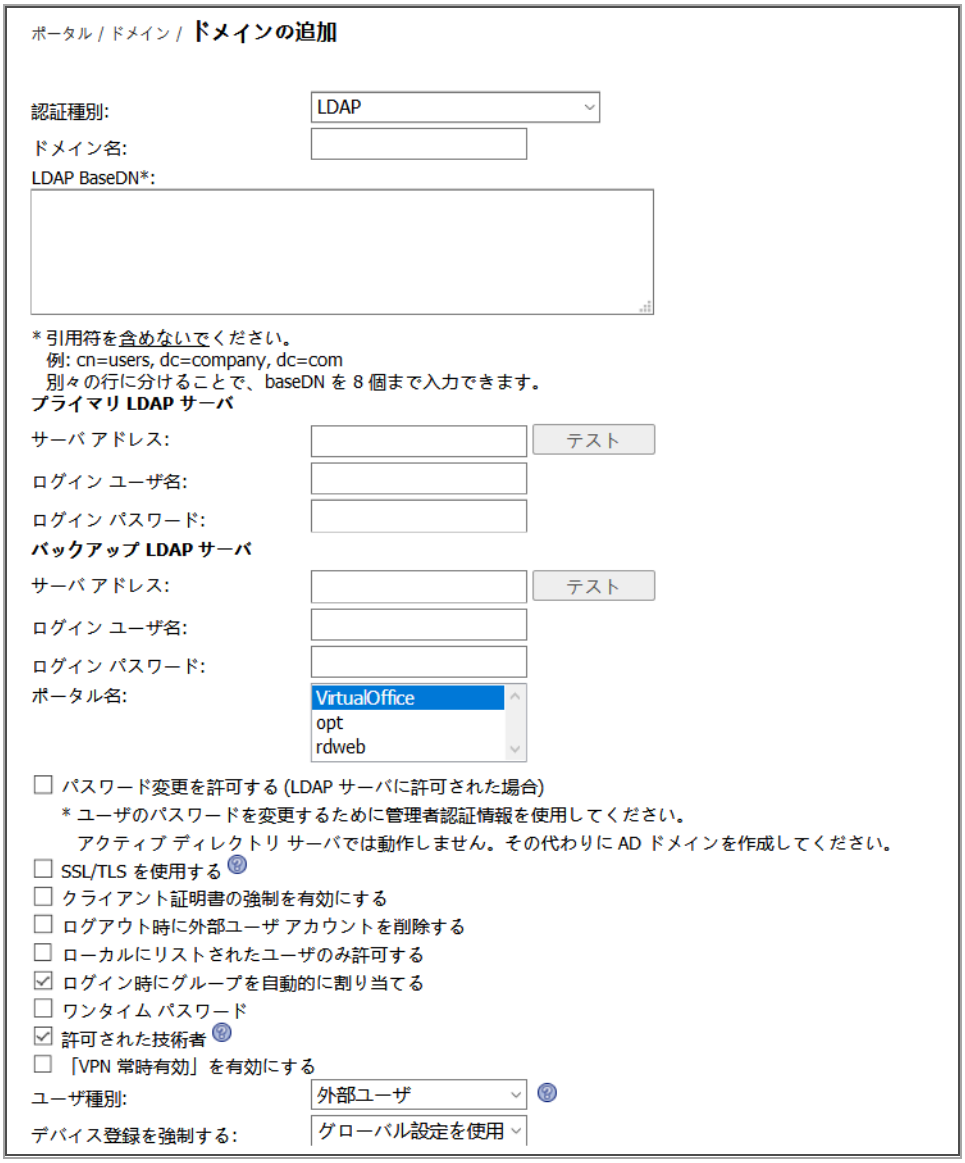
Lightweight Directory Access Protocol (LDAP) は、ディレクトリの問い合わせと更新のための標準です。LDAP は多層的な階層 (例えば、グループや組織単位) をサポートしているので、SMA/SRA 装置は、この情報を問い合わせ、LDAP 属性に基づいて特定のグループ ポリシーまたはブックマークを提供することができます。LDAP 属性を設定することで、SMA/SRA 装置の管理者は、LDAP またはアクティブ ディレクトリ データベースに既に設定されているグループを利用できるので、SMA/SRA 装置で同じグループを手動で再作成する必要がありません。

LDAP 認証ドメインを作成すると、既定の LDAP グループが LDAP ドメインと同じ名前で作成されます。このドメインでグループを追加または削除することもできますが、既定の LDAP グループは削除できません。LDAP 属性が作成されたユーザが仮想オフィス ホーム ページを開くと、そのユーザが所属するグループに対して作成したブックマークがブックマーク テーブルに表示されます。

LDAP グループについては、LDAP 属性を定義できます。例えば、LDAP グループのユーザは LDAP サーバで定義されている特定のグループまたは組織単位のメンバーでなければならないというような指定ができます。あるいは特定の LDAP 識別名を指定することもできます。

グループの LDAP 属性を追加して、ユーザが仮想オフィス環境に入ったときに、設定されているブックマークが表示されるようにするには、以下の手順を実行します。

1. 「**ポータル > ドメイン**」ページを開き、「**ドメインの追加**」を選択して「ドメインの追加」ウィンドウを表示します。
2. 「**認証種別**」メニューから「**LDAP**」を選択します。LDAP ドメイン設定フィールドが表示されます。



3 「**ドメイン名**」フィールドに認証ドメインの説明的な名前を入力します。これは、Secure Mobile Access ユーザ ポータルにログインするためにユーザが選択するドメイン名です。「**サーバ アドレス**」フィールドと同じ値でも構いません。

4 「**サーバ アドレス**」フィールドにサーバの IP アドレスまたはドメイン名を入力します。

5 「**LDAP BaseDN**」フィールドに LDAP 問い合わせの検索ベースを入力します。検索ベースの文字列としては、例えば **CN=Users**, **DC=yourdomain**, **DC=com** などがあります。

> **ヒント**：単一のドメインに対して複数の OU を設定することが可能です。それには、「**LDAP BaseDN**」フィールドで各 OU を別個の行に入力します。さらに、このフィールドに追加した OU にサブ OU がある場合には、自動的に含まれます。

> **メモ**：「**LDAP BaseDN**」フィールドに入力する場合は、引用符 (“”) を省いてください。

6 サーバの格納先となるコンテナの制御を委譲される「**サーバ アドレス**」を入力します。

7 ユーザ名とパスワードを「**ログイン ユーザ名**」フィールドと「**ログイン パスワード**」フィールドに入力します。

> ⓘ **メモ**:「**ログイン ユーザ名**」と「**ログイン パスワード**」を入力すると、SMA/SRA 装置と LDAP ツリーはこれらの資格情報でバインドされ、ユーザは SMA AccountName を使ってログインできます。

8 **バックアップ サーバ アドレス**を入力します。

9 バックアップ ユーザ名とバックアップ パスワードを「**ログイン ユーザ名**」フィールドと「**ログイン パスワード**」フィールドに入力します。

10 「**ポータル名**」フィールドでポータルの名前を選択します。他のレイアウトを「**ポータル > ポータル**」ページで追加定義することもできます。

11 ユーザのパスワードを変更可能にする場合は、「**パスワード変更を許可する (LDAP サーバに許可された場合)**」をオンにします。ユーザのパスワードを変更する際は admin アカウントを使用する必要があります。

12 必要に応じて、「**SSL/TLS を使用する**」をオンにします。このオプションを選択すると、アクティブ ディレクトリのパスワード交換で必要な SSL/TLS 暗号化を使用できます。このチェックボックスは、アクティブ ディレクトリ認証を使用したドメインの設定時に有効にする必要があります。

13 必要に応じて、「**クライアント証明書の強制を有効にする**」をオンにして、ログインに際してクライアント証明書を要求するようにします。このチェックボックスをオンにすることによって、強力な相互認証のためにクライアント証明書を提示することをクライアントに要求します。さらに次の 2 つのフィールドが表示されます。

- **ユーザ名がクライアント証明書の一般名 (CN) と一致していることを確認する** - ユーザのアカウント名がクライアント証明書と一致することを要件とする場合は、このチェックボックスをオンにします。
- **サブジェクト内の部分 DN を確認する** - 次の変数を使ってクライアント証明書と一致する部分 DN を設定します。
  - ユーザ名: %USERNAME%
  - ドメイン名: %USERDOMAIN%
  - アクティブ ディレクトリ ユーザ名: %ADUSERNAME%
  - ワイルドカード: %WILDCARD%

14 ドメイン アカウントにログインしなかったユーザをログアウト後に削除するには、「**ログアウト時に外部ユーザ アカウントを削除する**」をオンにします。

15 「**ローカルにリストされたユーザのみ許可する**」をオンにして、アクティブ ディレクトリにローカル レコードを持つユーザのみにログインを許可します。

16 「**ログイン時にグループを自動的に割り当てる**」をオンにして、ユーザをログイン時にグループに割り当てるようにします。

アクティブ ディレクトリ ドメインにログインするユーザは、外部 AD グループ メンバーシップに基づいて、リアルタイムで Secure Mobile Access グループに自動的に割り当てられます。ユーザの外部グループ メンバーシップが変更された場合は、Secure Mobile Access グループ メンバーシップが外部グループ メンバーシップに対応するように自動的に変更されます。

17 オプションで、ワンタイム パスワード機能を有効にするには、「**ワンタイム パスワード**」をオンにします。表示されるドロップダウン リストから「**設定する場合**」、「**全てのユーザに必要**」、または「**ドメイン名を使用**」を選択できます。各オプションには次の機能があります。

- **設定する場合** - ワンタイム パスワード電子メール アドレスが設定されているユーザだけがワンタイム パスワード機能を使用します。
- **全てのユーザに必要** - すべてのユーザがワンタイム パスワード機能を使わなければなりません。ワンタイム パスワード電子メール アドレスが設定されていないユーザはログインを許可されません。
- **ドメイン名を使用** - ドメインに所属するユーザはワンタイム パスワード機能を使用します。ドメイン内のすべてのユーザのワンタイム パスワード電子メールが username@domain.com に送信されます。

18 「**ワンタイム パスワード**」ドロップダウン リストで「**設定する場合**」または「**全てのユーザに必要**」を選択した場合は、アクティブ ディレクトリの「**AD 電子メール属性**」ドロップダウン リストが表示され、そこで「**mail**」、「**mobile**」、「**pager**」、「**userPrincipalName**」、または「**個別**」を選択できます。各オプションには次の機能があります。

- **mail** - AD サーバが mail 属性を使って電子メール アドレスを保存するように設定されている場合は、「**mail**」を選択します。
- **mobile** または **pager** - AD サーバが mobile 属性または pager 属性を使ってそれらの番号を保存するように設定されている場合は、それぞれ「mobile」、「pager」を選択します。処理されていない番号は使えませんが、SMS アドレスは使えます。
- **userPrincipalName** - AD サーバが userPrincipalName 属性を使って電子メール アドレスを保存するように設定されている場合は、「**userPrincipalName**」を選択します。
- **個別** - AD サーバが個別属性を使って電子メール アドレスを保存するように設定されている場合は、「**個別**」を選択します。ユーザに指定された属性が見つからない場合は、個別のユーザ ポリシーの設定で割り当てられた電子メール アドレスが使われます。「**個別**」を選択すると、「**個別属性**」フィールドが表示されます。AD サーバで電子メール アドレスの保存に使用される個別属性を入力します。ユーザに指定された属性が見つからない場合は、個別のポリシーの設定で割り当てられた電子メール アドレスが使われます。

「**ドメイン名を使用**」を選択すると、ドロップダウン リストの後に「**電子メール ドメイン**」フィールドが表示されます。ワンタイム パスワード電子メールの送信先となるドメイン名 (例えば、abc.com) を入力してください。

19 「**許可された技術者**」を有効にすると、セキュア仮想アシストは技術担当者の役割としてこのドメインにログインできます。

20 「**ユーザ種別**」ドロップダウン リストからユーザの種別を選択します。このドメインを通してログインするすべてのユーザは、このユーザ種別として扱われます。選択肢は既に定義されたユーザ種別に依存します。いくつかの利用可能な選択肢は、以下の通りです。

- **外部ユーザ** - このドメインにログインするユーザは、管理権限の無い一般ユーザとして扱われます。
- **外部管理者** - このドメインにログインするユーザは、ローカルの Secure Mobile Access 管理資格のある管理者として扱われます。これらのユーザには、管理者ログイン ページが表示されます。

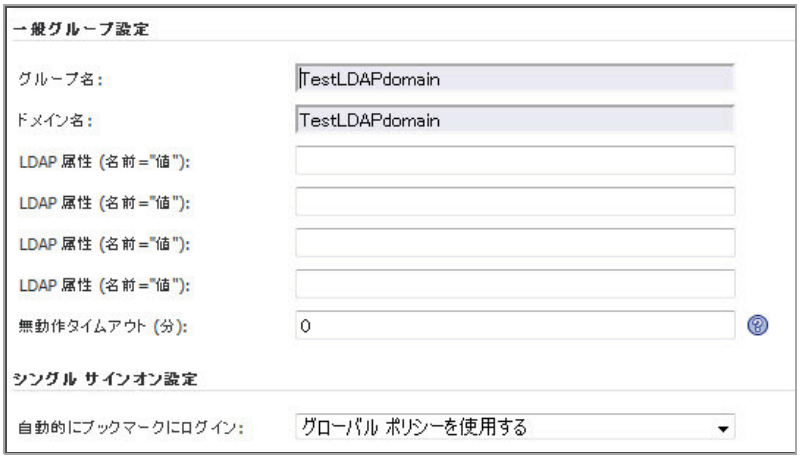
  このオプションにより Secure Mobile Access 管理者は、ドメインにログインするすべてのユーザに Secure Mobile Access 管理権限を許可するドメインを設定することが可能です。

  SonicWall Inc. は、正しいグループ内のユーザにのみ管理アクセスを許可するフィルタを追加することを推奨します。これは、「**ユーザ > ローカル グループ**」ページ上でドメインを編集することで可能です。

- **読み込み専用管理者** - このドメインにログインするユーザは、読み込み専用管理者として扱われ、すべての情報と設定を参照できますが、設定の変更は一切適用できません。これらのユーザには、管理者ログイン ページが表示されます。

21 「**適用**」を選択して設定を更新します。ドメインが追加されると、「**ポータル > ドメイン**」ページのテーブルにそのドメインが追加されます。

22 「**ユーザ** > ローカル グループ」ページを開いて、設定アイコンを選択します。「**グループ設定の編集**」ページの「**一般**」ページに LDAP 属性のフィールドが表示されます。



23 「**一般**」ページで、必要に応じて 1 つまたは複数の「**LDAP 属性**」フィールドに適切な名前を入力できます。各フィールドでは、**名前=値**という形式で一連の LDAP 属性を追加します。LDAP 属性の完全なリストについては、『*SonicWall Inc. LDAP Attribute document*』 を参照してください。

一般的な例としては、属性フィールドに memberOf= 属性を入力します。これには次の一般変数種別をまとめて指定できます。

CN= - 共通名、DN= - 識別名、DC=- ドメイン コンポーネント。

memberOf 行に変数をまとめて指定するときは、全体を引用符で囲む必要があります。変数と変数の間はカンマで区切ります。**CN** および **DC** 変数を使用する場合の構文は次のようになります。

```
memberOf="CN=<文字列>, DC=<文字列>"
```

次は、**CN** および **DC** 変数を使用した場合の「**LDAP 属性**」フィールドの入力例です。

```
memberOf="CN=Terminal Server Computers, CN=Users, DC=sonicwall, DC=net"
```

24 無動作タイムアウト値 (分単位) を「**無動作タイムアウト**」フィールドに入力します。グローバル タイムアウトの設定を使用する場合は **0** (ゼロ) を入力します。

25 「**シングル サインオン設定**」の「**自動的にブックマークにログイン**」で、次のいずれか 1 つを選択します。

- **グローバル ポリシーを使用する** - ブックマークへのログインに使用するシングル サインオンにグローバル ポリシーを適用します。
- **ユーザ制御 (新しいユーザに既定で有効)** - 新規ユーザにシングル サインオンでのブックマーク ログインを許可し、この設定の変更をユーザに許可します。
- **ユーザ制御 (新しいユーザに既定で無効)** - 新規ユーザにシングル サインオンでのブックマーク ログインを許可しませんが、この設定の変更は許可します。
- **有効** - ブックマークへのシングル サインオンでのログインを許可します。
- **無効** - ブックマークへのシングル サインオンでのログインを許可しません。

26 設定の完了後、「**適用**」を選択します。

LDAP 属性の情報

次に、LDAP 属性を設定するときに役立つ情報を示します。

- グループに複数の属性が定義されている場合、LDAP ユーザはすべての属性を満たさなければなりません。
- LDAP 認証は、認証時に指定されたのと同じ資格情報を使用して LDAP ツリーにバインドされます。アクティブ ディレクトリに対して使用する場合、これは指定されたログイン資格情報が、SMAAccountName (ログイン名) ではなく CN (一般名) 属性と一致しなければならないことを意味します。例えば、アクティブ ディレクトリ ログイン名が **gkam** で、フルネームが **guitar kam** の場合、LDAP 認証を使用して SMA/SRA 装置にログインするときは、ユーザ名を次のように指定する必要があります。ログイン名が指定されている場合は、その名前を使ってツリーにバインドします。フィールドが空白の場合は、フルネームを使ってログインする必要があります。フィールドにフル ログイン名が入力されている場合は、SMAAccountName を使ってログインします。
- 属性が定義されていない場合は、LDAP サーバによって承認されたすべてのユーザがグループのメンバーになることができます。
- 複数のグループが定義されていて、ユーザが 2 つのグループのすべての LDAP 属性を満たしている場合、そのユーザは一番多くの LDAP 属性が定義されているグループに所属するものと見なされます。対応する LDAP グループの属性の数が等しいときは、グループのアルファベット順に所属グループが決められます。
- LDAP ユーザが、SMA/SRA 装置に設定されたどの LDAP グループの LDAP 属性も満たしていない場合、そのユーザはポータルにログインできません。つまり、LDAP 属性機能を使用することで、管理者は LDAP グループまたは組織ごとに個別のルールを作成できるだけでなく、特定の LDAP ユーザだけをポータルにログインさせることもできます。

LDAP ユーザおよび属性の例

LDAP グループに手動で追加したユーザの設定は LDAP 属性よりも優先されます。

例えば、LDAP 属性 **objectClass="Person"**がグループ Group1 に対して定義され、LDAP 属性 **memberOf="CN=WINS Users, DC=sonicwall, DC=net"**が Group2 に対して定義されているとします。

ユーザ Jane が LDAP サーバで Person オブジェクト クラスのメンバーとして定義されており、WINS Users グループのメンバーではない場合、Jane は SMA/SRA 装置の Group1 のメンバーになります。

しかし、管理者が手動でユーザ Jane を SMA/SRA 装置の Group2 に追加すると、LDAP 属性は無視され、Jane は Group2 のメンバーになります。

LDAP 属性の例

グループごとに最高 4 つの LDAP 属性を入力できます。次は、アクティブ ディレクトリの LDAP ユーザの LDAP 属性の例です。

```
name="Administrator"
memberOf="CN=Terminal Server Computers, CN=Users, DC=sonicwall, DC=net"
objectClass="user"
msNPAllowDialin="FALSE"
```

LDAP サーバの問い合わせ

LDAP またはアクティブ ディレクトリ サーバに問い合わせてユーザの LDAP 属性を調べるには、いくつか方法があります。コンピュータに LDAP 検索ツールがある場合 (例えば、OpenLDAP がインストールされた Linux コンピュータでは) 次のコマンドを実行します。

```
ldapsearch -h 10.0.0.5 -x -D
"cn=demo, cn=users, dc=sonicwall, dc=net" -w demo123 -b
"dc=sonicwall, dc=net" > /tmp/file
```

ここで、

- **10.0.0.5** は、LDAP またはアクティブ ディレクトリ サーバの IP アドレス
- **cn=demo, cn=users, dc=sonicwall, dc=net** は、LDAP ユーザの識別名
- **demo123** は、ユーザ `demo` のパスワード
- **dc=sonicwall,dc=net** は、問い合わせるベース ドメイン
- **> /tmp/file** は、オプションで、LDAP の問い合わせの結果を保存するファイル

ウィンドウズ サーバから LDAP サーバに問い合わせを行う方法については、以下を参照してください。

http://technet.microsoft.com/en-us/library/cc783845(v=ws.10).aspx

http://technet.microsoft.com/en-us/library/cc755809(v=ws.10).aspx

http://technet.microsoft.com/en-us/library/cc731033(v=ws.10).aspx

アクティブ ディレクトリおよび RADIUS ドメインのグループ設定

RADIUS またはアクティブ ディレクトリ サーバの認証を (Kerberos を使用して) 受ける場合、AAA ユーザおよびグループを個別に定義できます。これは必須でありませんが、個別の AAA ユーザに対してポリシーやブックマークを別々に作成できます。

ユーザがログインするときに、SMA/SRA 装置は、適切なアクティブ ディレクトリまたは RADIUS サーバを調べて、ユーザのログインが承認されているかどうかを確認します。ユーザが承認されている場合、SMA/SRA 装置は、ユーザがユーザおよびグループに関する SMA/SRA 装置データベースで定義されているかどうかを確認します。ユーザが定義されていれば、そのユーザに定義されているポリシーとブックマークを適用します。

例えば、"Miami RADIUS server" という名前の RADIUS ドメインを SMA/SRA 装置に作成した場合、"Miami RADIUS server" ドメインのメンバーであるユーザをグループに追加することができます。これらのユーザ名は、RADIUS サーバで設定されている名前と一致していなければなりません。その後、ユーザがポータルにログインすると、ポリシー、ブックマーク、その他のユーザ設定がユーザに適用されます。AAA ユーザが SMA/SRA 装置で定義されていなければ、グローバルな設定、ポリシー、およびブックマークだけがユーザに適用されます。

このセクションは、次のサブセクションから構成されています。

- 外部 (非ローカル) ユーザに対するブックマークのサポート (471 ページ)
- RADIUS グループの追加 (471 ページ)
- アクティブ ディレクトリ グループの追加 (472 ページ)

外部 (非ローカル) ユーザに対するブックマークのサポート

仮想オフィスのブックマーク システムでは、グループとユーザの両方のレベルでブックマークを作成することができます。管理者は該当ユーザに適用されるグループとユーザの両方のブックマークを作成できますが、個々のユーザは個人のブックマークしか作成できません。

ブックマークは SMA/SRA 装置のローカル設定ファイルに保存されるので、グループおよびユーザのブックマークを定義済みのグループおよびユーザ エンティティと対応づける必要があります。ローカル (LocalDomain) グループおよびユーザを操作するときは、管理者が装置上のグループおよびユーザを手動で定義しなければならないので、対応づけが自動的に行われます。同様に、外部 (非 LocalDomain、例えば、RADIUS または LDAP) グループを操作するときは、外部ドメインの作成によって対応するローカル グループが作成されるので、この対応づけが自動的に行われます。

ただし、外部 (非 LocalDomain) ユーザを操作するときは、ユーザ作成 (個人) のブックマークを Secure Mobile Access の設定ファイル内に保存できるように、ローカル ユーザ エンティティが存在していなければなりません。ブックマークを SMA/SRA 装置自体に保存する必要があるのは、LDAP および RADIUS の外部ドメインが、ブックマークなどの情報を保存する仕組みを提供していないからです。

個人のブックマークを使用する外部ドメイン ユーザのために、管理者がローカル ユーザを手動で作成せずに済むように、SMA/SRA 装置はユーザのログイン時に、対応するローカル ユーザ エンティティを自動的に作成します。ローカルに作成されたユーザにブックマークを追加することができます。

例えば、myRADIUS という名前の RADIUS ドメインが作成されていて、RADIUS ユーザの jdoe が SMA/SRA 装置にログインした場合、jdoe が個人のブックマークを追加した時点で、jdoe というローカル ユーザが SMA/SRA 装置に External 種別で作成され、管理者はそれを他のローカル ユーザと同じように管理できるようになります。外部ローカル ユーザは、管理者が削除するまで存続します。

RADIUS グループの追加

メモ：RADIUS グループを設定する前に、グループが関連付けられている RADIUS ドメインで RADIUS Filter-Id オプションが有効になっていることを確認してください。このオプションは、「**ポータル > ドメイン**」ページで設定します。

「**RADIUS グループ**」ページでは、既存の RADIUS グループのメンバーシップに基づいて SMA/SRA 装置へのユーザ アクセスを有効にできます。1 つまたは複数の RADIUS グループを Secure Mobile Access グループに追加することにより、指定の RADIUS グループに関連付けられているユーザのみがログインできます。

RADIUS グループを追加するには:

1. 「**ユーザ > ローカル グループ**」ページで、設定する RADIUS グループの「**設定**」を選択します。
2. 「**RADIUS グループ**」ページで、「**グループの追加...**」を選択します。「RADIUS グループの追加」ページが表示されます。
3. 「**RADIUS グループ**」名を該当のフィールドに入力します。グループ名は RADIUS Filter-Id と正確に一致する必要があります。
4. 「**適用**」を選択します。設定したグループが「RADIUS グループ」セクションに表示されます。

アクティブ ディレクトリ グループの追加

「**AD グループ**」ページでは、既存の AD グループのメンバーシップに基づいて SMA/SRA 装置へのユーザ アクセスを有効にできます。1 つまたは複数の AD グループを Secure Mobile Access グループに追加することにより、指定の AD グループに関連付けられているユーザのみがログインできます。

ⓘ **メモ**：アクティブ ディレクトリ グループを設定する前に、アクティブ ディレクトリ ドメインを既に作成済みであることを確認します。このオプションは、「**ポータル > ドメイン**」ページで設定します。

AD グループを追加するには:

1 「**ユーザ > ローカル グループ**」ページで、設定する AD グループの「**設定**」を選択します。

2 「**AD グループ**」ページで、「**グループの追加...**」を選択します。「アクティブ ディレクトリ グループの追加」ページが表示されます。

3 「**アクティブ ディレクトリ グループ**」名を該当のフィールドに入力します。

4 オプションで、Secure Mobile Access グループを AD グループと関連付けたい場合は、「**AD グループに関連付ける**」をオンにします。この手順は後でも、「**AD グループ**」ページの「**グループの編集**」から実行できます。

5 「**適用**」を選択します。設定したグループが「アクティブ ディレクトリ グループ」セクションに表示されます。グループの追加処理には数分かかる場合があります。この処理中に「**追加**」を複数回クリックしないでください。

ローカル グループの Citrix ブックマークの作成

ユーザの Citrix ブックマークを設定するには:

1 「**ユーザ > ローカル グループ**」に移動します。

2 設定するグループの横にある設定アイコンを選択します。

3 「**グループ設定の編集**」ウィンドウで、「**ブックマーク**」タブを選択します。

4 「**ブックマークの追加**」を選択します。

5 ブックマークの名前を「**ブックマーク名**」フィールドに入力します。

6 ブックマークの名前または IP アドレスを「**名前または IP アドレス**」フィールドに入力します。

7 「**サービス**」ドロップダウン リストで、「**Citrix ポータル (Citrix)**」を選択します。

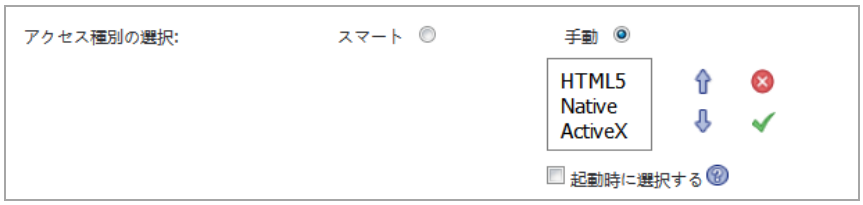
8 ドロップダウン リストから「**リソース ウィンドウ サイズ**」を選択します。

9 「**アクセス タイプの選択**」を選びます。「**スマート**」または「**手動**」のどちらかです。

- 「**スマート**」: ファームウェアにクライアントを起動するモードを決定させます。

新しい統合ブックマークを作成する場合は、「**スマート**」がデフォルトで選択されています。ブックマークの起動時には、ブックマーク固有の既定モードを使用して自動検出の処理が行われます。

- 「**手動**」: モードや優先順位を設定し、方法を選択するオプションを提供します。選択ボックスで、少なくとも 1 つのモードが有効になっている必要があります。



起動シーケンスは、「**HTML5**」、「**Native**」、「**ActiveX**」です。「手動」を選択すると、起動方法を変更、有効化、または無効化できます。Citrix ブックマークの起動に「**Native**」を選択すると、SMA Connect Agent がローカル マシンの Citrix Receiver を起動して Citrix 接続を行います。

「**上**」と「**下**」の矢印を使って起動順序を調整します。バツとチェックのアイコンを使ってモードの有効と無効を切り替えます。無効にしたモードはリストの下に移動し、グレー表示されます。

「**手動**」モードでは、デフォルトで「**起動中に選択**」オプションは有効ではありません。この設定では、ブックマークの起動時に、設定済みリストの先頭にある使用可能なモードが自動検出後に実行されます。

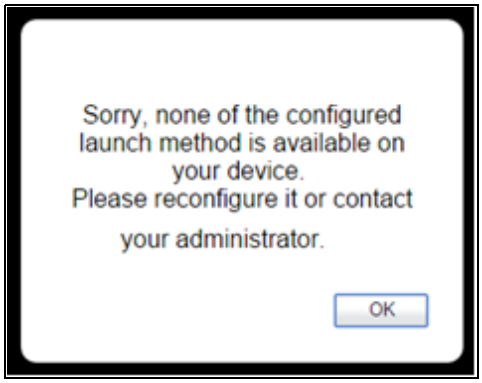
「**起動時に選択する**」オプションが有効になっていて、複数のモードがクライアントで使用可能な場合は、統合ブックマークの起動時にメニューが表示されます。このメニューでは、5 秒のカウントダウンが行われている間にモードを選択できます。使用可能なモードが 1 つしかない場合、ブックマークはただちに実行されます。

起動時に「**この選択を記憶する**」オプションが有効になっている場合は、選択されたモードが Cookie によって記憶されます。

その場合、次にブックマークを起動すると、記憶したモードが 2 秒以内に直接実行されます。HTML のどこかをクリックすると、記憶したモードを「忘れる」ので、再選択を行うことができます。

同じブラウザでブックマークの編集や削除しても、記憶したモードがリセットされます。

設定されたクライアントでどのモードも実行できない場合、次の通知が表示されます。



10 必要に応じて、「**HTTPS モード**」をオンにして HTTPS モードを有効にします。

11 オプションで「**指定した Citrix ICA サーバを常に使用する**」を選択して、現れた「**Citrix ICA サーバ アドレス**」フィールドに IP アドレスを指定します。この設定により、Citrix ICA セッションに対する Citrix ICA サーバのアドレスを指定することが可能です。既定では、ブックマークは Citrix サーバ上の ICA 設定内で提供される情報を使用します。

12 「**適用**」を選択します。

グローバル設定

SMA/SRA 装置のグローバル設定は、「**ローカル ユーザ**」または「**ローカル グループ**」環境から定義します。これらを表示するには、左側のナビゲーション メニューで「**ユーザ**」オプションを選択し、「**ローカル ユーザ**」オプションまたは「**ローカル グループ**」オプションを選択します。このセクションでは、次の構成方法について説明します。

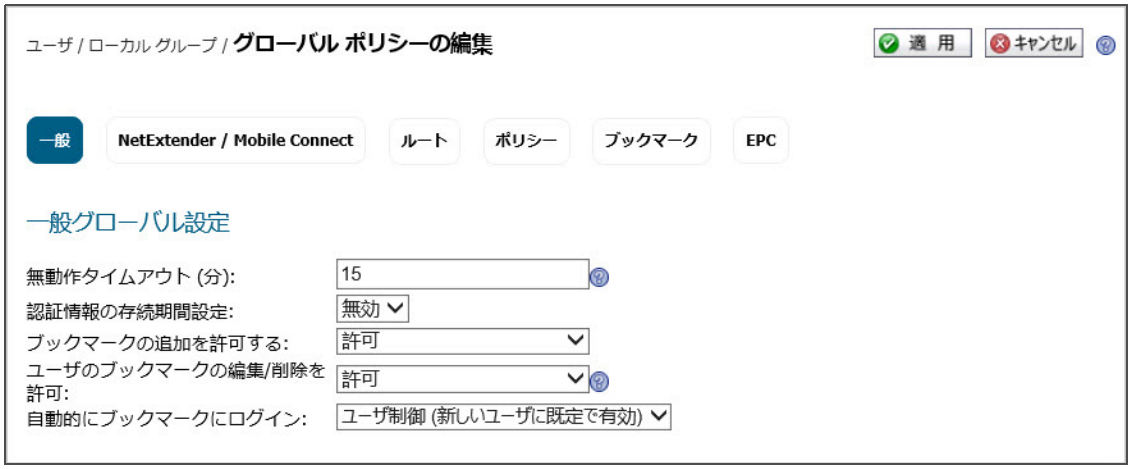
- グローバル設定の編集 (474 ページ)
- グローバル ポリシーの編集 (477 ページ)
- グローバル ブックマークの編集 (479 ページ)

グローバル設定の編集

グローバル設定を編集するには:

1 「**ユーザ** > **ローカル ユーザ**」または「**ユーザ** > **ローカル グループ**」ウィンドウに移動します。

2 「**グローバル ポリシー**」の横の設定アイコンを選択します。「**グローバル ポリシーの編集**」ページが表示されます。



3 「**一般**」タブで、すべてのユーザまたはグループの無動作タイムアウトを設定し、指定した時間が経過したらユーザを仮想オフィスからログアウトさせるには、許容する無動作時間 (分) を「**無動作タイムアウト**」フィールドに入力します。

> **メモ**：無動作タイムアウトは、ユーザ、グループ、グローバルの各レベルで設定できます。特定のユーザに複数のタイムアウトが設定されている場合は、ユーザ タイムアウトの設定がグループ タイムアウトよりも優先され、グループ タイムアウトがグローバル タイムアウトよりも優先されます。グローバル タイムアウトを 0 に設定すると、グループまたはユーザ タイムアウトが設定されていないユーザの無動作タイムアウトは無効になります。

4 ユーザが新しいブックマークを追加できるようにするには、「**ブックマークの追加を許可する**」ドロップダウン メニューで「**許可**」を選択します。ユーザが新しいブックマークを追加できないようにするには、「**拒否**」を選択します。

5 このグループのユーザが自分自身のブックマークを編集または削除できるようにするには、「**ユーザのブックマークの編集/削除を許可**」ドロップダウン メニューで「**許可**」を選択します。ユーザが自分自身のブックマークを編集または削除できないようにするには、「**拒否**」を選択します。

> **メモ**：ユーザはグループおよびグローバル ブックマークを編集または削除できません。

6 「**自動的にブックマークにログイン**」ドロップダウン リストから、次のいずれかのオプションを選択します。

- **ユーザ制御 (新しいユーザに既定で有効)**: ブックマークのシングル サインオン (SSO) 自動ログインをユーザが有効または無効にできるようにします。新規ユーザの場合は、この設定によって自動ログインが既定で有効になります。
- **ユーザ制御 (新しいユーザに既定で無効)**: ブックマークのシングル サインオン (SSO) 自動ログインをユーザが有効または無効にできるようにします。新規ユーザの場合は、この設定によって自動ログインが既定で無効になります。
- **有効**: ブックマークの自動ログインを有効にします。
- **無効**: ブックマークの自動ログインを無効にします。

7 「**適用**」を選択して設定の変更を保存します。

8 「**NetExtender / Mobile Connect**」ページに移動します。

9 クライアント アドレス範囲を設定するには、開始アドレスを「**クライアント アドレス範囲の開始**」フィールドに入力し、終了アドレスを「**クライアント アドレス範囲の終了**」フィールドに入力します。

10 クライアント IPv6 アドレス範囲を設定する場合は、先頭の IPv6 アドレスを「**クライアント IPv6 アドレス範囲開始**」フィールドに入力して、最後の IPv6 アドレスを「クライアント IPv6 アドレス範囲終了」フィールドに入力します。

11 「**切断後にクライアントを終了**」ドロップダウン リストで、「**有効**」または「**無効**」を選択します。

12 「**クライアント終了後にアンインストール**」ドロップダウン リストで、「**有効**」または「**無効**」を選択します。

13 「**クライアント接続プロファイルを作成**」ドロップダウン リストで、「**有効**」または「**無効**」を選択します。

14 「**ユーザ名とパスワードの保存**」ドロップダウン リストで、次のいずれかを選択します。

- **ユーザ名だけ保存を許可** - クライアントでユーザ名をキャッシュします。NetExtender を起動するときにユーザはパスワードのみを入力します。
- **ユーザ名とパスワードの保存を許可** - クライアントでユーザ名とパスワードをキャッシュします。最初のログイン後は、NetExtender を起動するとユーザは自動的にログインします。
- **ユーザ名とパスワードの保存は不可** - クライアントでユーザ名とパスワードをキャッシュしません。NetExtender を起動するときにユーザはユーザ名とパスワードを入力する必要があります。

15 「**ルート** 」タブに移動します。

16 「**強制トンネル方式**」ドロップダウン リストで「**有効**」を選択します。こうすると、このユーザへのすべてのトラフィック (リモート ユーザのローカル ネットワーク宛てのトラフィックも含む) で Secure Mobile Access NetExtender トンネルが使用されます。「**強制トンネル方式**」は既定では無効です。

17 クライアント ルートを追加するには、「**クライアント ルートの追加**」を選択します。

18 「**クライアント ルートの追加**」ウィンドウで、送信先ネットワークを「**送信先ネットワーク**」フィールドに入力します。たとえば、IPv4 ネットワーク アドレスを 10.202.0.0、IPv6 ネットワーク アドレスを 2007::1:2:3:0 形式で入力します。

19 IPv4 の送信先ネットワークに対しては、「**サブネット マスク/接頭辞**」フィールドに、サブネット マスクを 10 進形式 (255.0.0.0、255.255.0.0、または 255.255.255.0) で入力します。IPv6 の送信先ネットワークに対しては、112 のように接頭辞を入力します。

