SonicWall®
Secure Mobile Access 12.1
管理ガイド

SONICWALL®

目次

第 1 部 はじめに

第 2 部 インストール

第 3 部 管理

第 4 部 認証

第 8 部 Mobile Connect

第 9 部 付録

第 1 部

はじめに

- Secure Mobile Access について

1

Secure Mobile Access について

SMA アプライアンスの Secure Mobile Access

『*Secure Mobile Access 12.1* 管理ガイド』へようこそ。このマニュアルでは、SonicWall SMA アプライアンスの Secure Mobile Access (SMA) を正常に有効化、設定、管理するために必要な情報を提供します。

SonicWall SMA アプライアンスは、従業員、ビジネス パートナー、顧客に対して、安全なアクセス (Web アプリケーションへのクライアントレス アクセス、クライアント/サーバー アプリケーションへのアクセス、ファイル共有を含む) を提供します。すべてのトラフィックは、Secure Sockets Layer (SSL) によって暗号化されており、許可を受けていないユーザーのアクセスを防止します。

このアプライアンスを使用すると、Windows、Macintosh、Linux などの広範なプラットフォームから、さまざまなアクセス方式 (標準の Web ブラウザ、Windows クライアント、モバイル デバイスなど) でアプリケーションを利用できます。

このアプライアンスを使用すると、以下を作成できます。

- リモート アクセス VPN。これにより、リモートの従業員が電子メールなどのプライベートな企業アプリケーションにインターネットで安全にアクセスできます。
- ビジネス パートナー VPN。これにより、指定されたサプライヤーが内部のサプライ チェーン アプリケーションにインターネットでアクセスできます。

このアプライアンスが提供する細かいアクセス制御により、ユーザーやリソースのレベルでポリシーを定義してアクセスを制御できます。ポリシーの管理やアプライアンスの構成も、Web ベースの管理コンソールを使用して素早く簡単に実行できます。

SonicWall Secure Mobile Access アプライアンスの構成および展開の計画の概要については、『*SonicWall SMA Deployment Planning Guide*』を参照してください。

SMA のマニュアルについて

お使いの SonicWall SMA アプライアンスには、印刷版の『*Getting Started Guide*』と『*SonicWall SMA Deployment Planning Guide*』が付属し、VPN の重要なコンセプトやコンポーネントについて説明している他、VPN を展開する際に活用できるようになっています。すべての製品マニュアルの電子版にアクセスするには、SonicWall サポート ポータルにアクセスするか、MySonicWall のアカウントにログインして、アプライアンスを登録してください。詳細については、SMA アプライアンスの登録を参照してください。

このマニュアルの規則

このマニュアル全体を通して、

- 「外部」とはインターネットに接続するネットワーク インターフェースを指します。
- また、「内部」とは企業の内部ネットワークに接続するネットワーク インターフェースを示します。

このマニュアルでは、次の表記規則を使用しています。

このマニュアルの規則

表記規則	使用法
太字	ユーザー インターフェース コンポーネント (UI ページ、ダイアログ、テキスト フィールド、またはボタンなど)
`Monospace font`	ユーザーが入力する情報
`commandname -x [-y]`	コマンド構文で、角かっこはオプション パラメータを表します

本リリースの新機能

SonicWall Secure Mobile Access (SMA) 12.1 には次の新機能が含まれています。

- 生体 ID 認証
- Web ベースの RDP、VNC、SSH および Telnet
- CAM を使用したレガシーおよび SAML SSO サポート
- エンドポイント セキュリティ統合 SDK (OESIS) バージョン 4
- アプライアンス管理コンソール (AMC) および WorkPlace 管理インターフェースのページ レイアウトを使いやすく再設計
- GTO によるグローバル高可用性機能 (グローバル HA)
- Outlook Anywhere、Exchange ActiveSync、カスタム FQDN、カスタム WorkPlace の GTO サポート
- Capture Advanced Threat Protection (キャプチャ ATP)

廃止された機能

次の機能は、SMA 12.1 のすべての SMA アプライアンスで廃止されました。

GMS	SMA 12.1 では GMS はサポートされていません。詳細については、『*SMA 12.1 Central Management Server with Global High Availability Administration Guide (グローバル高可用性機能付き中央管理サーバー管理ガイド)*』を参照してください。
セキュア ソケット レイヤ (SSL) バージョン 3.0	セキュア ソケット レイヤ (SSL) プロトコルは非効率で安全性の低いプロトコルであることが証明されており、顧客は削除を要求してきました。 SMA 12.1 のすべての SMA 1000 シリーズアプライアンスでセキュア ソケット レイヤ (SSL) バージョン 3.0 が非推奨になりました。SSLv3 を有効にするオプションは、SSL 設定ページでは使用できません。 SMA 12.1 にアップグレード、またはその設定をインポートすると、システムは自動的に SSLv3 を無効にします。これは、スタンドアロン装置と CMS のインストールに適用されます。SSLv3 プロトコルは、SMA 12.1 でのいずれの接続でもサポートまたはネゴシエートされません。システム アップグレードまたは設定のインポートの間に、その新しい設定で SSLv3 が有効になると、その設定は削除され、アップグレードまたはインポート プロセスは正常終了します。 管理 API、列挙型 SSL_V3_AND_TLS_1_0_AND_HIGHER は、暗号化リソース経由で SSL 暗号化を設定するときには有効ではなくなりました。

仮想アシスト	以前のリリースから SMA 12.1 にアップグレード、または SMA 12.1 の設定をインポートしようとすると、システムは、そのアップグレードまたはインポートを拒否し、次のメッセージが通知されます。
	`SMA 12.1 では仮想アシストを使用できません。`
	`SMA 12.1 にアップグレードする前に仮想アシストを無効にする必要があります。`
	その後、仮想アシストを無効にして、アップグレード プロセスを再開します。今回はアップグレードが完了します。

レプリケーション	CMS は、グローバル高可用性機能 (グローバル HA) を提供します。これにより、冗長化が可能です。そのため、レプリケーション機能は、SMA から削除され、レプリケーション機能へのすべての参照が AMC から削除されました。「**Replicate (レプリケート)**」セクションは、今後「**Maintenance (メンテナンス)**」ページに表示されず、「**Configure (設定)**」ボタンで表示されていた「**Configure Replication (レプリケーションの設定)**」ページ全体が廃止になっています。 **重要**：CMS ポリシーの同期は、SMA レプリケーションと同等です。

高可用性ペア	SMA 12.1 のすべての SMA 1000 シリーズ アプライアンスで高可用性 (HA) ペアが非推奨になりました。GTO はこれらの機能をより効率的に提供します。SMA 12.1 にアップグレードする前に、HA ペアのすべての接続を無効にする必要があります。HA ペアのノードを SMA 12.1 にアップグレードしようとすると失敗して、次のエラー メッセージを生成します。 例外： 特別な CEM を使用すると、ノード ペアを解除してアップグレードすることができます。 SMA 12.1 の完全な設定のインポートは正常に実行できませんが、SMA 12.1 の部分的な設定のインポートを正常に実行できます。 セントラル ユーザー ライセンスが HA ペア ライセンスに置き換わります。
IP アドレスの設定のある仮想ホスト	IP アドレスの設定のある仮想ホストは廃止される予定です。この機能により、専用 IP アドレスを以下に使用できるようになりました。 • WorkPlace サイト • ホスト マップ URL リソース • Activesync URL リソース この機能は不要で、10.7.0 リリース以来隠されています。 IP アドレスの設定がある仮想ホストを現在の設定内で定義していると、SMA 12.1 へのアップグレードが正常終了しない場合があります。SMA 12.1 の完全な設定のインポートは正常に実行できませんが、事前に余分な IP アドレスを現在の設定から削除すると、SMA 12.1 の部分的な設定のインポートを正常に実行できます。

SMA アプライアンスの特徴

トピック:

- SonicWall SMA アプライアンスモデル
- アプライアンスとサービスを管理するための管理者コンポーネント
- ユーザー アクセス コンポーネント
- アクセシビリティの改善事項
- 関連資料

SonicWall SMA アプライアンスモデル

SonicWall では、次の SMA および EX シリーズ アプライアンスのモデルを提供しています。各モデルの詳細については、このマニュアルで説明します。

この文書では、SMA アプライアンスという用語は SMA アプライアンスモデルにリストされているアプライアンスを指します。SMA 8200v 仮想アプライアンスを除き、すべての SMA アプライアンスは、1 つ

の仮想 IP アドレスにより 2 台の同一アプライアンスをクラスタリングできます。また、1 台の外部ロード バランサを使用することで、最大 8 台のアプライアンスによるクラスタリングもサポートします。

SMA アプライアンスモデル

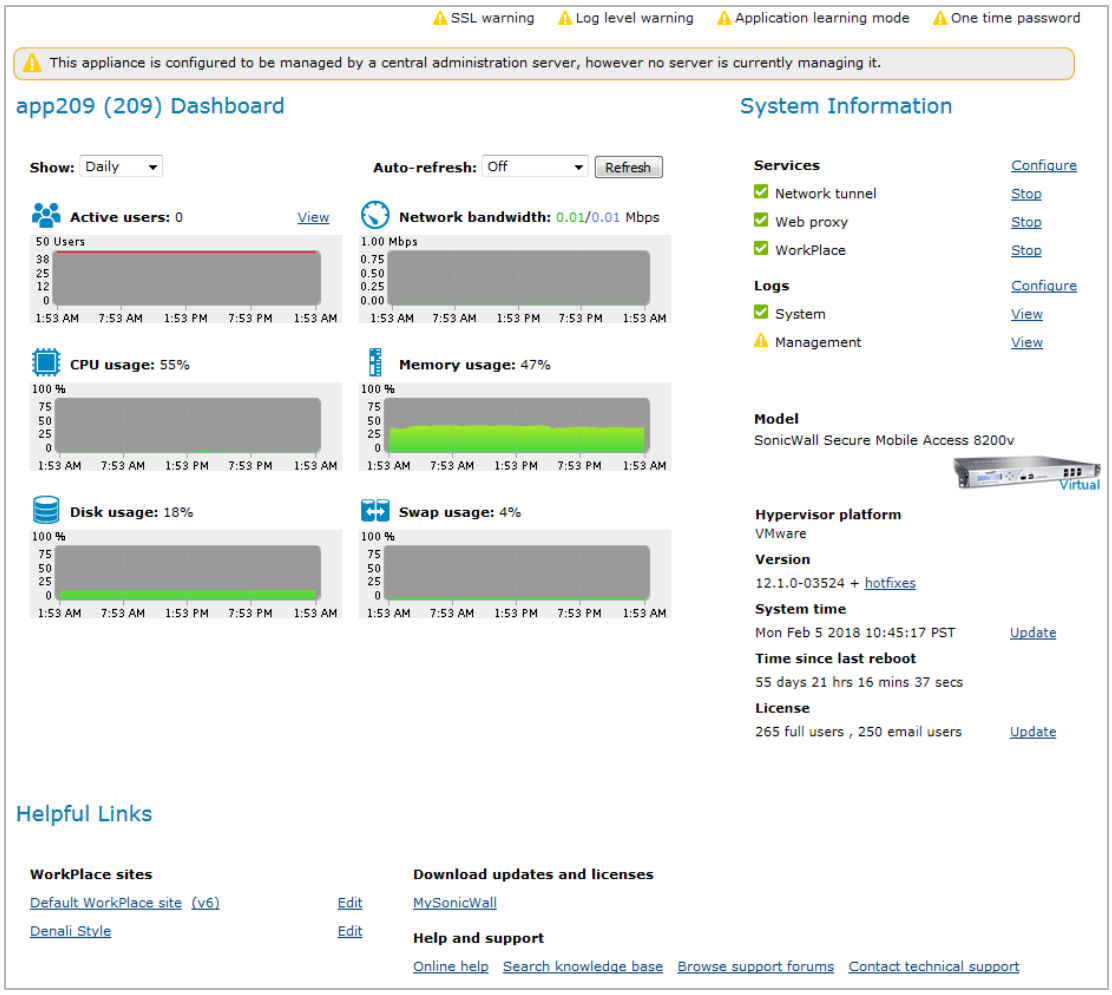
装置	サポートしている最大同時ユーザー数
E-Class SMA EX9000	20,000
E-Class SMA EX7000	5,000
E-Class SMA EX6000	250
SMA 7200	10,000
SMA 6200	2,000
SMA 8200v Virtual Appliance	Hyper-V と ESX の 5,000 ユーザ

アプライアンスとサービスを管理するための管理者コンポーネント

- **アプライアンス管理コンソール (AMC)** は、以下への一元的アクセスを提供してアプライアンスを管理する Web ベースの管理ツール (AMC ダッシュボード を参照) です。
  - セキュリティ ポリシーの管理
  - システムの設定 (ネットワークと証明書の設定を含む)
  - 監視