20 「**適用**」を選択して設定の変更を保存します。

21 「**ポリシー**」タブを開きます。

22 ポリシーを追加するには、「**ポリシーの追加**」を選択します。

23 「**ポリシーの適用先**」ドロップダウン リストで、以下のいずれかを選択します : **IP アドレス、IP アドレス範囲、すべてのアドレス、ネットワーク オブジェクト、サーバ パス、URL オブジェクト、すべての IPv6 アドレス、IPv6 アドレス、IPv6 アドレス範囲**。

24 ポリシーの名前を「**ポリシー名**」フィールドに入力します。

25 「**ポリシーの適用先**」で選択した設定に応じて表示されるフィールドで、適切な情報を指定します。例えば、「**ポリシーの適用先**」ドロップダウン リストで「**IP アドレス**」を選択した場合は、「**IP アドレス**」フィールドに IP アドレスを入力し、「**サービス**」ドロップダウン リストでサービスを選択する必要があります。「**IPv6 アドレス範囲**」を選択した場合は、先頭の IPv6 アドレスを「**IPv6 ネットワーク アドレス**」フィールドに入力して、この IPv6 アドレス範囲を定義する接頭辞を「**IPv6 接頭辞**」フィールドに入力します。オプションで、ポート範囲

(80-443 など) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。このフィールドは、「**ポリシーの適用先**」ドロップダウン リストで「**IP アドレス**」、「**IP アドレス範囲**」、「**IPv6 アドレス**」、または「**IPv6 アドレス範囲**」を選択すると使用できます。

26 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

メモ：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

27 「**適用**」を選択して設定の変更を保存します。

28 「**ブックマーク**」タブを選択します。

29 ブックマークを追加するには、「**ブックマークの追加**」を選択します。

30 ブックマークの名前を「**ブックマーク名**」フィールドに入力します。

31 ブックマークの名前または IP アドレスを「**名前または IP アドレス**」フィールドに入力します。

32 次のいずれかのサービスを「**サービス**」ドロップダウン リストで選択します。選択できるサービスは、「**ターミナル サービス (RDP)**」、「**仮想ネットワーク コンピューティング (VNC)**」「**Citrix Portal (Citrix)**」、「**ウェブ (HTTP)**」、「**セキュア ウェブ (HTTPS)**」、「**ファイル共有 (CIFS)**」、「**ファイル転送プロトコル (FTP)**」、「**SSH ファイル転送プロトコル (SFTP)**」、「**Telnet**」、「**セキュア シェル バージョン 2 (SSHv2)**」です。

メモ：IPv6 はファイル共有ブックマークではサポートされません。

33 「**サービス**」で選択した設定に応じて表示されるフィールドで、適切な情報を指定します。例えば、「**ターミナル サービス (RDP)** 」を選択した場合は、「**画面サイズ**」ドロップダウン リストで目的の画面サイズを選択する必要があります。

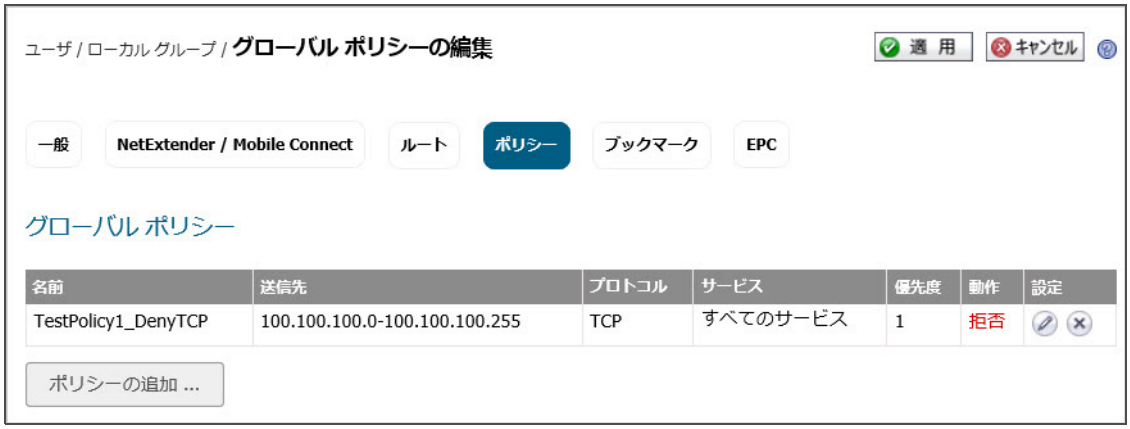
34 「**適用**」を選択して設定の変更を保存します。

グローバル ポリシーの編集

グローバル アクセス ポリシーを定義するには:

1 「**ユーザ > ローカル ユーザ**」または「**ユーザ > ローカル グループ**」ウィンドウに移動します。

2 「**グローバル ポリシー**」の横の設定アイコンを選択します。「**グローバルポリシーの編集**」ウィンドウが表示されます。



3 「**ポリシー**」タブで「**ポリシーの追加**」を選択します。「**ポリシーの追加**」ウィンドウが表示されます。

メモ:ユーザとグループのアクセス ポリシーはグローバル ポリシーよりも優先されます。

4 「**ポリシーの適用先**」ドロップダウン リストで、以下のいずれかを選択します：**IP アドレス**、**IP ネットワーク**、**すべてのアドレス**、**ネットワーク オブジェクト**、**サーバ パス**、**URL オブジェクト**、**すべての IPv6 アドレス**、**IPv6 アドレス**、**IPv6 ネットワーク**。

5 ポリシーの名前を「**ポリシー名**」フィールドに入力します。

メモ：SMA/SRA 装置のポリシーは、SMA/SRA 接続の送信元アドレスではなく送信先アドレスに適用されます。インターネット上の特定の IP アドレスがポリシー エンジンを通じて SMA/SRA 装置の認証を受けることを許可または阻止することはできません。

- ポリシーを特定の IPv4 ホストに適用する場合は、「**ポリシーの適用先**」ドロップダウン リストで「**IP アドレス**」オプションを選択し、ローカル ホスト コンピュータの IPv4 アドレスを「**IP アドレス**」フィールドに入力します。
- ポリシーを IPv4 アドレス範囲に適用する場合は、「**ポリシーの適用先**」ドロップダウン リストで「**IP ネットワーク**」オプションを選択し、IPv4 ネットワーク アドレスを「**IP ネットワーク アドレス**」フィールドに入力し、サブネット マスクを「**サブネット マスク**」フィールドに入力します。
- ポリシーを特定の IPv6 ホストに適用する場合は、「**ポリシーの適用先**」ドロップダウン リストで「**IPv6 アドレス**」オプションを選択し、ローカル ホスト コンピュータの IPv6 アドレスを「**IPv6 アドレス**」フィールドに入力します。
- ポリシーを IPv6 アドレス範囲に適用する場合は、「**ポリシーの適用先**」ドロップダウン リストで「**IPv6 ネットワーク**」オプションを選択し、IPv6 ネットワーク アドレスを「**IPv6 ネットワーク アドレス**」フィールドに入力し、IPv6 プレフィックスを「**IPv6 プレフィックス**」フィールドに入力します。

6 必要な**プロトコル**を選択します。「プロトコル」フィールドの値として選択できるのは、「**TCP**」、「**UDP**」、「**ICMP**」、および「**すべて**」です。「**TCP**」、「**UDP**」、「**ICMP**」は、複数を同時に選択できます。ただし、「**すべて**」が選択されている場合は、他のオプションはいずれも選択されません。

メモ：プロトコル設定は、サービスとして「NetExtender & Mobile Connect」または「すべてのサービス」が設定されている場合のみ、表示されます。

7 オプションで、ポート範囲 (80-443 など) や単独のポート番号を「**ポート範囲/ポート番号**」フィールドに入力します。このフィールドは、「**ポリシーの適用先**」ドロップダウン リストで「**IP アドレス**」、「**IP アドレス範囲**」、「**IPv6 アドレス**」、または「**IPv6 アドレス範囲**」を選択すると使用できます。

8 サービスの種類を「**サービス**」ドロップダウン リストで選択します。ポリシーの適用先がネットワーク オブジェクトの場合は、そのネットワーク オブジェクトで定義されたサービスが使用されます。

9 「**状況**」ドロップダウン リストから「**許可**」または「**拒否**」を選択し、指定したサービスおよびホスト コンピュータの SMA/SRA 接続を許可または拒否します。

10 「**適用**」を選択して設定を更新します。設定を更新すると、新しいポリシーが「**グローバルポリシーの編集**」ウィンドウに表示されます。グローバル ポリシーは、「**グローバルポリシーの編集**」ウィンドウのポリシー リストに、優先度の高いものから順番に表示されます。

ファイル共有のポリシーの編集

ファイル共有アクセス ポリシーを編集するには:

1 「**ユーザ** > **ローカル ユーザ**」または「**ユーザ** > **ローカル グループ**」ウィンドウに移動します。

2 「**グローバル ポリシー**」の横の設定アイコンを選択します。「**グローバルポリシーの編集**」ウィンドウが表示されます。

3 「**ポリシー**」タブを選択します。

4 「**ポリシーの追加**」を選択します。

5 「**ポリシーの適用先**」ドロップダウン リストで「**サーバ パス**」を選択します。

6 ポリシーの名前を「**ポリシー名**」フィールドに入力します。

7 「**リソース**」フィールドで、リソース種別を以下のラジオ ボタンから 1 つ選択します。

- 共有 (サーバ パス)
- ネットワーク (ドメイン リスト)
- サーバ (コンピュータ リスト)

8 「**サーバ パス**」フィールドに、サーバ パスを *servername/share/path* または *servername\share\path* の形式で入力します。使用できる接頭辞は \\、//、\、および / です。

メモ：共有とパスによって、ポリシーをより細かく管理できるようになります。どちらの設定もオプションです。

9 「**状況**」ドロップダウン リストで「**許可**」または「**拒否**」を選択します。

10 「**適用**」を選択します。

グローバル ブックマークの編集

グローバル ブックマークを編集するには:

1 「**ユーザ** > **ローカル ユーザ**」または「**ユーザ** > **ローカル グループ**」ページに移動します。

2 「**グローバル ポリシー**」の横の設定アイコンを選択します。「**グローバル ポリシーの編集**」ページが表示されます。

3 「**ブックマークの追加**」を選択します。「**ブックマークの追加**」ウィンドウが表示されます。

メモ: グローバル ブックマークを定義すると、すべてのユーザが Secure Mobile Access ユーザ ポータルで定義済みのブックマークを見ることができます。個々のユーザがグローバル ブックマークを削除または変更することはできません。

4 ブックマークを編集するには、わかりやすい名前を「**ブックマーク名**」フィールドに入力します。

5 LAN 上のホスト コンピュータのドメイン名または IP アドレスを「**名前または IP アドレス**」フィールドに入力します。

6 サービスの種類を「**サービス**」ドロップダウン リストで選択します。

7 「**適用**」を選択して設定を更新します。設定を更新すると、新しいグローバル ブックマークが「**グローバルポリシーの編集**」ウィンドウのブックマーク リストに表示されます。

EPC 設定の編集

ローカル グループまたはユーザが使用するエンド ポイント制御プロファイルを設定するには:

1 「**ユーザ** > **ローカル ユーザ**」または「**ユーザ** > **ローカル グループ**」ページに移動します。

2 「**グローバル ポリシー**」の横の設定アイコンを選択します。「**グローバル ポリシーの編集**」ページが表示されます。

3 「EPC」タブを選択します。「**EPC の設定**」ページが表示されます。

4 ユーザ > ローカル グループ (440 ページ) およびユーザ > ローカル グループ (440 ページ) で説明しているように、EPC グローバル設定を構成して、デバイス プロファイルを追加または削除します。

17

ログの設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**ログ**」ページと、このページで行う設定タスクについて説明します。

トピック:

ログ > 表示

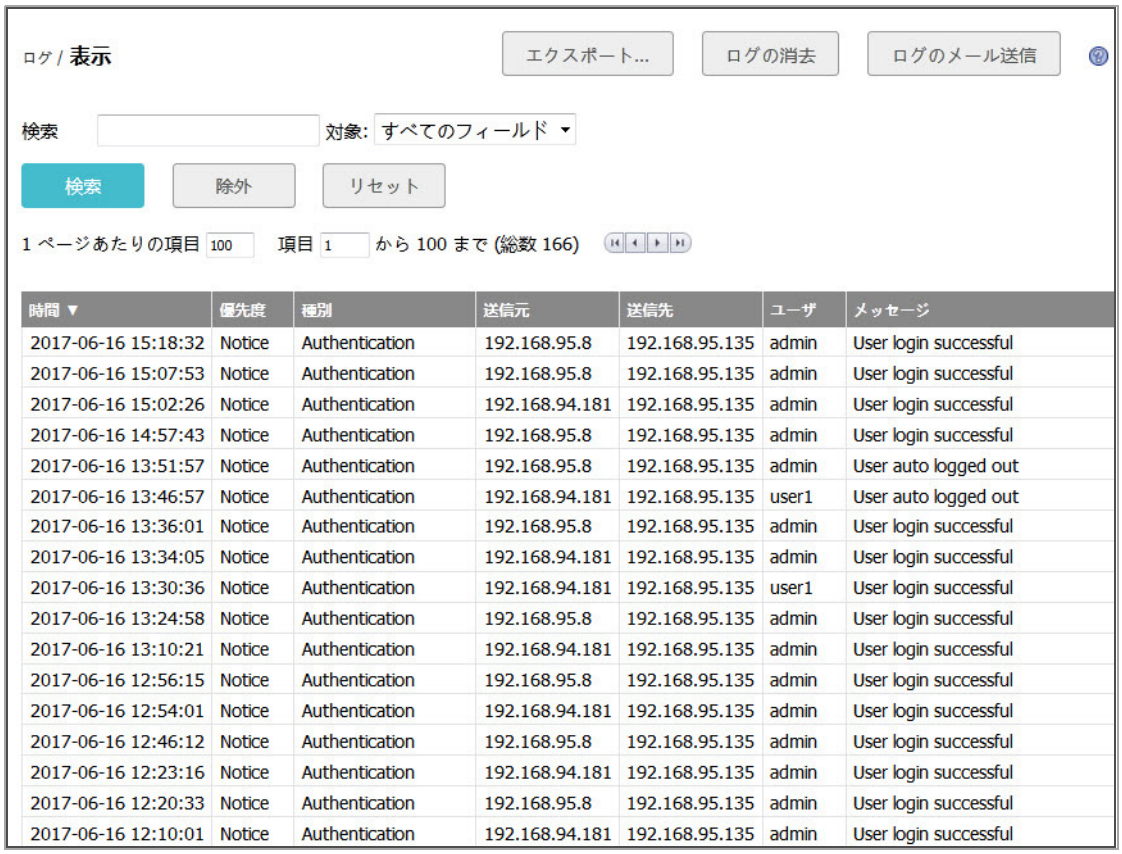
SMA/SRA 装置は、ウェブベースのログ、Syslog ログ、および電子メール警告メッセージをサポートしています。また、SMA/SRA 装置は、イベント ログ ファイルを消去する前に Secure Mobile Access 管理者の電子メール アドレスに送信するように設定することもできます。

このセクションでは、「**ログ > 表示**」ページの概要、およびこのページで行う設定タスクについて説明します。

「ログ > 表示」の概要

「**ログ > 表示**」ページには、Secure Mobile Access のイベント ログを表示することができます。イベント ログは、利便性とアーカイブのために電子メール アドレスに自動的に送信することもできます。

ログ > 表示



時間 ▼	優先度	種別	送信元	送信先	ユーザ	メッセージ
2017-06-16 15:18:32	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 15:07:53	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 15:02:26	Notice	Authentication	192.168.94.181	192.168.95.135	admin	User login successful
2017-06-16 14:57:43	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 13:51:57	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User auto logged out
2017-06-16 13:46:57	Notice	Authentication	192.168.94.181	192.168.95.135	user1	User auto logged out
2017-06-16 13:36:01	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 13:34:05	Notice	Authentication	192.168.94.181	192.168.95.135	admin	User login successful
2017-06-16 13:30:36	Notice	Authentication	192.168.94.181	192.168.95.135	user1	User login successful
2017-06-16 13:24:58	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 13:10:21	Notice	Authentication	192.168.94.181	192.168.95.135	admin	User login successful
2017-06-16 12:56:15	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 12:54:01	Notice	Authentication	192.168.94.181	192.168.95.135	admin	User login successful
2017-06-16 12:46:12	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 12:23:16	Notice	Authentication	192.168.94.181	192.168.95.135	admin	User login successful
2017-06-16 12:20:33	Notice	Authentication	192.168.95.8	192.168.95.135	admin	User login successful
2017-06-16 12:10:01	Notice	Authentication	192.168.94.181	192.168.95.135	admin	User login successful

「**ログ > 表示**」ページには、ログ メッセージが、並べ替え可能で検索可能なテーブルに表示されます。SMA/SRA 装置は、最大 1GB のログ データをログ ファイル システムに保存できます。ログ ファイルごとに 50MB の制限があります。各ログ項目には、イベントの日時、およびイベントを説明する簡単なメッセージが含まれます。ログ ファイルがログ サイズ制限に達すると、ログ エントリは消去され、必要に応じて Secure Mobile Access 管理者の電子メール アドレスに送信されます。

ログ テーブル サイズは、「**システム > 管理**」ページの「既定のテーブル サイズ」で設定できます。

列の表示

ログ エントリに表示される情報は以下のとおりです。

ログ ページの列

列	説明
時間	タイムスタンプには、ログ イベントの日時が *YY/MM/DD/HH/MM/SS* (年/月/日/時/分/秒) の形式で表示されます。時間は 24 時間形式で表示される。日時は、「**システム > 時間**」ページで設定された SMA/SRA ゲートウェイのローカル時間に基づきます。
優先度	イベントに関連付けられた深刻度。重大度の値は、**緊急**、**警告**、**重大**、**エラー**、**注意**、**通告**、**情報**、および**デバッグ**のいずれか。
種別	イベント メッセージの種別です。種別には、認証、認証とアクセス、GMS、NetExtender、システム、仮想アシスト、およびウェブ アプリケーション ファイアウォールがあります。

ログ ページの列 (続き)

列	説明
送信元	送信元の IP アドレスは、そのログ イベントを生成したユーザまたは管理者の装置の IP アドレスを示します。システム エラーなど、送信元の IP アドレスが表示できないイベントもあります。
送信先	送信先の IP アドレスは、そのイベントに関連付けられたサーバまたはサービスの名前または IP アドレスを示します。例えば、ユーザが Secure Mobile Access ポータルを介してイントラネットのウェブ サイトにアクセスした場合、対応するログ エントリには、アクセスしたウェブ サイトの IP アドレスまたは完全修飾ドメイン名 (FQDN) が表示されます。
ユーザ	メッセージが生成されたときにセキュリティ装置にログインしていたユーザの名前
場所	各イベント ログ メッセージの送信元 IP の地理的な場所。
メッセージ	ログ メッセージのテキスト

ログ テーブルのエントリのナビゲートおよび並べ替え

「**ログ > 表示**」ページでは、多数のログ イベントを簡単に閲覧できるようにページ付けがされています。これらのログ イベントにナビゲートするには、以下の表で説明する機能を使用します。

ログ テーブルのナビゲーション機能

ナビゲーション ボタン	説明
検索	基準リストで選択した基準タイプに基づき、指定した設定を含むログを検索できます。検索基準には、時間、優先順位、送信元、送信先、およびユーザがあります。検索結果にリストされる結果の順序は、選択した基準のタイプによって異なります。
除外	基準リストで指定したタイプ以外のすべてのログ エントリを表示できます。
リセット	検索ボタンを使用してログ エントリの表示順序を変更した後、ログ エントリのリストを既定の順序にリセットします。

「ログ > 表示」のボタン

「**ログ > 表示**」ページには、ログを送信したり保存したりして、外部で表示または処理できるようにするオプションもあります。

ログ送付オプション

ボタン	動作
エクスポート	現在のログの内容をテキストベースのファイルにエクスポートします。ログのエクスポート コマンドを実行した後で、ローカル ログの内容は消去されます。
ログの消去	現在のログの内容を消去します。
ログのメール送信	現在のログの内容を「**ログ > 設定**」画面で指定されたアドレスに電子メールで送信します。電子メール ログ コマンドを実行した後で、ローカル ログの内容は消去されます。

ログの表示

「**ログ > 表示**」ページには、SMA のイベント ログを表示することができます。SMA/SRA 装置は、失敗したログイン試行、NetExtender セッション、ログアウト イベントなどのシステム イベントを追跡するためのイベント ログを保持します。このログは、「**ログ** > 表示」ページに表示するほか、特定の電子メール アドレスに自動的に送信して、何かに役立てたりアーカイブしたりできます。

SMA/SRA 装置は、最大 1GB のログ データをログ ファイル システムに保存できます。ログは並び替えや検索が可能な表に表示されます。装置は、ログインが成功した場合や設定がエクスポートされた場合などにイベントを通知することができます。警告は、発生時にすぐに電子メールで送信することも、管理者が電子メールに含めるログの形式を選択することもできます。ログの形式は、電子メール本文内に表示するインライン テキストか、zip で圧縮した添付ファイル (既定) です。各ログ項目には、イベントの日時、およびイベントを説明する簡単なメッセージが含まれます。ログ ファイルが 50 MB のログ サイズ制限に達すると、ログ エントリは消去され、必要に応じて Secure Mobile Access 管理者の電子メール アドレスに送信されます。

ログ エントリに表示される情報は以下のとおりです。

ログ ページの列

列	説明
時間	ログ イベントの日時が *YY/MM/DD/HH/MM/SS* (年/月/日/時/分/秒) の形式で表示される。時間は 24 時間形式で表示される。日時は、「**システム > 時間**」ページで設定された SMA/SRA ゲートウェイのローカル時間に基づきます。
優先度	イベントに関連付けられた重大度が表示される。重大度の値は、**緊急**、**警告**、**重大**、**エラー**、**注意**、**通告**、**情報**、および**デバッグ**のいずれか。
種別	イベント メッセージの種別です。
送信元	そのログ イベントを生成したユーザまたは管理者の装置の IP アドレスを表示する。システム エラーなど、送信元の IP アドレスが表示できないイベントもあります。
送信先	そのイベントに関連付けられたサーバまたはサービスの名前または IP アドレスを表示する。例えば、ユーザが Secure Mobile Access ポータルを介してインターネットのウェブ サイトにアクセスした場合、対応するログ エントリには、アクセスしたウェブ サイトの IP アドレスまたは完全修飾ドメイン名 (FQDN) が表示されます。
ユーザ	メッセージが生成されたときにセキュリティ装置にログインしていたユーザの名前
メッセージ	ログ メッセージのテキスト

ログの電子メール送信

「**ログのメール送信**」ボタンを使うと、Secure Mobile Access イベント ログを即時に送信および受信することができます。この機能は、電子メールをアーカイブする場合や、複数の SMA/SRA 装置に対して電子メールの設定やフィルタをテストする場合に便利です。

電子メール ログ機能を使用するには:

1 「**ログ > 表示**」にナビゲートします。

2 「**ログのメール送信**」を選択します。

3 「**ログは正常に送信されました**」というメッセージが表示されます。

メモ：エラー メッセージが表示された場合は、管理者の電子メールや電子メール サーバの情報が「**ログ > 設定**」ページの「**電子メール ログと警告**」セクションに指定されているかを確認してください。管理者の電子メールの設定方法については、ログの設定 (486 ページ) を参照してください。

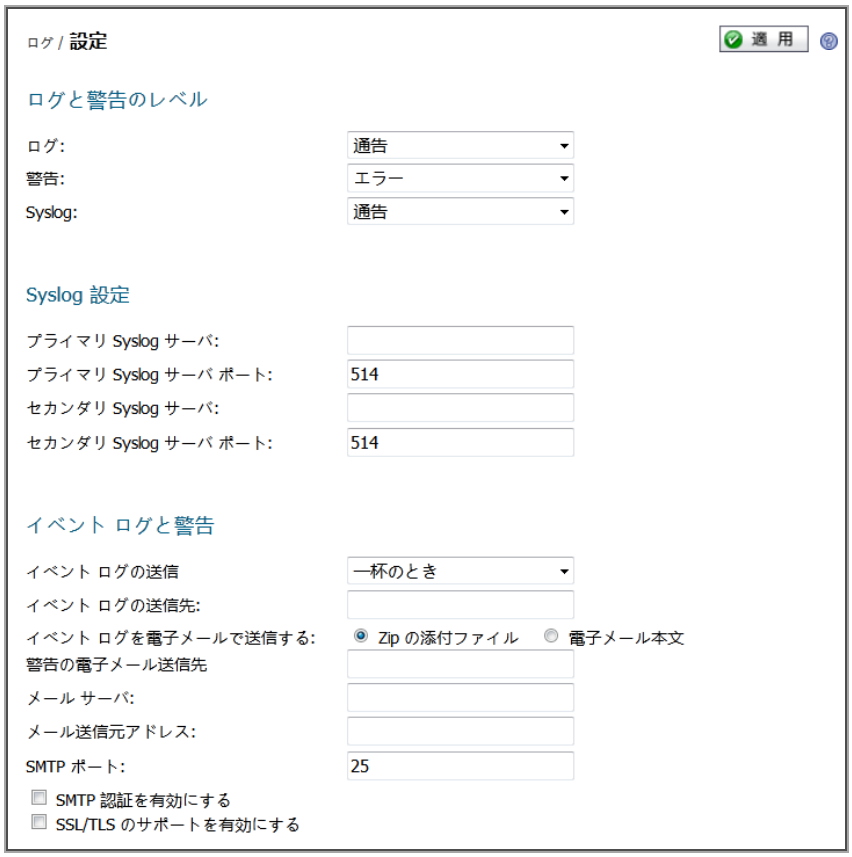
ログ > 設定

ログ > 設定このセクションでは、「**ログ > 設定**」ページの概要、およびこのページで行う設定タスクについて説明します。

「ログ > 設定」の概要

「**ログ > 設定**」ページでは、ログ警告および syslog サーバの設定を構成できます。Syslog は、システム アクティビティとネットワーク アクティビティを記録する業界標準のログ プロトコルです。Syslog メッセージは、WELF (WebTrends Enhanced Log Format) で送信されるので、通常の標準的なファイアウォールやネットワーク レポート製品はログ ファイルを受け取って解釈することができます。Syslog サービスは、UDP ポート 514 で待機している外部の Syslog サーバに Syslog メッセージを送信します。

ログ > 設定ページ



ログと警告のレベル

「ログと警告のレベル」セクションでは、Syslog、イベント ログ、および警告の種別を選択できます。種別には、緊急、警告、重大、エラー、注意、通知、情報、およびデバッグがあります。

Syslog 設定

「Syslog の設定」セクションでは、プライマリ Syslog サーバおよびセカンダリ Syslog サーバを指定できます。

イベント ログと警告

「イベント ログと警告」セクションでは、ログの送信先の電子メール アドレス、メール サーバ、メールの送信元アドレス、および警告の電子メールを送信する頻度を指定して、電子メール警告を設定できます。イベント ログを電子メールで送信する日時をスケジュールすることも、電子メールを 1 週間ごとに送信するようにスケジュールすることも、ログが一杯になったときに電子メールを送信することもできます。SMTP 認証を有効にし、SMTP ポートとともにユーザ名とパスワードを設定することができます。

ログの設定

ログと警告の設定を行うには、以下の手順を実行します。

1 イベント ログ、Syslog、警告の設定を始めるには、「**ログ > 設定**」ページにナビゲートします。

2 「**ログと警告のレベル**」セクションで、ログ (イベント ログ)、警告、または Syslog メッセージとして識別されるログ メッセージの深刻度レベルを定義します。ログ レベルは重要度の最高から最低へと並べられています。特定のログ サービスに対してレベルが選択されると、そのログ レベルとそれより重要度の高いイベントがログ記録されます。例えば、ログ サービスに対して「エラー」レベルが選択された場合は、「緊急」、「警告」、「重大」、および「エラー」のすべてのイベントが内部ログ ファイルに記録されます。

3 「**プライマリ Syslog サーバ**」フィールドに、Syslog サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。Syslog ログが必要ない場合は、このフィールドを空白のままにしておきます。

4 バックアップ用または 2 台目の Syslog サーバがある場合は、そのサーバの IP アドレスまたはドメイン名を「**セカンダリ Syslog サーバ**」フィールドに入力します。

5 ログ ファイルを消去し、管理者に電子メールで送信する時期を「**イベント ログの送信**」フィールドで指定します。「**一杯のとき**」オプションを選択すると、イベント ログは 50MB の最大ファイル サイズに到達したときに送信されます。その後、ログ ファイルは消去されます。「**1 日ごと**」を選択した場合は、イベント ログを電子メールで送信する時刻を選択します。「**1週間ごと**」を選択した場合は、曜日と時刻を選択します。「**1 日ごと**」または「**1 週間ごと**」を選択した場合でも、その期限の前にログ ファイルが一杯になると、ログ ファイルは送信されます。「**ログ > 表示**」ページで、「**ログの消去**」を選択して、現在のイベント ログを削除することができます。この場合は、イベント ログは電子メールで送信されません。

6 電子メールでイベント ログ ファイルを受け取るには、「イベント ログと警告」領域の「**イベント ログの送信先**」フィールドに完全な電子メール アドレス (username@domain.com) を入力します。イベント ログ ファイルは、イベント ログが消去される前に、指定された電子メール

アドレスに送信されます。このフィールドを空白のままにした場合、ログ ファイルは電子メールで送信されません。

7 電子メールで警告メッセージを受け取るには、「**警告の電子メール送信先**」フィールドに完全な電子メール アドレス (username@domain.com) または電子メール ページャ アドレスを入力します。警告イベントが発生すると、指定された電子メール アドレスに電子メールが送信されます。このフィールドを空白のままにした場合、警告メッセージは電子メールで送信されません。

ⓘ **メモ**：警告メッセージを生成するイベントのタイプを、「**ログ > 種別設定**」ページで定義します。

8 ログ ファイルまたは警告メッセージを電子メールで送信するには、「**メール サーバ**」フィールドにメール サーバのドメイン名または IP アドレスを入力します。このフィールドを空白のままにした場合、ログ ファイルと警告メッセージは電子メールで送信されません。

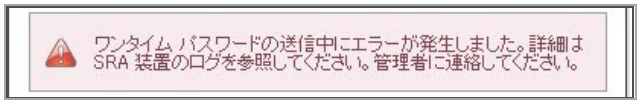
9 「**メール送信元アドレス**」に、送信元の電子メール アドレスを入力します。このアドレスは、ログと警告の電子メールの差出人として使用されます。

10 ログ ファイルの送信時に SMTP 認証を使用するには、「**SMTP 認証を有効にする**」をオンにします。関連するフィールドが画面に表示されます。ユーザ名、パスワード、および SMTP ポートを入力します。既定のポートは 25 です。

11 「**適用**」を選択して構成の設定を更新します。

メール サーバの設定

電子メールで通知を受け取る場合や、ワンタイム パスワード機能を有効にする場合は、「**ログ > 設定**」ページでメール サーバを設定する必要があります。メール サーバを設定せずにワンタイム パスワード機能を使用すると、次のエラー メッセージが表示されます。



ワンタイム パスワード機能の設定の詳細については、ワンタイム パスワードの概要 (52 ページ) を参照してください。

メール サーバを設定するには:

1 管理者の資格情報を使用して、Secure Mobile Access 管理インターフェースにログインします。

2 「**ログ > 設定**」にナビゲートします。

3 「**イベント ログの送信先**」フィールドに、ログの送信先となる電子メール アドレスを入力します。

4 「**警告の電子メール送信先**」フィールドに、警告の送信先となる電子メール アドレスを入力します。

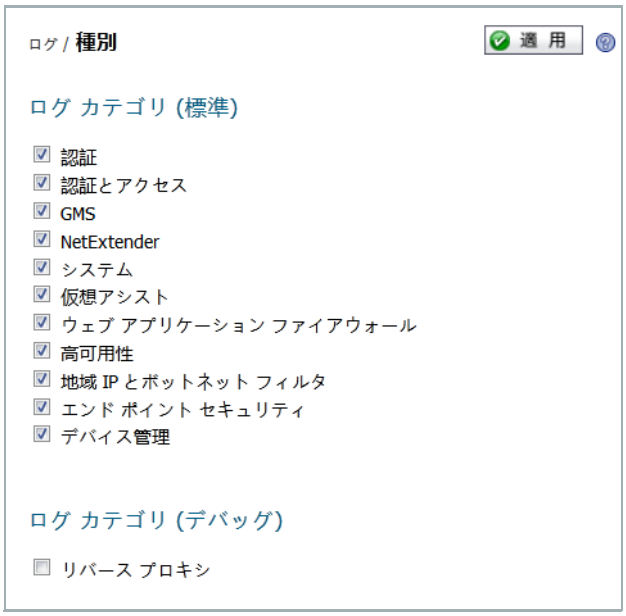
5 「**メール サーバ**」フィールドに、使用しているメール サーバの IP アドレスを入力します。

6 「**メール送信元アドレス**」フィールドに、SMA/SRA 装置から送信する電子メールの送信元アドレスを入力します。

7 右上隅にある「**適用**」を選択します。

ログ > 種別

このセクションでは、「**ログ > 種別**」ページの概要を示し、ログに記録されるイベント メッセージの種別について説明します。このページでは、種別ごとに有効/無効を設定することができます。この機能は、デバッグ プロセス中にログをフィルタする場合に特に便利です。



管理者は、以下のログ種別について、有効または無効をチェック ボックスで設定できます。

- 認証
- 認証とアクセス
- GMS
- NetExtender
- システム
- 仮想アシスト
- ウェブ アプリケーション ファイアウォール
- 高可用性 (SMA 400/200、SRA 4600)
- 地域 IP とボットネット フィルタ
- エンド ポイント セキュリティ
- デバイス管理
- リバース プロキシ

すべての選択を終えたら、画面の右上隅にある「**適用**」を選択して種別の設定を終了します。

ログ > ViewPoint

このセクションでは、「**ログ > ViewPoint**」ページの概要、およびこのページで行う設定タスクについて説明します。

「ログ > ViewPoint」の概要

「**ログ > ViewPoint**」ページでは、SonicWall Inc. ViewPoint が利用可能なインストール環境、または SonicWall Inc. グローバル管理システム (GMS) 装置管理ソフトウェアによって管理されているインストール環境で、ViewPoint サーバに SMA/SRA 装置を追加することができます。この機能には、ViewPoint ライセンス キーが必要です。

ViewPoint は、統合された装置管理ソリューションであり、以下の機能を提供します。

- SMA/SRA 装置およびリモート アクセス アクティビティに関する動的なウェブベース レポートの作成
- SMA/SRA 装置のすべてのアクティビティを示すリアルタイム レポートおよび履歴レポートの生成
- リモート アクセス監視
- ネットワーク セキュリティの強化
- 将来必要となる帯域幅の予測

ヒント：ViewPoint を使って SonicWall Inc. 装置を監視する方法については、以下を参照してください。http://www.sonicwall.com/us/support/3887.html

ViewPoint サーバの追加

この機能には、ViewPoint ライセンス キーが必要です。

ViewPoint サーバに SMA/SRA 装置を追加し、SMA/SRA 装置で ViewPoint レポーティングを有効にするには:

1 ウェブベースの Secure Mobile Access 管理インターフェースの「**ログ > ViewPoint**」ページに移動します。

メモ：この装置で ViewPoint を初めて使用する場合、または有効なライセンスがない場合は、「**システム > ライセンス**」ページが表示され、ライセンスを有効化するように求められます。

2 「ViewPoint の設定」セクションで、「**追加**」を選択します。「ViewPoint サーバの追加」画面が表示されます。

3 「ViewPoint サーバの追加」画面で、ViewPoint サーバの「**ホスト名または IP アドレス**」を入力します。

4 ViewPoint サーバが管理機器との通信に使用する「**ポート**」を入力します。

5 ページ上部の「**適用**」ボタンを選択して、このサーバを追加します。

6 追加したサーバについて、ViewPoint のレポート ログを開始するには、「**ViewPoint を有効にする**」をオンにします。

ログ > Analyzer

このセクションでは、「**ログ > Analyzer**」ページの概要、およびこのページで行う設定タスクについて説明します。

「ログ > Analyzer」の概要

「**ログ > Analyzer**」ページでは、SonicWall Inc. Analyzer が利用可能なインストール環境、または SonicWall Inc. グローバル管理システム (GMS) バージョン 7.0 以降の装置管理ソフトウェアによって管理されているインストール環境で、Analyzer サーバに SMA/SRA 装置を追加することができます。この機能には、Analyzer ライセンス キーが必要です。

SonicWall Inc. Analyzer は、動的なウェブ ベースのネットワーク レポートを作成するソフトウェア アプリケーションです。Analyzer レポーティング モジュールはリアルタイムおよび履歴レポートの両方を生成して、SonicWall Inc. ネットワーク セキュリティ装置を介するすべてのアクティビティに対する完全な視野を提供します。Analyzer レポートを使用すると、ネットワーク アクセスの監視、セキュリティの強化、帯域幅に関する将来のニーズの予測を行うことができます。Analyzer レポート モジュールは以下の通りです。

- 帯域幅の使用量を IP アドレスおよびサービス別に表示します。
- 不適切なウェブ使用を識別します。
- 攻撃の詳細なレポートを提供します。
- システムおよびネットワークのエラーを収集して集計します。
- VPN に関するイベントや問題を表示します。
- 訪問者によるウェブ サイトへのトラフィックを提示します。
- 特定のイベントを分析するために 1 日ごとの詳細なログを提供します。

ヒント：Analyzer を使って SonicWall Inc. 装置を監視する方法については、以下を参照してください。〈http://www.sonicwall.com/us/support/6631.html〉

Analyzer サーバの追加

この機能には、Analyzer ライセンス キーが必要です。

Analyzer サーバに SMA/SRA 装置を追加し、SMA/SRA 装置で Analyzer レポーティングを有効にするには:

1 ウェブベースの Secure Mobile Access 管理インターフェースの「**ログ > Analyzer**」ページに移動します。

メモ：この装置で Analyzer を初めて使用する場合、または有効なライセンスがない場合は、ライセンスを有効化するために「**システム > ライセンス**」ページへのリンクが表示されます。