  AMC には Web ブラウザからアクセスできます。

AMC ダッシュボード



- **Web プロキシ サービス (Web プロキシ サービス)** によりユーザーは、Web ベースのアプリケーション、Web サーバー、ネットワーク ファイル サーバーに Web ブラウザから安全にアクセスできます。Web プロキシ サービスは、Web ベースのリソースに対するアクセスを中継および暗号化する安全な HTTP リバース プロキシです。
- **ネットワーク トンネル サービス**は、以下を使用する多様なアプリケーションに安全なネットワーク トンネル アクセスを提供するネットワーク ルーティング テクノロジーです。
    - VoIP (Voice Over IP) や ICMP などの非 TCP プロトコル
    - 逆方向接続プロトコル
    - FTP などの双方向プロトコル

  ネットワーク トンネル サービスは、Connect Tunnel クライアントや OnDemand Tunnel エージェントと連動して、アクセスの認証と暗号化を提供します。このサービスでは、ファイアウォールや NAT デバイスの他、従来型の VPN デバイスと干渉する可能性があるプロキシ サーバーもトラバースできます。
- **管理 API ライブラリ**このコンポーネントは、JSON 形式のアプライアンス データの表示と変更のための URL を提供します。API は、アプライアンスが最初の構成を完了する前と後で HTTP リクエストを処理する次の 2 つのプライマリ URL に分割されます。
    - 初期設定時: `https://<AMC IP アドレス:8443>/Setup`

- アプライアンスの設定後: `https://<AMC IP アドレス:8443>/Console`

<AMC IP アドレス> は、AMC アプライアンスの IP アドレスです。

メモ：仮想マシンを使用する場合は、ポート 8443 の代わりに仮想マシンのポート番号を使用します。

ブラウザ ベースのマニュアルは次の場所から入手できます。

- `https://<AMC IP アドレス:8443>/Setup/UserGuide`
- `https://<AMC IP アドレス:8443>/Console/UserGuide`

ユーザー アクセス コンポーネント

SMA アプライアンスは、ユーザーがネットワーク上のリソースにアクセスするためのコンポーネントをいくつか提供します。

- WorkPlace
- Connect および OnDemand Tunnel クライアント
- End Point Control (EPC)

WorkPlace

WorkPlace ポータルを使用すると、ネットワーク上のリソースに素早くアクセスできます。このポータルには、SSL をサポートし JavaScript が有効な任意の Web ブラウザからアクセスできます。WorkPlace では、次のような多様なアクセス方法から選択できます。

- 基本的な Web(HTTP) リソースは、Web 変換エンジンを使用してアクセスできます。Web 変換エンジンは、シングル サインオンや詳細なアクセス制御が可能なリバース プロキシです。Web 変換エンジンの処理には、次の 3 種類があります。
  - **エイリアス** ベースの変換により、ユーザーがアクセスする URL の最後にカスタムのエイリアスが付けられます (URL リライト)。例えば、エイリアスの「`hr`」を使用する URL リソースとして `http://hr.mycompany.com/` を指定すると、ユーザーがこのリソースにアクセスするために Workplace でクリックするリンクは、`https://vpn.mycompany.com/hr/` のように表示されます。このような構成は、Java アプレット、JavaScript (AJAX) などの高度な機能を必要としない単純な Web アプリケーションに推奨されます。SonicWall はエイリアス ベース変換された Web アクセス方法で、限られた数のアプリケーションをサポートします。Web アプリケーション サービスを参照してください。
  - **ホスト マップ URL** アクセスは、リソースがアクセスを受けるホスト名を変更します。例えば、`http://hr.mycompany.com/` という URL リソースがカスタムのホスト名の hr.vpn.mycompany.com により構成される場合、ユーザーがこのリソースにアクセスするために Workplace でクリックするリンクは、`https://hr.vpn.mycompany.com/` のように表示されます。ホスト マップ URL アクセスは、Java アプレット、高度な AJAX (およびその他の高度な Web テクノロジー) を使用する複雑な Web アプリケーション向けとして推奨されます。

    ヒント： ホスト マップ URL リソースのを容易に拡張するには、ワイルドカード SSL 証明書、またはワイルドカードを含む SAN 証明書のいずれかを購入することが推奨されます。

- **ポート マップ URL**アクセスは、リソースがアクセスを受けるポート番号を変更します。例えば、`http://hr.mycompany.com/` という URL リソースがカスタムのアクセス用ポート (8888) により構成される場合、ユーザーがこのリソースにアクセスするために Workplace でクリックするリンクは、`https://vpn.mycompany.com:8888/` のように表示されます。カスタムポート URL アクセスの問題として、ポート マップ URL アクセスを使用するためには構成する各 Web アプリケーション向けにポートを開く必要がある点が挙げられます。

  ヒント： ポート マップ URL リソースは、Java アプレット、高度な AJAX、その他の高度な Web テクノロジーを使用する複雑な Web アプリケーション向けとして推奨されます。

- ファイル システム リソースは、WorkPlace に統合されている Web ベースの Network Explorer からアクセスできます。
- クライアント/サーバー トラフィック (TCP/IP) は、いずれかのネットワーク リダイレクション クライアント または OnDemand Tunnel を使用してアクセスできます。クライアントは、ユーザーが WorkPlace にログインするときに自動的に設定され有効になります。

アクセス方法は、アプリケーションが使用するネットワーク プロトコル、セキュリティ要件、エンド ユーザーの利便性、対象プラットフォームなど、複数の要因に基づいて選択します。

Connect および OnDemand Tunnel クライアント

トンネル クライアントは、すべてのリソースに対してネットワーク レベルでのアクセスを提供するので、ネットワーク上で各ユーザー デバイスが事実上の仮想ノードになります。

- Connect Tunnel クライアントを使用すると、Web に展開された Windows クライアント (Windows 7 SP1、10、Mac OS、Linux オペレーティング システムが動作するコンピュータ向け) から、ネットワークおよびアプリケーションに対するフル アクセスが可能になります。クライアントのプロビジョニングは、WorkPlace ポータルのリンクから透過的に、または実行可能インストール パッケージを使用して行われます。Connect Tunnel クライアントは、分割トンネル制御、細かいアクセス制御、自動プロキシ検出、および認証の機能を提供します。
- OnDemand Tunnel エージェントには、Connect Tunnel とほぼ同じ機能があります。ただし、ドメイン ログイン用のダイヤルアップ アダプタとして使用できず、また ASAP WorkPlace に統合されている点において異なります。OnDemand は、「スプリット トンネル モード」または「リダイレクト オール モード」で動作できます。

End Point Control (EPC)

EPC コンポーネントは、ネットワークが、信頼されていない環境の PC からアクセスされた場合に危険にさらされることのないようにします。このコンポーネントを使用すると、デバイスを照会し、必要なプログラムが動作しているかを判定します。また **AdvancedEPC** では、OPSWAT、McAfee、Computer Associates、Sophos、Kaspersky などの大手ベンダーのセキュリティ ソリューションを含む包括的な定義済みチェックリストを使用して、(Microsoft Windows が動作するクライアントに対して) デバイス プロファイルを設定することにより、詳細なエンド ポイント保護を簡単に行うことかできます。Advanced EPC は、SMA 6200、SMA 7200、EX9000 および EX7000 アプライアンスに付属していますが、EX シリーズのその他のアプライアンスについては別途ライセンスが必要です。

アクセシビリティの改善事項

お使いのアプライアンスで提供される管理者 (AMC) およびユーザー アクセス (WorkPlace と Connect Tunnel) のコンポーネントは、アクセシビリティの改善事項に示すオペレーティング システムについて、米国リハビリテーション法第 508 条および ADA (Americans with Disabilities) 法への準拠に関するアクセシビリティの改善事項があります。

アクセシビリティの改善事項

コンポーネント	Windows	Mac OS X	Linux
AMC	✓		
WorkPlace	✓	✓	✓
Connect Tunnel	✓	✓	

米国リハビリテーション法第 508 条および ADA (Americans with Disabilities) 法への準拠に関するアクセシビリティについて、次の機能によりキーボードの使いやすさや支援技術への適合性が改善されています。

- キーボード ショートカット、および適切なキーボード タブ順序
- ページ上でのユーザーの場所を識別し、タブ キーによるページ上の要素間の移動を可能にするビジュアル フォーカス。この機能は、タブ付けされたページ、ラジオ ボタン、チェックボックス、プッシュ ボタンなどの選択方法を使用する上で、特に役立ちます。
- プロパティ ウィンドウ、ダイアログ ボックス、および非テキスト要素上での、有意なポップアップ キャプション。
- Connect Tunnel がインストールを正常に完了したときの完了メッセージ
- 設定ウィザードでのユーザー操作のアクセシビリティ向上
- ブラウザ ベースのハイ コントラスト テーマによる、コンピュータ画面上での見やすいテキスト表示。この機能は Internet Explorer、Chrome、Firefox の各ブラウザで利用できますが、オペレーティング システムとブラウザの組み合わせによって結果は異なります。

ログインおよび実行時のダイアログ、セッション統計、およびステータスの再編成によるアクセシビリティ向上。

メモ：SonicWall は、NVDA (Non Visual Desktop Access) または JAWS の画面読み込みソフトウェアの使用を推奨しています。

関連資料

SMA 12.1 のさまざまな機能と製品の詳細については、以下の SonicWall SMA マニュアルを参照してください。

- *SMA 12.1 CMS 管理ガイド*
- *SMA12.1WorkPlace ユーザー ガイド*
- *SMA 12.1 アップグレード ガイド*
- *SMA 12.1 Connect Tunnel ユーザー ガイド*
- *SMA 12 8200v 導入ガイド*

システム要件

このセクションでは、Secure Mobile Access のクライアントおよび管理者 (サーバー) のコンポーネントのシステム要件について説明します。

メモ：SMA 12.1 のシステム要件および制限事項に関する追加情報および更新情報については、『*Secure Mobile Access 12.1 リリース ノート*』を参照してください。

サポート状況については、表に一覧された項目のフォントの種類で示します。

- 完全にサポート (通常のフォント)
- ***対応、サポート予定、必要に応じて問題に対応 (太字斜体フォント)***
- *対応、サポート終了予定 (斜体フォント)*

「対応」の構成で既知の問題はありませんが、現行リリースでは具体的にテストされていません。このため、SonicWall では顕著な問題が発生しないことを保証せず、このような問題についてのサポートの保証はありません。

メモ：Microsoft Internet Explorer (IE) v10 では、Metro View はサポートされません。

トピック:

- クライアント コンポーネント
- サーバー コンポーネント

クライアント コンポーネント

クライアント コンポーネントのシステム要件は、次の表にリストされています。

- WorkPlace Lite アクセス
- Web ベースのクライアント
- Tunnel クライアント
- プロキシ クライアント
- エンド ポイント制御

メモ：次の表は、対応する SonicWall Secure Mobile Access (SMA) リリースの時点で入手可能な最新リリース バージョンのソフトウェアを示しています。

WorkPlace Lite アクセス

WorkPlace Lite の要件

オペレーティング システム	ブラウザ	注
• Windows 10 • Windows 10 Creators	• IE (32 ビットのみ) • Firefox • Chrome • Edge	アクセス エージェントまたは EPC は必要ありません。ブラウザは HTML5 をサポートしている必要があります。
• Windows 7 x86/x64 SP1	• IE (32 ビットのみ) • Firefox • Chrome	
• iPhone/iPad OS v9.0 • iPhone/iPad OS v8.0 • iPhone/iPad OS v7.0	• Safari	
• Android 6.x • Android 5.x • Android 4.x	• Firefox • Chrome	
• Chrome OS		
• Windows Phone 10	• Edge	
• Mac OSX 10.12.X • Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari	
• Linux x86/x64 カーネル 4.X 以降	• Firefox	
サポートされている HTML5 のブックマーク: • RDP • Telnet • SSH • VNC • Citrix (Storefront 経由) • ネットワーク エクスプローラ		

Web ベースのクライアント

WorkPlace ポータル、変換 Web、Network Explorer、ホスト/ポート マップ URL アクセス

Web ベース クライアントのシステム要件

オペレーティング システム	ブラウザ	注
• Windows 10	• 該当なし	• 該当なし
• Windows 7 x86/x64 SP1	• 該当なし	• 該当なし

Web ベース クライアントのシステム要件

オペレーティング システム	ブラウザ	注
• Mac OSX 10.12.X • Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari	• Java
• Linux x86/x64 カーネル 4.X 以降	• Firefox	• Java (Firefox バージョン 52 以降では無効)

Web アプリケーション サービス

変換/カスタム ポート マップ/カスタム FQDN マップ Web アプリケーション サービスの要件

オペレーティング システム	ブラウザ	注
• Outlook Web Exchange 2016	• IE (32 ビットのみ)	
• Outlook Web Access 2013	• IE (32 ビットのみ) • Firefox	
• Outlook Web Access 2010	• IE (32 ビットのみ) • Firefox	
• SharePoint 2013	• IE (32 ビットのみ)	
• SharePoint 2010	• Windows 8.1 では IE を使用	

Web アプリケーション: 一般 (簡略)

ブラウザ: Internet Explorer、Firefox、および Chrome

メモ： エイリアス ベースの変換を使用する特定 Web アプリケーションに対するサポートは、これらの基盤 Web アプリケーションの互換性と複雑性に基づきます。一部の Web アプリケーションは、エイリアス ベースの変換に対応していないため、カスタムのホスト マップまたはポート マップ URL アクセスを使用する必要があります。SonicWall は、エイリアス ベースの変換アクセスについて、このセクションで特にリストされているアプリケーションのみをサポートし、テストします。NTLM、BASIC、およびフォーム ベースのシングル サインオン (SSO) をサポートします。

カスタム ポート マップ/カスタム FQDN マップ Web アプリケーション サービスの要件

オペレーティング システム	ブラウザ	注
• Domino Web Access 9.0.1	• IE (9.0.1 のみ) • Firefox • Chrome	

Web アプリケーション: 一般 (詳細)

ブラウザ: Internet Explorer、Firefox、および Chrome

メモ： Java Applets、AJAX、その他の高度な Web テクノロジーを使用する高度な Web アプリケーション向けとして推奨されます。NTLM、BASIC、およびフォーム ベースのシングル サインオン (SSO) をサポートします。

Tunnel クライアント

Connect Tunnel クライアントの要件

オペレーティング システム	ブラウザ	注
• Windows 10	• 該当なし	• 該当なし
• Windows 8.1 x86/x64 Update	• 該当なし	• 該当なし
• Windows 7 x86 SP1/x64	• 該当なし	• 該当なし
• Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari	• Java
• Linux x86/x64 カーネル 4.X 以降	• Firefox	• Java

Connect Tunnel サービスの要件

オペレーティング システム	ブラウザ	注
• Windows 2016 Server R2	• 該当なし	
• Windows 2012 Server R2	• 該当なし	
• Windows 2008 Server R2 x64	• 該当なし	

OnDemand Tunnel エージェントの要件

オペレーティング システム	ブラウザ	注
• Windows 10 Threshold 2 (build 10586) x86/x64	• 該当なし	• 該当なし
• Windows 8.1 x86/x64 Update	• 該当なし	• 該当なし
• Windows 7 x86 SP1/x64	• 該当なし	• 該当なし
• Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari	• Java
• Linux x86/x64 カーネル 3.X 以降	• Firefox	• Java
• TurboLinux v7	• Mozilla	• Java

プロキシ クライアント

Web プロキシ クライアントの要件

オペレーティング システム	ブラウザ	注
• Windows 10	• IE (32 ビットのみ)	• Active X
• Windows 8.1 x86/x64 Update	• IE (32 ビットのみ)	• Active X
• Windows 7 x86 SP1/x64	• IE (32 ビットのみ)	• Active X

OnDemand プロキシ エージェントの要件 (マップ モード)

オペレーティング システム	ブラウザ	注
• Windows 10	• IE (32 ビットのみ) • Firefox	• Active X
• Windows 8.1 x86/x64 Update	• IE (32 ビットのみ) • Firefox	• Active X
• Windows 7 x86/x64 SP1	• IE (32 ビットのみ) • Firefox	• Active X
• Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari	• Java
• Linux x86/x64 カーネル 3.X 以降	• Firefox	• Java

エンド ポイント制御

End Point Control (インタロゲーションおよびインストーラ) クライアントの システム要件

オペレーティング システム	ブラウザ	注
• Windows 10	• IE (32 ビットのみ) • Firefox • Chrome	• Active X
• Windows 8.1 x86/x64 Update	• IE (32 ビットのみ) • Firefox • Chrome	• Active X
• Windows 7 x86 SP1/x64	• IE (32 ビットのみ) • Firefox • Chrome	• Active X
• Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari v9.x • Safari v8.x	• Java
• Linux x86 • Linux x64	• Firefox	• Java

サードパーティ コンポーネント (OESIS、Cache Cleaner) の要件

オペレーティング システム	ブラウザ	注
• Windows 10	• IE (32 ビットのみ) • Firefox	• Active X • OESIS は Firefox ではサポート されていない
• Windows 8.1 x86/x64 Update	• IE (32 ビットのみ) • Firefox	• Active X • OESIS は Firefox ではサポート されていない
• Windows 7 x86 SP1/x64	• IE (32 ビットのみ) • Firefox	• Active X • OESIS は Firefox ではサポート されていない

サードパーティ コンポーネント (OESIS、Cache Cleaner) の要件

オペレーティング システム	ブラウザ	注
• Mac OSX 10.11.X • Mac OSX 10.10.X	• Safari	• Java
• Linux x86 • Linux x64	• Firefox	• Java • OESIS は Firefox ではサポートされていない
• Cache Cleaner 3.6	• Windows • MAC	• Java

GTO クライアント

サポートされる GTO クライアントにリストされている 11.4.0 以上のクライアントだけが GTO ベースのアプライアンスに接続できます。また、以前のバージョンからサポートされているバージョンへのアップグレードもサポートされています。

サポートされる GTO クライアント

クライアント
Windows CT
MAC CT
Linux
Mobile Connect for Android
Mobile Connect for Chrome
Mobile Connect for iOS
Mobile Connect for Mac
Mobile Connect for Windows 10

サーバー コンポーネント

管理者コンポーネントおよび認証サーバーのシステム要件は、次の表にリストされています。

- システム管理
- 認証サーバー
- ActiveSync クライアント
- ActiveSync サーバー
- Outlook Anywhere
- Citrix サーバー ファーム
- サーバー ファーム
- Native Access Modules (NAMs)
- SMA 8200v および CMS プラットフォーム
- API のサポート

システム管理

AMC にアクセスする管理コンピュータのシステム要件

オペレーティング システム	ブラウザ	注
アプライアンス管理コンソール (AMC)		
• Windows 10	• IE (32 ビットのみ) • Firefox	
• Windows 8.1 x86/x64 Update	• IE (32 ビットのみ) • Firefox	
• Windows 7 x86 SP1/x64	• IE (32 ビットのみ) • Firefox	

認証サーバー

要件

オペレーティング システム	バージョン	注
Microsoft		
• Windows 2012 Server R2 x64 • Windows 2008 Server R2 SP1 x64 • Outlook Anywhere		
LDAP サーバ		
• LDAP v3 互換サーバー		IDS では LDAP のパスワード変更をサポート
• IBM Tivoli Directory Server Enterprise Edition	• V6.x	IDS では LDAP のパスワード変更をサポート
• Oracle Directory Server Enterprise Edition	• V11	
• ノベル イーディレクトリ	• V8.8 SP7	
RADIUS プロトコル		
• RSA Authentication Manager	• v8.1 • v7.x	
• 全般	• IP アドレス指定をサポート予定	
• Quest Defender	• v5.81 • v5.7	
シングル サインオン サーバー		
• RSA Federated Identity Manager (Clear Trust)	• RSA Clear Trust Agent 5.5	
SAML サーバー/プロバイダ		
• Office 365	• Azure AD またはローカル AD と同期された Azure AD	
• WorkPlace	• SonicWall CAM	

要件

オペレーティング システム	バージョン	注
• Google Apps/電子メール	• Azure AD または内部の Shibboleth IdP	
• Salesforce.com	• Azure AD または他の IdP	
• Box	• Azure AD または他の IdP	
• Onelogin.com	• Onelogin.com	
• AWS	• Azure AD または他の IdP	
• WorkPlace	• CA SiteMinder	

ActiveSync クライアント

要件

サーバ	バージョン
• Android スマートフォン/タブレット	• Android 6.x • Android 5.x • Android 4.x
• iPhone/iPad	• iPhone/iPad OS V9.x • iPhone/iPad OS v8.x • iPhone/iPad OS v7.x
• Windows Phone	• Windows Phone 10

ActiveSync サーバー

要件

サーバ	バージョン
• Microsoft Exchange	• Exchange 2016 • Exchange 2013 • Exchange 2010

Outlook Anywhere

MAPI over HTTP を使用する Outlook Anywhere

サーバ	クライアント
• Windows 10 Threshold 2 (build 10586) x86/x64	• Outlook 2016
• Windows 8.1 x86/x64 Update	• Outlook 2010 SP2
• Windows 7 SP1 x86/x64	• Outlook 2013 SP1

RPC over HTTP を使用する Outlook Anywhere

サーバ	クライアント
• Windows 10 Threshold 2 (build 10586) x86/x64	• Outlook 2016
• Windows 8.1 x86/x64 Update	• Outlook 2010
• Windows 7 SP1 x86/x64	• Outlook 2013

Citrix サーバー ファーム

要件

サーバ	バージョン
• Citrix	• Citrix XenApp 7.7 • Citrix XenApp 7.6 • Citrix XenDesktop v7.6 • Citrix XenDesktop v7.7

サーバー ファーム

要件

サーバ	バージョン
• vWorkspace	8.6
• VMware Horizon View	6.X

Native Access Modules (NAMs)

Secure Mobile Access アプライアンスは、いくつかの一般的なサードパーティ エージェントと統合します。統合に必要なファイルは、すでにアプリケーション上に用意されていることもありますが、アプライアンスへのコピーが必要となる場合もあります。

要件

説明	注
Terminal Services エージェント	
• Windows V4.x	
• Mac v12.x	• Java
• Linux v13.x	• Java
Citrix Receiver	
• Windows v3.x	
• Mac v3.x	
• Linux v3.x	
VMware View	
• Windows v3.x	

要件

説明	注
• Mac v3.x • Linux v3.x	
vWorkspace • Windows - vWorkspace Connector 8.6 • Mac OSX - vWorkspace Connector 8.6 • 事前インストール済みの Linux vWorkspace Connector 8.6	

SMA 8200v および CMS プラットフォーム

vWorkspace サーバー ファームの要件

コンポーネント Web ベース	バージョン
• VMWare	• ESX/ESXi 6.0、7.x
• Microsoft Hyper-V	• Windows Server 2016

API のサポート

API のサポート

コンポーネント Web ベース	バージョン
• 管理 API	• Ruby 1.9.3 • Mechanize 2.7.4
• 認証 API	• Ruby 1.9.3 • Mechanize 2.7.4

第 2 部

インストール

- インストールと初期セットアップ

2

インストールと初期セットアップ

ネットワークのアーキテクチャ

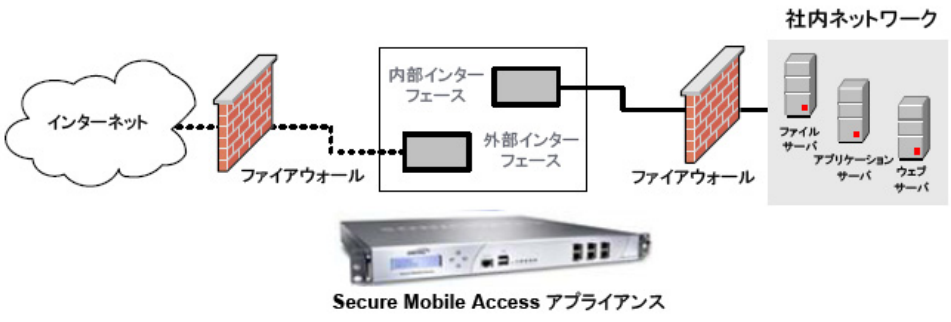
このセクションでは、ネットワーク環境におけるアプライアンスの位置付けを示し、インストールと配線の手順を紹介します。また、Web ベースの Setup Wizard (またはコマンドラインのSetup Tool) によるネットワーク基本構成についても説明します。

すべての SonicWall SMAアプライアンスは、デュアル インターフェースまたはシングル インターフェース構成のいずれかで設定できます。

メモ：SMA7200、SMA6200、EX9000、EX7000、および EX6000 アプライアンスには、外部ロードバランサを使用するように設定できる物理ネットワーク インターフェースが含まれています。