2 「Analyzer 設定」セクションで、「**追加**」を選択します。「Analyzer サーバの追加」画面が表示されます。

3 「Analyzer サーバの追加」画面で、Analyzer サーバの「**ホスト名または IP アドレス**」を入力します。

4 Analyzer サーバが管理機器との通信に使用する「**ポート**」を入力します。既定値は 514 です。

5 ページ上部の「**適用**」ボタンを選択して、このサーバを追加します。

6 追加したサーバについて、Analyzer のレポート ログを開始するには、「**Analyzer を有効にする**」をオンにします。

第 3 部

仮想オフィスの使用

- 仮想オフィスの設定

18

仮想オフィスの設定

このセクションでは、ウェブベースの Secure Mobile Access 管理インターフェースの「**仮想オフィス**」ページと、このページで行う設定タスクについて説明します。

トピック:

仮想オフィス

このセクションでは、仮想オフィスページの概要とこのページで設定するタスクについて説明します。

仮想オフィスとは

「**仮想オフィス**」オプションは、Secure Mobile Access 管理インターフェースのナビゲーション バーにあります。

「**仮想オフィス**」オプションを選択すると、個別のウェブ ブラウザ ウインドウで仮想オフィス ユーザ ポータルが起動します。仮想オフィスはユーザがブックマークやファイル共有、NetExtender セッション、セキュア仮想アシスト、およびセキュア仮想ミーティングを作成するために利用するポータルです。

仮想オフィスの使用

仮想オフィスを使用するには:

1 ウェブベースの Secure Mobile Access 管理インターフェースで、ナビゲーション バーの「**仮想オフィス**」を選択します。

2 新しいブラウザ ウィンドウが開き、仮想オフィスのホームページが表示されます。

> ⓘ **メモ:** 仮想オフィスをウェブベースの Secure Mobile Access 管理インターフェースから起動すると、自動的にそのユーザの管理者資格情報でログインします。

仮想オフィスに管理者としてログオンしている場合、「**ログアウト**」ボタンは表示されません。ログアウトするには、ブラウザ ウィンドウを閉じる必要があります。

3 仮想オフィスのホーム ページからは、以下のタスクが可能です。

- Secure Mobile Access Connect Agent の起動およびインストール
- NetExtender の起動およびインストール
- ファイル共有の使用
- 仮想アシスト セッションの開始
- ブックマークの追加及び設定
- オフロードされたポータルに対するブックマークの追加及び設定
- ブックマーク リンクの選択
- 証明書のインポート

- 仮想オフィスのヘルプの参照
- 管理者によって許可されている場合は、セキュア仮想アクセス モードのためのシステム設定
- パスワードの設定
- シングル サインオン オプションの設定

メモ: 仮想オフィス ユーザ ポータルと上記のタスクに関する設定の詳細情報については、『*Secure Mobile Access ユーザ ガイド*』を参照してください。

SMA Connect Agent

ブラウザ プラグイン (NPAPI および ActiveX) は、NetExtender、仮想アシスト、EPC などのネイティブ アプリケーションを起動するために使用されます。セキュリティ上の理由から、普及度の高いブラウザでは、これらのプラグインが遮断されています。例えば、Chrome ブラウザではすべての NPAPI プラグインが無効になっており、最新の Microsoft Edge ブラウザは ActiveX をサポートしていません。そのため、ブラウザからの直接起動という便利な方法はもう機能せず、シームレスな起動を行うための新しい方法が必要になります。

特定のスキーマの URL を開くことで、異なるアプリケーションを起動することができます。Windows/OS X では、*mailto* などのいくつかのスキーマがすでに定義されています。SMA Connect Agent は、ブラウザ プラグインの代わりにスキーマ URL を使用します。SMA Connect Agent は、スキーマ URL リクエストを受け取って特定のネイティブ アプリケーションを開くブリッジのようなものです。

Citrix ブックマークから Citrix Receiver を起動するには、最初に SMA Connect Agent をインストールする必要があります。

トピック:

- サポートされるオペレーティング システム (495 ページ)
- ダウンロードとインストール (495 ページ)
- SMA Connect Agent の設定 (496 ページ)

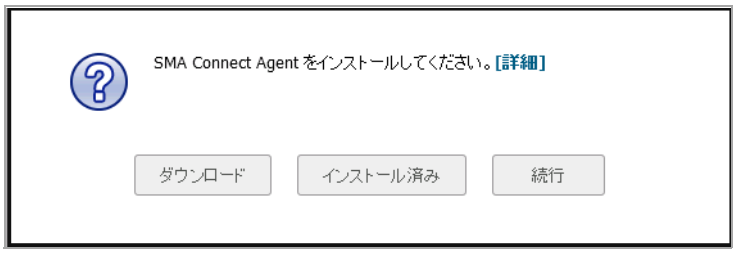
サポートされるオペレーティング システム

SMA Connect Agent は、Windows (7、8、10) と Macintosh (OS X) オペレーティング システムをサポートします。

ダウンロードとインストール

ようこそページで EPC または PDA 機能を使用する必要がある場合、ダウンロードとインストールの通知が表示されます。

「ポータル」ページでは、ユーザが NetExtender、仮想アシスト、仮想ミーティング、RDP ブックマーク (ネイティブ)、または Citrix ブックマーク (ネイティブ) を起動しようとすると、次のようなダウンロードとインストールに関する通知が表示されます。



- **「ダウンロード」**-**「ダウンロード」**をクリックし、SMA 接続エージェントをダウンロードしてインストールします。その後、ユーザは「インストール済み」をクリックして、SMA 接続エージェントがインストールされたことをブラウザに「記憶」させることができます。または、**「続行」**をクリックしてページをバイパスし、StoreFront にログインすることもできます。
- **インストール済み** - この通知が再び表示されることはありません。
- **続行** - 通知を閉じ、操作を続行します。
- **[詳細]** - SMA Connect Agent を説明するウィンドウを開きます。

ダウンロード完了後には、インストーラが表示されます。Windows 用インストーラは「`SMAConnectAgent.msi`」、Macintosh 用インストーラは「`SMAConnectAgent.dmg`」です。Windows のインストーラには、インストールの権限が必要です。Macintosh のインストーラでは、SMA Connect Agent を `/Application` ディレクトリに入れるよう表示されます。

SMA Connect Agent の設定

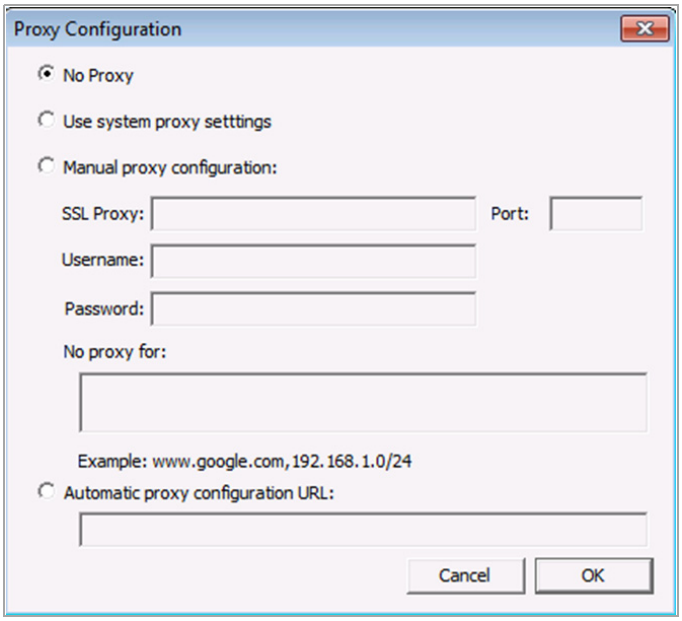
プロキシの設定

SMA はプロキシの配備をサポートしています。その場合、装置がクライアント ブラウザとプロキシ サーバの間に存在し、すべてのクライアント ブラウザがプロキシ サーバにリダイレクトされるよう設定されます。このシナリオでは、ドメインが仮想ホスティング サーバに含まれる場合のドメイン除外や同じサーバ IP を複数のドメインで使用できるクラウド配備のサポートなど、すべての SMA 機能がサポートされています。

また、通常のデータ センター サーバ ファームでは、サーバ上の SSL 処理の負荷を軽減するために、前面に負荷分散装置やリバース SSL プロキシを配置しています。サーバの前面に位置して復号化を行っている負荷分散装置の場合、通常、装置には負荷分散装置の IP しかわかりません。負荷分散装置は、内容を復号化し、この接続の割り当て先となる特定のサーバを決定します。今回、DPI-SSL には IP ベースの除外キャッシュを無効にするためのグローバル ポリシー オプションが用意されました。IP ベースの除外キャッシュがオフの場合でも、除外の動作は継続します。SMA Connect Agent では、ユーザによるプロキシ設定が可能です。

次の 4 つのプロキシ設定オプションが用意されています。

- 「**プロキシなし**」- プロキシ サーバが設定されていない場合は、IPv6 属性は破棄されます。
- 「**システム プロキシ設定を使用**」
- 「**手動のプロキシ設定**」
- 「**自動プロキシ設定 URL**」

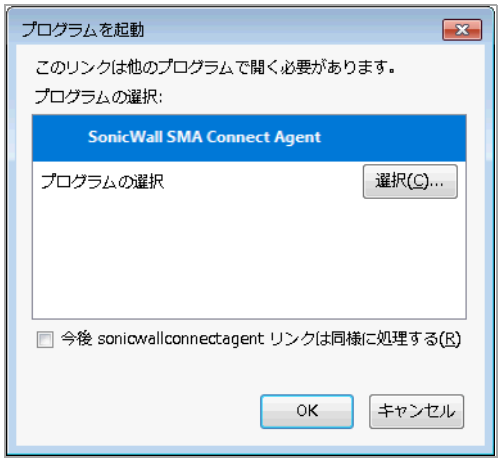


ログ

システム ツール バーにはログ トレイがあります。このトレイを右クリックし、該当するポップアップ メニューを選択すると、ログを表示できます。

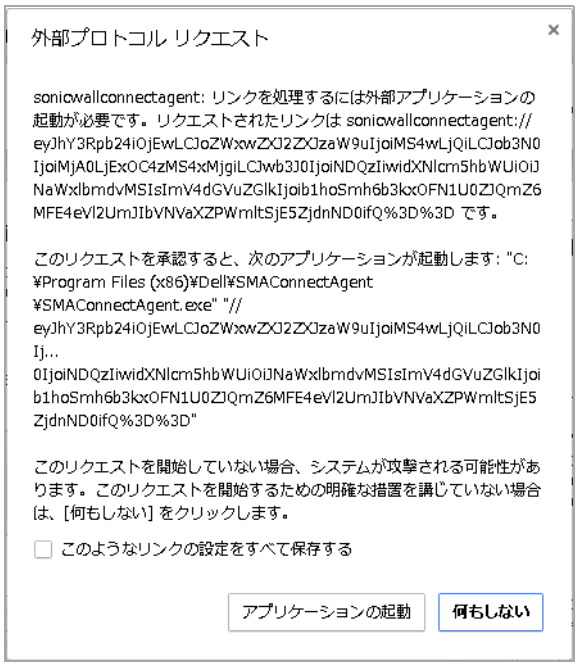
ブラウザによる警告

スキーム URL から SMA Connect Agent を起動しようとする場合、ブラウザから SMA Connect Agent を起動するかどうかを確認する警告メッセージがポップアップで表示される場合があります。

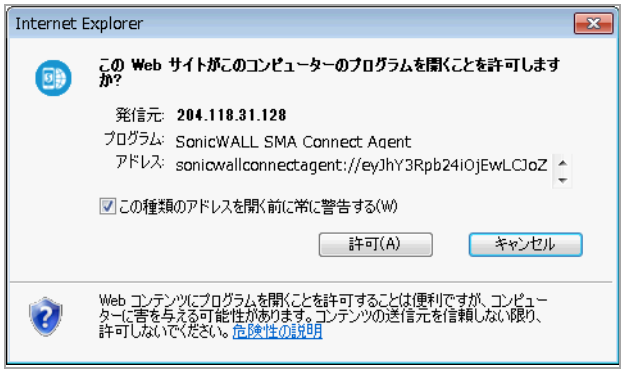


Firefox の警告ウィンドウでは、「**OK**」を押すと SMA Connect Agent が起動されます。

Citrix ネイティブ ブックマークを起動する場合は、StoreFront にログインした後で Citrix デスクトップまたはその他の Citrix ブックマークなどのアプリケーションを起動します。ブラウザの確認メッセージが表示される場合があります。



Chrome では、警告ウィンドウで「**アプリケーションの起動**」を押して Citrix または SMA Connect Agent を起動します。



Internet Explorer では、警告ウィンドウで「許可」を押して SMA Connect Agent を起動します。

エンド ポイント制御 (EPC)

SMA Connect Agent では、ブラウザからの EPC チェックがサポートされています。ログイン ページで EPC チェックを有効にすると、ブラウザは SMA Connect Agent に EPC チェックを行わせて特定のスキーマ URL を起動します。

SMA Connect Agent は、マシン上の EPC サービスをチェックします。EPC サービスがローカル マシン上にない場合や、装置に新しいバージョンがある場合、SMA Connect Agent は EPC サービスをダウンロードしてインストールするか、アップグレードします。インストールやアップグレードの完了後、SMA Connect Agent は EPC チェックを行います。

EPC 機能 (装置側) でクライアント側に EPC 失敗メッセージを詳細に表示する設定が有効な場合、SMA Connect Agent は詳細な失敗メッセージをログに記録します。その後、ログのトレイを表示することができます。

PDA (個人機器認証)

SMA Connect Agent は、PDA 機能によるローカル マシンの情報取得をサポートします。ログイン ページでユーザが PDA 機能を有効にしている場合、ブラウザは SMA Connect Agent を起動します。SMA Connect Agent はローカル マシンの情報を取得し、その情報を装置に送信します。

SonicWallアプリケーション

ポータル ページには、サポート対象の SonicWall アプリケーション (NetExtender、仮想アシスト、仮想ミーティングなど) を起動するためのボタンがあります。

ただし、Macintosh では NetExtender を実行できません。そのため、SMA Connect Agent は Macintosh 上で NetExtender 接続をサポートしていません。

第 4 部

付録

- オンライン ヘルプの使用
- SMA/SRA 装置をサードパーティ ゲートウェイ用に設定する
- プリンタのリダイレクト
- 使用事例
- NetExtender のトラブルシューティング
- よくある質問と回答
- コマンド ライン インターフェースの使用
- SMS 電子メール形式の使用
- サポート情報
- SonicWall サポート
- 用語集

A

オンライン ヘルプの使用

この付録では、ウェブベースの Secure Mobile Access 管理インターフェースの**オンライン ヘルプ**の使用方法について説明します。また、状況依存のヘルプについても解説します。

オンライン ヘルプ ボタン

「**オンライン ヘルプ**」は、Secure Mobile Access 管理インターフェースの右上隅にあります。

「**オンライン ヘルプ**」を選択すると、ウェブ ブラウザが起動し、オンライン ヘルプが表示されます。「**オンライン ヘルプ**」は、オンライン ヘルプ マニュアルのメイン ページにリンクされています。

状況依存のヘルプの使用

状況依存のヘルプは、ウェブベースの Secure Mobile Access 管理インターフェースの、ほとんどのページで利用できます。ページ右上隅にある状況依存のヘルプのボタン を選択すると、使用中の Secure Mobile Access 管理ページに対応したヘルプが表示されます。状況依存のヘルプのボタンを選択すると、ブラウザ ウィンドウが開き、対応するマニュアルが表示されます。

Secure Mobile Access 管理インターフェースの至る所で、特定のフィールドとチェックボックスの隣に同じヘルプ アイコンがあります。マウス カーソルをこのヘルプ アイコンに合わせると、関連するオプションの設定についての重要な情報を含んだツールチップが表示されます。

B

SMA/SRA 装置をサードパーティ ゲートウェイ用に設定する

この付録では、さまざまなサードパーティ ファイアウォールを Secure Mobile Access (SMA) または Secure Remote Access (SRA) 装置と共に配備するための設定方法について説明します。

トピック:

Cisco PIX を SMA/SRA 装置と共に配備するための設定

トピック:

準備

PIX のコンソール ポートへの管理接続、または PIX のいずれかのインターフェースに対する Telnet/SSH 接続が必要です。PIX にアクセスして設定の変更を発行するためには、PIX のグローバル パスワードと有効レベル パスワードを知っている必要があります。これらのパスワードを知らない場合は、ネットワーク管理者に確認してから次の作業に進んでください。

SonicWall Inc. では、PIX の OS を、使用する PIX がサポートしている最新バージョンへと更新することをお勧めしています。このマニュアルは PIX OS 6.3.5 を実行している Cisco PIX 515e を対象にしており、これが SMA/SRA 装置と相互運用するための推奨バージョンです。新しいバージョンの PIX OS を

入手するためには、お使いの Cisco PIX についての Cisco SmartNET サポート契約と CCO ログインが必要です。

メモ：以降の配備例で使用する WAN/DMZ/LAN の IP アドレスは、実際に有効なものではなく、お使いのネットワーク環境に合わせて変更する必要があります。

Cisco PIX に関する管理上の考慮事項

以降のセクションで説明する 2 つの配備方法では、PIX の WAN インターフェース IP アドレスを、内部の SMA/SRA 装置に対する外部接続の手段として使用しています。PIX は HTTP/S 経由での管理が可能ですが、推奨バージョンの PIX OS では、既定の管理ポート (80、443) の再割り当てができません。そのため、HTTP/S 管理インターフェースを無効にする必要があります。HTTP/S 管理インターフェースを無効にするには、“clear http”コマンドを発行します。

メモ：SMA/SRA 装置に独立した静的な WAN IP アドレスを割り当てている場合は、PIX 上の HTTP/S 管理インターフェースを無効にする必要はありません。

方法 1 - LAN インターフェース上に SMA/SRA 装置を配備する

1 管理システムから SMA/SRA 装置の Secure Mobile Access 管理インターフェースにログインします。既定の管理インターフェースは X0 で、既定の IP アドレスは 192.168.200.1 です。

2 「**ネットワーク > インターフェース**」ページに進み、X0 インターフェースの設定アイコンを選択します。表示されるポップアップで、X0 のアドレスを **192.168.100.2** に変更し、マスクを **255.255.255.0** にします。その後、「**OK**」を選択して変更を保存、適用します。

3 「**ネットワーク > ルート**」ページを開き、デフォルト ゲートウェイを **192.168.100.1** に変更します。その後、右上隅の「**適用**」を選択して変更を保存、適用します。

4 「**NetExtender > クライアント アドレス**」ページにナビゲートします。内部 LAN ネットワーク上で使用されていない 192.168.100.0/24 ネットワークの IP アドレスの範囲を入力する必要があります。既存の DHCP サーバがある場合、または PIX が内部インターフェース上で DHCP サーバを実行している場合は、これらのアドレスと競合しないように注意してください。例:「**クライアント アドレス範囲の開始**」の隣にあるフィールドに **192.168.100.201**と入力し、「**クライアント アドレス範囲の終了**」の隣にあるフィールドに **192.168.100.249** と入力します。その後、右上隅の「**適用**」を選択して変更を保存、適用します。

5 「**NetExtender > クライアント ルート**」ページにナビゲートします。**192.168.100.0**に関するクライアント ルートを追加します。**192.168.200.0**に関するエントリが既にある場合は、既存のものを削除します。

6 「**ネットワーク > DNS**」ページにナビゲートし、内部ネットワークの DNS アドレス、内部ドメイン名、WINS サーバ アドレスを入力します。これらは NetExtender を正しく機能させるために重要な情報なので正確に入力してください。その後、右上隅の「**適用**」を選択して変更を保存、適用します。

7 「**システム > 再起動**」ページを開き、「**再起動**」を選択します。

8 SMA/SRA 装置の X0 インターフェースを PIX の LAN ネットワークにインストールします。装置のその他のインターフェースにフックしないよう注意してください。

9 コンソール ポート、telnet、または SSH を使用して PIX の管理 CLI に接続し、設定モードに入ります。

10 **“clear http”**コマンドを発行して、PIX の HTTP/S 管理インターフェースを無効にします。

11 “**access-list sslvpn permit tcp any host x.x.x.x eq www**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

12 “**access-list sslvpn permit tcp any host x.x.x.x eq https**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

13 “**static (inside,outside) tcp x.x.x.x www 192.168.100.2 www netmask 255.255.255.255 0 0**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

14 “**static (inside,outside) tcp x.x.x.x https 192.168.100.2 https netmask 255.255.255.255 0 0**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

15 “**access-group sslvpn in interface outside**”コマンドを発行します。

16 設定モードを抜け、“**wr mem**”コマンドを発行して変更を保存、適用します。

17 外部システムから、HTTP と HTTPS の両方を使用して SMA/SRA 装置に接続してみます。SMA/SRA 装置にアクセスできない場合は、上記すべてのステップを確認して、もう一度テストしてください。

最終的な設定例 – 関連部分を太字で記載

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security4
enable password SqjOo0II7Q4T90ap encrypted
passwd SqjOo0II7Q4T90ap encrypted
hostname tenaya
domain-name vpntestlab.com
clock timezone PDT -8
clock summer-time PDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list sslvpn permit tcp any host 64.41.140.167 eq www
access-list sslvpn permit tcp any host 64.41.140.167 eq https
pager lines 24
logging on
logging timestamp
logging buffered warnings
logging history warnings
mtu outside 1500
mtu inside 1500
mtu dmz 1500
```

```
ip address outside 64.41.140.167 255.255.255.224
ip address inside 192.168.100.1 255.255.255.0
no ip address dmz
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
static (inside,outside) tcp 64.41.140.167 www 192.168.100.2 www netmask
255.255.255.255 0 0
static (inside,outside) tcp 64.41.140.167 https 192.168.100.2 https netmask
255.255.255.255 0 0
access-group sslvpn in interface outside
route outside 0.0.0.0 0.0.0.0 64.41.140.166 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
ntp server 192.43.244.18 source outside prefer
no snmp-server location
no snmp-server contact
snmp-server community SF*&^SDG
no snmp-server enable traps
floodguard enable
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 15
ssh 0.0.0.0 0.0.0.0 outside
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 15
console timeout 20
dhcpd address 192.168.100.101-192.168.100.199 inside
dhcpd dns 192.168.100.10
dhcpd lease 600
dhcpd ping_timeout 750
dhcpd domain vpntestlab.com
dhcpd enable inside
terminal width 80
banner motd Restricted Access.Please log in to continue.
Cryptochecksum:422aa5f321418858125b4896d1e51b89
: end
tenaya#
```

方法 2 - DMZ インターフェース上に SMA/SRA 装置を配備する

この方法はオプションであり、使用されていない第三のインターフェースを備えた PIX (PIX 515、PIX 525、PIX 535 など) が必要です。ここでは SMA/SRA 装置の既定のナンバリング スキーマを使用します。

1 管理システムから SMA/SRA 装置の Secure Mobile Access 管理インターフェースにログインします。既定の管理インターフェースは X0 で、既定の IP アドレスは 192.168.200.1 です。

2 「**ネットワーク > ルート**」ページを開き、デフォルト ゲートウェイが 192.168.200.2 に設定されていることを確認します。その後、右上隅の「**適用**」を選択して変更を保存、適用します。

3 「**NetExtender > クライアント アドレス**」ページにナビゲートします。「**クライアント アドレス範囲の開始**」の隣にあるフィールドに **192.168.200.201** と入力し、「**クライアント アドレス範囲の終了**」の隣にあるフィールドに **192.168.200.249** と入力します。その後、右上隅の「**適用**」を選択して変更を保存、適用します。

4 「**NetExtender > クライアント ルート**」ページにナビゲートします。**192.168.100.0** と **192.168.200.0** に関するクライアント ルートを追加します。

5 「**ネットワーク > DNS**」ページにナビゲートし、内部ネットワークの DNS アドレス、内部ドメイン名、WINS サーバ アドレスを入力します。これらは NetExtender を正しく機能させるために重要な情報なので正確に入力してください。その後、右上隅の「**適用**」を選択して変更を保存、適用します。

6 「**システム > 再起動**」ページを開き、「**再起動**」を選択します。

7 SMA/SRA 装置の X0 インターフェースを PIX の使用されていない DMZ ネットワークにインストールします。装置のその他のインターフェースにフックしないよう注意してください。

8 コンソール ポート、telnet、または SSH を使用して PIX の管理 CLI に接続し、設定モードに入ります。

9 **“clear http”**コマンドを発行して、PIX の HTTP/S 管理インターフェースを無効にします。

10 “**interface ethernet2 auto**”コマンドを発行します (インターフェース名は、実際に使用しているインターフェースに置き換えます)。

11 “**nameif ethernet2 dmz security4**”コマンドを発行します (インターフェース名は、実際に使用しているインターフェースに置き換えます)。

12 “**ip address dmz 192.168.200.2 255.255.255.0**”コマンドを発行します。

13 “**nat (dmz) 1 192.168.200.0 255.255.255.0 0 0**”コマンドを発行します。

14 “**access-list sslvpn permit tcp any host x.x.x.x eq www**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

15 “**access-list sslvpn permit tcp any host x.x.x.x eq https**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

16 “**access-list dmz-to-inside permit ip 192.168.200.0 255.255.255.0 192.168.100.0 255.255.255.0**”コマンドを発行します。

17 “**access-list dmz-to-inside permit ip host 192.168.200.1 any**”コマンドを発行します。

18 “**static (dmz,outside) tcp x.x.x.x www 192.168.200.1 www netmask 255.255.255.255 0 0**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

19 “**static (dmz,outside) tcp x.x.x.x https 192.168.200.1 https netmask 255.255.255.255 0 0**”コマンドを発行します (x.x.x.x の部分はお使いの PIX の WAN IP アドレスで置き換えます)。

20 “**static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0**”コマンドを発行します。

21 “**access-group sslvpn in interface outside**”コマンドを発行します。

22 “**access-group dmz-to-inside in interface dmz**”コマンドを発行します。

23 設定モードを抜け、“**wr mem**”コマンドを発行して変更を保存、適用します。

24 外部システムから、HTTP と HTTPS の両方を使用して SMA/SRA 装置に接続してみます。SMA/SRA 装置にアクセスできない場合は、上記すべてのステップを確認して、もう一度テストしてください。

最終的な設定例 – 関連部分を太字で記載

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security4
enable password SqjOo0II7Q4T90ap encrypted
passwd SqjOo0II7Q4T90ap encrypted
hostname tenaya
domain-name vpntestlab.com
clock timezone PDT -8
clock summer-time PDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list sslvpn permit tcp any host 64.41.140.167 eq www
access-list sslvpn permit tcp any host 64.41.140.167 eq https
access-list dmz-to-inside permit ip 192.168.200.0 255.255.255.0 192.168.100.0
255.255.255.0
access-list dmz-to-inside permit ip host 192.168.200.1 any
pager lines 24
logging on
logging timestamp
logging buffered warnings
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 64.41.140.167 255.255.255.224
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.200.2 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
nat (dmz) 1 192.168.200.0 255.255.255.0 0 0
static (dmz,outside) tcp 64.41.140.167 www 192.168.200.1 www netmask 255.255.255.255
0 0
static (dmz,outside) tcp 64.41.140.167 https 192.168.200.1 https netmask
255.255.255.255 0 0
static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0
```

```
access-group sslvpn in interface outside
access-group dmz-to-inside in interface dmz
route outside 0.0.0.0 0.0.0.0 64.41.140.166 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
ntp server 192.43.244.18 source outside prefer
floodguard enable
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 15
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 15
console timeout 20
dhcpd address 192.168.100.101-192.168.100.199 inside
dhcpd dns 192.168.100.10
dhcpd lease 600
dhcpd ping_timeout 750
dhcpd domain vpntestlab.com
dhcpd enable inside
terminal width 80
banner motd Restricted Access.Please log in to continue.
Cryptochecksum:81330e717bdbfdc16a140402cb503a77
: end
```

Linksys WRT 54 GS

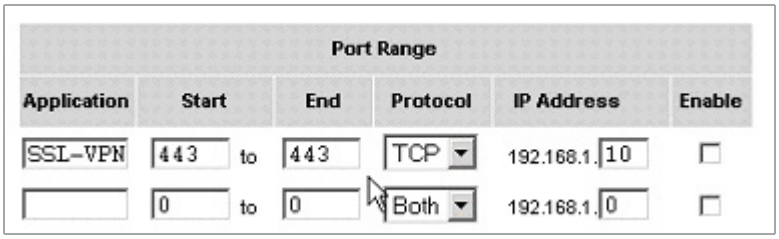
SMA/SRA 装置は Linksys ワイヤレス ルータの LAN スイッチ上で設定する必要があります。ここでは、お使いの Linksys にケーブル ISP が DHCP 経由で単一の WAN IP を割り当てており、この Linksys が 192.168.1.0/24 という既定の LAN IP アドレス スキーマを使用していることを前提にしています。

メモ：このセットアップでは、バージョン 2.07.1 以上のファームウェアを推奨します。

Linksys を SMA/SRA 装置と相互運用できるように設定するには、SSL (443) ポートを SMA/SRA 装置の IP アドレスに転送する必要があります。

1 Linksys デバイスにログインします。

2 「**Applications & Gaming**」タブにナビゲートします。



3 次の情報を入力します。

「Applications & Gaming」タブに追加する情報

アプリケーション	SMA/SRA	ポート転送先アプリケーションの名前
Port Range Start	443	アプリケーションで使用される開始ポート番号
Port Range End	443	アプリケーションで使用される終了ポート番号
プロトコル	TCP	SMA/SRA アプリケーションは TCP を使用
IP アドレス	192.168.1.10	SMA/SRA 装置に割り当てられる IP アドレス
有効	オン	SSL ポート転送を有効にするにはチェックボックスをオン

4 設定が完了したら、ページの下部にある「**Save Settings**」を選択します。

これで、Linksys が SMA/SRA 装置と相互運用できるようになります。

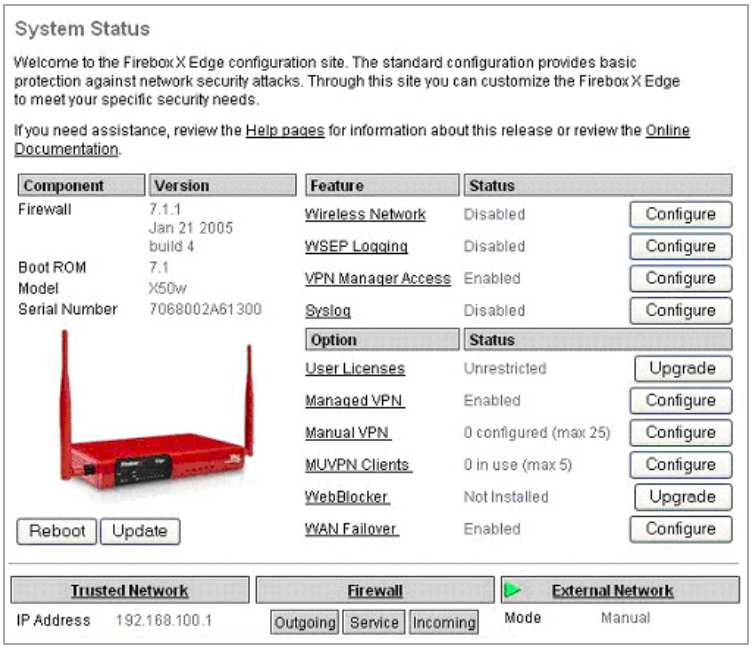
Watchguard Firebox X Edge

ここでは、WatchGuard Firebox X Gateway の IP アドレスが 192.168.100.1 に設定され、SMA/SRA 装置の IP アドレスが 192.168.100.2 に設定されているものと想定します。

メモ：以降のステップは、WatchGuard SOHO6 シリーズのファイアウォールでも同様です。

作業を始める前に、WatchGuard のどのポートを管理に使用しているかを確認します。WatchGuard を HTTPS (443) ポートで管理していない場合は、次の手順に従います。WatchGuard を HTTPS (443) ポートで管理している場合は、最初にこの設定方法の注意事項を参照してください。

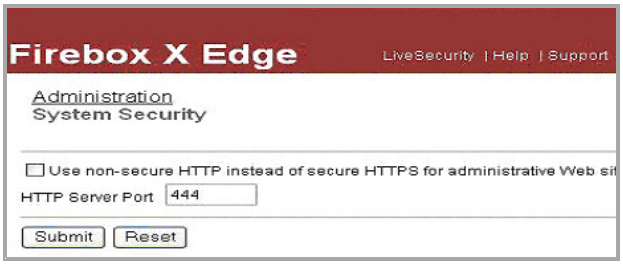
1 ブラウザを開き、WatchGuard Firebox X Edge 装置の IP アドレスを入力します (例: 192.168.100.1)。アクセスに成功すると、次のような「System Status」ページが表示されます。



2 WatchGuard の管理インターフェースが既に HTTPS をポート 443 で受け付けるように設定されている場合は、SMA/SRA と WatchGuard 装置の両方を管理できるようにポートを変更する必要があります。

3 「**Administration > System Security**」にナビゲートします。

WatchGuard の Administration > System Security ダイアログ ボックス

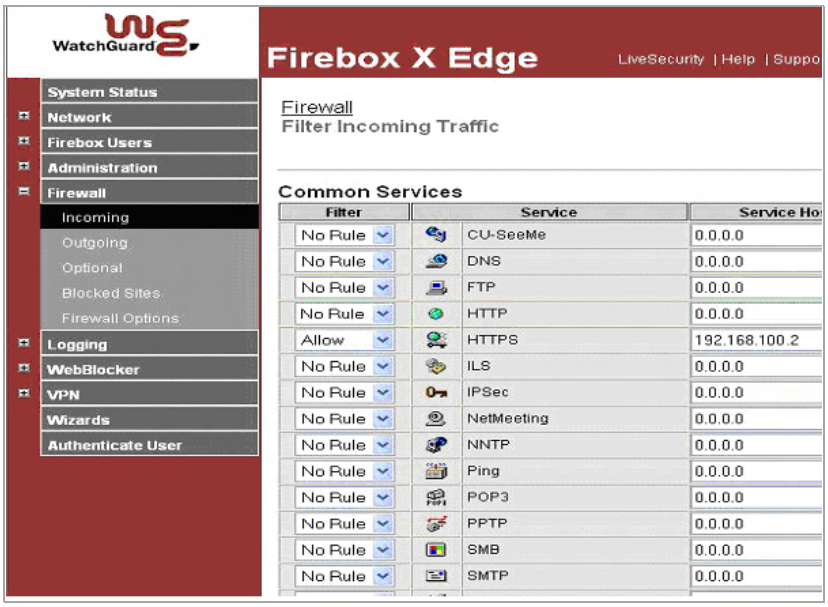


4 「**Use non-secure HTTP instead of secure HTTPS for administrative Web site**」をオフにします。

5 「**HTTP Server Port**」を 444 に変更し、「**Submit**」を選択します。

これで、WatchGuard を WAN からポート 444 で管理できるようになります。WatchGuard にアクセスするには次のようにします。〈https://<watchguard wan ip>:444〉

6 左側のナビゲーション メニューで「**Firewall > Incoming**」を開きます。



7 「**HTTPS Service**」の「**Filter**」を「Allow」に設定し、「**Service Host**」フィールドに SMA/SRA 装置の WAN IP アドレス (192.168.100.2) を入力します。

8 ページの下部にある「**Submit**」を選択します。

これで、Watchguard Firebox X Edge が SMA/SRA 装置と相互運用できるようになります。

Netgear FVS318

ここでは、NetGear FVS318 Gateway の IP アドレスが 192.168.100.1 に設定され、SMA/SRA 装置の IP アドレスが 192.168.100.2 に設定されているものと想定します。

1 Netgear 管理インターフェースの左側のインデックスから「**Remote Management**」を選択します。

SMA/SRA 装置を Netgear ゲートウェイ デバイスと連携させるためには、NetGear の管理ポートが SMA/SRA 装置で使用する管理ポートと競合しないようにする必要があります。

2 「**Allow Remote Management**」ボックスをオフにします。

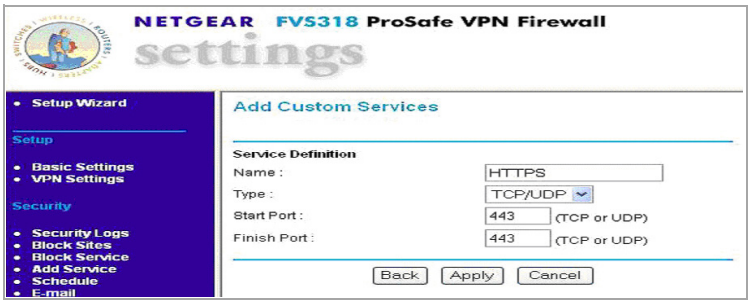
3 「**適用**」ボタンを選択して、変更内容を保存します。

ⓘ **メモ**：NetGear の Remote Management が必要な場合は、このチェックボックスをオンのままにして、既定のポートを変更します (8080 を推奨)。

4 左側のナビゲーションで「**Add Service**」を開きます。

5 「**Add Custom Service**」を選択します。

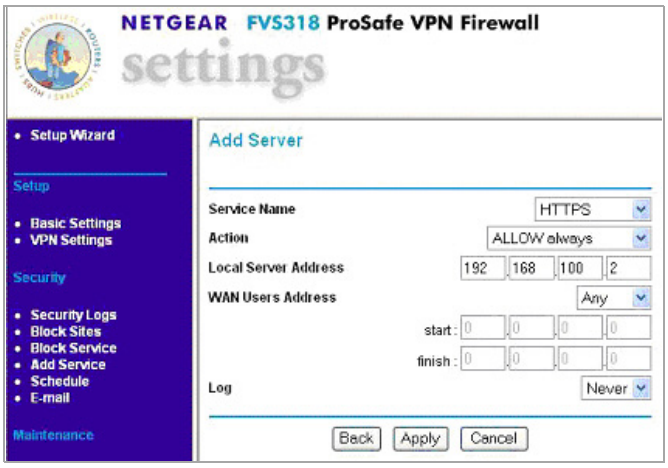
6 サービス定義を作成するために、次の情報を入力します。



名前	HTTPS
種別	TCP/UDP
Start Port	443
Finish Port	443

7 左側のナビゲーションで「**Ports**」を開きます。

「**追加**」を選択します。



8 「**Service Name**」プルダウン メニューから HTTPS を選択します。

9 「**Action**」プルダウン メニューでは ALLOW always を選択します。

10 「**Local Server Address**」フィールドに SMA/SRA 装置の WAN IP アドレス (192.168.100.2 など) を入力します。