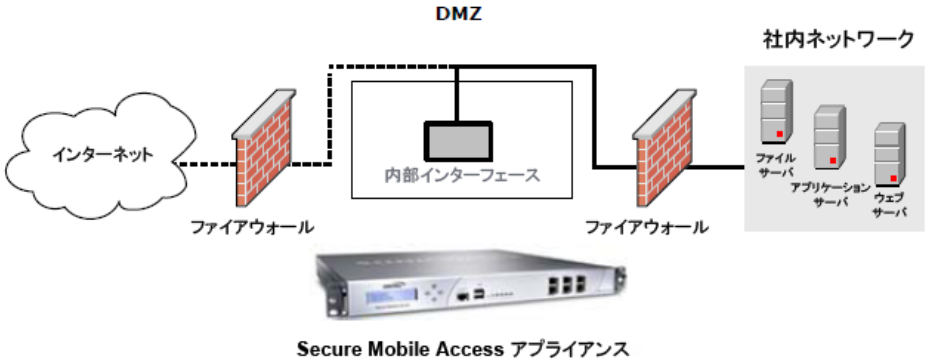
- デュアルホーム インターフェース構成 (内部および外部インターフェース、デュアルホーム インターフェース構成を参照): 外部トラフィック (インターネットとの通信) 用にネットワーク インターフェースを 1 つ使用し、もう 1 つのインターフェースは内部トラフィック (企業ネットワークとの通信) 用に使用します。

  デュアルホーム インターフェース構成



- シングルホーム インターフェース構成 (内部インターフェース、シングルホーム インターフェース構成参照): 単一のネットワーク インターフェースが、内部トラフィックと外部トラフィックの両方で使用されます。アプライアンスは通常、非武装地帯 (略称 DMZ、境界ネットワークとも呼ばれる) にインストールされます。

シングルホーム インターフェース構成



どちらの構成でも、Secure Mobile Access サービスが受け取る要求 (Web プロキシ サービスの HTTP/S トラフィックを含む) は、ポート 80 (HTTP) およびポート 443 (HTTPS) を通って送信されます。ただし、OnDemand エージェントからのトラフィックは常にポート 443 経由で送信されます。ほとんどのネットワークでは、トラフィックがこれらのポート経由で送られるように構成されているため、ネットワークのファイアウォールを再構成する必要はありません。

アプライアンスは、ネットワーク上の次のようなリソースに接続できる場所にインストールする必要があります。

- Web サーバー、Windows サーバー、クライアント/サーバー アプリケーションを含む、アプリケーション サーバーおよびファイル サーバー。
- 外部認証リポジトリ (LDAP サーバー、Microsoft Active Directory サーバー、RADIUS サーバーなど)。
- 1 つまたは複数の Domain Name System (DNS) サーバー。
- (オプション) Windows Internet Name Service (WINS) サーバー。これは、WorkPlace を 使用して Windows ネットワークをブラウズするために必要です。

△ **注意：SonicWall SMA アプライアンスは完全なファイアウォール機能を提供しないため、ファイアウォール内でセキュリティを確保しなければなりません。ファイアウォールなしで動作させると、アプライアンスが攻撃に対して弱くなり、セキュリティが脅かされたりパフォーマンスが低下したりする可能性があります。**

必須ではありませんが、アプライアンスが次のリソースと通信できるようにすることで、機能と使い勝手が向上します。

- アプライアンスの時刻を同期するための Network Time Protocol (NTP) サーバー。
- syslog 出力を保管しておくための外部サーバー。
- Secure Shell (SSH) アクセスのための管理者用ワークステーション。

アプライアンスは、自己署名サーバー証明書を使用する構成にできる他、商用認証局 (CA) から証明書を取得してセキュリティを強化する構成にすることもできます。詳細については、商用 CA からの証明書の取得を参照してください。

インストールの準備

インストールを始める前に、ネットワーキング環境についての情報を収集し、アプライアンスとの間のトラフィックを許可するようにファイアウォールが正しく構成されていることを確認する必要があります。

トピック:

- 情報の収集
- ファイアウォール ポリシーの確認
- 便利な管理ツール

情報の収集

アプライアンスを設定する前に、次の情報を収集する必要があります。この情報の一部については、Setup Wizard (を参照Setup Wizard による Web ベースでの構成) または Setup Tool (を参照 Setup Tool による新しいアプライアンスの構成) を実行するときに指定しますが、ほとんどの情報は AMC (を参照ネットワークと認証の構成) でアプライアンスを構成するときに使用します。

トピック:

- アプライアンス管理コンソールの起動に必要な設定
- 証明書情報
- ネーム ルックアップ情報
- 認証情報
- 仮想アドレス プールの情報
- オプションの構成情報

アプライアンス管理コンソールの起動に必要な設定

- アプライアンスを管理するための root パスワード
- アプライアンスの名前 (この名前はログ ファイルのみで使用されるため、DNS に追加する必要はありません)
- 内部 IP アドレス、および (オプションで) 外部 IP アドレス
- ルーティング モードを選択し、インターネットと企業ネットワークに接続するためのネットワーク ゲートウェイ用 IP アドレスをそれぞれ指定します。

証明書情報

サーバー証明書と AMC 証明書を生成するときは、次の情報が使用されます。

- アプライアンスの完全修飾ドメイン名 (FQDN)。また、固有名を使用する WorkPlace サイトがある場合は、その FQDN。これらの名前はパブリック DNS に追加する必要があります。また、これらの名前はユーザーが Web ベースのリソースに接続するときにも参照できます。
- アプライアンス管理コンソール (AMC) サーバーの FQDN。AMC サーバー名は、アプライアンス管理用 Web ツールである AMC へのアクセスに使用されます。

ネーム ルックアップ情報

- アプライアンスが接続するネットワークの内部 DNS ドメイン名
- プライマリ内部 DNS サーバー アドレス (追加の DNS サーバーはオプション)
- 内部 WINS サーバーの IP アドレスと Windows ドメインの名前 (WorkPlace を使用して Windows ネットワークのファイルをブラウズする場合は必要ですが、それ以外はオプション)

認証情報

- 認証サーバー (LDAP、Active Directory、または RADIUS) の名前とログイン情報

仮想アドレス プールの情報

- ネットワーク トンネル クライアント (Connect Tunnel または OnDemand トンネル) を展開する場合は、1 つまたは複数のアドレス プールに IP アドレスを割り当てる必要があります。詳細については、IP アドレス プールの構成を参照してください。

オプションの構成情報

- リモート マシンからの SSH アクセスのためには、リモート ホストの IP アドレスを知っておく必要があります。
- NTP サーバーと同期させるときは、1 つまたは複数の NTP サーバーの IP アドレスを知っておく必要があります。
- データを syslog サーバーに送信するときは、1 つまたは複数の syslog サーバーの IP アドレスとポート番号を知っておく必要があります。

ファイアウォール ポリシーの確認

アプライアンスが正しく機能するためには、外部 (インターネット側) と内部のファイアウォールでポートを開かなければなりません。

外部ファイアウォール

Web ブラウザまたは OnDemand からアプライアンスへ安全にアクセスできるようにするには、サイトのファイアウォールでポート 80 とポート 443 を開いておかなければなりません。SMA が外部ネットワークで使用するトラフィックの種類とポートを参照してください。SSH アクセスを許可するためにファイアウォールを開いておくことは必須条件ではありませんが、リモート システムから管理作業をする上で便利です。

SMA が外部ネットワークで使用するトラフィックの種類とポート

トラフィック種別	ポート/プロトコル	使用法	必須かどうか
HTTP	80/tcp	非暗号化ネットワーク アクセス	Y
HTTPS	443/tcp	暗号化ネットワーク アクセス	Y

SMA が外部ネットワークで使用するトラフィックの種類とポート

トラフィック種別	ポート/プロトコル	使用法	必須かどうか
SSH	22/tcp	アプライアンスへの管理アクセス	
ESP	4500/UDP	トンネル ネットワーク トラフィックの ESP カプセル化を有効にする	

内部ファイアウォール

内部ネットワークにファイアウォールがある場合、ポリシーを調整して、アプライアンスが通信するバックエンド アプリケーション用にポートを開く必要があります。場合によっては、DNS や電子メールなどの標準ネットワーク サービス用のポートを開く以外に、アプライアンスが SMA が内部ネットワークで使用するトラフィックの種類とポートに示されているサービスにアクセスできるようにファイアウォール ポリシーを変更する必要があります。

SMA が内部ネットワークで使用するトラフィックの種類とポート

トラフィック種別	ポート/プロトコル	使用法
Microsoft ネットワーキング	• 138/tcp および 138/udp • 137/tcp および 137/udp • 139/udp • 162/snmp • 445/smb	WorkPlace が WINS 名前解決、要求のブラウズ、ファイル共有へのアクセスのために使用
LDAP (非暗号化)	389/tcp	LDAP ディレクトリまたは Microsoft Active Directory との通信
LDAP over SSL (暗号化)	636/tcp	SSL を介した LDAP ディレクトリまたは Microsoft Active Directory との通信
RADIUS	1645/udp または 1812/udp	RADIUS 認証サーバーとの通信
NTP	123/udp	アプライアンスのクロックと NTP サーバーとの同期
Syslog	514/tcp	システム ログ情報の syslog サーバーへの送信
SNMP	161/udp	SNMP 管理ツールからのアプライアンスの監視

便利な管理ツール

Microsoft Windows が動作するリモート システムからアプライアンスを管理するときは、次の管理ツールを使用すると便利です。どちらのツールも、標準 FTP や Telnet ユーティリティと異なり、暗号化により情報漏洩を防止します。

- **Secure Shell (SSH) クライアント**このツールを使用すると、アプライアンスに安全にログインして、コマンドラインから構成を行うことができます。システムのバックアップ、ログ ファイルの表示、高度なネットワーク設定の構成などを行う際に便利です。一般的な Windows 用 SSH クライアントの 1 つに、VanDyke Software の SecureCRT があります。
  http://www.vandyke.com/products/securecrt/ から評価版をダウンロードできます。また、Telnet

と SSH を Windows プラットフォームに無料で実装できる PuTTY も広く使用されています。PuTTY は Cisco が推奨しています。

SSH を使用してアプライアンスに接続するときは、ユーザー名に `root` と入力し、Setup Wizard で作成したパスワードを入力します。

- **Secure Copy (SCP) クライアント** このツールを使用すると、Windows が動作する PC からアプライアンスへファイルを簡単かつ安全に転送できます。証明書などのデータをアプライアンスにコピーする際に便利です。Windows クライアントとしては WinSCP が広く使用されており、http://winscp.sourceforge.net/eng/ で提供されています。

実行する必要があるほとんどの構成管理作業 (アプライアンス構成のバックアップとリストア、アップグレードの適用など) は、AMC の [**Maintenance (メンテナンス)**] ページから実行できます (構成データの管理を参照)。このような作業をコマンドラインから実行したい場合は、構成データの保存とリストアを参照してください。

インストールと展開のプロセス

このセクションでは、アプライアンスのインストール、構成、テスト、および実稼働環境への展開について概説します。概要については、インストール手順を参照してください。

インストール手順

インストール手順	説明
アプライアンスのシリアル番号と認証コードを書き留める	この情報は、MySonicWall で製品を登録する際に必要です。シリアル番号と認証コードは、アプライアンスのラベルに印刷されている他、AMC の [**General Settings (一般設定)**] ページにも表示されます。
アプライアンスをラックマウントし、ケーブルに接続する	仕様およびラックのインストールおよびアプライアンスの接続を参照してください。
アプライアンスの電源をオンにして、構成を開始する	内部ネットワークでアプライアンスを接続するには、内部 IP アドレスとサブネット マスクを指定し、またアプライアンスがクラスタの一部かどうかを指定する必要があります。アプライアンスのフロントパネルの操作ボタンを使用します。電源投入とネットワークの基本設定を参照してください。
Setup Wizard を実行する	ウィザードの指示に従い、SMA アプライアンスの初期セットアップ操作を実行します。Setup Wizard による Web ベースでの構成を参照してください。
MySonicWall でアプライアンスを登録する	MySonicWall でアプライアンスを登録します。製品登録により、ライセンス ファイルやアップデートなどの重要リソースにアクセスできるようになります。登録には、アプライアンスのシリアル番号と認証コードの両方が必要です。

SMA アプライアンスのライセンスには、いくつかの種類があります。すべてのライセンス ファイルを MySonicWall から取得して、アプライアンスにインポートする必要があります。ソフトウェア ライセンスを参照してください。

MySonicWall で無料評価ライセンスを選択すると、30 日間 24 時間サポートを受けることができます。

CMS 仮想マシンをインストールして MySonicWall に登録しない場合、次のライセンスが取得されます。

- 15 セントラル ユーザー ライセンスを 3 日間
- 3 台の管理対象アプライアンスを 3 日間

Setup Wizard と AMC は、いずれもアプライアンスを構成するための Web アプリケーションです。これらのアプリケーションを実行する PC では、JavaScript が有効になっていなければなりません。JavaScript は、WorkPlace へのアクセスに使用するブラウザでも有効にする必要があります。