11 「適用」ボタンを選択して、変更内容を保存します。

これで、Netgear ゲートウェイ デバイスが SMA/SRA 装置と相互運用できるようになります。

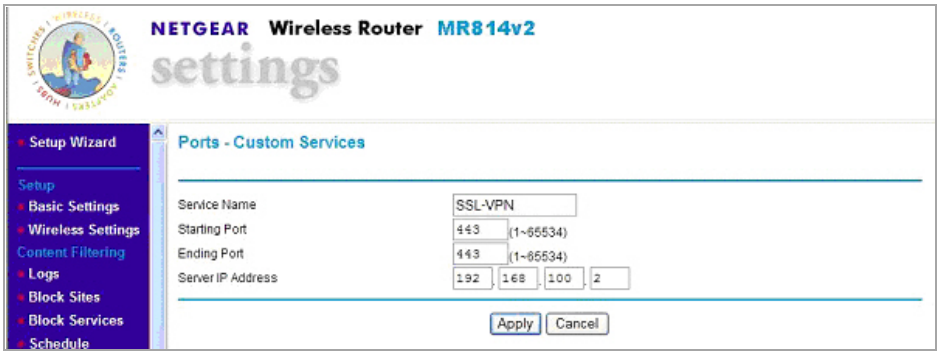
Netgear Wireless Router MR 814 SSL の設定

ここでは、NetGear Wireless Router の IP アドレスが 192.168.100.1 に設定され、SMA/SRA 装置の IP アドレスが 192.168.100.2 に設定されているものと想定します。

1 Netgear の管理インターフェースの左側のインデックスから「**Advanced > Port Management**」を開きます。

2 ページ中央の「**Add Custom Service**」を選択します。

3 「**Service Name**」フィールドにサービス名を入力します (例: SMA)



4 「**Starting Port**」フィールドに **443** と入力します。

5 「**Ending Port**」フィールドに **443** と入力します。

6 「**Local Server Address**」フィールドに SMA/SRA 装置の WAN IP アドレス (192.168.100.2 など) を入力します。

7 「**適用**」を選択します。

これで、Netgear ワイヤレス ルータが SMA/SRA 装置と相互運用できるようになります。

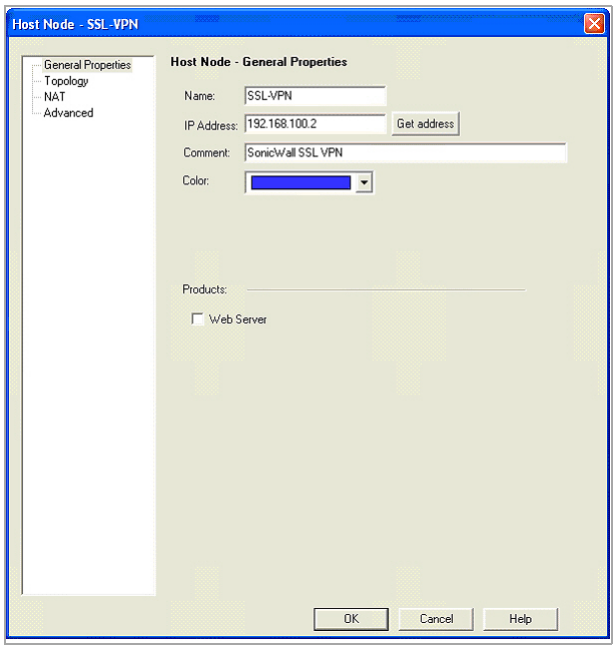
Check Point AIR 55

トピック:

SMA/SRA 装置と Check Point AIR 55 を連携させるための設定

まず必要なのは、ホストベースのネットワーク オブジェクトを定義することです。そのためには、File メニューの“Manage”と“Network Objects”を使用します。

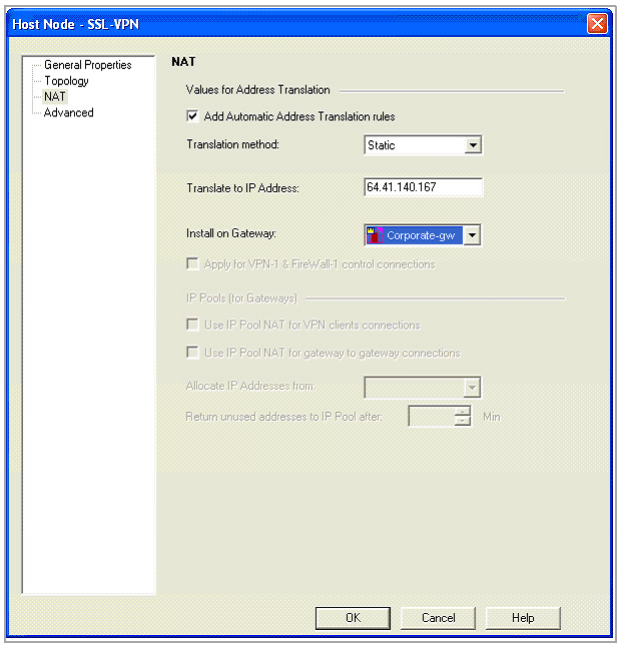
Check Point の Host Node Object ダイアログ ボックス



メモ：このオブジェクトは、内部ネットワークに存在するものとして定義されます。SMA/SRA 装置をセキュア セグメント (非武装地帯とも呼ばれます) に配置する場合は、後述のファイアウォール規則でセキュア セグメントから内部ネットワークへの必要なトラフィックを通過させる必要があります。

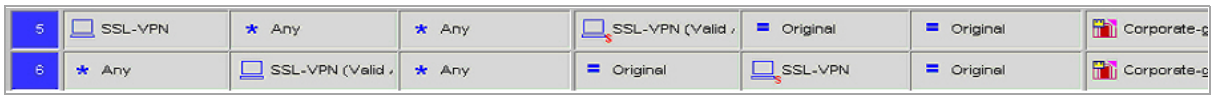
次に、作成したオブジェクトの **NAT** タブを選択します。

Check Point の NAT Properties ダイアログ ボックス



ここで外部 IP アドレスを入力します (ファイアウォールの既存の外部 IP アドレスでない場合)。変換方法として「**Static**」を選択します。「**OK**」を選択すると、次のセクションに示すように、必要な NAT ルールが自動的に作成されます。

Check Point の NAT Rule ウィンドウ



静的ルート

Check Point AIR55 の大部分のインストール環境では、静的ルートが必要です。このルートは、SMA/SRA 装置のパブリック IP アドレスからの全トラフィックを内部 IP アドレスに送信します。

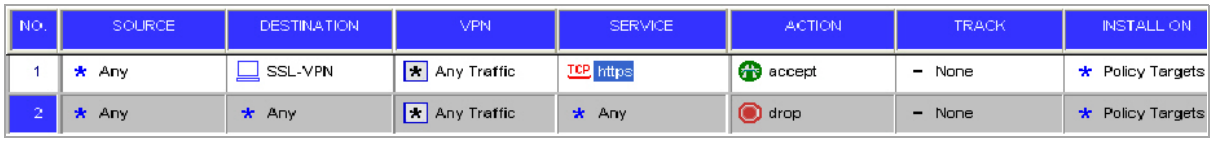
#route add 64.41.140.167 netmask 255.255.255.255 192.168.100.2

ARP

Check Point AIR55 には、自動 ARP 作成と呼ばれる機能があります。この機能により、セカンダリ外部 IP アドレス (SMA/SRA 装置のパブリック IP アドレス) に関する ARP エントリが自動的に追加されます。Nokia のセキュリティ プラットフォーム上で Check Point を実行する場合は、この機能を無効にするよう推奨されています。そのため、外部 IP アドレスに関する ARP エントリを Nokia Voyager インターフェースの中で手動で追加する必要があります。

さらに、すべてのトラフィックをインターネットから SMA/SRA 装置に流すためのトラフィック規則またはポリシー規則が必要になります。

Check Point の Policy Rule ウィンドウ



ここでも、SMA/SRA 装置を Check Point ファイアウォールのセキュア セグメントに配置する場合は、関連トラフィックを SMA/SRA 装置から内部ネットワークに流すための第二の規則が必要になります。

C

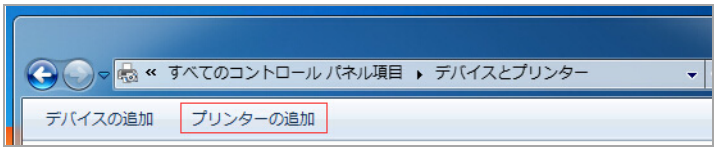
プリンタのリダイレクト

この付録では、特定のプリンタ ドライバ リダイレクト (MS Publisher Imagesetter) をインストールする方法を説明します。リモート デスクトップ セッション ホスト サーバにドライバがインストールされている場合、HTML5 RDP は特定のプリンタのリダイレクトをサポートします。HTML5 RDP はプリンタをクライアント側にリダイレクトできます。ユーザは「プリンタをリダイレクトする」をオンにしてファイルを PDF に出力できます。PDF が作成されると、ファイル ポップアップ ビューアが表示されます。PDF ファイルの「印刷プレビュー」を表示することも、ファイルを直接印刷することもできます。

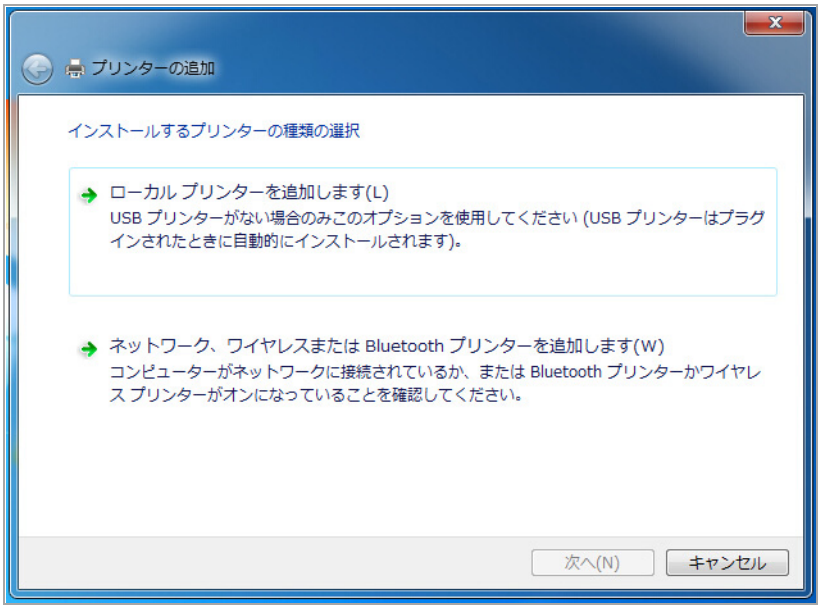
Windows 7 で MS Publisher Imagesetter をインストールするには、以下の手順に従います。

1 **Windows コントロール パネル**を開いて、「**デバイスとプリンター**」をクリックします。

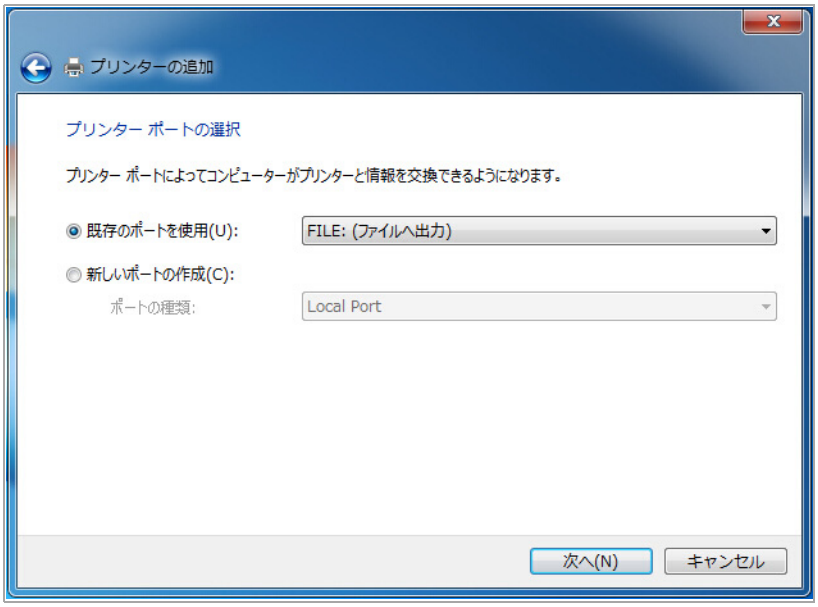
2 「**プリンターの追加**」をクリックします。



3 「**ローカル プリンターを追加します**」を選択します。

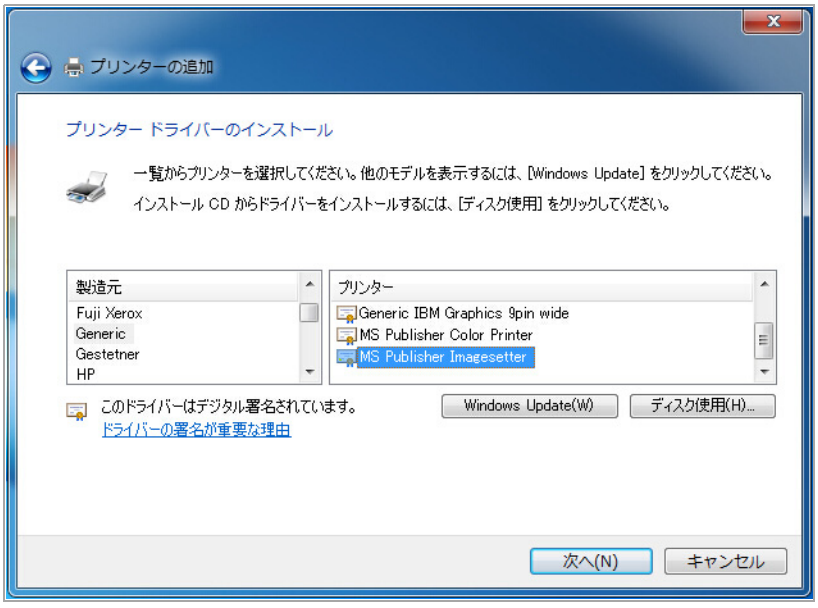


4 「**既存のポートを使用**」を選択し、ドロップダウン ボックスで「**FILE: (ファイルへ出力)**」を選択します。



5 「**次へ**」ボタンを選択します。

6 「**製造元**」の一覧で「**Generic**」を選択します。次に、「**プリンター**」の一覧で「**MS Publisher Imagesetter**」を選択します。



7 「**次へ**」ボタンを選択します。

8 「**現在インストールされているドライバーを使う**」を選択します。

9 「**次へ**」ボタンを選択します。

10 プリンタ名には既定の設定である「**MS Publisher Imagesetter**」を使用します。

11 「**次へ**」ボタンを選択します。

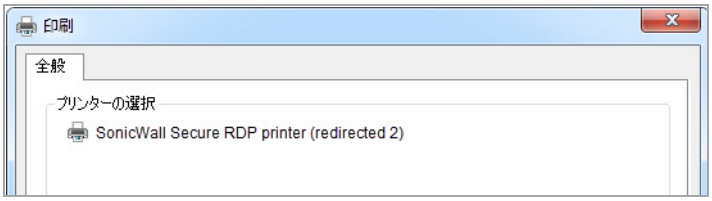
12 使用する共有条件に最も適したオプションを選択します。

13 「**次へ**」ボタンを選択します。

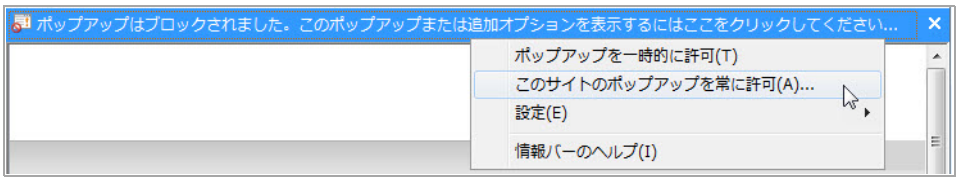
14 「**完了**」をクリックします。新しいプリンタが「プリンターと FAX」領域に表示されます。

「プリンタをリダイレクトする」の有効化

1 ブックマークの「詳細な Windows オプションを表示」で「プリンタをリダイレクトする」を有効にします。「プリンタをリダイレクトする」を有効にすると、リモート サーバのプリンタ リストに「SonicWall Secure RDP Printer」が表示されます。



2 このプリンタを選択してファイルを印刷します。ポップアップ ウィンドウがブラウザによってブロックされる場合があります。「このサイトのポップアップを常に許可」を選択します。



3 これでファイルをプレビューし、ローカル プリンタで印刷できるようになります。

タイム ゾーンのリダイレクト

HTML5 RDP では、ローカル タイム ゾーンをリモート サーバにリダイレクトすることもできます。リモート サーバでこの機能を有効にする必要があります。

Windows 2008 R2 でタイム ゾーンのリダイレクトを有効にするには、以下の手順に従います。

1 「**ローカル グループ ポリシー エディタ**」または「**グループ ポリシーの管理**」を開きます。

2 次のパスを使用します。

「コンピュータの構成 > (ポリシー) > 管理用テンプレート > Windows コンポーネント > リモート デスクトップ サービス > リモート デスクトップ セッション ホスト > デバイスとリソースのリダイレクト > タイム ゾーン リダイレクトを許可する」

3 プリンタ名をダブルクリックし、「**有効**」を選択します。

4 「**OK**」を選択します。

リモート サーバで設定を有効にすると、ローカル タイム ゾーンがリモート サーバにリダイレクトされます。

5 タイム ゾーンのリダイレクトは、RDP 5.1 以降を使用するクライアントで、Windows Server 2003 以降のターミナル サーバに接続している場合にのみ可能です。

D

使用事例

この付録では、次の使用事例を紹介します。

ウィンドウズでの CA 証明書のインポート

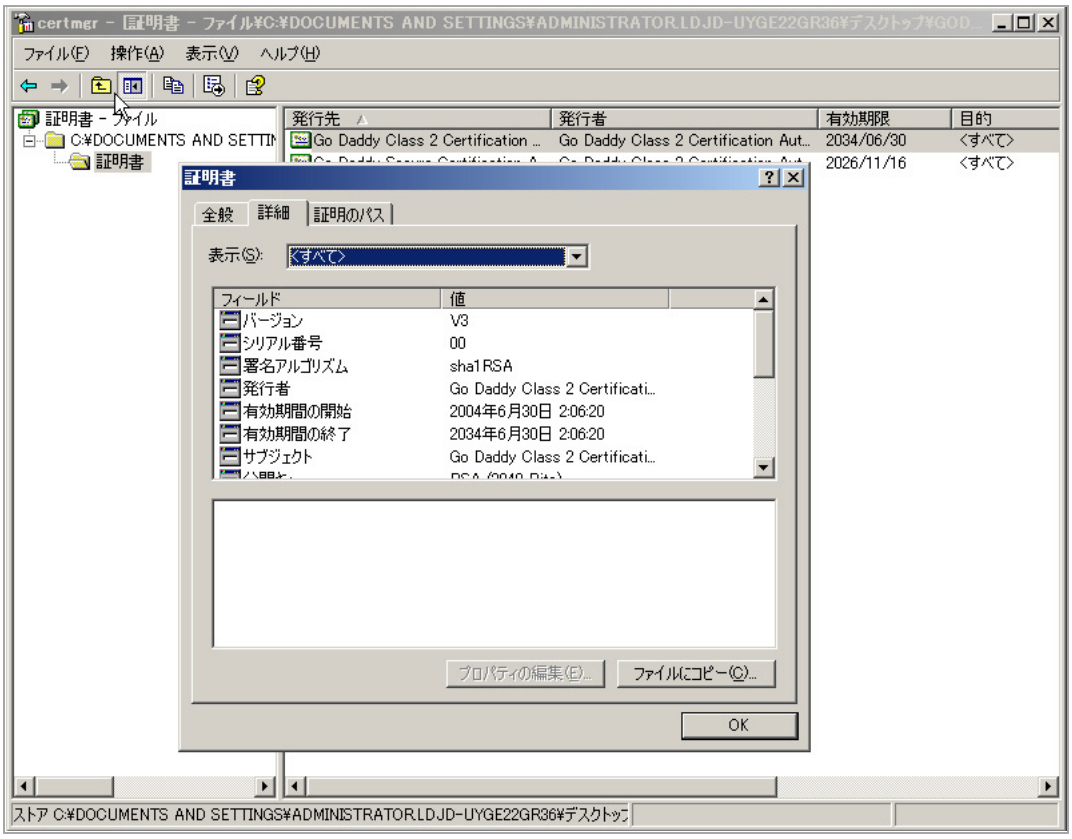
この使用事例では、goDaddy 証明書とサーバ証明書という 2 つの証明書をインポートします。以下のセクションを参照してください。

ウィンドウズでの goDaddy 証明書のインポート

この使用事例では、Windows システム上で goDaddy ルート CA 証明書をフォーマットし、それを Secure Mobile Access (SMA) および Secure Remote Access (SRA) 装置にインポートします。

1 **goDaddy.p7b** ファイルをダブルクリックして「証明書」ウィンドウを開き、goDaddy 証明書にナビゲートします。
.p7b 形式は PKCS#7 形式の証明書ファイルであり、ごく一般的な証明書形式です。

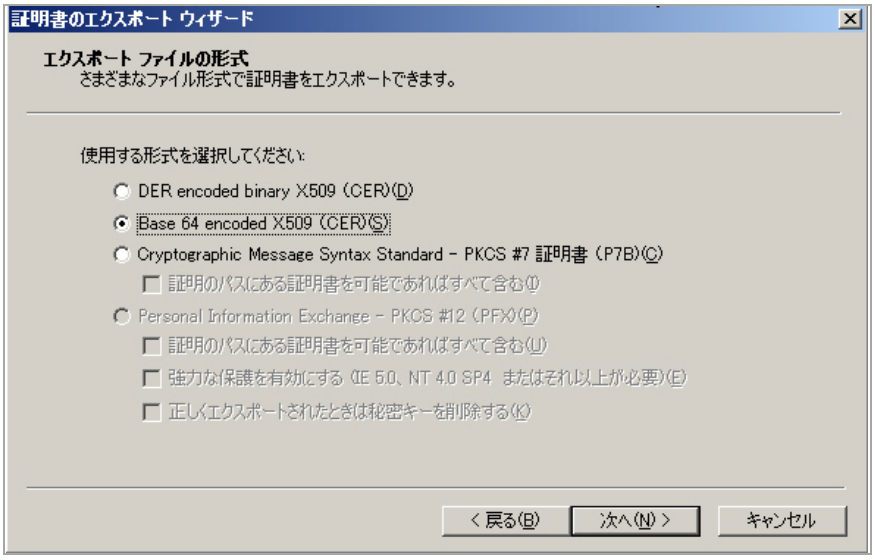
2 証明書ファイルをダブルクリックし、「**詳細**」タブを選択します。



3 「**ファイルにコピー**」を選択します。証明書のエクスポート ウィザードが起動します。

4 証明書のエクスポート ウィザードで、「**次へ**」を選択します。

5 「**Base-64 encoded X 509 (CER)**」を選択し、「**次へ**」を選択します。



6 「エクスポートするファイル」画面で、ファイル名として **goDaddy.cer** を入力し、「**次へ**」を選択します。

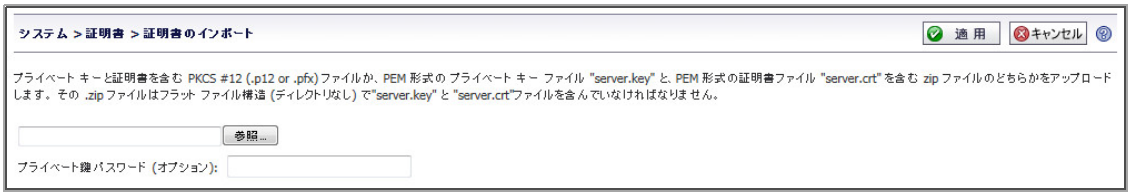
7 証明書のエクスポートの完了ウィザードの画面で、パスと形式を確認し、「**終了**」を選択します。

8 確認のダイアログ ボックスで、「**OK**」を選択します。

証明書が base-64 encoded 形式でエクスポートされます。これはテキスト エディタで表示することができます。

9 Secure Mobile Access 管理インターフェースで、「**システム > 証明書**」を開きます。

10 「**追加の CA 証明書**」セクションで、「**CA 証明書のインポート**」を選択します。「証明書のインポート」ウィンドウが表示されます。



11 「証明書のインポート」ウィンドウで「**参照**」を選択し、ウィンドウズ システム上の **goDaddy.cer** ファイルにナビゲートし、それをダブルクリックします。

12 「**アップロード**」をクリックします。証明書が「**追加の CA 証明書**」テーブル内に表示されます。

13 「**システム > 再起動**」に移動し、SMA/SRA 装置を再起動して、CA 証明書を有効にします。

ウィンドウズでのサーバ証明書のインポート

この使用事例では、マイクロソフト CA サーバ証明書をウィンドウズ システムにインポートします。ここでの目的は、メール サーバへのアプリケーション オフロードに SSL 証明書を使用することにあります。

サーバ証明書は **mail.chaoslabs.nl** です。この証明書を **server.crt** ファイルとして base-64 形式にエクスポートする必要があります。このファイルを .zip ファイルに入れ、サーバ証明書としてアップロードします。

.p7b ファイルには秘密鍵は含まれていません。秘密鍵を所定の場所からエクスポートし、base-64 形式で保存し、.zip ファイル内の **server.key** ファイルに含める必要があります。

1 **mail.chaoslabs.nl.pb7** ファイルをダブルクリックし、証明書にナビゲートします。

2 証明書ファイルをダブルクリックし、「**詳細**」タブを選択します。

3 「**ファイルにコピー**」を選択します。

4 証明書のエクスポート ウィザードで、「**Base-64 encoded X.509 (.CER)**」を選択します。

5 「**次へ**」を選択し、ファイルを **server.crt** としてウィンドウズ システム上に保存します。

証明書が base-64 encoded 形式でエクスポートされます。

6 server.crt ファイルを .zip ファイルに追加します。

7 秘密鍵は別に **server.key** として base-64 形式で保存します。

8 **server.crt** を入れた .zip ファイルに **server.key** ファイルを 追加します。

9 .zip ファイルをサーバ証明書としてサーバにアップロードします。

AD グループの一意アクセス ポリシーの作成

この使用事例では、Outlook Web Access (OWA) リソースを SMA/SRA 装置に追加します。また、複数のアクティブ ディレクトリ (AD) グループのユーザに対するアクセス ポリシーを設定する必要があります。AD グループごとにローカル グループを作成し、それぞれのローカル グループに別々のアクセス ポリシーを適用します。

アクティブ ディレクトリではユーザは複数のグループのメンバーになれますが、SMA/SRA 装置では各ユーザが 1 つのグループにしか属せません。ユーザに割り当てられるアクセス ポリシーはこのグループによって決まります。

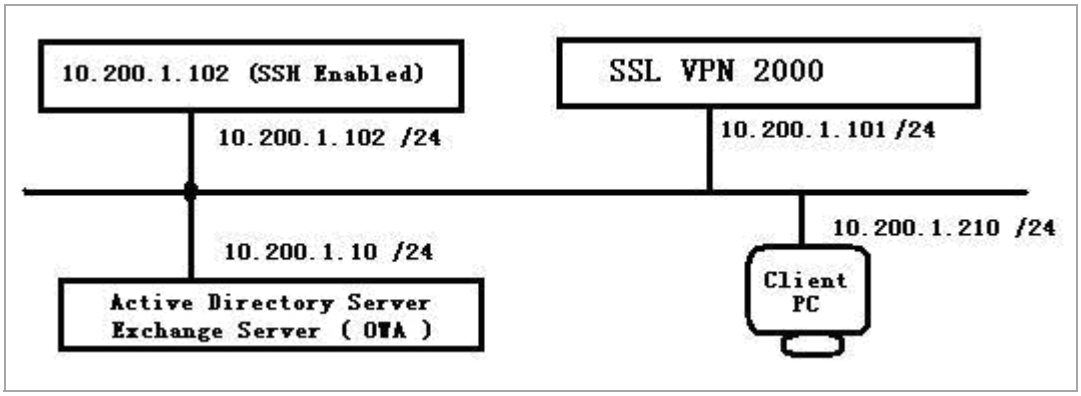
AD からユーザをインポートすると、そのユーザは最も多くの AD グループを共通に持つローカルの Secure Mobile Access グループに入れられます。以下に例を示します。Bob は Users、Administrators、Engineering の各 AD グループに属しています。Secure Mobile Access グループのうち、あるグループが Users に関連付けられていて、別のグループが Administrators と Engineering の両方に関連付けられている場合、Bob は Administrators と Engineering の両方に関連付けられている Secure Mobile Access グループに割り当てられます。なぜなら、そのグループのほうが、Bob の属している AD グループが多いからです。

この使用事例の目的は、次の設定を行うことにより、Secure Mobile Access ファームウェアがグループベースのアクセス ポリシーをサポートしていることを示すことにあります。

- アクティブ ディレクトリの Acme Group に対して、10.200.1.102 のサーバへの SSH によるアクセスを許可する。
- アクティブ ディレクトリの Mega Group に対して、10.200.1.10 のアウトルック ウェブ アクセス (OWA) へのアクセスを許可する。
- アクティブ ディレクトリの IT Group に対して、上記で定義した SSH と OWA の両方のリソースへのアクセスを許可する。
- 他のすべてのグループに対して、これらのリソースへのアクセスを拒否する。

この設定例は、Vincent Cai の好意によって 2008 年 6 月に提供されたものです。

ネットワーク トポロジ



以下のセクションの順番に従ってタスクを実行します。

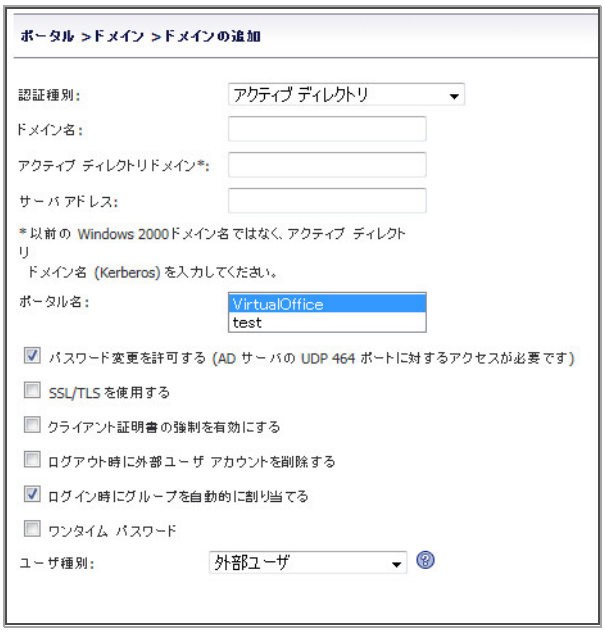
- アクティブ ディレクトリ ドメインの作成 (522 ページ)
- グローバルな「すべて拒否」ポリシーの追加 (523 ページ)
- ローカル グループの作成 (524 ページ)
- SSHv2 許可ポリシーの追加 (527 ページ)
- OWA 許可ポリシーの追加 (528 ページ)
- アクセス ポリシー設定の確認 (529 ページ)

アクティブ ディレクトリ ドメインの作成

このセクションでは、Secure Mobile Access のローカル ドメインである SNWL_AD の作成方法を説明します。SNWL_AD は OWA サーバのアクティブ ディレクトリ ドメインと関連付けられています。

1 Secure Mobile Access 管理インターフェースにログインし、「**ポータル > ドメイン**」ページを開きます。

2 「**ドメインの追加**」を選択します。「ドメインの追加」ウィンドウが表示されます。



3 「**認証種別**」ドロップダウン リストから「**アクティブ ディレクトリ**」を選択します。

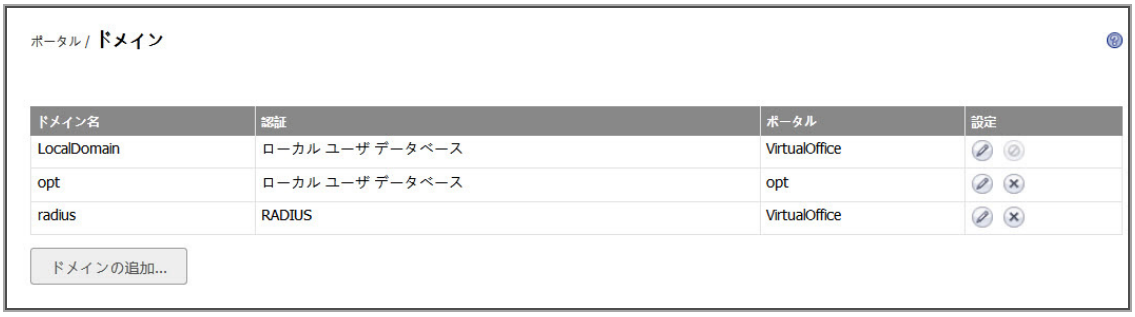
4 「**ドメイン名**」フィールドに **SNWL_AD** と入力します。

5 「**アクティブ ディレクトリ ドメイン**」フィールドに、AD ドメイン名として **in.loraxmfg.com** と入力します。

6 「**サーバ アドレス**」フィールドに、OWA サーバの IP アドレスとして **10.200.1.10** と入力します。

7 「**追加**」を選択します。

8 「**ポータル > ドメイン**」ページで新しいドメインを確認します。



グローバルな「すべて拒否」ポリシーの追加

この手順では、明示的な許可ポリシーが設定されたグループを除く全グループに対して OWA リソースへのアクセスを拒否するポリシーを作成します。

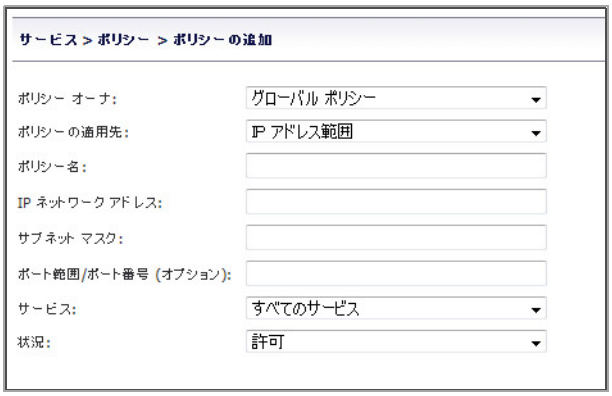
Secure Mobile Access の既定のポリシーは**すべて許可**です。よりきめ細かな制御を行うため、ここで**すべて拒否**ポリシーを追加します。後でグループごとに一度に 1 つずつ**許可**ポリシーを追加することができます。

1 「**ユーザ > ローカル ユーザ**」ページに移動します。

2 「**グローバル ポリシー**」行の「**設定**」 を選択します。「**グローバル ポリシーの編集**」ウィンドウが表示されます。

3 「**グローバル ポリシーの編集**」ウィンドウで「**ポリシー**」タブを選択します。

4 「**ポリシーの追加**」を選択します。「ポリシーの追加」ウィンドウが表示されます。



5 「**ポリシーの適用先**」ドロップダウン リストから「**IP ネットワーク**」を選択します。

6 「**ポリシー名**」フィールドに、「**IP ネットワーク すべて拒否**」のようなわかりやすい名前を入力します。

7 「IP**ネットワーク アドレス**」フィールドに、ネットワーク アドレスとして **10.200.1.0** と入力します。

8 「**サブネット マスク**」フィールドに、10 進形式のサブネット マスクとして **255.255.255.0**と入力します。

9 「**サービス**」ドロップダウン リストから「**すべてのサービス**」を選択します。

10 「**状況**」ドロップダウン リストで「**許可**」を選択します。

11 「**追加**」を選択します。

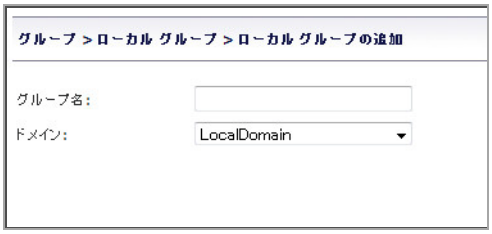
12 「**グローバル ポリシーの編集**」ウィンドウで、**すべて拒否**ポリシー設定を確認し、「**OK**」を選択します。

ローカル グループの作成

この手順では、SMA/SRA 装置上の SNWL_AD ドメインに属するローカル グループを作成します。アクティブ ディレクトリ グループごとにローカル グループを 1 つずつ作成します。

ローカル グループの追加

1 「**ユーザ > ローカル グループ**」ページにナビゲートし、「グループの追加」を選択します。「**ローカル グループの追加**」ウィンドウが表示されます。3 つのアクティブ ディレクトリ グループに対応して、3 つのローカル グループを追加することにします。



2 「**ローカル グループの追加**」ウィンドウの「**グループ名**」フィールドに **Acme_Group** と入力します。

3 「**ドメイン**」ドロップダウン リストから「**SNWL_AD**」を選択します。

4 「**追加**」を選択します。

5 「**ユーザ > ローカル グループ**」ページで「**グループの追加**」を選択して、2 番目のローカル グループを追加します。

6 「ローカル グループの追加」ウィンドウの「**グループ名**」フィールドに **Mega_Group** と入力します。

7 「**ドメイン**」ドロップダウン リストから「**SNWL_AD**」を選択します。

8 「**追加**」を選択します。

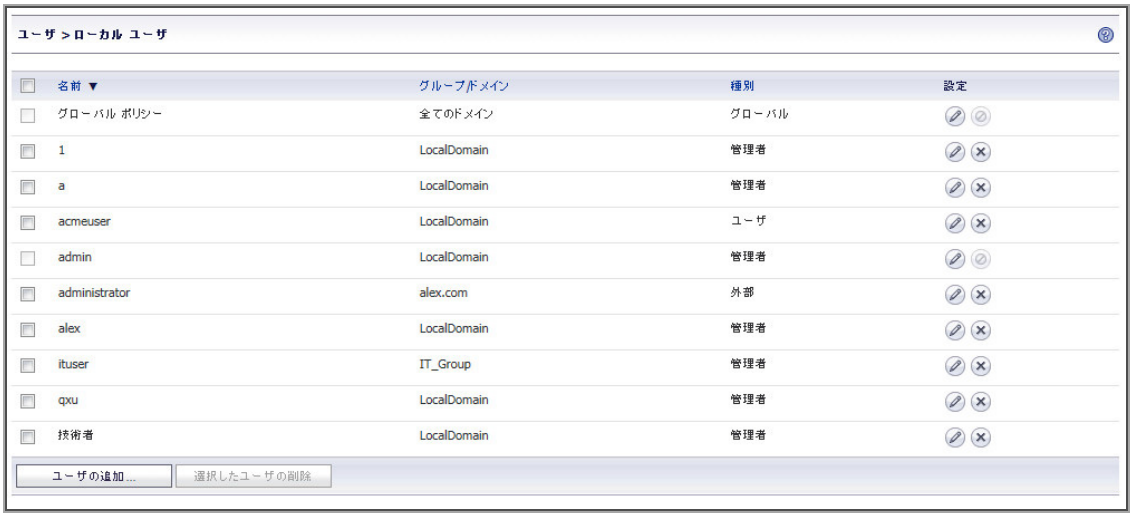
9 「**ユーザ > ローカル グループ**」ページで「**グループの追加**」を選択して、2 番目のローカル グループを追加します。