トピック:

- 仕様およびラックのインストール
- フロント パネルの操作ボタンとインジケータ
- アプライアンスの接続
- 電源投入とネットワークの基本設定
- Setup Wizard による Web ベースでの構成
- 管理コンソールでのアプライアンスの構成
- アプライアンスの実稼動
- アプライアンスの電源停止と再起動
- SMA 8200v の Hyper-V

仕様およびラックのインストール

アプライアンスのパッケージを開いたら、ネットワーク上でインストールと構成を行います。アプライアンスは、標準の 19 インチ テレコム ラックに収容できるように設計されています。アプライアンスを接続する前に、十分なスペースと適切な電力を使用できることを確認します。各アプライアンス モデルの仕様は次のとおりです。

- SonicWall SMA 7200 および SMA 6200ハードウェア
- SonicWall E-Class SMA EX9000 ハードウェア
- SonicWall E-Class SMA EX7000 および EX6000 ハードウェア

SonicWall SMA 7200 および SMA 6200ハードウェア

SMA 7200 および SMA 6200 には、次のものが含まれています。

- レール (キット内、取り付けられていません)
- IEC 60320 C13 コネクタから NEMA 15 プラグへの標準的な米国用電源コード
- 1Gb イーサネット ポート × 6
- 10Gb SFP+ ポート (SMA7200) × 2
- USB ポート × 2
- DIAG ポート × 1
- 500 GB SATA ハード ドライブ × 2

仕様

	SMA 7200	SMA 6200
規制モデル/タイプ	1RK30-0AF	1RK31-0B0
CPU	E3-1275 3.5GHz	I5-4570S 2.9GHz

仕様

	SMA 7200	SMA 6200
RAM	16GB DDR3 1600MHz ECC × 4	8GB DDR3 1600MHz ECC × 4
ネットワーク ポート	8 (6 ポート 1GE + 2 ポート 10Gb SFP+)	6 (6 ポート 1GE)
電力供給	デュアル ホット スワップ可能	固定
フロント パネル 図解	SMA 6200/7200 フロント パネルを参照してください。	SMA 6200/7200 フロント パネルを参照してください。

SonicWall E-Class SMA EX9000 ハードウェア

SonicWall E-Class SMA EX9000 には、次のものが含まれています。

- レール (キット内、取り付けられていません)
- IEC 60320 C13 コネクタから NEMA 15 プラグへの標準的な米国用電源コード
- 1 GB Ethernet ポート
- 10 GB Ethernet ポート
- USB ポート × 2
- DIAG ポート × 1
- 80 GB SATA ハード ドライブ × 2
- アプライアンスへのシリアル接続 (115,200 ボーレート)

SonicWall E-Class SMA EX7000 および EX6000 ハードウェア

SonicWall E-Class SMA EX7000 および EX6000には、次のものが含まれています。

- レール (キット内、取り付けられていません)
- IEC 60320 C13 コネクタから NEMA 15 プラグへの標準的な米国用電源コード
- 1 GB Ethernet ポート
- USB ポート × 2
- 80 GB SATA ハード ドライブ
- アプライアンスへのシリアル接続 (115,200 ボーレート)

プロセッサの性能、RAM、ネットワーク ポート、および電力供給は、モデル間で異なります。

ハードウェア仕様

	SMA EX9000	SMA EX7000	SMA EX6000
規制モデル/タイプ	2RK03-092	1RK15-059	1RK20-05A
Intel プロセッサ		Core 2 Duo 2.1GHz CPU	Celeron 2.0GHz CPU
RAM	32 GB	2 GB DDR533	1 GB DDR533
PCIe Gigabit ネットワーク ポート	12 (8 ポート 1GE + 4 ポート 10GE)	6 (HA ペアはサポートされていません)	4 (HA ペアはサポートされていません)

ハードウェア仕様

	SMA EX9000	SMA EX7000	SMA EX6000
電力供給	デュアル ホット スワップ可能	デュアル ホット スワップ可能	固定
フロント パネル (図解)	EX9000 アプライアンスのフロント パネルの操作ボタンを参照してください。	EX7000 アプライアンスのフロント パネルの操作ボタンを参照してください。	EX6000 アプライアンスのフロント パネルの操作ボタンを参照してください。

フロント パネルの操作ボタンとインジケータ

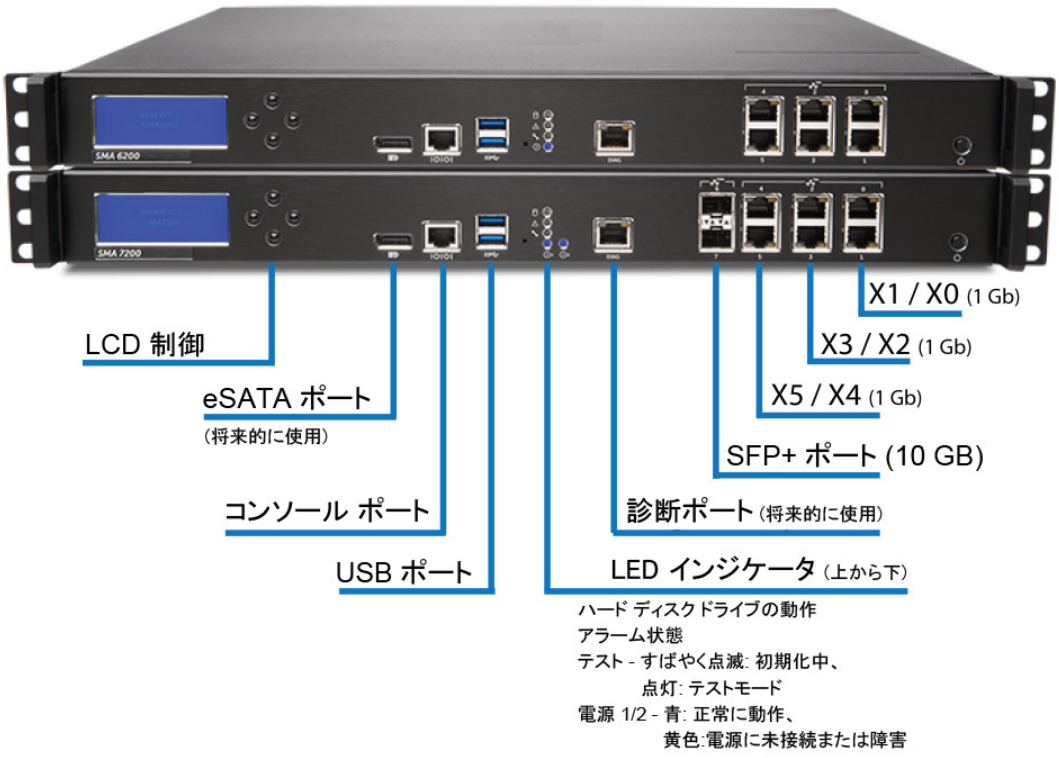
アプライアンスの電源を投入する前に、フロント パネルの操作ボタンを確認しておきます。

- SMA 6200/7200 フロント パネル
- EX9000 アプライアンスのフロント パネルの操作ボタン
- EX7000 アプライアンスのフロント パネルの操作ボタン
- EX6000 アプライアンスのフロント パネルの操作ボタン
- SMA 7200、SMA 6200、EX9000、EX7000、EX6000 の LCD 操作ボタン

SMA 6200/7200 フロント パネル

電源ボタンは、フロント パネルの右下にあります。

SMA 6200 および SMA 7200のフロント パネル



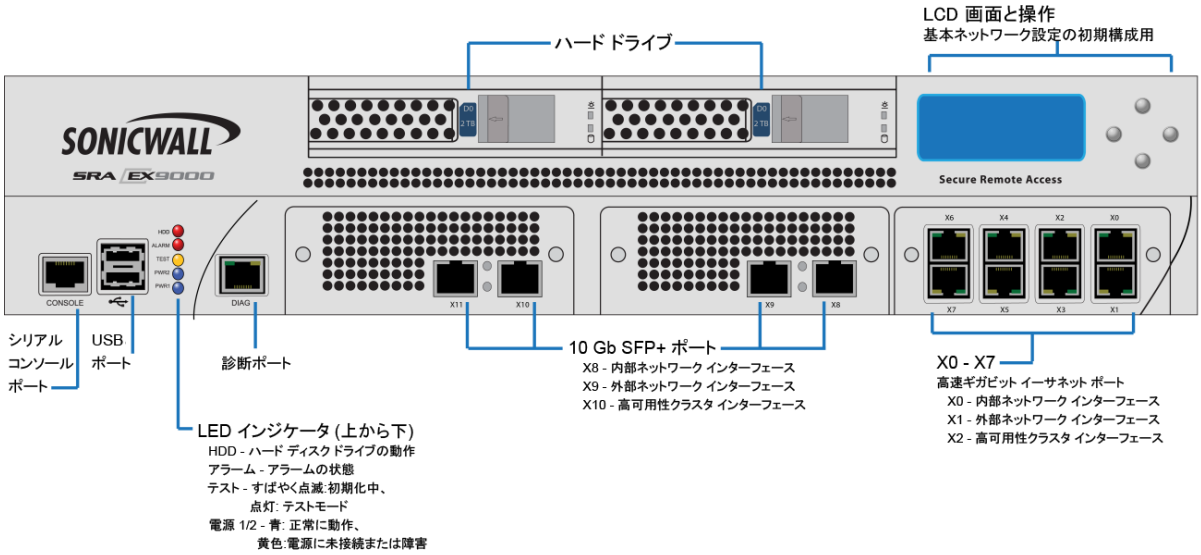
フロント パネルの操作ボタンとインジケータ

項目	説明
ハード ドライブ モジュール	デュアル ハード ドライブ。
LCD 表示画面と操作ボタン	アプライアンスのステータスと構成を示します。キーパッド ボタンはアプライアンスのステータス表示と初期設定の構成に使用します。 • アプライアンスのステータス表示、およびキーパッドによるアプライアンスの終了や再起動の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、EX6000 の LCD 操作ボタンを参照してください。 • 初期構成時の LCD 操作ボタンの使用 (Setup Wizard を実行するため) の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、または EX6000 アプライアンスの設定を参照してください。
コンソール ポート	イーサネット ケーブルを使用してアプライアンスをパーソナル コンピュータに接続します。
USB ポート	2 個の USB ポートがあります。
LED インジケータ	LED インジケータは、上から次の順に配置されています。 • ハード ディスク ドライブの動作 • アラーム • テスト • 電源 1 および 2: •青: 正常に動作 •黄色: 電源に未接続または障害
DIAG ポート	診断ポート。
X0: 内部ネットワーク	内部ネットワークにアプライアンスを接続します。
X1: 外部ネットワーク	外部ネットワークにアプライアンスを接続します。
X2: クラスタ インターフェース	SMA 12 では、X2 インターフェースでのクラスタリングはサポートされなくなりました。廃止された機能を参照してください。
X3-X5	使用しません。
X6 SFP+: 内部ネットワーク	内部 10Gb ネットワークにアプライアンスを接続します。
X7 SFP+: 外部ネットワーク	外部 10Gb ネットワークにアプライアンスを接続します。

EX9000 アプライアンスのフロント パネルの操作ボタン

電源スイッチは、背面パネルにあります。

EX9000 のフロント パネル



EX9000 フロント パネルの操作ボタンとインジケータ

項目	説明
ハード ドライブ モジュール	デュアル ハード ドライブ。
LCD 表示画面と操作ボタン	アプライアンスのステータスと構成を示します。キーパッド ボタンはアプライアンスのステータス表示と初期設定の構成に使用します。 • アプライアンスのステータス表示、およびキーパッドによるアプライアンスの終了や再起動の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、EX6000 の LCD 操作ボタンを参照してください。 • 初期構成時の LCD 操作ボタンの使用 (Setup Wizard を実行するため) の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、または EX6000 アプライアンスの設定を参照してください。
コンソール ポート	DB-9 シリアル ケーブルを使用してアプライアンスを PC に接続します。
USB ポート	2 個の USB ポートがあります。
LED インジケータ	LED インジケータは、上から次の順に配置されています。 • HDD ハード ディスク ドライブ (赤のライトはディスク稼働中を示します) • アラーム • テスト • 電源 2 および 1 •青: 正常に動作 •黄色: 電源に未接続または障害
DIAG ポート	診断ポート。
X8: 10GigE ネットワーク	内部 10GigE ネットワークにアプライアンスを接続します。
X9: 10GigE ネットワーク	外部 10GigE ネットワークにアプライアンスを接続します。

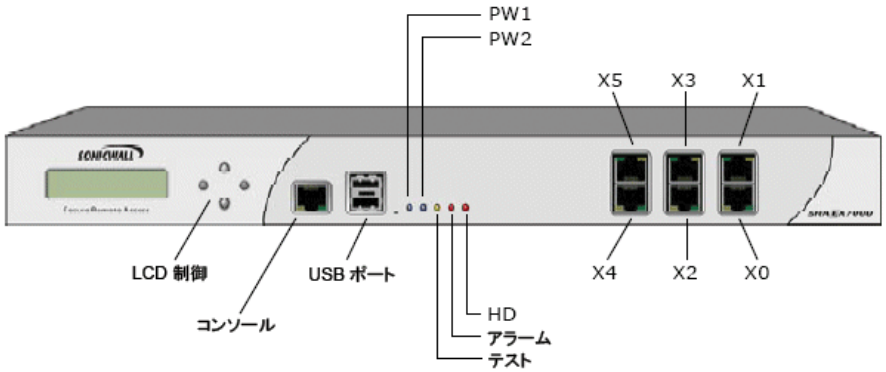
EX9000 フロント パネルの操作ボタンとインジケータ

項目	説明
X10: 10GigE ネットワーク	SMA 12 では、X2 インターフェースでのクラスタリングはサポートされなくなりました。廃止された機能を参照してください。
X11	使用しません。
X0: 内部ネットワーク	内部ネットワークにアプライアンスを接続します。
X1: 外部ネットワーク	外部ネットワークにアプライアンスを接続します。
X2: クラスタ インターフェース	SMA 12 では、X2 インターフェースでのクラスタリングはサポートされなくなりました。廃止された機能を参照してください。
X3 ～ X7	使用しません。

EX7000 アプライアンスのフロント パネルの操作ボタン

電源スイッチは、背面パネルにあります。

EX7000 のフロント パネル



EX7000 フロント パネルの操作ボタンとインジケータ

項目	説明
LCD 表示画面と操作ボタン	アプライアンスのステータスと構成を示します。キーパッド ボタンはアプライアンスのステータス表示と初期設定の構成に使用します。 • アプライアンスのステータス表示、およびキーパッドによるアプライアンスの終了や再起動の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、EX6000 の LCD 操作ボタンを参照してください。 • 初期構成時の LCD 操作ボタンの使用 (Setup Wizard を実行するため) の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、または EX6000 アプライアンスの設定を参照してください。
コンソール	DB-9 シリアル ケーブルを使用してアプライアンスを PC に接続します。
USB ポート	2 個の USB ポートがあります。
LED インジケータ	LED インジケータは、左から次の順に配置されています。 • 電源 1 および 2 • テスト • アラーム • ハード ディスク ドライブ (赤のライトはディスク稼働中を示します)
X0: 内部ネットワーク	内部ネットワークにアプライアンスを接続します。

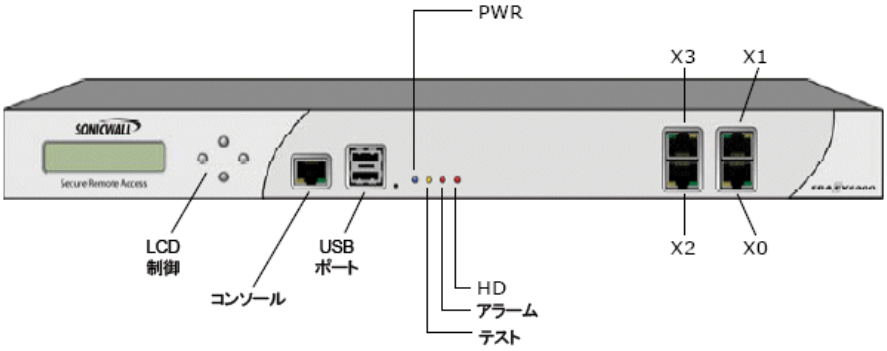
EX7000 フロント パネルの操作ボタンとインジケータ

項目	説明
X1: 外部ネットワーク	外部ネットワークにアプライアンスを接続します。
X2: クラスタ インターフェース	SMA 12 では、X2 インターフェースでのクラスタリングはサポートされなくなりました。廃止された機能を参照してください。
X3-X5	使用しません。

EX6000 アプライアンスのフロント パネルの操作ボタン

電源スイッチは、背面パネルにあります。

EX6000 のフロント パネル



EX6000 フロント パネルの操作ボタンとインジケータ

項目	説明
LCD 表示画面と操作ボタン	アプライアンスのステータスと構成を示します。キーパッド ボタンはアプライアンスのステータス表示と初期設定の構成に使用します。 • アプライアンスのステータス表示、およびキーパッドによるアプライアンスの終了や再起動の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、EX6000 の LCD 操作ボタンを参照してください。 • 初期構成時の LCD 操作ボタンの使用 (Setup Wizard を実行するため) の詳細については、SMA 7200、SMA 6200、EX9000、EX7000、または EX6000 アプライアンスの設定を参照してください。
コンソール	DB-9 シリアル ケーブルを使用してアプライアンスを PC に接続します。
USB ポート	2 個の USB ポートがあります。
LED インジケータ	LED インジケータは、左から次の順に配置されています。 • 電源 • テスト • アラーム • ハード ディスク ドライブ
X0: 内部ネットワーク	内部ネットワークにアプライアンスを接続します。
X1: 外部ネットワーク	外部ネットワークにアプライアンスを接続します。
X2: クラスタ インターフェース	SMA 12 では、X2 インターフェースでのクラスタリングはサポートされなくなりました。廃止された機能を参照してください。
X3	使用しません。

SMA 7200、SMA 6200、EX9000、EX7000、EX6000 の LCD 操作ボタン

SMA および EX シリーズ アプライアンスの LCD 表示の右側にある 4 ボタンのキーパッドを使用して、次の操作を行います。

- アプライアンスのステータスと構成情報を示します。
- アプライアンスを終了または再起動します。

注意：SMA 6200、SMA 7200、EX9000、EX7000、および EX6000 アプライアンス: アプライアンスを再起動する前には、USB デバイスをアプライアンスから取り外します。再起動時に USB デバイスがアプライアンスに接続されていると、アプライアンスはそれを起動デバイスとして使用しようとします。その結果、アプライアンスの BIOS に保存される起動情報が上書きされ、デバイスを使用できなくなります。

LCD キーパッドの機能

キーパッドの機能	説明

左ボタン	アプライアンスを再起動するには、**左**ボタンを 1 回押します。次のプロンプトが表示されます。
	`Restart appliance?`
	`<Yes No>`
	そのままアプライアンスを再起動する場合は、**左**ボタンを再び押します。再起動を中止する場合は、**右**ボタンを押します。

上ボタン	アプライアンスのネットワーク設定の構成を表示するには、**上**ボタンを 1 回押します。上ボタンを 1 回押すたびに、次のネットワーク設定が順に表示されます。 • 内部アドレス • 外部アドレス • デフォルト ゲートウェイ • ホスト名 • ドメイン名 • IP アドレス • ネットマスク

右ボタン	アプライアンスを終了するには、**右**ボタンを 1 回押します。次のプロンプトが表示されます。
	`Shut down now?`
	`<Yes No>`
	そのままアプライアンスを終了する場合は、**左**ボタンを押します。終了を中止する場合は、**右**ボタンを再び押します。

下ボタン	デフォルト表示に戻る場合や画面をリフレッシュする場合は、下ボタンを 1 回押します。

アプライアンスの接続

アプライアンスをネットワークに接続する場合、それぞれのアプライアンス モデルに対応する手順に従います。

- SMA 6200 または SMA 7200 アプライアンスの接続
- EX9000 アプライアンスの接続
- EX7000 アプライアンスの接続
- EX6000 アプライアンスの接続
- 電源投入とネットワークの基本設定

SMA 6200 または SMA 7200 アプライアンスの接続

アプライアンスの図は、SMA 6200/7200 フロント パネルを参照してください。

SMA 6200/7200 アプライアンスを接続するには

1 内部ネットワークとアプライアンスの内部インターフェースをネットワーク ケーブルで接続します（X0 は 1GB、X6 は 10GB）。

2 必要に応じて、外部ネットワークとアプライアンスの外部インターフェースをケーブルで接続します（X1 は 1GB、X7 は 10GB）。

3 付属の電源コードをアプライアンスの電源と AC コンセントに接続します。

EX9000 アプライアンスの接続

アプライアンスの図は、EX9000 アプライアンスのフロント パネルの操作ボタンを参照してください。

EX9000 アプライアンスを接続するには

1 内部ネットワークとアプライアンスの内部インターフェース (X0) をネットワーク ケーブルで接続します。

2 必要に応じて、外部ネットワークとアプライアンスの外部インターフェース (X1) をケーブルで接続します。

3 標準 AC 電源コードを電源端子に接続します。

EX7000 アプライアンスの接続

アプライアンスの図は、EX7000 アプライアンスのフロント パネルの操作ボタンを参照してください。

EX7000 アプライアンスを接続するには

1 内部ネットワークとアプライアンスの内部インターフェース (X0) をネットワーク ケーブルで接続します。

2 必要に応じて、外部ネットワークとアプライアンスの外部インターフェース (X1) をケーブルで接続します。

3 標準 AC 電源コードを電源端子に接続します。

EX6000 アプライアンスの接続

アプライアンスの図は、EX6000 アプライアンスのフロント パネルの操作ボタンを参照してください。

EX6000 アプライアンスを接続するには

1 内部ネットワークとアプライアンスの内部インターフェース (X0) をネットワーク ケーブルで接続します。

2 必要に応じて、外部ネットワークとアプライアンスの外部インターフェース (X1) をケーブルで接続します。

3 標準 AC 電源コードを電源端子に接続します。

電源投入とネットワークの基本設定

アプライアンスの接続が終わったら、ここで初めて電源を投入し、構成プロセスに移ります。アプライアンスの運用を迅速に実現する上で必要な設定を構成するには、Web ベースの Setup Wizard を使用します。しかし、ウィザードを開始するには、まず Web ブラウザをアプライアンスに接続するための情報を指定する必要があります。

アプライアンスの構成が完了すると、構成と処理の制御をアプライアンス管理コンソール (AMC) から実行できるようになります。アプライアンスの LCD 画面では、アプライアンスに関する基本情報 (名前や内部アドレスなど) を確認したり、再起動したりできます。これは、AMC の実行に使用するブラウザと同じ領域にアプライアンスがない場合に便利な機能です。

メモ：アプライアンスを工場出荷時のデフォルト設定に戻す場合を除いて、すでに構成が終わっているアプライアンスで Setup Wizard を実行することはできません。これは、アプライアンスの初期構成に Setup Wizard を使用した場合も、コマンドラインから `setup_tool` を実行した場合も同じです。管理コンソールでのアプライアンスの構成を参照してください。

基本ネットワーク設定の構成

Setup Wizard を開始する前に、Web ブラウザをアプライアンスに接続するための情報を指定する必要があります。初期セットアップでは、LCD 操作ボタンを使用して最低限の設定を行ってから Setup Wizard を実行する手順が推奨されます。LCD 操作ボタンは、アプライアンス前面の LCD 画面の右手にあります。または、コマンドラインで Setup Tool を使用する操作も任意に選択できます。それぞれの手順については後述します。

基本設定を入力したら、Web ベースの Setup Wizard を実行できます (Setup Wizard による Web ベースでの構成を参照)。

SMA 7200、SMA 6200、EX9000、EX7000、または EX6000 アプライアンスの設定

アプライアンス前面の LCD 画面の右にある 4 つのボタンを使用して、設定項目を入力します。

LCD 操作ボタンによるネットワーク基本設定の構成

LCD 操作ボタンで設定するには、

1 **上**ボタンまたは**下**ボタンを押して初期画面を表示させます。

2 **右**ボタンを押して進めます。

3 内部インターフェース用 IP アドレスの設定。表示される IP アドレスを変更するには:

   a **左**および**右**ボタンを使用して、変更したい番号にカーソルを合わせます。

   b **上**および**下**ボタンを使用して、番号を変更します。

   c **右**ボタンを押して次の画面に進みます。

4 サブネット マスクの入力:

   a 4 つのボタンを使用して、LCD 画面に表示される IP アドレスを変更します。

   b **右**ボタンを押して次の画面に進みます。

5 設定を見直して確定します。しばらくすると設定が保存され、デスクトップ PC で特定の URL にブラウズするように指示が表示されます。これは、Setup Wizard でアプライアンスの構成を続行するための URL です。例えば、LCD ディスプレイには次のように表示されます。

```
Please browse to: https://172.31.0.140:8443
```

Setup Wizard でのアプライアンスの構成については、Setup Wizard による Web ベースでの構成を参照してください。

コマンドラインでの Setup Tool によるアプライアンスの構成

Setup Wizard を実行するために必要な最低限の構成項目を設定するには、Setup Tool を使用する必要があります。手順の概要を次に示します。詳細な手順については Setup Tool による新しいアプライアンスの構成を参照してください。