10 「ローカル グループの追加」ウィンドウの「**グループ名**」フィールドに **IT_Group** と入力します。

11 「**ドメイン**」ドロップダウン リストから「**SNWL_AD**」を選択します。

12 「**追加**」を選択します。

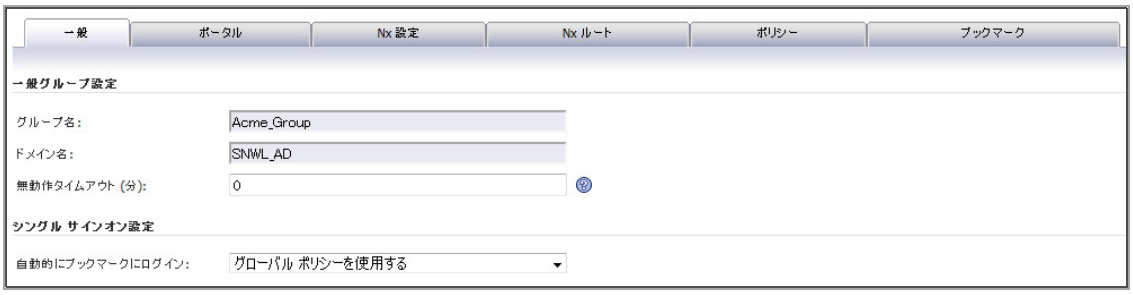
13 「**ユーザ > ローカル グループ**」ページで、追加したグループを確認します。



ローカル グループの設定

この手順では、新たに作成した各ローカル グループを編集し、それぞれを対応するアクティブ ディレクトリ グループと関連付けます。

1 「**Acme_Group**」行の「**設定**」を選択します。「**グループ設定の編集**」ウィンドウが表示されます。



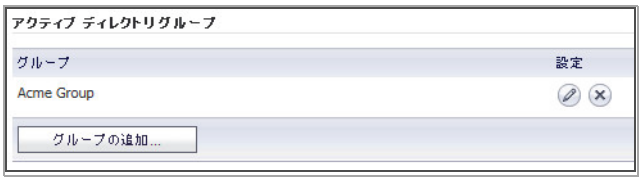
2 「**グループ設定の編集**」ウィンドウで「**AD グループ**」タブを選択します。

3 「**AD グループ**」タブで「**グループの追加**」を選択します。

4 「**アクティブ ディレクトリ グループの編集**」ウィンドウの「**アクティブ ディレクトリ グループ**」ドロップダウン リストから「**Acme Group**」を選択します。

5 「**編集**」を選択します。

「**AD グループ**」タブの「**アクティブ ディレクトリ グループ**」テーブルに「**Acme Group**」が表示されます。



6 「**グループ設定の編集**」ウィンドウで「**OK**」を選択します。

7 「**ユーザ > ローカル グループ**」ページで、「**Mega_Group**」行の「**設定**」を選択します。「**グループ設定の編集**」ウィンドウが表示されます。

8 「**グループ設定の編集**」ウィンドウで「**AD グループ**」タブを選択し、「**グループの追加**」を選択します。

9 「**アクティブ ディレクトリ グループの編集**」ウィンドウの「**アクティブ ディレクトリ グループ**」ドロップダウン リストから「**Mega Group**」を選択し、「**編集**」を選択します。

「**AD グループ**」タブの「**アクティブ ディレクトリ グループ**」テーブルに「**Mega Group**」が表示されます。

10 「**グループ設定の編集**」ウィンドウで「**OK**」を選択します。

11 「**ユーザ > ローカル グループ**」ページで、「**IT_Group**」行の「**設定**」を選択します。「**グループ設定の編集**」ウィンドウが表示されます。

12 「**グループ設定の編集**」ウィンドウで「**AD グループ**」タブを選択し、「**グループの追加**」を選択します。

13 「**アクティブ ディレクトリ グループの編集**」ウィンドウの「**アクティブ ディレクトリ グループ**」ドロップダウン リストから「**IT Group**」を選択し、「**編集**」を選択します。

「**AD グループ**」タブの「**アクティブ ディレクトリ グループ**」テーブルに「**IT Group**」が表示されます。

14 「**グループ設定の編集**」ウィンドウで「**OK**」を選択します。

以上で、3 つのローカル グループを作成し、それぞれをアクティブ ディレクトリ グループと関連付けたことになります。

SSHv2 許可ポリシーの追加

このセクションでは、**Acme_Group** と **IT_Group** の両方に対して 10.200.1.102 のサーバへの SSH によるアクセスを許可する SSHv2 許可ポリシーを追加します。

この手順では、**Acme_Group** という Secure Mobile Access のローカル グループのためのポリシーを作成して、Acme Group というアクティブ ディレクトリ グループのメンバーに SSH アクセスを許可します。

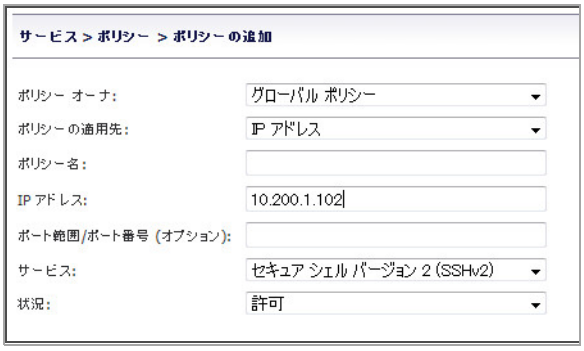
IT_Group についても同じ手順を繰り返し、それによって IT Group アクティブ ディレクトリ グループのメンバーにも SSH アクセスを許可します。

1 「**ユーザ > ローカル グループ**」ページで、「**Acme_Group**」行の「**設定**」を選択します。「**グループ設定の編集**」ウィンドウが表示されます。

2 「**グループ設定の編集**」ウィンドウで「**ポリシー**」タブを選択します。

3 「**ポリシー**」タブで「**ポリシーの追加**」を選択します。

4 「**ポリシーの追加**」ウィンドウの「**ポリシーの適用先**」ドロップダウン リストから「**IP アドレス**」を選択します。



5 「**ポリシー名**」フィールドに **SSH 許可**と入力します。

6 「**IP アドレス**」フィールドに、ターゲット サーバの IP アドレスとして **10.202.1.102** と入力します。

7 「**サービス**」ドロップダウン リストから「**セキュア シェル バージョン 2 (SSHv2)**」を選択します。

8 「**状況**」ドロップダウン リストで「**許可**」を選択し、「**適用**」を選択します。

OWA 許可ポリシーの追加

このセクションでは、**Mega_Group** と **IT_Group** の両方に対して OWA サービスへのセキュア ウェブ (HTTPS) によるアクセスを許可する 2 つの OWA 許可ポリシーを追加します。

この手順では、**Mega_Group** という Secure Mobile Access のローカル グループのためのポリシーを作成して、Mega Group というアクティブ ディレクトリ グループのメンバーに OWA アクセスを許可します。

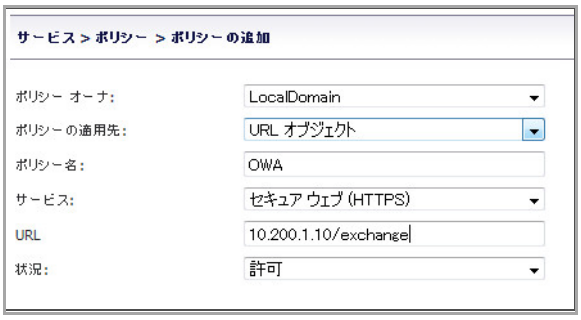
Exchange サーバにアクセスするには、**10.200.1.10/exchange** URL オブジェクト自体に許可ポリシーを追加するだけでは十分ではありません。**10.200.1.10/exchweb** へのアクセスを許可する URL オブジェクト ポリシーも必要です。なぜなら、OWA ウェブ コンテンツの中には **exchweb** ディレクトリに置かれているものもあるからです。

IT_Groupについても同じ手順を繰り返し、それによって IT Group アクティブ ディレクトリ グループのメンバーにも OWA アクセスを許可します。

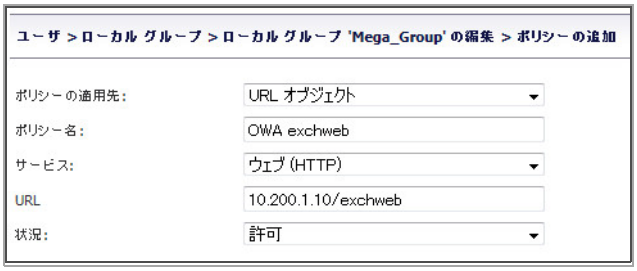
メモ：この設定では、IT_Group と Mega_Group のメンバーは 〈https://owa-server/public〉フォルダへのアクセスを拒否されます。なぜなら、これらのグループは /exchange サブフォルダと /exchweb サブフォルダにしかアクセスできないからです。

OWA はウェブ サービスなので、これらの OWA ポリシーはサーバ IP アドレスではなく、Exchange サーバ URL オブジェクトに適用されます。

1. 「**ユーザ > ローカル グループ**」ページで、「**Mega_Group**」行の「**設定**」を選択します。Mega_Group が OWA Exchange サーバにアクセスできるようにするため、**2** つの許可ポリシーを作成することにします。
2. 「**グループ設定の編集**」ウィンドウで「**ポリシー**」タブを選択し、「**ポリシーの追加**」を選択します。
3. 「**ポリシーの追加**」ウィンドウの「**ポリシーの適用先**」ドロップダウン リストから「URL**オブジェクト**」を選択します。



4. 「**ポリシー名**」フィールドに **OWA** と入力します。
5. 「**サービス**」ドロップダウン リストから「**ウェブ (HTTPS)**」を選択します。
6. 「**URL**」フィールドに、ターゲット アプリケーションの URL として **10.200.1.10/exchange** と入力します。
7. 「**状況**」ドロップダウン リストで「**許可**」を選択し、「**適用**」を選択します。
8. 「**グループ設定の編集**」ウィンドウの「**ポリシー**」タブで、「**ポリシーの追加**」を選択します。
9. 「**ポリシーの追加**」ウィンドウの「**ポリシーの適用先**」ドロップダウン リストから「**URL オブジェクト**」を選択します。



10 「**ポリシー名**」フィールドに **OWA exchweb** と入力します。

11 「**サービス**」ドロップダウン リストから「**ウェブ (HTTPS)**」を選択します。

12 「**URL**」フィールドに、ターゲット アプリケーションの URL として **10.200.1.10/exchweb** と入力します。

13 「**状況**」ドロップダウン リストで「**許可**」を選択し、「**適用**」を選択します。

14 これで Mega_Group 用のポリシーは完成しました。IT_Group についても同じ手順を繰り返し、それによって IT Group アクティブ ディレクトリ グループのメンバーにも OWA アクセスを許可します。

アクセス ポリシー設定の確認

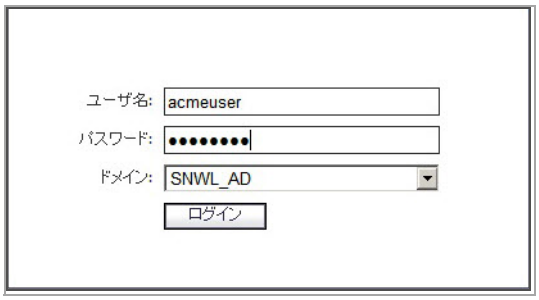
この時点で次のような設定になっています。

- Acme_Group のユーザには 10.200.1.102 への SSH アクセスが許可されている。
- Mega_Group のユーザには 10.200.1.10 の OWA へのアクセスが許可されている。
- IT_Group のユーザには上記の SSH と OWA の両方へのアクセスが許可されている。

この設定を確認するには、別々の AD グループのメンバーとして SMA/SRA 装置上の SNWL_AD ドメインにログインし、これらのリソースへのアクセスを試みます。

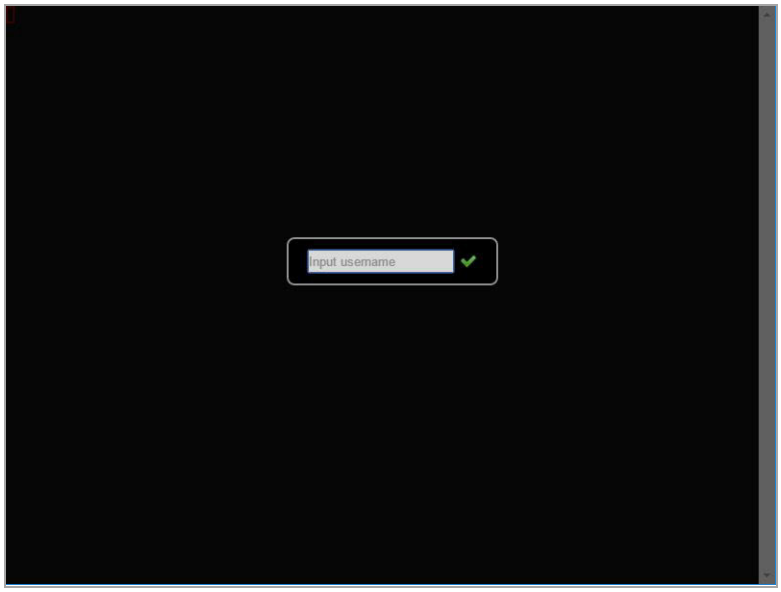
テスト結果: acmeuser によるアクセスの試み

acmeuserが **SNWL_AD** ドメインにログインします。

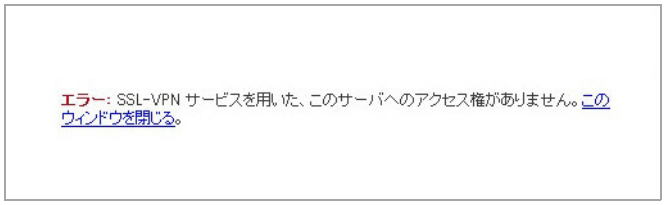


「**ユーザ > 状況**」ページに、**acmeuser** が **Acme_Group** ローカル グループのメンバーであることが示されます。

acmeuser は予想どおり SSH アクセスができます。

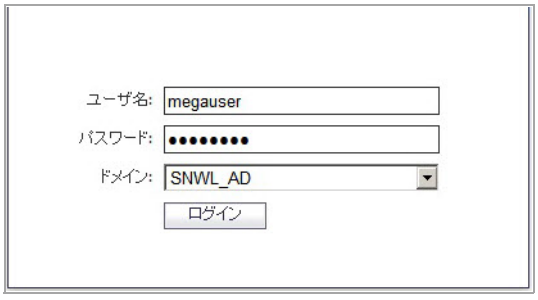


acmeuser は他のリソース (OWA 10.200.1.10 など) へのアクセスを試みますが、予想どおり拒否されます。

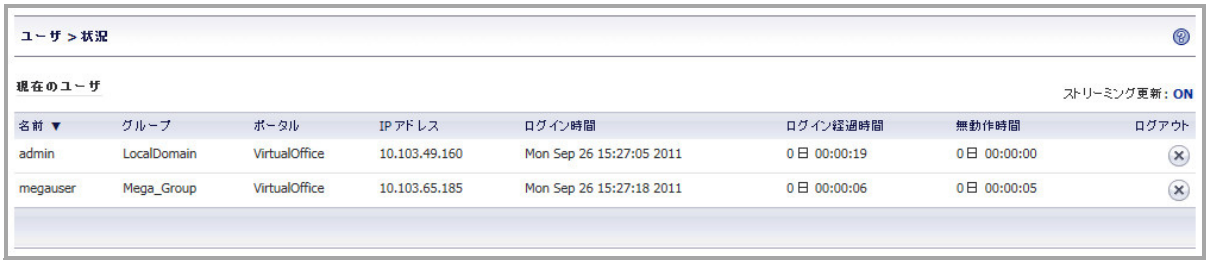


テスト結果: megauser によるアクセスの試み

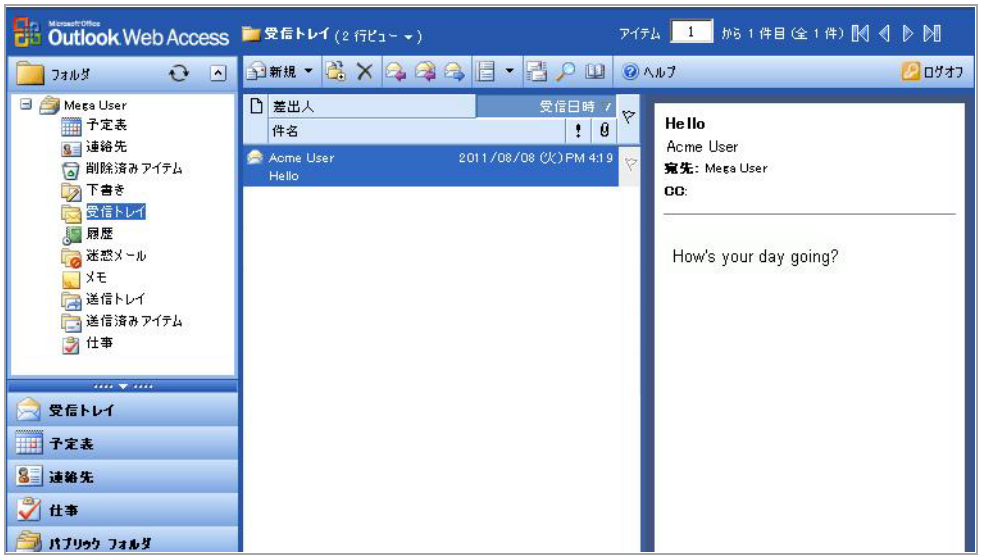
megauserが **SNWL_AD** ドメインにログインします。



「**ユーザ > 状況**」ページに、**megauser** が **Mega_Group** ローカル グループのメンバーであることが示されます。



megauser は予想どおり OWA リソースにアクセスできます。

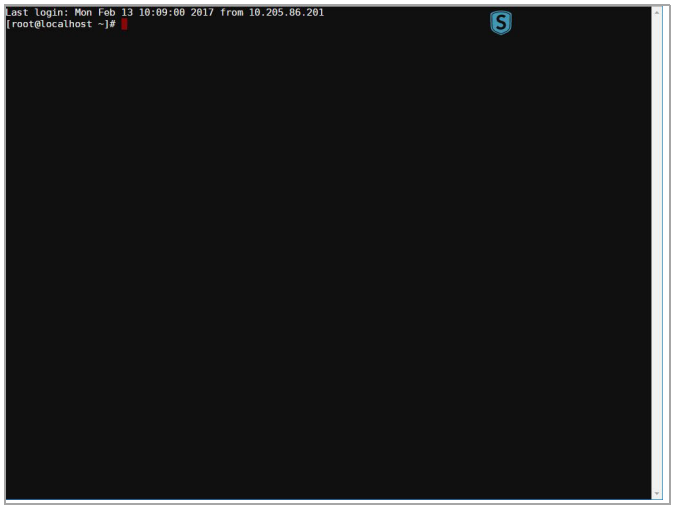


megauserは SSH アクセスを試みますが、予想どおり拒否されます。

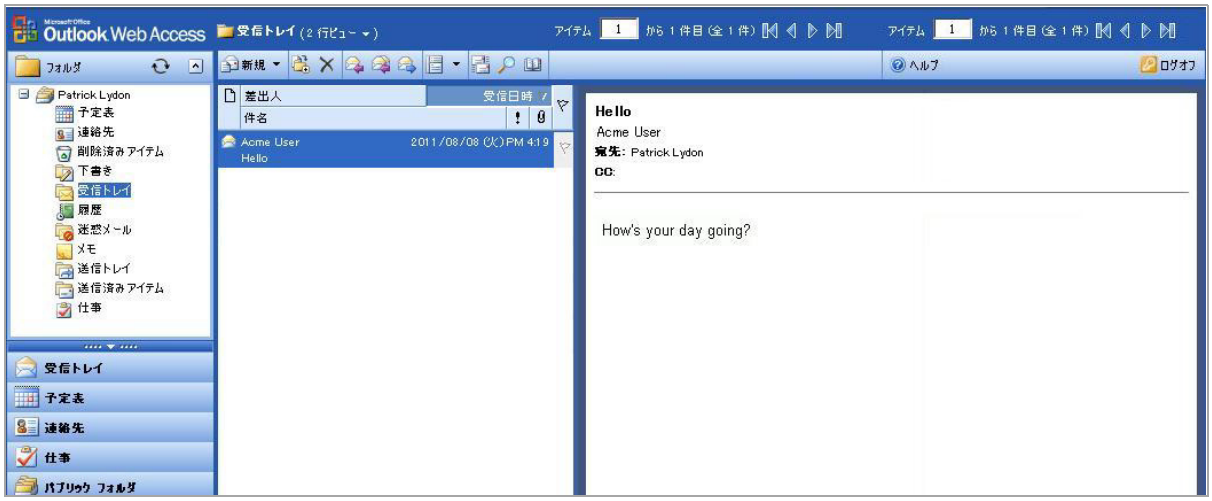
テスト結果: ituser によるアクセスの試み

ituserが **SNWL_AD** ドメインにログインします。「**ユーザ > 状況**」ページに、**ituser** が **IT_Group** ローカル グループのメンバーであることが示されます。

ituser は予想どおり 10.200.1.102 への SSH アクセスができます。



ituser は予想どおり OWA リソースにアクセスできます。



E

NetExtender のトラブルシューティング

Secure Mobile Access (SMA) または Secure Remote Access (SRA) の NetExtender ユーティリティのトラブルシューティング情報を以下の表に示します。

NetExtender をインストールできない

問題	解決法
NetExtender をインストールできない。	1 OS のバージョンを確認します。NetExtender は、Windows Vista またはそれ以降のバージョン、Apple Java 1.6.0_10 以降を持つ Mac OS X 10.5 以降のバージョン、そして Linux については Fedora Core と Ubuntu に加え OpenSUSE に対応しています。Linux は、i386 デストリビューションと Sun Java 1.6.0 10 以降が必要です。 2 ユーザが管理者権限を持っていることを確認します。NetExtender をインストールおよび実行するには、管理者権限のあるユーザアカウントを使用する必要があります。 3 インターネット エクスプローラまたはサードパーティ製の遮断プログラムによって ActiveX が遮断されていないかどうかを確認します。 4 上記によっても問題が解決しない場合は、以下の情報を取得してサポートまで連絡してください。 • デバイス マネージャから取得した Secure Mobile Access NetExtender アダプタのバージョン情報。 • **C:\Program files\SonicWall\SMA\NetExtender.dbg.** にあるログ ファイル。 • Windows のコントロール パネルの「**管理ツール**」フォルダにある「**イベント ビューア**」から取得したイベント ログ。 「アプリケーションおよびシステム」イベントを選択し、「**操作 > ログ ファイルの名前を付けて保存**」メニューを使って、イベントをログ ファイルに保存します。

NetExtender の接続エントリを作成できない

問題	解決法
NetExtender の接続エントリを作成できない	1 「デバイス マネージャ」を開いて、Secure Mobile Access NetExtender アダプタが正しくインストールされているかどうかを確認します。正しくインストールされていない場合は、デバイス リストからアダプタを削除し、コンピュータを再起動して、NetExtender を再度インストールします。 2 「**コントロール パネル > 管理ツール > サービス**」を選択し、Windows のサービス マネージャを開きます。「**Remote Access Auto Connection Manager**」および「**Remote Access Connection Manager**」を探して、この 2 つのサービスが開始されているかどうかを確認します。開始されていない場合は、それらが自動で開始するように設定し、コンピュータを再起動して、NetExtender を再度インストールします。 3 別のダイヤルアップ接続が使用中でないかどうかを確認します。使用中の場合は、その接続を切断し、コンピュータを再起動して、NetExtender を再度インストールします。 4 上記によっても問題が解決しない場合は、以下の情報を取得してサポートまで連絡してください。 • デバイス マネージャから取得した Secure Mobile Access NetExtender アダプタのバージョン情報。 • **C:\Program files\SonicWall\SMA\NetExtender.dbg** にあるログ ファイル。 • 「**コントロール パネル > 管理ツール > イベント ビューア**」から取得したイベント ログ。「**アプリケーションおよびシステム**」イベントを選択し、「**操作 > ログ ファイルの名前を付けて保存**」メニューを使って、イベントをログ ファイルに保存します。

NetExtender で接続できない

問題	解決法
NetExtender で接続できない	1 「デバイス マネージャ」を開いて、Secure Mobile Access NetExtender アダプタが正しくインストールされているかどうかを確認します。正しくインストールされていない場合は、デバイス リストからアダプタを削除し、コンピュータを再起動して、NetExtender を再度インストールします。 2 ネットワーク接続を開いて、Secure Mobile Access NetExtender のダイヤルアップ接続エントリが作成されているかどうかを確認します。作成されていない場合は、コンピュータを再起動し、NetExtender を再度インストールします。 3 別のダイヤルアップ接続が使用中でないかどうかを確認します。使用中の場合は、その接続を切断し、コンピュータを再起動して、NetExtender を再度接続します。 4 上記によっても問題が解決しない場合は、以下の情報を取得してサポートまで連絡してください。 • デバイス マネージャから取得した Secure Mobile Access NetExtender アダプタのバージョン情報。 • **C:\Program files\SonicWall\SMA\NetExtender.dbg** にあるログ ファイル。 • 「**コントロール パネル > 管理ツール > イベント ビューア**」から取得したイベント ログ。「**アプリケーションおよびシステム**」イベントを選択し、「**操作 > ログ ファイルの名前を付けて保存**」メニューを使って、イベントをログ ファイルに保存します。

接続後に NetExtender でブルースクリーン エラーが発生する

問題	解決法
接続後に NetExtender でブルースクリーン エラーが発生する	1 NetExtender をアンインストールし、コンピュータを再起動して、最新バージョンの NetExtender を再インストールします。 2 以下の情報を取得してサポートまで連絡してください。 • デバイス マネージャから取得した Secure Mobile Access NetExtender アダプタのバージョン情報。 • **C:\Program files\SonicWall\SMA\NetExtender.dbg** にあるログ ファイル。 • **C:\Windows\MEMORY.DMP** にある Windows のメモリ ダンプ ファイル。このファイルが見つからない場合は、「システムのプロパティ」を開いて、「**詳細**」タブの「**起動/回復**」を選択します。「**デバッグ情報の書き込み**」プルダウン メニューで、「**完全メモリ ダンプ**」、「**カーネル メモリ ダンプ**」、または「**最小メモリ ダンプ**」を選択します。もちろん、ダンプ ファイルを取得するには、ブルースクリーン エラーを再現する必要もあります。 • 「**コントロール パネル > 管理ツール > イベント ビューア**」から取得したイベント ログ。「**アプリケーションおよびシステム**」イベントを選択し、「**操作 > ログ ファイルの名前を付けて保存**」メニューを使って、イベントをログ ファイルに保存します。

F

よくある質問と回答

この付録では、Secure Mobile Access (SMA) または Secure Remote Access (SRA) 装置に関してよく寄せられる質問 (FAQ) を示します。

ハードウェアに関してよく寄せられる質問

1 SMA 400 と SMA 200 のハードウェア仕様を教えてください。

回答:

インターフェース

SMA 200: ギガビット イーサネット × 2、USB × 2、コンソール × 1

SMA 400: ギガビット イーサネット × 4、USB × 2、コンソール × 1

プロセッサ

SMA 200: 1.74 GHz Intel Atom™ C2358 デュアル コア プロセッサ

SMA 400: 2.40 GHz Intel Atom™ C2358 クアッド コア プロセッサ

メモリ (RAM)

SMA 200: 2 GB

SMA 400: 4 GB

フラッシュ dd メモリ

SMA 200: 2 GB (CFAST)

SMA 400: 2 GB (CFAST)

電源

SMA 200: 内蔵 (固定)、60W アダプター

SMA 400: 内蔵 (固定)、60W アダプター

最大電力消費量

SMA 200: 26.9 W

SMA 400: 31.9 W

放熱総量

SMA 200: 92 BTU

SMA 400: 109 BTU

寸法

SMA 200: 17.00 × 10.13 × 1.75 インチ (43.18 × 25.73 × 4.45cm)

SMA 400: 17.00 × 10.13 × 1.75 インチ (43.18 × 25.73 × 4.45cm)

重み

SMA 200: 11lbs (5 kg)

SMA 400: 11lbs (5 kg)

主要な適合規格

SMA 200/400:

FCC Class A、ICES Class A、CE、C-Tick、VCCI Class A、KCC、ANATEL、BSMI、NOM、UL、cUL、TUV/GS、CB

設置環境:

気温:

SMA 200/400: 32〜105° F、0〜40° C

相対湿度:

SMA 200/400: 5 〜 95%、結露のないこと

MTBF

SMA 200: 7.060 年

SMA 400: 6.870 年

2 SRA 4600/1600 のハードウェア仕様を教えてください。

回答:

インターフェース

SRA 1600: ギガビット イーサネット × 2、USB × 2、コンソール × 1

SRA 4600: ギガビット イーサネット × 4、USB × 2、コンソール × 1

プロセッサ

SRA 1600: 1.66 GHz Intel Atom プロセッサ、x86

SRA 4600: 1.66 GHz Intel Atom Dual Core プロセッサ、x86

メモリ (RAM)

SRA 1600: 1 GB

SRA 4600: 2 GB

フラッシュ dd メモリ

SRA 1600: 1 GB

SRA 4600: 1 GB

電源

SRA 1600: 内部、100-240 Vac、50-60 Mhz

SRA 4600: 内部、100-240 Vac、50-60 Mhz

最大電力消費量

SRA 1600: 47 W

SRA 4600: 50 W

放熱総量

SRA 1600: 158 BTU

SRA 4600: 171 BTU

寸法

SRA 1600: 17.00 × 10.13 × 1.75 インチ (43.18 × 25.73 × 4.45cm)

SRA 4600: 17.00 × 10.13 × 1.75 インチ (43.18 × 25.73 × 4.45cm)

重み

SRA 1600: 9.5lbs (4.3 kg)

SRA 4600: 9.5lbs (4.3 kg)

主要な適合規格

SRA 1600/4600:

FCC Class A、EMI/EMC、FCC、CE、VCCI Class A、UL、cUL、TUV/GS、CB

設置環境:

気温:

SRA 1600/4600: 32〜105° F、0〜40° C

相対湿度:

SRA 1600/4600: 5 〜 95%、結露のないこと

MTBF

SRA 1600: 18.3 年

SRA 4600: 17.8 年

3 SMA 500v Virtual Appliance の仮想環境の要件は何ですか。

ハイパーバイザー: VMWare ESXi (バージョン 5.0 以降)

装置サイズ (ディスク上): 2 GB

割り当てメモリ: 2 GB

メモ：SMA 500v Virtual Appliance は、VMware ESX/ESXi 4.0 および 4.1 上ではサポートされません。これらの ESXi バージョンのいずれかで Virtual Appliance を配備すると、動作はしますが、警告メッセージが表示される場合があります。

4 SMA/SRA 装置にハードウェア ベースの SSL アクセラレータは搭載されていますか。

回答: SRA 4600 と SRA 1600 には、ハードウェア ベースの SSL アクセラレータ プロセッサは搭載されていませんが、SMA 400/200 のプロセッサには、AES 暗号化を高速化する AES NI 命令セットが実装されています。

5 SMA/SRA 装置で実行されているオペレーティング システムは何ですか。

質問の答え: 装置では SonicWall Inc. 独自の堅牢な Linux ディストリビューションが実行されています。

6 複数の SMA/SRA 装置を負荷分散して配置できますか。

質問の答え: はい。負荷分散またはコンテンツ スイッチで SSL セッション ID の恒久性か Cookie ベースの恒久性に基づいてセッションを追跡できる限りは可能です。

7 各種の SMA/SRA 装置で許可される最大接続数はいくつですか。

次の SMA/SRA の諸元表を参照してください。

SMA/SRA の諸元表

種別	最大サポート数 (SMA 200)	最大サポート数 (SMA 400)	最大サポート数 (SRA 1600)	最大サポート数 (SRA 4600)	最大サポート数 (SMA 500v Virtual Appliance)
ポータル エントリ数	32	64	32	64	64
ドメイン エントリ数	32	64	32	64	64
グループ エントリ数	512	512	512	512	512
ユーザ エントリ数	1,000	2,000	1,000	2,000	2,000
NetExtender グローバル クライアント ルート数	100	100	100	100	100
NetExtender グループ クライアント ルート数	100	100	100	100	100
NetExtender ユーザ クライアント ルート数	100	100	100	100	100
最大同時ユーザ数	200	1024	200	1024	1024

SMA/SRA の諸元表 (続き)

種別	最大サポート数 (SMA 200)	最大サポート数 (SMA 400)	最大サポート数 (SRA 1600)	最大サポート数 (SRA 4600)	最大サポート数 (SMA 500v Virtual Appliance)
最大同時 Nx トンネル数	50	500	100	500	500
ルート エントリ数	32	32	32	32	32
ホスト エントリ数	32	32	32	32	32
ブックマーク エントリ数	500	500	500	500	500
ユーザ ポリシー エントリ数	64	64	64	64	64
グループ ポリシー エントリ数	64	64	64	64	64
グローバル ポリシー エントリ数	64	64	64	64	64
ポリシー アドレス エントリ数	32	32	32	32	32
ネットワーク オブジェクト	128	128	128	128	128
“アドレス” ネットワーク オブジェクト数	32	32	32	32	32
“ネットワーク” ネットワーク オブジェクト数	64	64	64	64	64
“サービス” ネットワーク オブジェクト数	64	64	64	64	64
SMB 共有数	1,024	1,024	1,024	1,024	1,024
SMB ノード数	1,024	1,024	1,024	1,024	1,024
SMB ワークグループ数	8	8	8	8	8
同時 FTP セッション数	8	8	8	8	8
ログ サイズ	250 KB	250 KB	250 KB	250 KB	250 KB

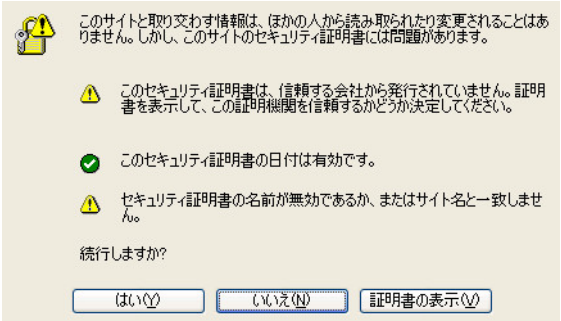
デジタル証明書と認証局に関してよく寄せられる質問

1 SMA/SRA 装置にログインしたら、ブラウザまたは Java コンポーネントからエラーが出力されました。どうすればよいですか。

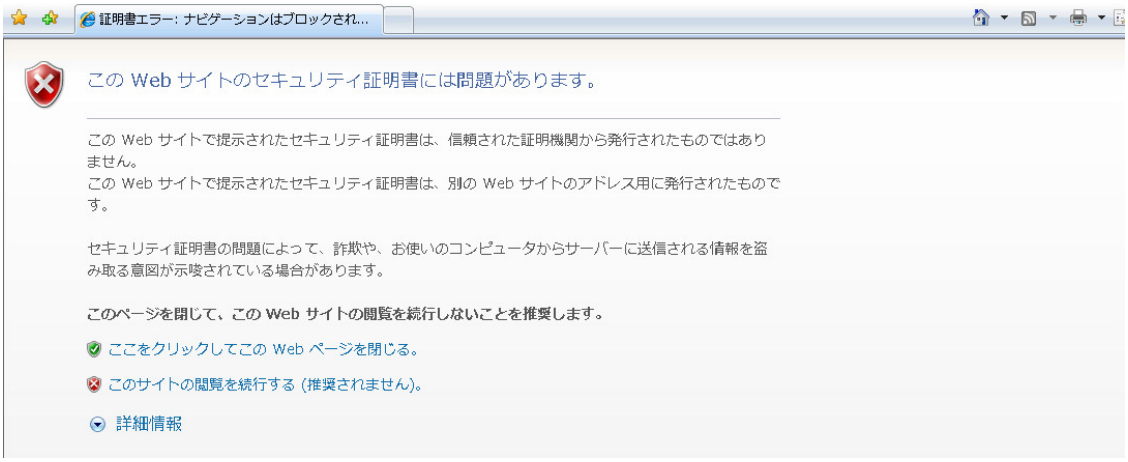
質問の答え: これらのエラーは、次の 3 つの要因の組み合わせが原因で発生します。

- SMA/SRA 装置内の証明書がブラウザによって信頼されていない。
- SMA/SRA 装置内の証明書の有効期限が切れている。
- クライアントのウェブ ブラウザが要求するサイトが、証明書に埋め込まれているサイト名に一致しない。

ウェブ ブラウザは、上記の 3 つの条件が完全に満たされない場合に警告を出力するようにプログラムされています。このセキュリティ メカニズムは、エンドツーエンドのセキュリティの実現を目的とするものですが、場合によっては何かが壊れたのではないかとユーザが混乱することがあります。既定の自己署名証明書を使用している場合は、ウェブ ブラウザが SMA/SRA 装置に接続するたびにこのエラーが表示されます。しかし、これは単なる警告であり、SSL ハンドシェーク時にネゴシエートされるセキュリティには影響しないため、無視しても問題ありません。このエラーを表示しないようにするには、信頼済みの SSL 証明書を購入して SMA/SRA 装置にインストールする必要があります。