Setup Tool でネットワーク基本設定を設定するには、

1 端末エミュレーション プログラムを使用して、ノート型 PC または端末からアプライアンスへのシリアル接続を確立します。

2 アプライアンスの電源をオンにします。シリアル接続から初めてシステムを起動するときは、Setup Tool が自動的に実行します。ログイン要求が表示されたら、ユーザー名として `root` と入力します。

3 アプライアンスを構成する際は、次の情報を指定するように求められます。

   - 内部インターフェースの IP アドレスとサブネット マスク
   - 内部インターフェースへのアクセスに使用するデフォルト ゲートウェイ (オプション)

Setup Wizard でのアプライアンスの構成については、Setup Wizard による Web ベースでの構成を参照してください。

Setup Wizard による Web ベースでの構成

Setup Wizard を使用すると、アプライアンスの構成で必須およびオプションの設定を順を、追って操作できます。AMC のホーム ページには、指定済みの項目を示す [**Setup Checklist (セットアップ確認リスト)**] が表示されます。

Setup Wizard を実行するには、AMC と同じシステム構成が必要となります (詳細はシステム要件を参照)。さらに、ブラウザで JavaScript を有効にしておく必要があります。

設定を行うには、

1 **License agreement: (ライセンス契約:)**使用許諾契約の条件を読みます。

2 **Basic Settings (基本設定:)**

- AMC へのアクセスに使用するパスワードを指定します。パスワードは 8 文字以上 20 文字以下で指定する必要があります。
- (オプション) 時間帯を選択して [**Change (変更)**] をクリックし、現在時刻を設定します。時刻は、後から AMC で NTP サーバーに同期できます。詳細については、時刻設定の構成を参照してください。ライセンス ファイルをインポートする前に、適切な時間帯でアプライアンスの日時設定が正しいことを確認することが重要です。

3 **Network Settings (ネットワーク設定):**

- アプライアンスの名前を入力します (デフォルトは *SMA1000SSLVPN*)。

  ヒント：この名前はログ ファイルのみで使用されるため、DNS に追加する必要はありません。

- 内部インターフェース (プライベート ネットワークに接続) の IP アドレスとサブネット マスクが表示されます。デュアルホーム構成では、外部インターフェースの IP アドレスとサブネット マスクを入力します。

4 **ルーティング**: 既存のルータを利用する場合は、リソースへのアクセスのためにデュアル ゲートウェイ オプションを選択します。アプライアンスが受信するトラフィックを少数のルータまたはサブネットに制限する場合は、シングル ゲートウェイ オプションを選択し、後で AMC でルータまたはサブネットをスタティック ルートとして入力します。

アプライアンスの場所が AMC にアクセスするのに使用するコンピュータとは異なるネットワーク上にある場合は、ルーティングをセットアップして AMC へのアクセスを保持する必要があります。

5 **名前解決**: アプライアンスでは、内部ネットワーク上のリソースにアクセスするために名前解決を実行できなければなりません。アプライアンスが配置されているドメイン (`yourcompany.com` など) をデフォルトとして入力します。

6 **ユーザー アクセス**: OnDemand Tunnel アクセス エージェントのプロビジョニングを行って、ネットワークへのフル アクセスを実行できる権限をユーザーに付与できます。この場合は、さらに Source NAT アドレスを指定する必要があります。このアドレスは、クライアント トラフィックのソースとしてバックエンド サーバーに表示されます。これは、内部インターフェースと同じサブネット上の IP アドレスであり、また他で使用されていないものでなければなりません。

ユーザーの初期アクセス ポリシーを決定します (ポリシーは後から AMC で調整できます)。ここでは、全面的な許可を与えるポリシー (SSL VPN で保護されるネットワーク全体へのアクセスを付与)、非常に限定的なポリシー (すべてのアクセスを拒否)、またはその中間のポリシー (AMC で定義したすべてのリソースに対するアクセスを付与) のいずれかを指定できます。

Setup Wizard のプロセスの最後に、設定内容が表示されます。構成プロセスの最終手順として、管理コンソールの AMC に進みます。詳細については、管理コンソールでのアプライアンスの構成を参照してください。

管理コンソールでのアプライアンスの構成

最後のインストールと展開の設定は AMC で実行します。

AMC でアプライアンスを設定するには、

1 AMC にログインします。

AMC (アプライアンスの管理に使用される Web アプリケーション) にログインし、右側に表示されるセットアップのチェックリストを確認します。

2 MySonicWall でアプライアンスを登録し、ライセンス ファイルを取得します。

アプライアンスを登録する際は、シリアル番号と認証コード (購入したアプライアンスのハードウェア ID) の両方を入力する必要があります。

- シリアル番号は、アプライアンス外面のラベルに記載されています。
- メイン ナビゲーション メニューの [**General Settings (一般設定)**] をクリックして、[**Licensing (購読中)**] エリアを確認します。

SMA アプライアンスを受け取るときは、無期限に有効な単一のユーザー ライセンスが付与されます。AMC の使用に慣れ、ユーザーを追加して環境で AMC をテストするには、ラボ ライセンスを要求します。初期セットアップとテストの後、MySonicWall からライセンス ファイルをダウンロードしてアプライアンスにインポートします。

ライセンスの管理を参照してください。

3 1 つまたは複数の認証サーバーを定義します。

ユーザーの ID を検証するために、認証が使用されます。認証サーバーを構成する際は、ディレクトリのタイプ (LDAP、Microsoft Active Directory、RADIUS、またはローカル ユーザー) とクレデンシャルのタイプ (ユーザー名/パスワード、トークン、または電子証明書) を指定する必要があります。

ユーザー認証の管理を参照してください。

4 サーバー証明書を構成します。

アプライアンスでは、Secure Sockets Layer (SSL) プロトコルを使用して情報を暗号化します。AMC を使用して自己署名サーバー証明書を作成できる他、任意に商用認証局 (CA) から証明書を取得することも可能です。

証明書を参照してください。

5 アプリケーションのリソースとグループを定義します。

アプリケーションのリソースには、TCP/IP ベースのリソース (クライアント/サーバー アプリケーション、ファイル サーバー、データベースなど)、HTTP 上で実行される Web ベースのリソース (Web アプリケーション、Web サイトなど)、および Windows ネットワーク共有リソース (WorkPlace からアクセス) が含まれます。リソースの定義には変数を含めることができます。これにより、単一のリソースでユーザーごとにネットワークの名前やアドレスを抽出するといったことが可能になります。

リソースの作成と管理を参照してください。

6 ユーザーとグループを定義します。

ユーザーとグループの定義がアクセス制御ルールで使用されることで、アプリケーション リソースへのアクセスが制御されます。

ユーザーおよびグループの管理を参照してください。

7 レルムとコミュニティを定義します。

レルムにより、アプライアンスは認証サーバーと直接統合できるので、ネットワークにアクセスする必要のある各ユーザーのアカウントを作成して管理する必要がなくなります。コミュニティにより、アクセスの必要性と End Point Control の要件が類似するユーザーが集約されます。

ユーザー認証の管理を参照してください。

8 アクセス制御ルールを作成します。

アクセス制御ルールにより、ユーザーとグループに対して提供されるリソースが決定されます。

アクセス制御ルールを参照してください。

9 WorkPlace のショートカットを構成します。

WorkPlace にショートカットを作成することで、ユーザーが WorkPlace 内から Web、ファイル システム、またはグラフィカル ターミナル リソースに簡単にアクセスできるようになります。

WorkPlace ショートカットについての作業を参照してください。

10 (オプション) ネットワーク トンネル サービスを構成します。

ネットワーク トンネル クライアントの展開を計画している場合は、ネットワーク トンネル サービスを構成して IP アドレス プールをクライアントに割り当てる必要があります。

ネットワーク トンネル サービスの構成を参照してください。

11 (オプション) End Point Control を有効にして構成します。

End Point Control では、重要データを保護し、信頼できない環境の PC からのアクセスによりネットワークの安全性が脅かされないように設計された、データ保護コンポーネントの展開を任意に選択できます。End Point Control はコミュニティを介して展開されます。

エンド ポイント制御およびコミュニティでの End Point Control 制約の使用を参照してください。

12 変更を適用します。

構成の変更を有効にするには、適用する必要があります。

構成変更の適用を参照してください。

13 システムのアクセシビリティをテストします。

アプライアンスが外部ユーザー レポジトリにアクセスできることを検証し、ネットワーク上のリソースへのアクセスを確認します。

トラブルシューティングを参照してください。

アプライアンスの実稼動

ネットワーク環境で十分にアプライアンスのテストを行い、期待される稼動状態を見極めたところで、アプライアンスを恒久的なホームに移す準備が整ったことになります。

アプライアンスを本番環境に移行するには、

1 新しいアドレス情報を使用してアプライアンスを再構成します。

アプライアンスを実稼動に移したときネットワーク環境が変更になった場合は、ネットワーク基本設定を再構成し、次の値の中で変更されたものを調整する必要があります。

- 内部インターフェースと外部インターフェースの IP アドレス
- デフォルト ゲートウェイの IP アドレス
- 静的ルート
- デフォルトの DNS ドメインおよび DNS サーバーの IP アドレス

2 DNS にアプライアンスを登録します。

企業の DNS へのアプライアンスの登録が済んでいない場合は、これを実行します。これにより、外部ユーザーは IP アドレスではなく完全修飾ドメイン名を使用して、ネットワーク リソースにアクセスできます。DNS サーバーのデータベースを編集して、アプライアンスの証明書および WorkPlace サイトに含まれる完全修飾ドメイン名を追加します。

3 商用 SSL 証明書を取得します。

ユーザーの ID 確認のために、アプライアンスの商用証明書を取得する必要がある場合があります(一般的に、AMC では自己署名証明書で十分です。)

サーバー証明書生成の詳細については、商用 CA からの証明書の取得を参照してください。

4 ファイアウォール ポリシーを調整します。

内部ネットワーク側にファイアウォールがある場合、ポリシーを調整して、アプライアンスに必要とされるポートを開く必要があります。デフォルトでは、Web プロキシ サービスはポート 443/tcp を使用して通信します (ポート 443/tcp は HTTPS 向け、ポート 80/tcp は HTTP 向け)。SSH を使用してネットワークの外部からアプライアンスに接続する場合は、ポート 22/tcp を開く必要があります。

内部ネットワーク側にファイアウォールがある場合は、このファイアウォールのポリシーを調整して、アプライアンスが通信するバックエンド アプリケーション用にポートを開く必要があります (ポートがまだ開かれていない場合)。例えば、認証に LDAP または Microsoft Active Directory サーバーを使用する場合、内部ファイアウォールでポート 389/tcp を開く必要があります。RADIUS の場合は、ポート 1645/ucp とポート 1812/udp を開きます。

また、WorkPlace を使用して Windows ネットワーク共有にアクセスする場合は、内部ファイアウォールの内部ポートを開き、これによって WorkPlace が名前解決を実行したり、ブラウズの要求を行ったり、ファイル共有に接続したりできるようにする必要があります。

詳細については、情報の収集を参照してください。

5 ショートカットを作成して WorkPlace を展開します。

Web ベースのリソースへのインターフェースとして WorkPlace を使用したり、Windows ネットワーク共有およびグラフィカル ターミナル リソースへの Web ベースのアクセスを提供するために WorkPlace を使用したりする場合は、ショートカットを作成する必要があります (WorkPlace ショートカットについての作業を参照)。また、WorkPlace URL を公開して、ユーザーが VPN を介してリソースにアクセスする方法を把握できるようにする必要があります。

WorkPlace の表示は、環境に合わせてカスタマイズできます。詳細については、WorkPlace の一般設定の構成を参照してください。

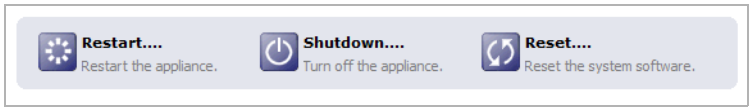
アプライアンスの電源停止と再起動

アプライアンスの電源を停止したり再起動したりする際は、必ず適切な手続きに従って操作してください。アプライアンスは、実行中に重要データをメモリに格納します。このようなデータを、電源を停止する前にディスクに書き込む必要があります。

注意：不適切な方法でアプライアンスの電源を停止すると、データが失われたり、システムのファイルが一貫性のない状態になることがあります。EX9000、EX7000、EX6000、SMA 7200、およびSMA 6200 アプライアンスの場合: アプライアンスを再起動する前には、USB デバイスをアプライアンスから取り外します。再起動時に USB デバイスがアプライアンスに接続されていると、アプライアンスはそれを起動デバイスとして使用しようとします。その結果、アプライアンスの BIOS に保存される起動情報が上書きされ、デバイスを使用できなくなります。