2 SMA/SRA 装置にログインすると次のメッセージが表示されます。どうすればよいですか。

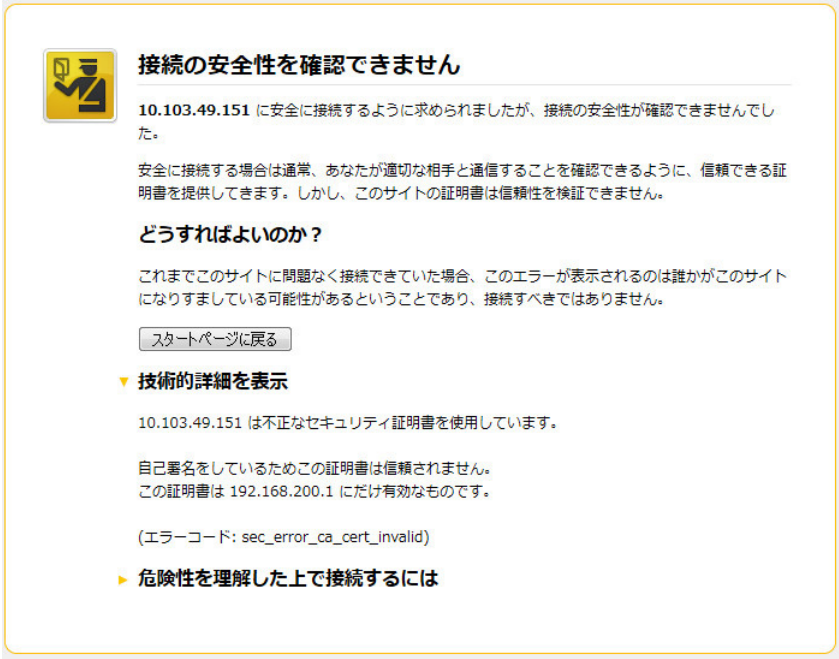


回答: 問題としては前の話題で指摘したものと同じですが、これは Microsoft Internet Explorer の新しい“改良された”セキュリティ警告画面です。IE5.x および IE6.x 以前は証明書が信頼されていない理由を示すポップアップが表示されましたが、IE ではユーザにそのページを閉じた方が

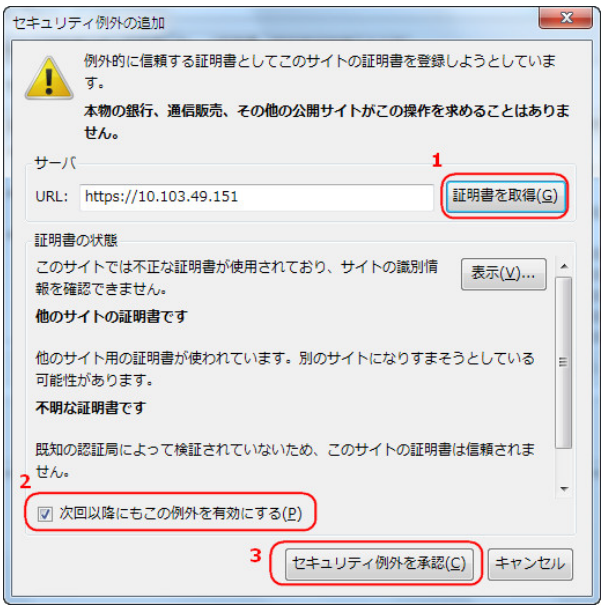
よいことを勧める一般的なエラー ページだけが表示されます。そのまま「はい」を選択して先に進むようにはなっておらず、ユーザは埋め込まれた「**このサイトの閲覧を続行する(推奨されません)。**」リンクを選択する必要があります。そのため、すべての SMA/SRA 装置に、ゆくゆくは信頼されているデジタル証明書をインストールすることを強くお勧めします。

3 Firefox を使用して SMA/SRA 装置にログインすると次のメッセージが表示されます。どうすればよいですか。

回答: Internet Explorer の場合の上記のエラーと同様に、Firefox も証明書に関する問題が検出されると独自のエラー メッセージを返します。このエラーが出る条件は上記の Internet Explorer のエラーと同じです。



この画面をパスするには、下部にある「**危険性を理解した上で接続するには**」リンクを選択し、「**例外を追加**」を選択します。「セキュリティ例外の追加」ウィンドウで「**証明書を取得**」を選択し、「**次回以降にもこの例外を有効にする**」をオンにし、最後に「**セキュリティ例外を承認**」を選択します。以下を参照してください。



これは不便なので、後ですべての SMA/SRA 装置に、信頼されているデジタル証明書をインストールすることを強くお勧めします。

4 Java コンポーネントを起動するとエラーが表示されます。どうすればよいですか。

回答: 前のセクションを参照してください。これが起こるのは、証明書がウェブ ブラウザによって信頼されていないか、ブラウザの要求したサイトの名前が、SSL ハンドシェーク プロセスの最中に SMA/SRA 装置から提示されたサイト証明書に埋め込まれている名前と一致しない場合です。このエラーは無視してかまいません。

5 SSL 証明書を購入する必要がありますか。

回答: 暗号化のレベルは低下しませんが、ユーザが信頼されていない証明書を受け入れると、中間者攻撃のリスクが発生します。信頼されている証明書のみをインストールするか、すべてのクライアントに既定の自己署名証明書をインストールすることをお勧めします。

6 デジタル証明書ではどの形式が使用されていますか。

回答: X509v3 です。

7 ワイルド カード証明書はサポートされていますか。

回答: はい。

8 SMA/SRA 装置ではどの CA の証明書が使用できますか。

回答: X509v3 形式の証明書であれば、Verisign、Thawte、Baltimore、RSA など、どの CA の証明書も使用できます。

9 SMA/SRA 装置は連鎖証明書をサポートしていますか。

回答: はい、サポートしています。「**システム > 証明書**」ページで以下の操作を行います。

- 「サーバ証明書」で「証明書のインポート」を選択し、SSL サーバ証明書と鍵をまとめて .zip ファイルとしてアップロードします。証明書の名前は“server.crt”とします。秘密鍵の名前は“server.key”とします。
- 「追加の CA 証明書」で「**証明書のインポート**」を選択し、中間 CA の証明書をアップロードします。この証明書は PEM エンコード形式のテキスト ファイルです。

中間 CA の証明書をアップロードした後、システムを再起動してください。CA 証明書バンドルに含められた新しい証明書を使用してウェブ サーバを再起動する必要があります。

10 SMA/SRA 装置の証明書を購入するとき、ほかにヒントはありますか。

回答: 毎年の更新は煩わしいので、複数年の証明書を購入することをお勧めします (更新を忘れがちで、証明書の期限が切れると管理者は大変な思いをするからです)。SMA/SRA 装置に接続するすべてのユーザに Windows Update (Microsoft Update とも呼ばれます) を実行させて、“ルート証明書”アップデートがインストールされるようにすることもポイントになるでしょう。

11 マイクロソフト証明書サーバで生成された証明書を使用できますか。

回答: はい。しかし、ブラウザからの警告を回避するには、マイクロソフト CA のルート証明書を、装置に接続するすべてのウェブ ブラウザにインストールする必要があります。

12 新しい証明書と秘密鍵をインポートできないのはなぜですか。

回答: 必ず PEM 形式の秘密鍵ファイル“server.key”と PEM 形式の証明書ファイル“server.crt”から成る .zip ファイルをアップロードしてください。この .zip ファイルはディレクトリを持たないフラットなファイル構造で、“server.key”ファイルと“server.crt”ファイルだけを含まなければなりません。また、鍵と証明書が対のものでないと、インポートは失敗します。

13 新しい証明書と秘密鍵をインポートした後にステータスが“保留”になるのはなぜですか。

質問の答え: 新しい証明書の横の「設定」アイコンを選択し、証明書署名リクエスト (CSR) を作成するときに指定したパスワードを入力して、証明書のインポートを完了します。この操作を行うと、SMA/SRA 装置で証明書を有効化できます。

14 複数の仮想ホストがあれば、複数の証明書を有効にできますか。

質問の答え: 各ポータルの証明書を「**ポータル > ポータル**: ポータルの編集 - 仮想ホスト」タブで選択できます。ポータルの「仮想ホストの設定」フィールドで別々の IP アドレスと、ポータルごとの証明書を指定できます。管理者が複数のポータルを設定している場合、各ポータルに別個の証明書を関連付けていることがあります。例えば、ブラウザで **virtualassist.test.sonicwall.com** を指せば、**sslvpn.test.sonicwall.com** にもアクセスされます。これらのポータル名それぞれに対し、別個の証明書を持たせることができます。このようにすると、「このサーバは abc ですが、証明書は xyz のものです。続行しますか?」といった証明書の不一致の警告がブラウザから表示されないようにするうえで役立ちます。

15 CSR を CA のオンライン登録サイトにインポートしましたが、目的のウェブ サーバの種類を指定するように要求されます。どうすればよいですか。

質問の答え: “Apache”を選択してください。

16 鍵と証明書を保存することはできますか。

質問の答え: はい。鍵は CSR の生成プロセスの際に CSR と共にエクスポートされます。CA から受け取る証明書と共に、これを安全な場所に保管することを強くお勧めします。こうしておけば、SMA/SRA 装置の交換が必要になるか装置が故障しても、鍵と証明書を再ロードできます。設定は「**システム > 設定**」ページからいつでもエクスポートできます。

17 SMA/SRA 装置はクライアント側のデジタル証明書をサポートしますか。

質問の答え: はい。クライアント証明書は「**ユーザ > ローカル ユーザ**: ユーザの編集 - ログイン ポリシー」タブでドメイン単位またはユーザ単位で強制されます。

- ドメイン単位/ユーザ単位のクライアント証明書の強制に関する設定:
  - ユーザの名前がクライアント証明書の一般名 (CN) と一致することを確認するオプション
  - クライアント証明書サブジェクトの部分 DN を確認するオプション (省略可能)。次の変数がサポートされています。

    ユーザ名: %USERNAME%

    ドメイン名: %USERDOMAIN%

    アクティブ ディレクトリ ユーザ名: %ADUSERNAME%

    ワイルドカード: %WILDCARD%

- マイクロソフト CA のサブジェクト名のサポート。CN はユーザのフル ネームで、例えば、CN=John Doe。アクティブ ディレクトリ ドメイン内のユーザに対してクライアント証明書を認証するときは、AD 内のユーザのフル ネームと CN を比較します。
- クライアント証明書の認証が失敗した場合の詳細なメッセージとログ メッセージは、「**ログ > 表示**」ページで表示できます。
- 証明書失効リスト (CRL) サポート。各 CA 証明書で、ファイルのインポートまたは URL からの定期的なインポートによるオプションの CRL がサポートされるようになりました。

  クライアント証明書をクライアントのブラウザにロードする必要があります。クライアント証明書の信頼チェーン内の証明書を SMA/SRA 装置にインストールすることも忘れないでください。

18 クライアント認証が要求されたとき、CA 証明書がロードされているにもかかわらずクライアントが接続できません。なぜでしょうか。

質問の答え: クライアント認証で CA 証明書を使用するには、CA 証明書をロードした後に、SMA/SRA 装置を再起動する必要があります。クライアント証明書の検証に失敗した場合も、ログオンできません。最も一般的な理由として、証明書がまだ有効でない、証明書の有効期限が切れている、ログイン名が証明書の共通名に一致しない、証明書が送付されていないことが挙げられます。

NetExtender に関してよく寄せられる質問

1 NetExtender はウィンドウズ以外のオペレーティング システムでも動作しますか。

回答: はい。以下のサポートされるプラットフォームを参照してください。

Mac の要件:

- Mac OS X 10.6.8+
- Apple Java 1.6.0_10 以上 (「**Apple メニュー > ソフトウェア更新**」でインストール/アップグレード可能。OS X 10.6.8 以上では事前インストール済み)

Linux の要件:

- Linux の i386 互換ディストリビューション
- Sun Java 1.6.0 10 以上
- Fedora 14+
- Suse: 10.3 でテストが成功しています。
- Ubuntu 11.04+

それぞれのリリースについて MySonicWall.com から NetExtender インストール パッケージを個別にダウンロードすることもできます。

2 NetExtender がサポートしているのはウィンドウズのどのバージョンですか。

回答: NetExtender がサポートするバージョン:

- Vista SP2
- Windows 10
- Windows 7

3 NetExtender クライアント間の通信を遮断できますか。

質問の答え: はい。ユーザ/グループ/グローバル ポリシーを使用して、NetExtender の IP 範囲に“拒否”ポリシーを追加することで実現できます。

4 NetExtender をウィンドウズのサービスとして実行できますか。

回答: NetExtender をインストールして、Windows のサービスとして実行するように設定できます。このサービスを使用すると、NetExtender クライアントをまたいでドメインにログインできます。

5 NetExtender の IP クライアント アドレス範囲として使用するのはどの範囲ですか。

回答: この範囲は外部からやってくる NetExtender クライアントに割り当てられるプールです。NetExtender クライアントは実際には内部ネットワーク上に存在するかのように見えます。これは SonicWall Inc. のグローバル VPN クライアントにおける仮想アダプタ機能とよく似ています。有効な NetExtender セッションごとに 1 つの IP アドレスを割り当てる必要があるので、最大で同時に 20 の NetExtender セッションを使うと予想される場合には、20 個の空き IP アドレスを持つ範囲を作成してください。これらの IP アドレスは空いていて他のネットワーク装置から使われていないか、他の DHCP サーバのスコープに含まれていなければなりません。例えば、SMA/SRA 装置が X0 インターフェース上で 1 ポート モードで既定の IP アドレス 192.168.200.1 を使用している場合は、192.168.200.151 ～ 192.168.200.171 の範囲のアドレスを持つプールを作成します。DHCP オプションを使用して動的に NetExtender の IP を割り当てることもできます。

6 NetExtender クライアント ルートには何を入力するのですか。

質問の答え: これらは、リモート NetExtender クライアントに送信されるネットワークであり、NetExtender クライアントにアクセスさせるすべてのネットワークを含む必要があります。例えば、SMA/SRA 装置が 1 ポート モードで、DMZ 上の SonicWall Inc. NSA 3500 装置にその DMZ のサブネットとして 192.168.200.0/24 を使用して接続しており、さらに SonicWall Inc. NSA 3500 に 192.168.168.0/24 と 192.168.170.0/24 という 2 つの LAN サブネットがある場合は、クライアント ルートとしてその 2 つの LAN サブネットを入力すれば、NetExtender クライアントが両方の LAN サブネット上のネットワーク リソースにアクセスできるようになります。

7 「トンネル オール モード」オプションはどのような機能を持ちますか。

質問の答え: この機能を有効にすると、SMA/SRA 装置は 2 つの既定ルートに対して、アクティブな NetExtender クライアントが SMA/SRA 装置を経由してすべてのトラフィックを送信するように設定します。SMA/SRA 装置が、すべての UTM サービスを実行する SonicWall Inc. セキュリティ装置と連携して配備される環境では、すべての送受信 NetExtender ユーザ トラフィックに対してウィルス、スパイウェア、侵入防御、およびコンテンツ フィルタが走査されるため、この機能が役立ちます。

8 SMA/SRA 装置が NetExtender を送信しているルートを確認する方法はありますか。

質問の答え: はい。タスクバーの NetExtender アイコンを右クリックし、「**ルート情報**」を選択してください。同じメニューで、ステータス情報と接続情報も入手できます。

9 インストールした NetExtender は、セッションを終了するときにアンインストールされますか。

質問の答え: 既定では、NetExtender が最初にインストールされると、システムに常駐します。ただし、これは、NetExtender の実行時にタスクバーの NetExtender アイコンから「**ブラウザ終了時にアンインストール** > **はい**」オプションを選択することによって制御できます。このオプションをオンにすると、NetExtender が閉じられるときに削除されます。コントロール パネルの「プログラムの追加と削除」からアンインストールすることもできます。以降のログイン時間を高速化するために、既定では NetExtender はシステムに常駐します。

10 新バージョンの NetExtender を入手するにはどうすればよいですか。

質問の答え: 新バージョンの NetExtender は、各 SonicWall Inc. Secure Mobile Access ファームウェア リリースに含まれており、バージョン管理情報を備えています。SMA/SRA 装置が新しいソフトウェアでアップグレードされている場合は、以前の旧バージョンの NetExtender を使用しているシステムから接続したとき、新バージョンに自動的にアップグレードされます。

自動アップグレード機能に、1 つ例外があり、MSI バージョンの NetExtender をサポートしていません。NetExtender が MSI パッケージを使ってインストールされた場合は、新しい MSI パッケージを使ってアップグレードする必要があります。MSI パッケージは管理者がアクティブ ディレクトリを通して NetExtender を配布するように設計されていて、アクティブ ディレクトリを通して完全なバージョン制御が可能です。

11 NetExtender は、SonicWall Inc. のグローバル VPN クライアント (GVC) など、従来の IPSec VPN クライアントとはどう異なりますか。

質問の答え: NetExtender は、ウェブ ブラウザ接続を通じてインストールされる非常に軽量なクライアントとして設計されており、ブラウザのセキュリティ変換を使用して、クライアントと SMA/SRA 装置間で安全な暗号化されたトンネルを作成します。

12 NetExtender は暗号化されますか。

質問の答え: はい。SSL 接続の際に NetExtender クライアントと SMA/SRA 装置がネゴシエーションした暗号を使用します。

13 SMA/SRA 装置とサーバ間のクリア テキスト トラフィックを保護する方法はありますか。

質問の答え: はい。暗号化された RDP ベースのセッションを使用し、HTTPS リバース プロキシを使用するようにマイクロソフト ターミナル サーバを設定できます。

14 NetExtender を使用するときにインストールされる PPP アダプタは何ですか。

質問の答え: これは、NetExtender が使用するトランスポート方法です。圧縮 (MPPC) も使用されます。NetExtender メニューから選択することによって、切断時には削除することを選択できます。

15 プロキシ アプリケーションの代わりに NetExtender を使うメリットは何ですか。

質問の答え: NetExtender を使用すると、暗号化および圧縮された PPP 接続を通じて完全な接続性が提供され、ユーザは内部ネットワーク リソースに直接接続できます。例えば、リモート ユーザは NetExtender を起動して企業ネットワーク上のファイル共有に直接接続できます。

16 プロキシの代わりに NetExtender を使用すると、パフォーマンスは変わりますか。

質問の答え: はい。NetExtender 接続では、SMA/SRA 装置に最低限の負荷しかかからないのに対して、プロキシベースの接続では SMA/SRA 装置に大量の負荷がかかる可能性があります。HTTP プロキシ接続では、負荷を削減してパフォーマンスを高めるために圧縮が使われることに注意してください。Secure Mobile Access がローカル ウェブ サーバから受け取ったコンテンツは gzip で圧縮してからインターネット経由でリモート クライアントへ送信されます。SMA/SRA から送信されるコンテンツを圧縮することで帯域幅が節約され、その結果、スループットが向上します。しかも、圧縮されたコンテンツのみがキャッシュされるので、必要なメモリのほぼ 40 ～ 50% が節約されます。gzip 圧縮は、SMA/SRA 装置のローカル (クリア テキスト側)、またはリモート クライアントからの HTTPS 要求には利用できないことに注意してください。

17 SMA/SRA 装置はアプリケーション依存ですが、標準的でないアプリケーションにはどのように対処すればよいですか。

回答: NetExtender を使用すると、内部プロキシ メカニズム (HTTP、HTTPS、FTP、RDP5、Telnet、SSHv2) を使用してアクセスできないアプリケーションにアクセスを提供できます。ウェブ アプリケーションにはアプリケーション オフローダも使用できます。こうすることで、SMA/SRA

装置は SSL オフローダのように動作し、URL を書き換えなくてもウェブ アプリケーションのページがプロキシされるようになります。

18 ActiveX コンポーネントのインストールが必要になるのはなぜですか。

質問の答え: NetExtender は ActiveX ベースのプラグインを通じて Internet Explorer からインストールされます。Firefox ブラウザを使用しているユーザは NetExtender を XPI インストーラでインストールすることもできます。NetExtender は MSI インストーラでもインストールできます。NetExtender の MSI インストーラは MySonicWall.com からダウンロードしてください。

19 NetExtender は、AV 署名ファイルのチェックやウィンドウズ レジストリのチェックなどの、デスクトップ セキュリティの強制をサポートしていますか。

回答: 現在のところサポートしていません。ただし、この種の機能を将来リリースされる NetExtender で提供することを計画しています。

20 NetExtender は 64 ビット版のマイクロソフト ウィンドウズで動作しますか。

回答: はい。NetExtender は 64 ビット版の Windows 7 および Vista をサポートしています。

21 NetExtender は 32 ビット版と 64 ビット版の Microsoft Windows 7 で動作しますか。

回答: はい。NetExtender は 32 ビット版と 64 ビット版の Windows 7 をサポートしています。

22 NetExtender はクライアント側の証明書をサポートしていますか。

回答: はい。Windows NetExtender クライアントはスタンドアロン クライアントからのクライアント証明書の認証をサポートしています。認証を受けて Secure Mobile Access ポータルに入れば、ユーザが NetExtender を起動することもできます。

23 ファイアウォールが、NetExtender 接続をなりすましとして SonicWall SMA/SRA 装置から切断してしまいます。なぜでしょうか。

質問の答え: NetExtender アドレスが X0 インターフェース以外のサブネット上にある場合は、このアドレスが SMA/SRA 装置から来ていることをファイアウォールに知らせる規則を作成する必要があります。

一般的によく寄せられる質問

1 SMA/SRA 装置は、真のリバース プロキシですか。

回答: はい。HTTP、HTTPS、CIFS、FTP はウェブベースのプロキシであり、ネイティブ ウェブ ブラウザがクライアントです。VNC、RDP、Citrix、SSHv2、SSHv2、および Telnet はブラウザを通じて配信される HTML5 クライアントを使用します。ウィンドウズ上の NetExtender はブラウザを通じて配信されるクライアントを使用します。

2 SMA/SRA 装置に接続するためには、どのブラウザとバージョンが必要ですか。

回答: 現在サポートされているブラウザとバージョンの一覧は、本書の「ブラウザ要件」セクションに記載されています。

3 SMA/SRA 装置に接続するためには、ブラウザ上で何をアクティブにする必要がありますか。

回答:

- TLS
- Cookie の有効化
- サイトのポップアップの有効化

- Java の有効化
- JavaScript の有効化
- ActiveX の有効化

4 Java のどのバージョンが必要ですか。

質問の答え: SMA/SRA 装置でいくつかの機能を使用するためには、SUN の JRE 1.6.0_10 以上 (〈http://www.java.com〉で入手可能) をインストールする必要があります。Google Chrome では、Java 1.6.0 アップデート 10 以上が必要になります。

5 どのようなオペレーティング システムがサポートされていますか。

回答:

- Microsoft Vista
- Microsoft Windows 7
- Apple OSX 10.6.8 以上
- Linux カーネル 2.6.x 以上

6 サーバ名が"ファイル共有"コンポーネントに認識されないのはなぜですか。

回答: NetBIOS 名でサーバにアクセスできない場合は、名前解決に関して問題がある可能性があります。SMA/SRA 装置の DNS 設定および WINS 設定を確認してください。また、NetBIOS 名と IP のマッピングを「**ネットワーク > ホスト解決**」セクションで手動で指定してみたり、IP アドレスを UNC パスに手動で指定したりできます (\\192.168.100.100\sharefolder など)。

また、認証がループするかエラーとなった場合、このファイル共有はウィンドウズ ドメイン ルート上の DFS サーバでしょうか。ファイル共有を作成するときは、DFS (Distributed File System) サーバをウィンドウズ ドメイン ルート システムに設定しないでください。ドメイン ルートはドメイン内の Windows コンピュータへのアクセスのみを提供するので、DFS サーバをドメイン ルートに設定すると、他のドメインから DFS ファイル共有にアクセスできません。SMA/SRA 装置は、ドメイン メンバではなく、このような DFS 共有に接続できません。スタンドアロン ルート上の DFS ファイル共有には、Microsoft の制限は適用されません。

7 SMA/SRA 装置は SPI ファイアウォールを備えていますか。

質問の答え: いいえ。SonicWall Inc. セキュリティ装置または他のサードパーティ ファイアウォール/VPN 機器と組み合わせる必要があります。

8 HTTP を使用して SMA/SRA 装置にアクセスできますか。

質問の答え: いいえ、HTTPS が必要です。HTTP 接続は即時に HTTPS にリダイレクトされます。https: と入力すべきところを誤って http:// と入力することが多いので、80 と 443 の両方を開くとよいでしょう。80 をブロックすると、リダイレクトされません。

9 SMA/SRA 装置の最も一般的な配備は、どのようなものですか。

質問の答え: X0 インターフェースだけが使用される 1 ポート モードで、装置は、SonicWall Inc. TZ 装置または NSA 装置などの SonicWall Inc. セキュリティ装置で分離され、保護された"DMZ" ネットワーク/インターフェースに配置されます。

10 SMA/SRA 装置を、1 ポート モードで SonicWall Inc. セキュリティ装置と共にインストールすることが推奨されるのはなぜですか。

質問の答え: この配備方法によって、新たなセキュリティ制御の階層に加えて、ゲートウェイ アンチウィルス、アンチスパイウェア、コンテンツ フィルタ、侵入防御など、SonicWall Inc. 統合脅威管理 (UTM) サービスを使用して、すべての送受信 NetExtender トラフィックを走査できます。

11 複数のインターフェースを使用したり、装置を 2 ポート モードでインストールするようなインストール シナリオもありますか。

質問の答え: はい。有効なサード インターフェースを持たない可能性があるファイアウォール/VPN デバイスや、SMA/SRA 装置の統合が困難であったり不可能であるような機器を回避する必要がある場合が、これに該当します。

12 複数の SMA/SRA 装置をカスケード接続して、複数の同時接続をサポートできますか。

質問の答え: いいえ、サポートされていません。

13 SMA/SRA 装置の Secure Mobile Access 管理インターフェースにログインできないのはなぜですか。

回答: 装置の既定の IP アドレスは、X0 インターフェース上の 192.168.200.1 です。装置にアクセスできない場合は、システムを X0 ポートにクロス接続し、それに 192.168.200.100 という一時的な IP アドレスを割り当て、〈https://192.168.200.1〉で SMA/SRA 装置へのログインを試みてください。その後、ネットワーク ページで DNS と既定のルートの設定を正しく構成したか確認してください。

14 SMA/SRA 装置を使用してサイト間 VPN トンネルを作成できますか。

質問の答え: いいえ。これはクライアント アクセス装置に過ぎません。サイト間 VPN トンネルが必要な場合は、SonicWall Inc. TZ、NSA、または SuperMassive シリーズのセキュリティ装置が必要です。

15 SonicWall Inc. グローバル VPN クライアント (または他のサードパーティ VPN クライアント) を SMA/SRA 装置に接続することはできますか。

質問の答え: いいえ。サポートされるのは NetExtender およびプロキシ セッションだけです。

16 モデム接続を通じて SMA/SRA 装置に接続できますか。

質問の答え: はい。パフォーマンスは低速ですが、56K 接続でも使用できます。

17 SMA/SRA 装置ではどの SSL 暗号がサポートされていますか。

質問の答え: 7.5 以降のファームウェアでは、SonicWall Inc. は TLSv1、TLSv1.1、および TLSv1.2 で高度なセキュリティ暗号だけを使用します。8.0 以降のファームウェアでは、SSL Perfect Forward Secrecy (PFS) がサポートされています。

18 SMA/SRA 装置で AES はサポートされますか。

質問の答え: はい。ブラウザがサポートしている場合はサポートされます。

19 IPSec VPN と同様のパフォーマンス (速度、遅延、スループット) を得ることができますか。

質問の答え: はい。NetExtender は多重化された PPP 接続を使用し、接続上ではパフォーマンスを向上するために圧縮を実行するため、実際、より優れたパフォーマンスを示すことがあります。

20 二段階認証 (RSA SecurID など) はサポートされますか。

回答: はい。サポートされています。

21 SMA/SRA 装置は VoIP をサポートしますか。

質問の答え: はい。接続を通じてサポートします。

22 Syslog はサポートされていますか。

質問の答え: はい。

23 NetExtender はマルチキャストをサポートしていますか。

回答: いいえ、今のところサポートしていません。これについては、将来のファームウェア リリースに期待してください。

24 SNMP と Syslog はサポートされていますか。

回答: 現行のソフトウェアでは、最大 2 つの外部サーバに対する Syslog 転送がサポートされています。SNMP は 5.0 リリースからサポートされています。MIB は MySonicWall からダウンロードできます。

25 SMA/SRA 装置はコマンド ライン インターフェース (CLI) を備えていますか。

質問の答え: はい。SMA/SRA 装置には、コンソール ポートに接続して使う簡素な CLI があります。SMA 500v Virtual Appliance も CLI から設定可能です。Secure Mobile Access の CLI は、SMA/SRA 装置または SMA 500v Virtual Appliance の X0 インターフェースの設定のみに使用可能です。

26 Telnet または SSH で SMA/SRA 装置に入ることはできますか。

回答: いいえ。現行の SMA/SRA 装置ソフトウェアでは、Telnet または SSH を管理手段として使用することはサポートされていません (これを、装置がサポートしている Telnet および SSH プロキシと混同しないでください)。

27 ウェブ キャッシュ クリーナはどのような処理を実行しますか。

質問の答え: ウェブ キャッシュ クリーナは ActiveX ベースのアプレットであり、セッションの中で生成されたすべての一時ファイルの削除、履歴ブックマークの削除、およびセッションの中で生成されたすべての Cookie の削除を実行します。

28 ウェブ ブラウザを終了するときにウェブ キャッシュ クリーナが動作しないのはなぜですか。

質問の答え: ウェブ キャッシュ クリーナを実行するためには、「**ログアウト**」を選択する必要があります。他の方法でウェブ ブラウザを閉じた場合は、ウェブ キャッシュ クリーナは実行されません。

29 「設定ファイルの暗号化」チェックボックスにはどのような機能がありますか。

質問の答え: この設定によって設定ファイルが暗号化されるため、ファイルがエクスポートされるときに、許可されていないソースはこれを読み取ることができません。暗号化されても、ファイルを SMA/SRA 装置 (または代替装置) にロードし直して復号化することはできます。このボックスがオフの場合は、エクスポートされる設定ファイルはクリアテキストであり、誰でもこれを読み取ることができます。

30 「設定の保存」ボタンにはどのような機能がありますか。

質問の答え: 既定では、プログラミングへの変更が行われるたびに、設定は SMA/SRA 装置に自動的に保存されますが、必要に応じてこれを無効にすることができます。これが無効の場合、保存されていない装置へのすべての変更は失われます。この機能は、変更によって装置がロックしたり、ネットワークから切断される可能性がある場合に最も役立ちます。設定が即時に保存されなければ、装置の電源を入れ直すことによって、変更を行う前の状態に戻すことができます。

31 「バックアップの作成」ボタンにはどのような機能がありますか。

質問の答え: この機能によって、ファームウェアと設定のバックアップ スナップショットを、管理インターフェースまたはセーフモードから復元できる特殊ファイルに作成できます。新しいソフトウェアをロードしたり、装置のプログラミングに大きな変更を加えたりする前には、SonicWall Inc. はシステムのバックアップを作成することを強くお勧めします。

32 “セーフモード”とは何ですか。

質問の答え: セーフモードは SMA/SRA 装置の機能であり、管理者はこの機能により、ソフトウェア イメージ ビルドを切り替えたり、ソフトウェア イメージに問題が生じたときに旧バージョンに戻すことができます。ソフトウェア イメージが壊れた場合、装置は特別なインターフェース モードで起動され、管理者は起動するバージョンを選択するか、またはソフトウェア イメージの新しいバージョンをロードできます。

33 セーフモード メニューにアクセスするにはどうすればよいですか。

質問の答え: 緊急時には、SMA/SRA 装置の**リセット** (SMA/SRA 装置の前面にある小さなピンホール ボタン) を、テスト LED が黄色で点滅するまで 12 ～ 14 秒間押すことで、セーフモード メニューにアクセスできます。SMA/SRA 装置のセーフモード メニューが起動されたら、ワークステーションに 192.168.200.x サブネット内の 192.168.200.100 のような一時 IP アドレスを割り当て、それを SMA/SRA 装置の X0 インターフェースに接続します。次に、ウェブ ブラウザ (マイクロソフト IE6.x 以上、Mozilla 1.4 以上) を使用して、装置の既定の IP アドレス 192.168.200.1 で特別なセーフモード GUI にアクセスします。以前に保存したバックアップ スナップショットを使用して装置を起動したり、「**新しいソフトウェア イメージのアップロード**」でソフトウェアの新バージョンをアップロードしたりできます。

34 ポータル ページの色を変更できますか。

回答: 現行ではサポートされていませんが、将来のソフトウェア リリースでサポートすることが計画されています。

35 どのような認証方式がサポートされていますか。

質問の答え: ローカル データベース、RADIUS、アクティブ ディレクトリ、および LDAP がサポートされています。

36 認証方式としてアクティブ ディレクトリを使用するように SMA/SRA 装置を設定したのですが、非常に奇妙なエラー メッセージが表示され、正しく動作しません。なぜでしょうか。

質問の答え: 装置はお互いの時間が正確に同期している必要があり、そうでなければ認証プロセスは失敗します。SMA/SRA 装置とアクティブ ディレクトリ サーバが両方とも NTP を使用して内部クロックを同期させていることを確認してください。

37 FTP ブックマークを作成しましたが、アクセスするとファイル名が文字化けします。なぜでしょう。

回答: Windows ベースの FTP サーバを使用している場合は、ディレクトリの表示スタイルを “MS-DOS”から“UNIX”に変更する必要があります。

38 VNC クライアントはどこで入手できますか。

質問の答え: SonicWall Inc. は、RealVNC について詳細なテストを行いました。これは、次からダウンロードできます。

http://www.realvnc.com/download.html

39 GMS または Analyzer で SRA 4600/1600 装置は完全にサポートされていますか。

回答: はい。

40 SMA/SRA 装置はプリンタ マッピングをサポートしますか。

回答: はい。これは ActiveX ベースの RDP クライアントでのみサポートされます。この機能を利用するには、最初にマイクロソフト ターミナル サーバ RDP コネクタを有効にする必要があります。アクセスするターミナル サーバに、接続プリンタのドライバ ソフトウェアをインストールすることが必要になる場合もあります。

41 SMA/SRA 装置をワイヤレスで統合できますか。

質問の答え: はい。Elsevier 〈http://www.elsevierdirect.com/〉 を通して入手可能な『*SonicWall Inc. Secure Wireless Networks Integrated Solutions Guide*』 を参照してください。

42 SMA/SRA 装置の任意のインターフェース IP アドレスで装置を管理できますか。

質問の答え: はい。任意のインターフェース IP アドレスで装置を管理できます。

43 特定のアクティブ ディレクトリ ユーザにのみ SMA/SRA 装置へのログインを許可することはできますか。

回答: はい。「**ユーザ > ローカル グループ**」ページで認証に使用するアクティブ ディレクトリ ドメインに属するグループを編集し、「**AD グループ**」タブで 1 つ以上の AD グループを追加します。

44 HTTP(S) プロキシはフル バージョンのアウトルック ウェブ アクセス (OWA プレミアム) をサポートしていますか。

回答: はい。

45 RDP セッションが頻繁に切断されるのはなぜですか。

質問の答え: SMA/SRA 装置、およびエンドポイント クライアントと接続先サーバの間に設置されている装置の、セッション タイムアウトと接続タイムアウトを調整してみてください。SMA/SRA 装置がファイアウォールの背後にある場合は、TCP タイムアウトを大きめに調整し、断片化を有効にしてください。

46 ブックマーク セクションで提供されているサービス以外に独自のブックマーク用サービスを作成できますか。

回答: 現行のソフトウェアではサポートされていませんが、将来のソフトウェア リリースでサポートされる可能性はあります。

47 ファイル共有コンポーネントでネットワーク上のすべてのサーバが表示されないのはなぜですか。

回答: CIFS 閲覧プロトコルは閲覧リストがサーバのバッファ サイズで制限されます。これらの閲覧リストには、ワークグループ内のホストの名前やホストからエクスポートされた共有の名前が含まれています。バッファ サイズはサーバ ソフトウェアに依存します。ウィンドウズ パーソナル ファイアウォールはアクセスを許可するように設定されていてもファイル共有で問題を起こすことが知られています。可能なら、どちらかの側にある該当ソフトウェアを無効にしてから再度テストしてみてください。

48 SMA/SRA 装置が Radius トラフィックのために使用しているポートは何ですか。

回答: ポート 1812 です。

49 SMA/SRA 装置は、同じユーザ アカウントによる同時ログインをサポートしていますか。

質問の答え: はい。ポータル レイアウトで、「多重ログインを禁止する」オプションをオンまたはオフにできます。このボックスがオフの場合、ユーザは同じユーザ名とパスワードを使用して同時にログインできます。

50 SMA/SRA 装置は NT LAN Manager (NTLM) 認証をサポートしていますか。

回答: 番号

51 ウィンドウズ認証が有効な場合に、ウェブ ブラウザに接続できません。接続しようとすると、次のエラー メッセージが表示されます: “ターゲットのウェブ サーバで SMA/SRA を通じてサポート対象外の HTTP(S) 認証方式が使用されています。現在サポートされているのは基本認証とダイジェスト認証方式だけです。”管理者に相談してください。”- なぜですか。

質問の答え: SRA 3.5 以前のリリースでは、HTTP プロキシは Windows 認証 (以前の名称は NTLM) をサポートしていません。基本認証のみがサポートされています。

52 Java サービス (Telnet や SSH など) がプロキシ サーバ経由で機能しないのはなぜですか。

回答: 開始された Java サービスは、プロキシ サーバを使用しません。トランザクションは SMA/SRA 装置で直接実行されます。

53 サービス ブックマークのポート オプションがありません。既定と違うポートにあるとどうなりますか。

回答: IP アドレス ボックスに、HTTP、HTTPS、Telnet、Java、および VNC の“IP アドレス:ポート ID”ペアを指定できます。

54 ブックマークでウェブ サーバ上のディレクトリをポイントするにはどうすればよいですか。

質問の答え: IP アドレス ボックスにIP/mydirectory/ というパスを追加します。

55 Telnet ブックマークを使用してマイクロソフト Telnet サーバにアクセスするときに、ユーザ名を入力できないのはなぜですか。

質問の答え: 現在、装置ではこの機能はサポートされていません。

56 どのバージョンの Citrix がサポートされていますか。

回答: Citrix ポータル ブックマークは、Citrix ウェブ インターフェースを通じて以下の Citrix アプリケーション仮想化プラットフォームで使用できることが検証されています。

サーバ:

- XenApp 7.6 (HTML 5 と ActiveX のみ)
- XenApp 6.5
- XenApp 6.0
- XenApp 5.0

クライアント:

- Receiver for Windows 4.2、4.1、または 4.0
- Receiver for Java 10.1.006
- XenApp Web Plugin バージョン 14.2、14.1、14.0

Citrix の実行に Java を必要とするブラウザでは、Sun Java 1.6.0_10 以上が必要です。

57 どのようなアプリケーションに対してアプリケーション オフローダの使用がサポートされていますか。

回答: アプリケーション オフローダは、HTTP/HTTPS を使うどのようなアプリケーションもサポートします。SMA/SRA では、ウェブ サービスを使うアプリケーションに対するサポートが制限され、HTTP 内にラップされた非 HTTP プロトコルはサポートされません。

アプリケーション オフローダを使用する際の 1 つの鍵となる状況は、アプリケーションはハード コードされた自己参照 URL を含むべきではないということです。これらがある場合は、アプリケーション オフローダ プロキシは URL を書き換えます。ウェブ サイト開発は常に HTML 標準に従うわけではないので、これらの URL を書き換える際にプロキシは最善の変換を行うことしかできません。ホスティング サーバが別の IP またはホスト名に移動するときは常にコンテンツ開発者がウェブ ページを編集する必要があるため、ウェブ サイトの開発時にハード コードされた、自己参照 URL の指定は推奨されません。

例えば、バックエンド アプリケーションが以下のように URL 内にハードコードされた IP とスキーマを持つ場合、アプリケーション オフローダは URL を書き換える必要が発生します。

<a href="http://1.1.1.1/doAction.cgi?test=foo">

これはアプリケーション オフローダ ポータルの「**自己参照 URL の URL 書き換えを有効化する**」設定を有効にすることで実行可能ですが、ウェブ アプリケーションがどのように開発されたかによって、必ずしもすべての URL を書き換えることはできない場合があります(この制限は通常、リバース プロキシ モードを用いる他の WAF/SMA ベンダと同様です)。

58 SSHv2 はサポートされていますか。

回答: はい。サポートされています。

59 グローバルな「すべて拒否」ポリシーを作成する必要がありますか。

質問の答え: はい。SonicWall Inc. では、管理者が、信頼済みホストへのアクセスのみを許可するグローバルな「すべて拒否」ポリシーを設定することを推奨します。これによって、Secure Mobile Access から悪意のあるホストへの発信要求を防御できます。グローバルな「すべて拒否」ポリシーの設定方法については、ポリシーの追加 (249 ページ) を参照してください。

G

コマンド ライン インターフェースの使用

コマンド ライン インターフェース (CLI) は、コマンドを入力することで指定したタスクを実行する、コンピュータ オペレーティング システムやソフトウェアと情報を交換するためのテキストだけの機構です。基本ネットワーキングをコンソールから設定する必要がある SMA 500v Virtual Appliance の配備において、CLI は重要な役割を担います。CLI は SRA 4600/1600 装置でもサポートされます。

SMA/SRA 物理装置には、接続するためにクライアント ネットワーク設定の再構成を必要とする既定の IP アドレスとネットワーク設定があり、既存の VMWare 仮想環境内でこのネットワーク設定が SMA/SRA 装置の既定値と競合する可能性があります。CLI ユーティリティは、仮想装置の配備の際にネットワーク設定の基本構成を許可することで、これを修正します。

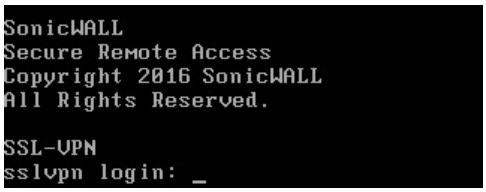
メモ: SonicWall Inc. Secure Mobile Access の CLI は、SRA 4600/1600 または SMA 500v Virtual Appliance の X0 インターフェースの設定のみに使用可能です。

メモ: シリアル接続または SSH 管理セッションで CLI を使用するには、ターミナル エミュレーション アプリケーション (Tera Term など) または SSH クライアント アプリケーション (PuTTY など) を使用する必要があります。環境に適した無料のターミナル エミュレータはインターネットで見つけることができます。

SMA/SRA 物理装置では、コンピュータをシリアル ポートに接続することでコンソールにアクセスします。以下の設定を使います。

- ボー: 115200
- データ ビット: 8
- パリティ: なし
- ストップ ビット: 1
- フロー制御なし

仮想装置では、ファームウェアの起動が完了した後で以下のログイン プロンプトが表示されます。



以下の例では、ユーザによって入力されたテキストを示すためにユーザの入力は太字で強調されています。

CLI にアクセスするために、**admin** としてログインします。パスワードは装置上で設定された admin アカウントのパスワードと同じです。既定では **password** です。

```
sslvpn login: admin
パスワード: パスワード
```

間違ったパスワードを入力すると、再度ログイン プロンプトが表示されます。正しいパスワードを入力すると、CLI が開始されます。

物理装置および仮想装置に対し、下記の例のようにメイン メニューのほかに、基本的なシステム情報とネットワーク設定が表示されます。

```
System Information
Model:              SRA 4600
Serial Number:      C0EAE42CB2EC
Version:             8.5.0.0-12sv
Safemode Version:   2.0.0.10
CPU (Utilization):  1.66 GHz Intel Atom Dual Core Processor (0%)
Total Memory:       2.0 GB RAM (30%), 1GB Flash
System Time:        2016/06/28 15:25:51
Up Time:            12 Days 06:14:18
X0 IP Address:      10.5.255.171
X0 Subnet mask:     255.255.252.0
Default Gateway:    10.5.104.1 (X1)
Primary DNS:        10.5.48.13
Secondary DNS:      10.5.48.13
Hostname:           sslvpn171

Main Menu
1. Setup Wizard
2. Reboot
3. Restart SSL VPN Services
4. Logout
5. Save TSR to Flash
6. Display EULA

Press <Ctrl-c> at any time to cancel changes and logout.
Select a number (1-6):
```

いつでも **Ctrl-C** を押してログアウトして CLI を抜けてログイン プロンプトに戻ることができます。

メイン メニューには 4 つのセクションがあります。

1 **Setup Wizard** - このオプションは、基本ネットワーク設定を変更するための、簡素なウィザードを開始し、X0 IP アドレス、X0 サブネット マスク、デフォルト ゲートウェイ、プライマリおよびセカンダリ DNS、そしてホスト名の順に設定します。下記の CLI アウトプットは、各フィールドを変更した例を示します。

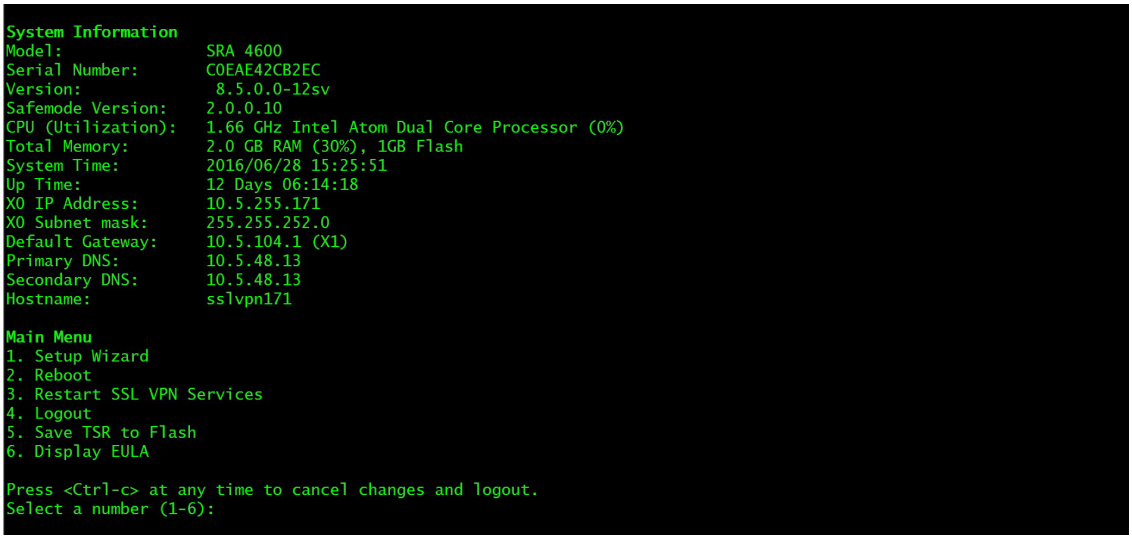
```
X0 IP Address (default 192.168.200.1): 192.168.200.201
X0 Subnet Mask (default 255.255.255.0): 255.255.0.0
Default Gateway (default 192.168.200.2): 192.168.200.1
プライマリ DNS: 10.50.128.52
Secondary DNS (optional, enter "none" to disable): 4.2.2.2
Hostname (default sslvpn): sslvpn

New Network Settings:
X0 IP Address:        192.168.200.201
X0 Subnet mask:       255.255.0.0
デフォルト ゲートウェイ:      192.168.200.1
プライマリ DNS:          10.50.128.52
セカンダリ DNS:        4.2.2.2
ホスト名:              sslvpn

Would you like to save these changes (y/n)?
```

フィールドに入力しないと、以前の値が保持され、1 つのフィールドのみ変更が許可されます。各フィールドが表示された後で、新しいネットワーク設定が表示され、変更を適用する前に再確認するように、ユーザに確認のメッセージが表示されます。下記は、変更を保存した場合の結果を示します。

```
Would you like to save these changes (y/n)? y
Saving changes...please wait....
```

```
Changes saved!
Press <Enter> to continue...
```

変更を保存した後で、**Enter** を押してシステム情報とネットワーク設定の表示する元の画面に戻り、変更が反映されていることを確認します。



変更を保存しなかった場合、下記のメッセージが表示され、Enter を押してシステム情報とネットワーク設定の表示する最初の画面に戻ります。

```
No changes have been made.
Press <Enter> to continue...
```

メモ：IP アドレスを変更する設定を適用した場合は、インターフェース設定が更新されるまで最大で 5 秒かかります。

2 **Reboot** - このオプションを選択すると、確認のプロンプトを表示してから再起動します。

再起動

```
Are you sure you want to reboot (y/n)?
```

3 **Restart SSL-VPN Services** - このオプションは確認のプロンプトを表示してから、ウェブ サーバおよび関連する Secure Mobile Access daemon サービスを再起動します。このコマンドは、**EasyAccessCtrl restart** コマンドを発行することと同じです。

SSL-VPN サービスの再起動

```
Are you sure you want to restart the SSL-VPN services (y/n)? y

Restarting SSL-VPN services...please wait.
Stopping SMM: [  OK  ]
Stopping Firebase :[  OK  ]
Stopping FTP Session:[  OK  ]
Stopping HTTPD: [  OK  ]
Cleaning Apache State: [  OK  ]
Stopping Graphd :[  OK  ]

Cleaning Temporary files........
Starting SMM: [  OK  ]
Starting firebase: [  OK  ]
Starting httpd: [  OK  ]
Starting ftpsession: [  OK  ]
Starting graphd: [  OK  ]
```

```
Restart completed...returning to main menu...
```

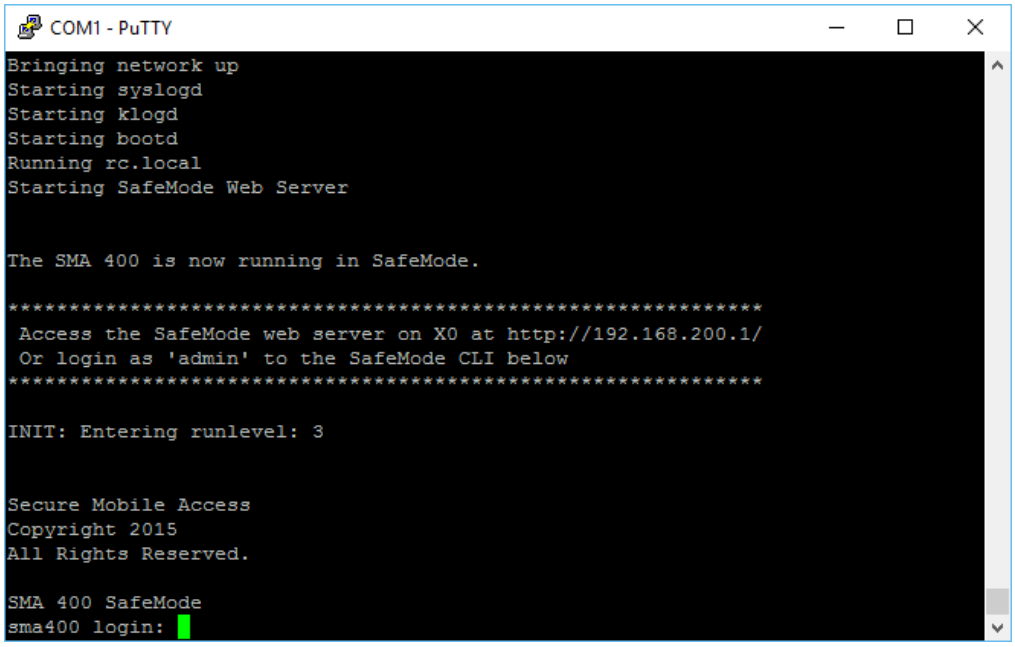
4 **Logout** - ログアウト オプションは CLI セッションを終了してログイン プロンプトに戻ります。

セーフモード

セーフモードは、コンピュータからファームウェアをアップロードし、装置を再起動することができる限定的なウェブ管理インターフェースです。

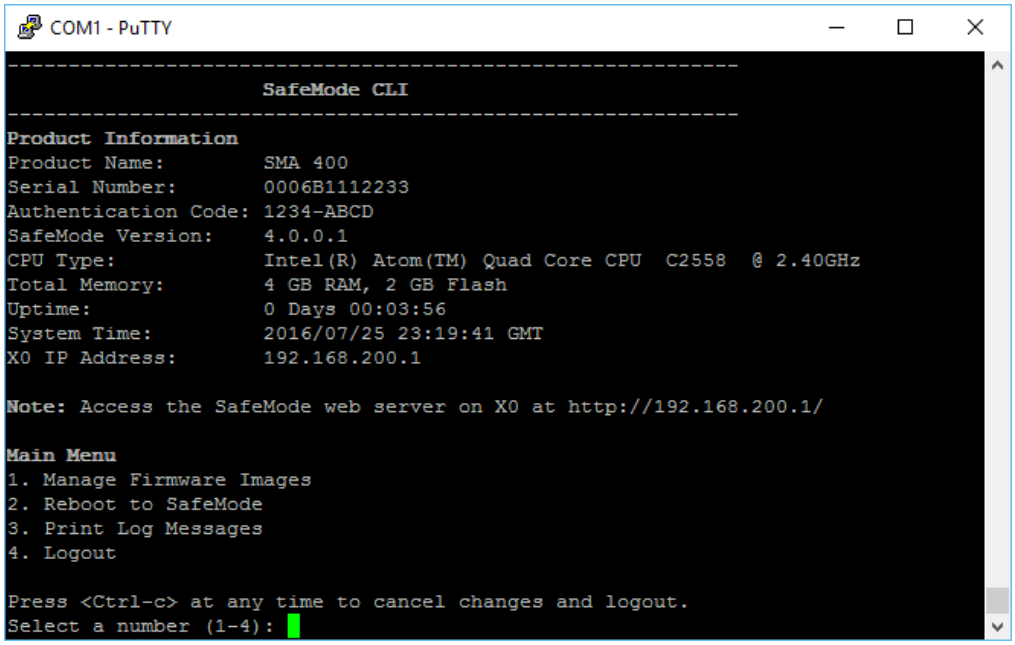
セーフモード機能を使用すると、「**システム > 設定**」ページで利用可能なものと同じ設定を含む簡素化された管理インターフェースを使って、不確実な設定状態から素早く回復できます。

セーフモード の CLI を起動するには、セーフモードのスイッチを押してセーフモードで再起動してから、**admin** としてログインします。パスワードは装置上で設定された admin アカウントのパスワードと同じです。既定では **password** です。

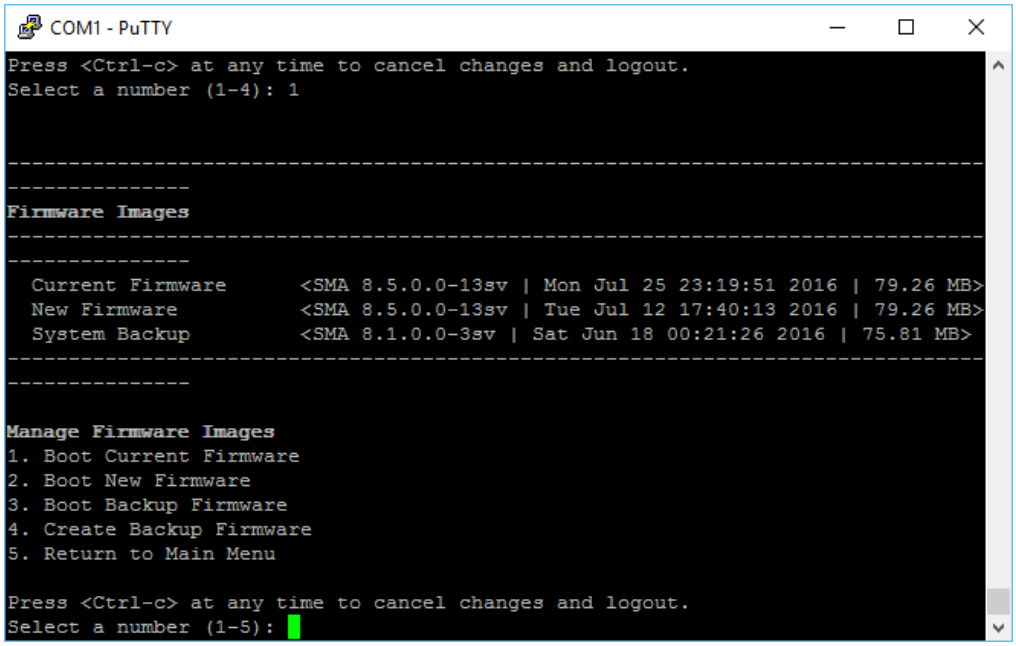


sma400 login: **admin**
パスワード: **パスワード**

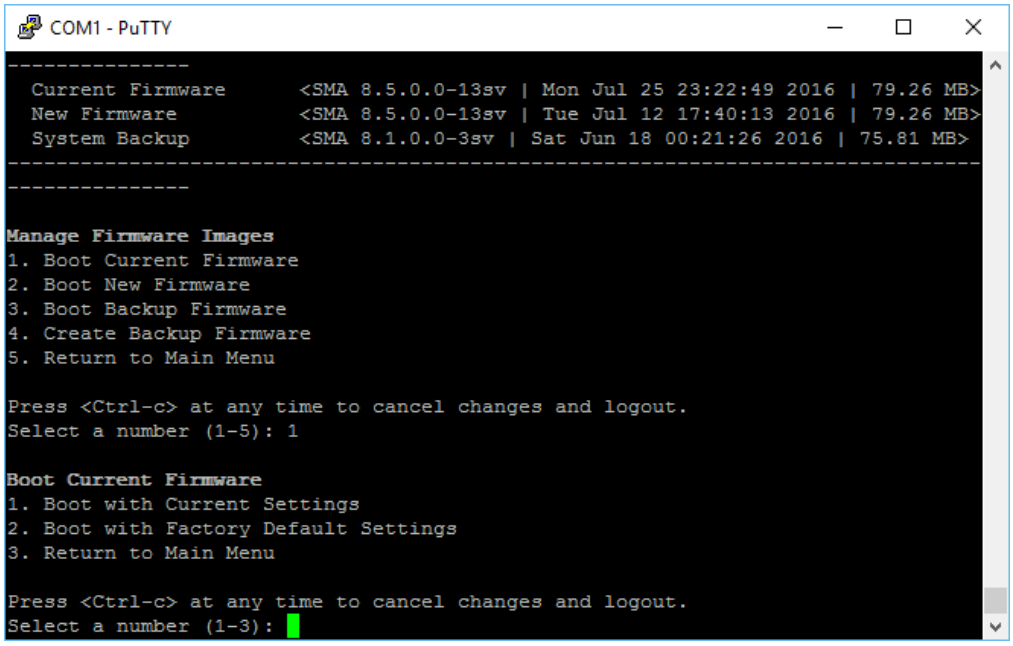
誤ったパスワードを入力すると、再度ログイン プロンプトが表示されます。正しいパスワードを入力すると、セーフモードの CLI が起動します。



番号が付けられたオプションが表示されます。オプションの機能は名前どおりです。実行するオプションの番号を選択します。最初のオプション (ファームウェア イメージを管理する) を使う場合は、1 を押します。次の画面が開き、他の 5 つのオプションが示されます。



他の 5 つのオプションの機能は名前どおりです。実行するオプションの番号を選択します。最初のオプション (現在のファームウェアで起動する) を使う場合は、1 を押します。次の画面が開き、他の 3 つのオプションが示されます。



他の 3 つのオプションの機能は名前どおりです。実行するオプションの番号を選択します。

ファイアウォールをセーフモードで再起動する手順については、使用する装置の『*導入ガイド*』を参照してください。

H

SMS 電子メール形式の使用

このセクションでは、世界各地の携帯電話事業者の SMS (ショート メッセージ サービス)形式リストを示します。ご使用の携帯電話事業者の形式を次のリストから見つけ、@ 記号より前の部分を自分の電話番号で置き換えてください。

メモ：これらの SMS 電子メール フォーマットは参考用です。これらの電子メール フォーマットは変更される可能性があります。SMS を使用する前に、サービス会社から追加的なサービスまたは情報を入手しなければならないこともあります。これらのフォーマットと、SMS のサービス、オプション、機能の詳細については、SMS を提供する会社に直接問い合わせてください。

携帯電話事業者による SMS 形式

携帯電話事業者	SMS 形式
3River Wireless	4085551212@sms.3rivers.net
AirTel	4085551212@airtelmail.com
AT&T Wireless	4085551212@mobile.att.net
Andhra Pradesh Airtel	4085551212@airtelap.com
Andhra Pradesh Idea Cellular	4085551212@ideacellular.net
Alltel PC	4085551212@message.alltel.com
Alltel	4085551212@alltelmessage.com
Arch Wireless	4085551212@archwireless.net
BeeLine GSM	4085551212@sms.beemail.ru
BeeLine (モスクワ)	4085551212@sms.gate.ru
Bell Canada	4085551212@txt.bellmobility.ca
Bell Canada	4085551212@bellmobility.ca
Bell Atlantic	4085551212@message.bam.com
Bell South	4085551212@sms.bellsouth.com
Bell South	4085551212@wireless.bellsouth.com
Bell South	4085551212@blsdcs.net
Bite GSM (リトアニア)	4085551212@sms.bite.lt
Bluegrass Cellular	4085551212@sms.bluecell.com
BPL mobile	4085551212@bplmobile.com
Celcom (マレーシア)	4085551212@sms.celcom.com.my
Cellular One	4085551212@mobile.celloneusa.com
Cellular One East Cost	4085551212@phone.cellone.net
Cellular One South West	4085551212@swmsg.com
Cellular One	4085551212@mobile.celloneusa.com
Cellular One	4085551212@cellularone.txtmsg.com

携帯電話事業者による SMS 形式 (続き)

携帯電話事業者	SMS 形式
Cellular One	4085551212@cellularone.textmsg.com
Cellular South	4085551212@csouth1.com
CenturyTel	4085551212@messaging.centurytel.net
Cingular	4085551212@mobile.mycingular.net
Cingular Wireless	4085551212@mycingular.textmsg.com
Comcast	4085551212@comcastpcs.textmsg.com
CZECH EuroTel	4085551212@sms.eurotel.cz
CZECH Paegas	4085551212@sms.paegas.cz
Chennai Skycell/Airtel	4085551212@airtelchennai.com
Chennai RPG Cellular	4085551212@rpgmail.net
Comviq GSM Sweden	4085551212@sms.comviq.se
Corr Wireless Communications	4085551212@corrwireless.net
D1 De TeMobil	4085551212@t-d1-sms.de
D2 Mannesmann Mobilefunk	4085551212@d2-message.de
DT T-Mobile	4085551212@t-mobile-sms.de
Delhi Airtel	4085551212@airtelmail.com
Delhi Hutch	4085551212@delhi.hutch.co.in
Dobson-Cellular One	4085551212@mobile.cellularone.com
Dobson Cellular Systems	4085551212@mobile.dobson.net
Edge Wireless	4085551212@sms.edgewireless.com
E-Plus (ドイツ)	4085551212 @eplus.de
EMT	4085551212@sms.emt.ee
Eurotel (チェコ)	4085551212@sms.eurotel.cz
Europolitan Sweden	4085551212@europolitan.se
Escotel	4085551212@escotelmobile.com
Estonia EMT	4085551212@sms-m.emt.ee
Estonia RLE	4085551212@rle.ee
Estonia Q GSM	4085551212@qgsm.ee
Estonia Mobil Telephone	4085551212@sms.emt.ee
Fido	4085551212@fido.ca
Georgea geocell	4085551212@sms.ge
Goa BPLMobil	4085551212@bplmobile.com
Golden Telecom	4085551212@sms.goldentele.com
Golden Telecom (ウクライナのキエフのみ)	4085551212@sms.gt.kiev.ua
GTE	4085551212@messagealert.com
GTE	4085551212@airmessage.net
Gujarat Idea	4085551212@ideacellular.net
Gujarat Airtel	4085551212@airtelmail.com
Gujarat Celforce/Fascel	4085551212@celforce.com
Goa Airtel	4085551212@airtelmail.com

携帯電話事業者による SMS 形式 (続き)

携帯電話事業者	SMS 形式
Goa BPLMobil	4085551212@bplmobile.com
Goa Idea Cellular	4085551212@ideacellular.net
Haryana Airtel	4085551212@airtelmail.com
Haryana Escotel	4085551212@escotelmobile.com
Himachal Pradesh Airtel	4085551212@airtelmail.com
Houston Cellular	4085551212@text.houstoncellular.net
Hungary Pannon GSM	4085551212@sms.pgsm.hu
Idea Cellular	4085551212@ideacellular.net
Inland Cellular Telephone	4085551212@inlandlink.com
Israel Orange IL	4085551212- @shiny.co.il
Karnataka Airtel	4085551212@airtelkk.com
Kerala Airtel	4085551212@airtelmail.com
Kerala Escotel	4085551212@escotelmobile.com
Kerala BPL Mobile	4085551212@bplmobile.com
Kyivstar (ウクライナのキエフのみ)	4085551212@sms.kyivstar.net
Kyivstar	4085551212@smsmail.lmt.lv
Kolkata Airtel	4085551212@airtelkol.com
Latvia Baltcom GSM	4085551212@sms.baltcom.lv
Latvia TELE2	4085551212@sms.tele2.lv
LMT	4085551212@smsmail.lmt.lv
Madhya Pradesh Airtel	4085551212@airtelmail.com
Maharashtra Idea Cellular	4085551212@ideacellular.net
MCI Phone	408555121 @mci.com
Meteor	4085551212@mymeteor.ie
Metro PCS	4085551212@mymetropcs.com
Metro PCS	4085551212@metorpcs.sms.us
MiWorld	4085551212@m1.com.sg
Mobileone	4085551212@m1.com.sg
Mobilecomm	4085551212@mobilecomm.net
Mobtel	4085551212@mobtel.co.yu
Mobitel (タンザニア)	4085551212@sms.co.tz
Mobistar Belgium	4085551212@mobistar.be
Mobility Bermuda	4085551212@ml.bm
Movistar (スペイン)	4085551212@correo.movistar.net
Maharashtra Airtel	4085551212@airtelmail.com
Maharashtra BPL Mobile	4085551212@bplmobile.com
Manitoba Telecom Systems	4085551212@text.mtsmobility
Mumbai Orange	4085551212@orangemail.co.in
MTS (ロシア)	4085551212@sms.mts.ru
MTC	4085551212@sms.mts.ru

携帯電話事業者による SMS 形式 (続き)

携帯電話事業者	SMS 形式
Mumbai BPL Mobile	4085551212@bplmobile.com
MTN (南アフリカのみ)	4085551212@sms.co.za
MiWorld (シンガポール)	4085551212@m1.com.sg
NBTel	4085551212@wirefree.informe.ca
Netcom GSM (ノルウェー)	4085551212@sms.netcom.no
Nextel	4085551212@messaging.nextel.com
Nextel	4085551212@nextel.com.br
NPI Wireless	4085551212@npiwireless.com
Ntelos	4085551212number@pcs.ntelos.com
One Connect Austria	4085551212@onemail.at
OnlineBeep	4085551212@onlinebeep.net
Omnipoint	4085551212@omnipointpcs.com
Optimus (ポルトガル)	4085551212@sms.optimus.pt
Orange - NL/Dutchtone	4085551212@sms.orange.nl
Orange	4085551212@orange.net
Oskar	4085551212@mujoskar.cz
Pacific Bell	4085551212@pacbellpcs.net
PCS One	4085551212@pcsone.net
Pioneer/Enid Cellular	4085551212@msg.pioneerenidcellular.com
PlusGSM (ポーランドのみ)	4085551212@text.plusgsm.pl
P&T Luxembourg	4085551212@sms.luxgsm.lu
Poland PLUS GSM	4085551212@text.plusgsm.pl
Primco	4085551212@primeco@textmsg.com
Primtel	4085551212@sms.primtel.ru
Public Service Cellular	4085551212@sms.pscel.com
Punjab Airtel	4085551212@airtelmail.com
Qwest	4085551212@qwestmp.com
Riga LMT	4085551212@smsmail.lmt.lv
Rogers AT&T Wireless	4085551212@pcs.rogers.com
Safaricom	4085551212@safaricomsms.com
Satelindo GSM	4085551212@satelindogsm.com
Simobile (スロベニア)	4085551212@simobil.net
Sunrise Mobile	4085551212@mysunrise.ch
Sunrise Mobile	4085551212@freesurf.ch
SFR France	4085551212@sfr.fr
SCS-900	4085551212@scs-900.ru
Southwestern Bell	4085551212@email.swbw.com
Sonofon Denmark	4085551212@note.sonofon.dk
Sprint PCS	4085551212@messaging.sprintpcs.com
Sprint	4085551212@sprintpaging.com

携帯電話事業者による SMS 形式 (続き)

携帯電話事業者	SMS 形式
Swisscom	4085551212@bluewin.ch
Swisscom	4085551212@bluemail.ch
Telecom Italia Mobile (イタリア)	4085551212@posta.tim.it
Telenor Mobil Norway	4085551212@mobilpost.com
Telecel (ポルトガル)	4085551212@sms.telecel.pt
Tele2	4085551212@sms.tele2.lv
Tele Danmark Mobil	4085551212@sms.tdk.dk
Telus	4085551212@msg.telus.com
Telenor	4085551212@mobilpost.no
Telia Denmark	4085551212@gsm1800.telia.dk
TIM	4085551212 @timnet.com
TMN (ポルトガル)	4085551212@mail.tmn.pt
T-Mobile Austria	4085551212@sms.t-mobile.at
T-Mobile Germany	4085551212@t-d1-sms.de
T-Mobile UK	4085551212@t-mobile.uk.net
T-Mobile USA	4085551212@tmomail.net
Triton	4085551212@tms.suncom.com
Tamil Nadu Aircel	4085551212@airsms.com
Tamil Nadu BPL Mobile	4085551212 @bplmobile.com
UMC GSM	4085551212@sms.umc.com.ua
Unicel	4085551212@utext.com
Uraltel	4085551212@sms.uraltel.ru
US Cellular	4085551212@email.uscc.net
US West	4085551212@uswestdatamail.com
Uttar Pradesh (West) Escotel	4085551212@escotelmobile.com
Verizon	4085551212@vtext.com
Verizon PCS	4085551212@myvzw.com
Virgin Mobile	4085551212@vmobl.com
Vodafone Omnitel (イタリア)	4085551212@vizzavi.it
Vodafone Italy	4085551212@sms.vodafone.it
Vodafone Japan	4085551212@pc.vodafone.ne.j
Vodafone Japan	4085551212@h.vodafone.ne.jp
Vodafone Japan	4085551212@t.vodafone.ne.jp
Vodafone Spain	4085551212@vodafone.es
Vodafone UK	4085551212@vodafone.net
West Central Wireless	4085551212@sms.wcc.net
Western Wireless	4085551212@cellularonewest.com

サポート情報

この付録は以下のセクションで構成されます。

GNU General Public License(GPL)のソース コード

SonicWall Inc. は、コンピュータで読み取り可能な GPL オープン ソースのコピーを CD でご提供します。コンピュータで読み取り可能なコピーを入手するには、"SonicWall, Inc." を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request
SonicWall, Inc. Attn: Jennifer Anderson

1033 McCarthy Blvd
Milpitas, CA 95035

ハードウェア限定保証

すべての SonicWall Inc. アプライアンス製品には、1 年間のハードウェア限定保証が付属しています。保証期間内に部品が故障した場合は、代替部品を提供いたします。お使いの製品の保証の詳細については、次の保証情報のページをご覧ください。
https://www.sonicwall.com/ja-jp/support/essentials/support-offerings

SonicWall Inc. は、お客様への納品日 (ただし、SonicWall Inc. から最初に出荷されて 90 日を超えない範囲とする) から 12 ヶ月の期間にわたって、通常の使用下で製品に欠陥が生じないことを保証します。この保証は、製品の原エンドユーザにのみ適用され、その権利を他に譲渡することはできません。この限定保証のもとで SonicWall Inc. およびその製造業者の法的責任とお客様への唯一限定的な賠償は、代替製品の出荷によって全うされるものとします。SonicWall Inc. の判断により、代替製品は、故障した製品と同等もしくは同等以上の性能/機能の製品となります。また、未使用品に限定されません。この限定保証に基づく SonicWall Inc. の責任は、SonicWall Inc. の当時最新のサポート サービス ポリシーの条項に従って欠陥製品を返却したとき生じます。

製品に異常な電気的ストレスを加えた場合、事故や誤用により製品を破損した場合、SonicWall Inc. に正式の許可を受けずに製品に変更を加えた場合、この保証は適用されません。

保証に関する免責事項。この保証で指定されている行為、明示的または暗黙的に示したすべての条件、表現、保証(暗黙的保証や販売条件を無制限に含む)を例外として、特定の目的、法遵守、十分な品質、または取引、法律、利用、商習慣による要件を満たすための行為は、この条項によって該当する法律で最大限許容される程度に除外されます。暗黙の保証を超えない範囲で、保証は当該保証期間の範囲に限定されます。関係国の法律や管轄裁判所が暗黙の保証への制限を認めていない場合、上記

の制限が適用されないこともあります。この保証は特定の法的権利を与えるものであって、管轄裁判所によってはそれ以外の権利が与えられることもあります。この権利放棄・免責条項は上記に明示された保証がその本来の目的を果たせない場合にも適用されるものとします。

責任に関する免責事項。SonicWall では、上記の限定保証に記載されているとおり、交換用製品の発送についてのみ責任を負います。SonicWall およびその製造業者は、本製品を使用したため、または使用できなかったために生じた損失、業務の中断、情報の消失、あるいはそれによって直接または間接に生じた偶発的、懲罰的損害について、SonicWall またはその製造業者が損害の可能性を忠告したかどうかに関係なく、本製品の使用または不使用によって生じる一切の法的責任を免れるものとします。SonicWall およびその製造業者は、いかなる場合にもお客様に対して、契約上の不法行為や、お客様が支払った価格を超える責任を負わないものとします。以上の制限は、上記の保証書がその本来の目的を果たせない場合にも適用されるものとします。関係国の法律や管轄裁判所が間接または偶発の損害に対する制限・免責を認めていない場合、上記の制限が適用されないこともあります。

エンド ユーザー ライセンス契約

本製品をご利用になる前に本契約を熟読して下さい。本製品をダウンロード、インストール、又は利用することにより、貴方 (貴社) は本契約の条件を承諾しこれに同意します。米国外での提供については、HTTPS://WWW.SONICWALL.COM/JA-JP/LEGAL/EUPA.ASPX にアクセスして、該当する地域のエンドユーザ製品契約をご覧ください。本契約に同意しない場合は、本製品のダウンロード、インストール、又は利用はお控え下さい。

This SonicWall End User Product Agreement (the ***"Agreement"***) is made between you, the Customer ("Customer" or "You") and the Provider, as defined below.

1 **Definitions.** Capitalized terms not defined in context shall have the meanings assigned to them below:

   a ***"Affiliate"*** means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

   b ***"Appliance"*** means a computer hardware product upon which Software is pre-installed and delivered.

   c ***"Documentation"*** means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

   d ***"Maintenance Services"*** means Provider's maintenance and support offering for the Products as identified in the *Maintenance Services* Section below.

   e ***"Partner"*** means the reseller or distributor that is under contract with Provider or another Partner and is authorized via such contract to resell the Products and/or Maintenance Services.

   f ***"Provider"*** means, (i) for the US and Taiwan, SonicWall Inc., with its principal place of business located at 4 Polaris Way, Aliso Viejo, CA 92656 USA and (ii) for Europe, Middle East, Africa, and Asia (other than Taiwan) SonicWall International Ltd. City Gate Park Mahon, Cork, Ireland.

   g ***"Products"*** means the Software and Appliance(s) provided to Customer under this Agreement.

   h ***"Software"*** means the object code version of the software that is delivered on the Appliance and any other software that is later provided to Customer as well as any new versions and releases to such software that are made available to Customer pursuant to this Agreement, and all copies of the foregoing.

2 **Software License**.

   a **General.** Subject to the terms of this Agreement, Provider grants to Customer, and Customer accepts from Provider, a non-exclusive, non-transferable (except as otherwise set forth herein) and non-sublicensable license to access and use the quantities of each item of Software

purchased from Provider or a Partner within the parameters of the license type ("**License Type(s)**") described below in the quantities purchased (***"License"***). Except for MSP Licenses (as defined below), Customer shall only use the Software to support the internal business operations of itself and its worldwide Affiliates.

b **License Types**. The License Type for the Software initially delivered on the Appliance is "**per Appliance**". Software licensed per Appliance may be used only on the Appliance on which it is delivered, but without any other quantitative limitations. Software that is purchased on a subscription, or periodic basis is licensed by User or by Managed Node. A "**User**" is each person with a unique login identity to the Software. A "**Managed Node**" is any object managed by the Software including, but not limited to firewalls, devices, and other items sold by Provider.

c **Software as a Service** When Customer purchases a right to access and use Software installed on equipment operated by Provider or its suppliers (the ***"SaaS Software"***), (i) the License for such SaaS Software shall be granted for the duration of the term stated in the order (the ***"SaaS Term"***), as such SaaS Term may be extended by automatic or agreed upon renewals, and (ii) the terms set forth in the *SaaS Provisions* Section of this Agreement shall apply to all access to and use of such Software. If any item of Software to be installed on Customer's equipment is provided in connection with SaaS Software, the License duration for such Software shall be for the corresponding SaaS Term, and Customer shall promptly install any updates to such Software as may be provided by Provider.

d MSP License.

"Management Services" include, without limitation, application, operating system, and database implementation, performance tuning, and maintenance services provided by Customer to its customers (each, a ***"Client"***) where Customer installs copies of the Software on its Clients' equipment or provides its Clients access to the Products. Customer shall be granted a License to use the Software and the associated Documentation to provide Management Services (the ***"MSP License"***). Each MSP License is governed by the terms of this Agreement and any additional terms agreed to by the parties.

If the Product is to be used by Customer as a managed service provider, then Customer shall ensure that (i) Customer makes no representations or warranties related to the Products in excess of SonicWall's representations or warranties contained in this Agreement, (ii) each Client only uses the Products and Documentation as part of the Management Services provided to it by Customer, (iii) such use is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the *Export* Section of this Agreement, and (iv) each Client cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent. At the conclusion of any Management Services engagement with a Client, Customer shall promptly remove any Appliance and Software installed on its Client's computer equipment or require the Client to do the same. Customer agrees that it shall be jointly and severally liable to Provider for the acts and omissions of its Clients in connection with their use of the Software and Documentation and shall, at its expense, defend Provider against any action, suit, or claim brought against Provider by a Client in connection with or related to Customer's Management Services and pay any final judgments or settlements as well as Provider's expenses in connection with such action, suit, or claim.

e **Evaluation/Beta License.** If Software is obtained from Provider for evaluation purposes or in beta form, Customer shall be granted a License to use such Software and the associated Documentation solely for Customer's own non-production, internal evaluation purposes (an ***"Evaluation License"***). Each Evaluation License shall be granted for an evaluation period of up to thirty (30) days beginning (i) five (5) days after the Appliance is shipped or (ii) from the date that access is granted to the beta Software or the SaaS Software, plus any extensions granted by Provider in writing (the "Evaluation Period"). There is no fee for an Evaluation License during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Beta Software licensed hereunder may include pre-release features and

capabilities which may not be available in SonicWall's generally available commercial versions of the Software. SonicWall retains the right during the term to modify, revise, or remove SonicWall beta software from Customer's premises. Customer acknowledges that SonicWall owns all modifications, derivative works, changes, expansions or improvements to beta software, as well as all reports, testing data or results, feedback, benchmarking or other analysis completed in whole or in part in conjunction with usage of beta software. NOTWITHSTANDING ANYTHING OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER UNDERSTANDS AND AGREES THAT EVALUATION AND BETA SOFTWARE IS PROVIDED "AS IS", WHERE IS, WITH ALL FAULTS AND THAT SONICWALL DOES NOT PROVIDE A WARRANTY OR MAINTENANCE SERVICES FOR EVALUATION OR BETA LICENSES, AND SONICWALL BEARS NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION OR BETA SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT TO CUSTOMER FOR SUCH SOFTWARE. BETA SOFTWARE MAY CONTAIN DEFECTS AND A PRIMARY PURPOSE OF LICENSING THE BETA SOFTWARE IS TO OBTAIN FEEDBACK ON THE SOFTWARE'S PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE BETA SOFTWARE AND/OR ACCOMPANYING MATERIALS.

f **Use by Third Parties.** Customer may allow its services vendors and contractors (each, a "**Third Party User**") to access and use the Products and Documentation provided to Customer hereunder solely for purposes of providing services to Customer, provided that Customer ensures that (i) the Third Party User's access to or use of the Products and Documentation is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the *Export* Section, (ii) the Third Party User cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent, and (iii) the Third Party Users promptly removes any Software installed on its computer equipment upon the completion of the Third Party's need to access or use the Products as permitted by this Section. Customer agrees that it shall be liable to Provider for those acts and omissions of its Third Party Users which, if done or not done by Customer, would be a breach of this Agreement.

3 **Restrictions.** Customer may not reverse engineer, decompile, disassemble, or attempt to discover or modify in any way the underlying source code of the Software, or any part thereof unless and to the extent (a) such restrictions are prohibited by applicable law and (b) Customer has requested interoperability information in writing from Provider and Provider has not provided such information in a timely manner. In addition, Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Products, Documentation or any part thereof, (ii) resell, sublicense or distribute the Products or Documentation, (iii) provide, make available to, or permit use of the Products, in whole or in part, by any third party (except as expressly set forth herein), (iv) use the Products or Documentation to create or enhance a competitive offering or for any other purpose which is competitive to Provider, (v) remove Software that was delivered on an Appliance from the Appliance on which it was delivered and load such Software onto a different appliance without Provider's prior written consent, or (vi) perform or fail to perform any other act which would result in a misappropriation or infringement of Provider's intellectual property rights in the Products or Documentation. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Notwithstanding anything otherwise set forth in this Agreement, the terms and restrictions set forth herein shall not prevent or restrict Customer from exercising additional or different rights to any open source software that may be contained in or provided with the Products in accordance with the applicable open source software licenses which shall be either included with the Products or made available to Customer upon request. Customer may not use any license keys or other license access devices not provided by Provider, including but not limited to "pirate keys", to install or access the Software.

4 **Proprietary Rights.** Customer understands and agrees that (i) the Products are protected by copyright and other intellectual property laws and treaties, (ii) Provider, its Affiliates and/or its licensors own the

copyright, and other intellectual property rights in the Products, (iii) the Software is licensed, and not sold, (iv) this Agreement does not grant Customer any rights to Provider's trademarks or service marks, and (v) Provider reserves any and all rights, implied or otherwise, which are not expressly granted to Customer in this Agreement.

5 **Title.** Provider, its Affiliates and/or its licensors own the title to all Software.

6 **Payment.** Customer agrees to pay to Provider (or, if applicable, the Partner) the fees specified in each order, including any applicable shipping fees. Customer will be invoiced promptly following delivery of the Products or prior to the commencement of any Renewal Maintenance Period and Customer shall make all payments due to Provider in full within thirty (30) days from the date of each invoice or such other period (if any) stated in an order. Provider reserves the right to charge Customer a late penalty of 1.5% per month (or the maximum rate permitted by law, whichever is the lesser) for any amounts payable to Provider by Customer that are not subject to a good faith dispute and that remain unpaid after the due date until such amount is paid.

7 **Taxes.** The fees stated in an order from Provider or a Partner may not include taxes. If Provider is required to pay sales, use, property, value-added or other taxes based on the Products or Maintenance Services provided under this Agreement or on Customer's use of Products or Maintenance Services, then such taxes shall be billed to and paid by Customer. This Section does not apply to taxes based on Provider's or a Partner's income.

8 **Termination.**

a This Agreement or the Licenses granted hereunder may be terminated (i) by mutual written agreement of Provider and Customer or (ii) by either party for a breach of this Agreement by the other party (or a Third Party User) that the breaching party fails to cure to the non-breaching party's reasonable satisfaction within thirty (30) days following its receipt of notice of the breach. Notwithstanding the foregoing, in the case of MSP Licenses, if Customer or its Client breaches this Agreement two (2) times in any twelve (12) consecutive month period, the breaching party shall not have a cure period for such breach and Provider may terminate this Agreement immediately upon providing written notice to the breaching party.

b Upon termination of this Agreement or expiration or termination of a License for any reason, all rights granted to Customer for the applicable Software shall immediately cease and Customer shall immediately: (i) cease using the applicable Software and Documentation, (ii) remove all copies, installations, and instances of the applicable Software from all Appliances, Customer computers and any other devices on which the Software was installed, and ensure that all applicable Third Party Users and Clients do the same, (iii) return the applicable Software to Provider together with all Documentation and other materials associated with the Software and all copies of any of the foregoing, or destroy such items, (iv) cease using the Maintenance Services associated with the applicable Software, (v) pay Provider or the applicable Partner all amounts due and payable up to the date of termination, and (vi) give Provider a written certification, within ten (10) days, that Customer, Third Party Users, and Clients, if applicable, have complied with all of the foregoing obligations.

c Any provision of this Agreement that requires or contemplates execution after (i) termination of this Agreement, (ii) a termination or expiration of a License, or (iii) the expiration of a SaaS Term, is enforceable against the other party and their respective successors and assignees notwithstanding such termination or expiration, including, without limitation, the *Restrictions*, *Payment*, *Taxes*, *Termination*, *Survival, Warranty Disclaimer, Infringement Indemnity, Limitation of Liability, Confidential Information*, *Compliance Verification*, and *General* Sections of this Agreement. Termination of this Agreement or a License shall be without prejudice to any other remedies that the terminating party or a Partner may have under law, subject to the limitations and exclusions set forth in this Agreement.

9 **Export.** Customer acknowledges that the Products and Maintenance Services are subject to the export control laws, rules, regulations, restrictions and national security controls of the United States and other applicable foreign agencies (the ***"Export Controls***") and agrees to abide by the Export Controls. Customer

hereby agrees to use the Products and Maintenance Services in accordance with the Export Controls, and shall not export, re-export, sell, lease or otherwise transfer the Products or any copy, portion or direct product of the foregoing in violation of the Export Controls. Customer is solely responsible for obtaining all necessary licenses or authorizations relating to the export, re-export, sale, lease or transfer of the Products and for ensuring compliance with the requirements of such licenses or authorizations. Customer hereby (i) represents that Customer, and if Customer is providing services under the MSP License herein each of its Clients, is not an entity or person to which shipment of Products, or provision of Maintenance Services, is prohibited by the Export Controls; and (ii) agrees that it shall not export, re-export or otherwise transfer the Products to (a) any country subject to a United States trade embargo, (b) a national or resident of any country subject to a United States trade embargo, (c) any person or entity to which shipment of Products is prohibited by the Export Controls, or (d) anyone who is engaged in activities related to the design, development, production, or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or chemical or biological weapons. Customer shall, at its expense, defend Provider and its Affiliates from any third party claim or action arising out of any inaccurate representation made by Customer regarding the existence of an export license, Customer's failure to provide information to Provider to obtain an export license, or any allegation made against Provider due to Customer's violation or alleged violation of the Export Controls (an ***"Export Claim"***) and shall pay any judgments or settlements reached in connection with the Export Claim as well as Provider's costs of responding to the Export Claim.

10 **Maintenance Services.**

a **Description.** During any Maintenance Period, Provider shall:

(i) Make available to Customer new versions and releases of the Software, if and when Provider makes them generally available without charge as part of Maintenance Services.

(ii) Respond to communications from Customer that report Software failures not previously reported to Provider by Customer. Nothing in the foregoing shall operate to limit or restrict follow up communication by Customer regarding Software failures.

(iii) Respond to requests from Customer's technical coordinators for assistance with the operational/technical aspects of the Software unrelated to a Software failure. Provider shall have the right to limit such responses if Provider reasonably determines that the volume of such non-error related requests for assistance is excessive or overly repetitive in nature.

(iv) Provide access to Provider's software support web site at https://www.sonicwall.com/ja-jp/support (the ***"Support Site"***).

(v) For Customers that have purchased Maintenance Services continuously since the purchase of such License, provide the repair and return program described on the Support Site for the Appliance on which the Software is delivered.

Maintenance Services are available during regional business support hours (***"Business Hours"***) as indicated on the Support Site, unless Customer has purchased 24x7 Support. The list of Software for which 24x7 Support is available and/or required is listed in the Global Support Guide on the Support Site.

The Maintenance Services for Software that Provider has obtained through an acquisition or merger may, for a period of time following the effective date of the acquisition or merger, be governed by terms other than those in this Section. The applicable different terms, if any, shall be stated on the Support Site.

b **Maintenance Period.** The first period for which Customer is entitled to receive Maintenance Services begins on the date of the registration of the Product at Provider's registration portal (the "**Registration**") and ends twelve (12) months thereafter (the ***"Initial Maintenance Period"***). Following the Initial Maintenance Period, Maintenance Services for the Product(s) may then be renewed for additional terms of twelve (12) or more months (each, a ***"Renewal Maintenance Period"***) For purposes of this Agreement, the Initial Maintenance Period and each Renewal Maintenance Period shall be considered a ***"Maintenance* Period."** For the avoidance of doubt, this Agreement shall apply to each Renewal Maintenance Period. Cancellation of Maintenance

Services will not terminate Customer's rights to continue to otherwise use the Products. Maintenance fees shall be due in advance of each Renewal Maintenance Period and shall be subject to the payment requirements set forth in this Agreement. The procedure for reinstating Maintenance Services for the Products after it has lapsed is posted at https://www.sonicwall.com/ja-jp/support/essentials/support-guide. Maintenance Services are optional and only provided if purchased separately.

For SaaS Software, the Maintenance Period is equal to the duration of the applicable SaaS Term. For non-perpetual Licenses or for non-perpetual MSP Licenses, the Maintenance Period is equal to the duration of the License.

11 **Warranties and Remedies.**

a **Software Warranties.** Provider warrants that, during the applicable Warranty Period (as defined in subsection (c) below),

(i) the operation of the Software, as provided by Provider, will substantially conform to its Documentation (the ***"Operational Warranty"***);

(ii) the Software, as provided by Provider, will not contain any viruses, worms, Trojan Horses, or other malicious or destructive code designed by Provider to allow unauthorized intrusion upon, disabling of, or erasure of the Software, except that the Software may contain a key limiting its use to the scope of the License granted, and license keys issued by Provider for temporary use are time-sensitive (the ***"Virus Warranty"***);

(iii) it will make commercially reasonable efforts to make the SaaS Software available twenty-four hours a day, seven days a week except for scheduled maintenance, the installation of updates, those factors that are beyond the reasonable control of Provider, Customer's failure to meet any minimum system requirements communicated to Customer by Provider, and any breach of this Agreement by Customer that impacts the availability of the SaaS Software (the ***"SaaS Availability Warranty"***).

b **Appliance Warranties.** Provider warrants that, during the applicable Warranty Period, the Appliance will operate in a manner which allows the SNWL Software, respectively, to be used in substantial conformance with the Documentation (the ***""Appliance Warranty***",).

c **Warranty Periods**. The ***"Warranty Period"*** for each of the above warranties (except for E-class appliances which do not include a Software warranty, shall be as follows: (i) for the Operational Warranty as it applies to Software and the Virus Warranty, ninety (90) days following the initial Registration of the Software; (ii) for the Operational Warranty as it applies to SaaS Software and the SaaS Availability Warranty, the duration of the SaaS Term; and (iv) for the Appliance Warranty, one (1) year following the date the Appliance is registered with Provider.

d **Remedies**. Any breach of the foregoing warranties must be reported by Customer to Provider during the applicable Warranty Period. Customer's sole and exclusive remedy and Provider's sole obligation for any such breach shall be as follows:

(i) For a breach of the *Operational Warranty* that impacts the use of Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach within a reasonable time considering the severity of the error and its effect on Customer or, at Provider's option, refund the license fees paid for the nonconforming Software upon return of such Software to Provider and termination of the related License(s) hereunder.

(ii) For a breach of the *Operational Warranty* that impacts the use of SaaS Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach and provide a credit or refund of the fees allocable to the period during which the Software was not operating in substantial conformance with the applicable Documentation.

(iii) For a breach of the *Virus Warranty*, Provider shall replace the Software with a copy that is in conformance with the Virus Warranty.

(v) For a breach of the *SaaS Availability Warranty*, Provider shall provide a credit or refund of the fees allocable to the period during which the SaaS Software was not available for use.

e **Warranty Exclusions**. The warranties set forth in this Section shall not apply to any non-conformance (i) that Provider cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the applicable Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; or (iii) arising from the modification of the Product by anyone other than Provider.

f **Third Party Products**. Certain Software may contain features designed to interoperate with third-party products. If the third-party product is no longer made available by the applicable provider, Provider may discontinue the related product feature. Provider shall notify Customer of any such discontinuation, however Customer will not be entitled to any refund, credit or other compensation as a result of the discontinuation.

g **Warranty Disclaimer.** THE EXPRESS WARRANTIES AND REMEDIES SET FORTH IN THIS SECTION ARE THE ONLY WARRANTIES AND REMEDIES PROVIDED BY PROVIDER HEREUNDER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALL OTHER WARRANTIES OR REMEDIES ARE EXCLUDED, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, AND ANY WARRANTIES ARISING FROM USAGE OF TRADE OR COURSE OF DEALING OR PERFORMANCE. PROVIDER DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE OPERATION OF THE PRODUCTS.

h **High-Risk Disclaimer.** CUSTOMER UNDERSTANDS AND AGREES THAT THE PRODUCTS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HIGH-RISK OR HAZARDOUS ENVIRONMENT, INCLUDING WITHOUT LIMITATION, THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION WHERE THE FAILURE OR MALFUNCTION OF ANY PRODUCT CAN REASONABLY BE EXPECTED TO RESULT IN DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR SEVERE ENVIRONMENTAL HARM (A ***"HIGH RISK ENVIRONMENT"***). ACCORDINGLY, (I) CUSTOMER SHOULD NOT USE THE PRODUCTS IN A HIGH RISK ENVIRONMENT, (II) ANY USE OF THE PRODUCTS BY CUSTOMER IN A HIGH RISK ENVIRONMENT IS AT CUSTOMER'S OWN RISK, (III) PROVIDER, ITS AFFILIATES AND SUPPLIERS SHALL NOT BE LIABLE TO CUSTOMER IN ANY WAY FOR USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT, AND (IV) PROVIDER MAKES NO WARRANTIES OR ASSURANCES, EXPRESS OR IMPLIED, REGARDING USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT.

12 **Infringement Indemnity.** Provider shall indemnify Customer from and against any claim, suit, action, or proceeding brought against Customer by a third party to the extent it is based on an allegation that the Software directly infringes any patent, copyright, trademark, or other proprietary right enforceable in the country in which Provider has authorized Customer to use the Software, including, but not limited to the country to which the Software is delivered to Customer, or misappropriates a trade secret in such country (a ***"Claim"***). Indemnification for a Claim shall consist of the following: Provider shall (a) defend or settle the Claim at its own expense, (b) pay any judgments finally awarded against Customer under a Claim or any amounts assessed against Customer in any settlements of a Claim, and (c) reimburse Customer for the reasonable administrative costs or expenses, including without limitation reasonable attorneys' fees, it necessarily incurs in responding to the Claim. Provider's obligations under this *Infringement Indemnity* Section are conditioned upon Customer (i) giving prompt written notice of the Claim to Provider, (ii) permitting Provider to retain sole control of the investigation, defense or settlement of the Claim, and (iii) providing Provider with cooperation and assistance as Provider may reasonably request in connection with the Claim. Provider shall have no obligation hereunder to defend Customer against any Claim (a) resulting from use of the Software other than as authorized by this Agreement, (b) resulting from a modification of the Software other than by Provider, (c) based on Customer's use of any release of the Software after Provider recommends discontinuation because of possible or actual infringement and has provided a non-infringing version at no charge, or (d) to the extent the Claim arises from or is based on the use of the Software with other products, services, or data not supplied by Provider if the infringement would not have occurred but for such use. If, as a result of a

Claim or an injunction, Customer must stop using any Software (***"Infringing Software"***), Provider shall at its expense and option either (1) obtain for Customer the right to continue using the Infringing Software, (2) replace the Infringing Software with a functionally equivalent non-infringing product, (3) modify the Infringing Software so that it is non-infringing, or (4) terminate the License for the Infringing Software and (A) for non-SaaS Software, accept the return of the Infringing Software and refund the license fee paid for the Infringing Software, pro-rated over a sixty (60) month period from the date of initial delivery of such Software, or (B) for SaaS Software, discontinue Customer's right to access and use the Infringing Software and refund the unused pro-rated portion of any license fees pre-paid by Customer for such Software. This Section states Provider's entire liability and its sole and exclusive indemnification obligations with respect to a Claim and Infringing Software.

13 **Limitation of Liability.** EXCEPT FOR (A) ANY BREACH OF THE *RESTRICTIONS* OR *CONFIDENTIAL INFORMATION* SECTIONS OF THIS AGREEMENT, (B) AMOUNTS CONTAINED IN JUDGMENTS OR SETTLEMENTS WHICH PROVIDER OR CUSTOMER IS LIABLE TO PAY TO A THIRD PARTY UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER IS LIABLE TO PAY ON BEHALF OF OR TO PROVIDER UNDER THE *CONDUCT, EXPORT, MSP LICENSE,* AND *USE BY THIRD PARTIES* SECTIONS OF THIS AGREEMENT, OR (C) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, IN NO EVENT SHALL CUSTOMER OR ITS AFFILIATES, OR PROVIDER, ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR (X) ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND OR (Y) LOSS OF REVENUE, LOSS OF ACTUAL OR ANTICIPATED PROFITS, LOSS OF BUSINESS, LOSS OF CONTRACTS, LOSS OF GOODWILL OR REPUTATION, LOSS OF ANTICIPATED SAVINGS, LOSS OF, DAMAGE TO OR CORRUPTION OF DATA, HOWSOEVER ARISING, WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR IN THE CONTEMPLATION OF THE PARTIES AND WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE.

EXCEPT FOR (A) ANY BREACH OF THE *SOFTWARE LICENSE, RESTRICTIONS,* OR *CONFIDENTIAL INFORMATION* SECTIONS OF THIS AGREEMENT, OR ANY OTHER VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (B) PROVIDER'S EXPRESS OBLIGATIONS UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER'S EXPRESS OBLIGATIONS UNDER THE *CONDUCT, EXPORT, MSP LICENSE,* AND *USE BY THIRD PARTIES* SECTIONS OF THIS AGREEMENT, (C) PROVIDER'S COSTS OF COLLECTING DELINQUENT AMOUNTS WHICH ARE NOT THE SUBJECT OF A GOOD FAITH DISPUTE; (D) A PREVAILING PARTY'S LEGAL FEES PURSUANT TO THE *LEGAL FEES* SECTION OF THIS AGREEMENT; OR (E) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY OF CUSTOMER AND ITS AFFILIATES, AND PROVIDER, ITS AFFILIATES AND SUPPLIERS, FOR DAMAGES UNDER THIS AGREEMENT, WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE, SHALL BE AN AMOUNT EQUAL TO (Y) THE GREATER OF THE FEES PAID AND/OR OWED (AS APPLICABLE) BY CUSTOMER OR ITS AFFILIATES FOR THE PRODUCTS THAT ARE THE SUBJECT OF THE BREACH OR FIVE HUNDRED DOLLARS ($500.00),EXCEPT FOR (Z) MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, FOR WHICH THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY SHALL BE THE GREATER OF THE AMOUNT PAID AND/OR OWED (AS APPLICABLE) FOR SUCH MAINTENANCE SERVICE OR PRODUCT DURING THE TWELVE (12) MONTHS PRECEDING THE BREACH OR FIVE HUNDRED DOLLARS ($500.00). THE PARTIES AGREE THAT THESE LIMITATIONS OF LIABILITY ARE AGREED ALLOCATIONS OF RISK CONSTITUTING IN PART THE CONSIDERATION FOR PROVIDER PROVIDING PRODUCTS AND SERVICES TO CUSTOMER, AND SUCH LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITIES OR FAILURES.

Provider's Affiliates and suppliers and Customer's Affiliates shall be beneficiaries of this *Limitation of Liability* Section and Customer's Clients and Third Party Users are entitled to the rights granted under the *MSP License* and *Use by Third Parties* Sections of this Agreement; otherwise, no third party beneficiaries exist under this Agreement. Provider expressly excludes any and all liability to Third Party Users, Clients and to any other third party.

14 Confidential Information.

a **Definition**. ***"Confidential Information"*** means information or materials disclosed by one party (the ***"Disclosing Party"***) to the other party (the ***"Receiving Party"***) that are not generally available to the public and which, due to their character and nature, a reasonable person under like circumstances would treat as confidential, including, without limitation, financial, marketing, and pricing information, trade secrets, know-how, proprietary tools, knowledge and methodologies, the Software (in source code and/or object code form), information or benchmark test results regarding the functionality and performance of the Software, any Software license keys provided to Customer, and the terms and conditions of this Agreement.

Confidential Information shall not include information or materials that (i) are generally known to the public, other than as a result of an unpermitted disclosure by the Receiving Party after the date that Customer accepts the Agreement (the ***"Effective Date"***); (ii) were known to the Receiving Party without an obligation of confidentiality prior to receipt from the Disclosing Party; (iii) the Receiving Party lawfully received from a third party without that third party's breach of agreement or obligation of trust; (iv) are protected by Provider in accordance with its obligations under the *Protected Data* Section below, or (v) are or were independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

b **Obligations.** The Receiving Party shall (i) not disclose the Disclosing Party's Confidential Information to any third party, except as permitted in subsection (c) below and (ii) protect the Disclosing Party's Confidential Information from unauthorized use or disclosure by exercising at least the same degree of care it uses to protect its own similar information, but in no event less than a reasonable degree of care. The Receiving Party shall promptly notify the Disclosing Party of any known unauthorized use or disclosure of the Disclosing Party's Confidential Information and will cooperate with the Disclosing Party in any litigation brought by the Disclosing Party against third parties to protect its proprietary rights. For the avoidance of doubt, this Section shall apply to all disclosures of the parties' Confidential Information as of the Effective Date, whether or not specifically arising from a party's performance under this Agreement.

c **Permitted Disclosures**. Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent to any of its Affiliates, directors, officers, employees, consultants, contractors or representatives (collectively, the ***"Representatives"***), but only to those Representatives that (i) have a "need to know" in order to carry out the purposes of this Agreement or to provide professional advice in connection with this Agreement, (ii) are legally bound to the Receiving Party to protect information such as the Confidential Information under terms at least as restrictive as those provided herein, and (iii) have been informed by the Receiving Party of the confidential nature of the Confidential Information and the requirements regarding restrictions on disclosure and use as set forth in this Section. The Receiving Party shall be liable to the Disclosing Party for the acts or omissions of any Representatives to which it discloses Confidential Information which, if done by the Receiving Party, would be a breach of this Agreement.

Additionally, it shall not be a breach of this Section for the Receiving Party to disclose the Disclosing Party's Confidential Information as may be required by operation of law or legal process, provided that the Receiving Party provides prior notice of such disclosure to the Disclosing Party unless expressly prohibited from doing so by a court, arbitration panel or other legal authority of competent jurisdiction.

15 **Protected Data**. For purposes of this Section, ***"Protected Data"*** means any information or data that is provided by Customer to Provider during this Agreement that alone or together with any other information relates to an identified or identifiable natural person or data considered to be personal data as defined under Privacy Laws, and "***Privacy Laws"*** means any applicable law, statute, directive or regulation regarding privacy, data protection, information security obligations and/or the processing of Protected Data.

Except as permitted herein or to the extent required by Privacy Laws or legal process, Provider shall implement reasonable technical and organizational measures to prevent unauthorized disclosure of or access to Protected Data by third parties, and shall only store and process Protected Data as may be

required to fulfill its obligations under this Agreement. If Provider complies with Customer's written instructions with respect to the Protected Data, Provider shall have no liability to Customer for any breach of this Section resulting from such compliance. Provider shall promptly notify Customer of any disclosure of or access to the Protected Data by a third party in breach of this Section and shall cooperate with Customer to reasonably remediate the effects of such disclosure or access. Provider further affirms to Customer that it has adequate agreements in place incorporating the EU standard contractual clauses for the transfer of Protected Data from the European Union (***"EU"***) to a country outside the EU.

Customer hereby (i) represents that it has the right to send the Protected Data to Provider, (ii) consents for Provider to store and use the Protected Data worldwide for the sole purpose of performing its obligations under this Agreement, (iii) agrees that the Protected Data may be accessed and used by Provider and its Representatives worldwide as may be needed to support Provider's standard business operations, and (iv) agrees that Protected Data consisting of Customer contact information (e.g., email addresses, names) provided as part of Maintenance Services may be sent to Provider's third party service providers as part of Provider's services improvement processes.

16 **Compliance Verification.** Customer agrees to maintain and use systems and procedures to accurately track, document, and report its installations, acquisitions and usage of the Software. Such systems and procedures shall be sufficient to determine if Customer's deployment of the Software or, if applicable, use of the SaaS Software is within the quantities, terms, and maintenance releases to which it is entitled. Provider or its designated auditing agent shall have the right to audit Customer's deployment of the Software or, if applicable, use of the SaaS Software for compliance with the terms and conditions of this Agreement. Any such audits shall be scheduled at least ten (10) days in advance and shall be conducted during normal business hours at Customer's facilities. Customer shall provide its full cooperation and assistance with such audit and provide access to the applicable records and computers. Without limiting the generality of the foregoing, as part of the audit, Provider may request, and Customer agrees to provide, a written report, signed by an authorized representative, listing Customer's then current deployment of the Software and/or the number of individuals that have accessed and used SaaS Software. If Customer's deployment of the Software or, if applicable, use of the SaaS Software is found to be greater than its purchased entitlement to such Software, Customer will be invoiced for the over-deployed quantities at Provider's then current list price plus the applicable Maintenance Services and applicable over-deployment fees. All such amounts shall be payable in accordance with this Agreement. Additionally, if the unpaid fees exceed five percent (5%) of the fees paid for the applicable Software, then Customer shall also pay Provider's reasonable costs of conducting the audit. The requirements of this Section shall survive for two (2) years following the termination of the last License governed by this Agreement.

17 **SaaS Provisions**.

a **Data.** Customer may store data on the systems to which it is provided access in connection with its use of the SaaS Software (the ***"SaaS Environment"***). Provider may periodically make back-up copies of Customer data, however, such back-ups are not intended to replace Customer's obligation to maintain regular data backups or redundant data archives. Customer is solely responsible for collecting, inputting and updating all Customer data stored in the SaaS Environment, and for ensuring that it does not (i) knowingly create and store data that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party, or (ii) use the SaaS Environment for purposes that would reasonably be seen as obscene, defamatory, harassing, offensive or malicious.. Provider shall have the right to delete all Customer data stored in connection with the use of the SaaS Software thirty (30) days following any termination of this Agreement or any License to SaaS Software granted hereunder.

Customer represents and warrants that it has obtained all rights, permissions and consents necessary to use and transfer all Customer and/or third party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other provider that is linked to or made accessible by the SaaS Software, Customer will be deemed to

have given its consent to Provider enabling such transmission and Provider shall have no liability to Customer in connection with any claims by a third party in connection with such transmission.

b **Conduct.** In connection with the use of SaaS Software, Customer may not (i) attempt to use or gain unauthorized access to Provider's or to any third-party's networks or equipment; (ii) permit other individuals or entities to copy the SaaS Software; (iii) provide unauthorized access to or use of any SaaS Software or the associated access credentials; (iv) attempt to probe, scan or test the vulnerability of the SaaS Software, the SaaS Environment, or a system, account or network of Provider or any of Provider's customers or suppliers; (v) interfere or attempt to interfere with service to any user, host or network; (vi) engage in fraudulent, offensive or illegal activity of any nature or intentionally engage in any activity that infringes the intellectual property rights or privacy rights of any individual or third party; (vii) transmit unsolicited bulk or commercial messages; (viii) intentionally distribute worms, Trojan horses, viruses, corrupted files or any similar items; (ix) restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the SaaS Software (except for tools with safety and security functions); or (x) restrict, inhibit, interfere with or otherwise disrupt or cause a performance degradation to any Provider (or Provider supplier) facilities used to provide the SaaS Environment. Customer shall cooperate with Provider's reasonable investigation of SaaS Environment outages, security issues, and any suspected breach of this Section, and shall, at its expense, defend Provider and its Affiliates from any claim, suit, or action by a third party (a ***"Third Party Claim"***) alleging harm to such third party caused by Customer's breach of any of the provisions of this Section. Additionally, Customer shall pay any judgments or settlements reached in connection with the Third Party Claim as well as Provider's costs of responding to the Third Party Claim.

c **Suspension.** Provider may suspend Customer's use of SaaS Software (a) if so required by law enforcement or legal process, (b) in the event of an imminent security risk to Provider or its customers, or (c) if continued use would subject Provider to material liability. Provider shall make commercially reasonable efforts under the circumstances to provide prior notice to Customer of any such suspension.

18 **General.**

a **Governing Law and Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the Santa Clara County, California. Each party hereby agrees to submit to the jurisdiction of such courts. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated.

b **Assignment.** Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement, the Licenses granted under this Agreement or any other rights, interest or obligations hereunder, whether voluntarily, by contract, by operation of law or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Provider. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void.

c **Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible by law to effect the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Notwithstanding the foregoing, the terms of this Agreement that limit, disclaim, or exclude warranties, remedies or damages are intended by the parties to be independent and remain in effect despite the failure or unenforceability of an agreed remedy. The parties have relied on the limitations and exclusions set forth in this Agreement in determining whether to enter into it.

d **Use by U.S. Government.** The Software is a “commercial item” under FAR 12.201. Consistent with FAR section 12.212 and DFARS section 227.7202, any use, modification, reproduction, release, performance, display, disclosure or distribution of the Software or Documentation by the U.S. government is prohibited except as expressly permitted by the terms of this Agreement. In addition, when Customer is a U.S. government entity, the language in Subsection (ii) of the *Infringement Indemnity* Section of this Agreement and the *Injunctive Relief* Section of this Agreement shall not be applicable.

e **Notices.** All notices provided hereunder shall be in writing and may be delivered by email, in the case of Provider to legal@sonicwall.com and in the case of Customer to the email address Provider has on file for Customer. All notices, requests, demands or communications shall be deemed effective upon delivery in accordance with this paragraph.

f **Disclosure of Customer Status.** Provider may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of Provider in its marketing communications.

g **Waiver.** Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

h **Injunctive Relief.** Each party acknowledges and agrees that in the event of a material breach of this Agreement, including but not limited to a breach of the *Software License, Restrictions* or *Confidential Information* Sections of this Agreement, the non-breaching party shall be entitled to seek immediate injunctive relief, without limiting its other rights and remedies.

i **Force Majeure.** Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures. For added certainty, this Section shall not operate to change, delete, or modify any of the parties’ obligations under this Agreement (e.g., payment), but rather only to excuse a delay in the performance of such obligations.

j **Equal Opportunity.** Provider is a federal contractor and Affirmative Action employer (M/F/D/V) as required by the Equal Opportunity clause C.F.R. § 60-741.5(a).

k **Headings.** Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term “including” is used in this Agreement it will be construed in each case to mean “including, but not limited to.”

l **Legal Fees**. If any legal action is brought to enforce any rights or obligations under this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys’ fees, court costs and other collection expenses, in addition to any other relief it may be awarded.

m **Entire Agreement.** This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter thereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any proceeding that may involve the Agreement. Each party acknowledges that in entering into the Agreement it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in the Agreement. In those jurisdictions where an original (non-faxed, non-electronic, or non-scanned) copy of an agreement or an original (non-electronic) signature

on agreements such as this Agreement is required by law or regulation, the parties hereby agree that, notwithstanding any such law or regulation, a faxed, electronic, or scanned copy of and a certified electronic signature on this Agreement shall be sufficient to create an enforceable and valid agreement. This Agreement, may only be modified or amended t by a writing executed by a duly authorized representative of each party. No other act, document, usage or custom shall be deemed to amend or modify this Agreement.

J

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様や、トライアル バージョンをお持ちのお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、https://www.sonicwall.com/ja-jp/support に移動します。

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- ビデオ チュートリアルを視聴する。
- MySonicWall にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要求する。

SonicWall サポートへの連絡方法は、https://www.sonicwall.com/ja-jp/support/contact-support をご覧ください。

このドキュメントについて

凡例

警告： **物的損害、けが、または死亡に至る可能性があることを示しています。**

注意： **手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。**

重要、メモ、ヒント、モバイル、またはビデオ: 補足情報があることを示しています。

SMA 管理ガイド
更新日 - 2018 年 12 月
ソフトウェア バージョン - 9.0
232-004629-00 Rev A

用語集

A

アクティブ ディレクトリ (AD)

Microsoft によって開発された、一元化されたディレクトリ サービス システムで、ユーザ データ、セキュリティ、およびリソースのネットワーク管理を自動化し、他のディレクトリとの相互運用を実現します。アクティブ ディレクトリは、分散ネットワーキング環境用に設計されています。

C

共通インターネット ファイル システム (CIFS)

リモート ファイルアクセスのために定義されている標準のプロトコルで、ユーザが異なるプラットフォームとコンピュータを使って、特別なソフトウェアをインストールしないでファイル共有することを可能にします。

F

ファイル共有

SMA/SRA 装置で動作する SonicWall Inc. のネットワーク ファイル ブラウジング機能。ウェブ ブラウザを使用してネットワーク上の共有ファイルをブラウズします。

L

Lightweight Directory Access Protocol (LDAP)

サーバからデータを取得するために電子メール プログラムなどのプログラムで使用されるインターネット プロトコル。

O

ワンタイム パスワード

ランダムに生成される使い捨てのパスワード。パスワードの特定のインスタンスを指す用語として使う場合と、この機能の総称として使う場合があります。

S

Simple Mail Transfer Protocol (SMTP)

サーバ間で電子メール メッセージを送信するためのプロトコル。

Secure Socket Layer Virtual Private Network (SMA/SRA)

ウェブ ブラウザを利用してプライベート アプリケーションへのクライアント不要のアクセスを可能にするリモート アクセス ツール。

V

仮想オフィス

SMA/SRA 装置のユーザ インターフェース。

W

Windows Internet Naming Service (WINS)

ネットワーク コンピュータに関連付けられた IP アドレスを確認するシステム。