AMC でアプライアンスの電源を停止したり再起動したりするには

1 メイン ナビゲーション ページから、[**Maintenance (メンテナンス)**] をクリックします。[**Maintenance (メンテナンス)**] ページが表示されます。



2 適切なボタンを選択します。

- アプライアンスを再起動するには、[**Restart (再起動)**] をクリックします。AMC の応答が停止します。アプライアンスが再起動した後は、AMC に再びログインできます。
- アプライアンスを終了するには、[**Shutdown (シャットダウン)**] をクリックします。AMC が応答を停止し、アプライアンスの電源が停止します。フロント パネルの電源ボタンを押す必要はありません。

アプライアンスのすべてのモデルでは、アプライアンスで次の操作により終了したり再起動したりできます。

a アプライアンスのフロント パネルで、4 ボタン キーパッドで**下**ボタンを押し、LCD のメイン メニューにアクセスします。

b 目的のオプション ([**Restart (再起動)**] または [**Shutdown (シャットダウン)**]) まで下方へスクロールします。

c いずれのオプションでも確認メッセージが表示されるので、**左**ボタンを押して続行します。

d 結果的に起こる動作は、AMC での再起動または終了と同じです。

- AMC は応答を停止します。アプライアンスが再起動した後は、AMC に再びログインできます。
- AMC が応答を停止し、アプライアンスの電源が自動的に停止します。フロント パネルの電源ボタンを押す必要はありません。

SMA 8200v の Hyper-V

Windows Server 2016 の Microsoft Hyper-V は、中央管理サーバー (CMS) と Secure Mobile Access (SMA) アプライアンスの両方のホスト プラットフォームとしてサポートされています。Microsoft Hyper-V ベースの仮想化/プライベート クラウド インフラストラクチャを使用するお客様は、SMA アプライアンスと CMS をホストできます。

SMA 8200v の Hyper-V の設定

メモ：Hyper-V は、Windows Server 2016 以降でのみサポートされています。

Hyper-V ホストに新しい SMA 8200v を作成するには、

1 SMA ISO ファイルを Hyper-V マネージャがアクセスできる場所にコピーします。

2 4 つのプロセッサと 4GB のメモリを持つ第 1 世代の仮想マシンを作成します。

3 `.vhd` 接尾辞の代わりに `.vhdx` 接尾辞を付けた新しい 64 Gb ダイナミック ハード ドライブを作成します。

4 ハード ドライブを IDE コントローラ 0 上の仮想マシンに追加します。

5 もう 1 つのネットワーク アダプターを作成します。NIC に VMXnet3 を選択します。

メモ：ネットワーク アダプターを 1 つだけ搭載した仮想マシンが作成されます。

6 DVD を搭載した仮想マシンが作成されます。

- DVD のメディアとして SMA ISO ファイルを指定します。
- この DVD が 1 番目になるように仮想マシンの BIOS ブート順を変更します。

7 仮想マシンを起動します。仮想マシンは DVD から起動します。

8 起動に成功すると、SMA アプライアンスが作成され、仮想マシンは自動的に停止します。

9 ISO SMA はもう必要ないので取り外します。

10 ハード ドライブが DVD よりも前にくるように BIOS ブート順を変更します。

11 ネットワーク アダプタを Hyper-V 環境内の適切な仮想スイッチに接続します。

仮想マシンの次回起動時には、ハード ドライブからの起動が行われ、SMA 8200v の設定をコンソールから行うことができます。

Hyper-V プラットフォームの最大同時ユーザー数は 5000 CCU です。

Hyper-V の設定の詳細については、『*Secure Mobile Access Virtual Appliance Hyper-V 導入ガイド*』を参照してください。

次のステップ

初期ネットワーク設定を完了したら、AMC を使用してアプライアンスの構成を続行します。AMC は、Web ブラウザを使用してアクセスできます。

ヒント：AMC を初めて使用する場合は、アプライアンス管理コンソールの操作を参照してください。

アプライアンスを構成する準備が整っている場合は、ネットワークと認証の構成を参照してください。

第 3 部

管理

- ユーザ管理
- アプライアンス管理コンソールの操作

3

ユーザ管理

ユーザー、グループ、コミュニティ、レルム

アクセス制御ルールでは、ユーザーやユーザーのグループがどのリソースを使用できるかを決定します。そのために、外部のユーザー ディレクトリや、アプライアンス上のローカルのユーザー認証リポジトリに保管されているユーザーやグループにマッピングするユーザーやグループを AMC で定義する必要があります。それらよりも高いコミュニティのレベルでも、共通の特性 (最もよくあるのはアクセス ポリシーやアクセス方式など) を共有するユーザーやユーザー グループを編成できます。また、これらはアクセス制御ルールで使用することも可能です。

トピック:

ユーザーとグループ

ユーザーとは、ネットワーク上のリソースにアクセスする必要がある個人を指し、ユーザー グループは、ユーザーの集まりを指します。アプライアンスでユーザーやグループを作成したら、アクセス制御ルール内で参照し、リソースへのアクセスを許可または拒否できます。

ユーザーとグループは、外部の認証サーバー、またはアプライアンス上のローカルのユーザー認証リポジトリに保管できます。LDAP や Microsoft Active Directory などの外部認証サーバーが使用される場合は、そのサーバーに保管されている既存のユーザーやグループへの参照を作成します。このようなユーザーやグループに加え、ローカルのユーザーやグループも、許可を制御する際にはアクセス制御ルールで参照されます。外部ディレクトリを照会し (例えば特定の属性を共有するユーザーを検索して)、その結果を使用して、アクセス制御ルールで使用するグループを作成することもできます。これは、アプライアンスで直接ユーザーを作成して管理したくない場合に役立ちます。

アプライアンスでローカルのユーザーとグループを作成するのは、例えば内部システムの特別なオーダー ステータス ページにアクセスする必要がある販売業者など、外部ユーザーに対して内部の企業リソースへのアクセスを許可する際に便利です。企業全体をカバーする既存のディレクトリ サーバーを使用しない導入環境の場合は、ローカルのユーザー認証リポジトリによってグループベースのポリシーが使用できます。別のサーバーを設置、構成し、メンテナンスする必要はありません。

ユーザーやグループを定義してからアクセス制御ルールで参照することもできますが、アクセス制御ルール インターフェースから新しいユーザーやグループを直接定義することも可能です。

コミュニティ

コミュニティはユーザーの集まりです。これによって、ユーザー集団のメンバーがレルムにログインするときに、どのアクセス方法と End Point Control エージェントが展開されるかが決まります。例えば、モバイル従業員に対しては OnDemand を有効にし、ビジネス パートナーには Web アクセスのみを提供するように構成できます。End Point Control が有効な場合、コミュニティは、コミュニティ内のどの「信頼ゾーン」にメンバーが所属するかを決定するために使用することも可能です。

レルム

レルムは、認証サーバーを参照して、ユーザーに対してどのアクセス エージェントをプロビジョニングし、どの End Point Control の制約を課すかを決定します。

レルムおよびコミュニティの使用

レルムとユーザー コミュニティを設定すると、AMC において、コミュニティのメンバーにどのアクセス エージェントがプロビジョニングされるようにするかを指定できます。またオプションで、コミュニティ メンバーのデバイスを「信頼ゾーン」に分類することも可能です。次の図は、レルムがユーザーを認証して、それらユーザーをコミュニティに割り当ててアクセス エージェントをプロビジョニングし、End Point Control が有効であれば、コンピュータの信頼性に基づいてコミュニティ メンバーを異なるゾーンに割り当てる過程を示しています。

ネットワークで 1 台の認証サーバーのみにユーザー情報を保管している場合、AMC でレルムを 1 つだけ作成する必要があります。ネットワークで複数の認証サーバーを使用している場合、サーバーごとに、レルムを 1 つ以上作成する必要があります。また、1 つの外部リポジトリで別々のユーザー グループを参照する複数のレルムを、AMC で作成することもできます。

認証レルムを 1 つしか使用しない場合でも、アクセス要件やその他のセキュリティ条件に基づいてユーザーのサブセットを作成できます。これは、レルムをユーザーのコミュニティと対応させる必要があるためです。コミュニティは、レルムのすべてのユーザーでも、選択したユーザーだけでも構成できます。また、アクセス エージェントを展開したり、コミュニティのメンバーに End Point Control の制約を適用したりするために使用することも可能です。コミュニティの詳細については、RADIUS アカウント レコードをファイアウォールに送信するように SMA アプライアンスを設定するを参照してください。

トピック:

- レルムの表示
- デフォルト、表示、非表示のレルム
- デフォルト レルムの指定
- レルムの有効化と無効化
- レルム定義におけるベスト プラクティス

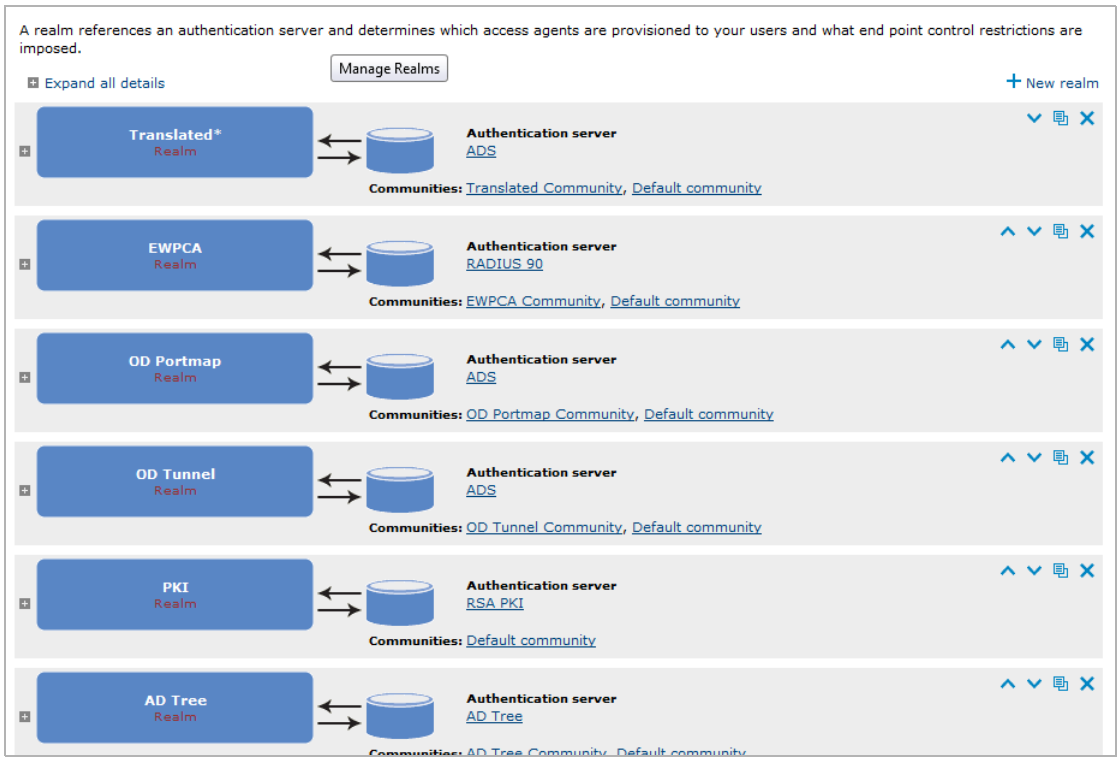
レルムの表示

構成したレルムを一覧表示できます。また、各レルムに対応する「構成要素」として、認証サーバーとコミュニティも表示されます。コミュニティはさらに、誰がどの方法でアクセスできるか、プロファイルに基づき、どのセキュリティ ゾーンにデバイスを配置するか、さらに WorkPlace の外観まで決定します。

構成したレルムを表示するには

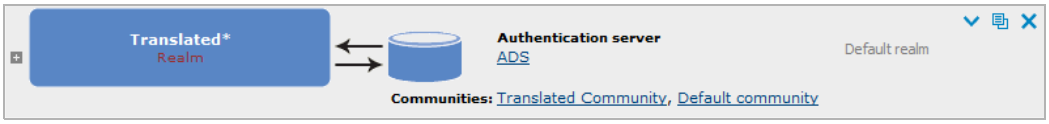
1 左側にあるナビゲーション ペインの [**User Access (ユーザー アクセス)**] で、[**Realms (レルム)**] を選択します。[**Realms (レルム)**] ページが表示されます。

折りたたみ表示



折りたたみ表示では、各レルムの概要を確認できます。いずれかの項目をクリックすると、それに対応する AMC の構成ページに直接移動できます。

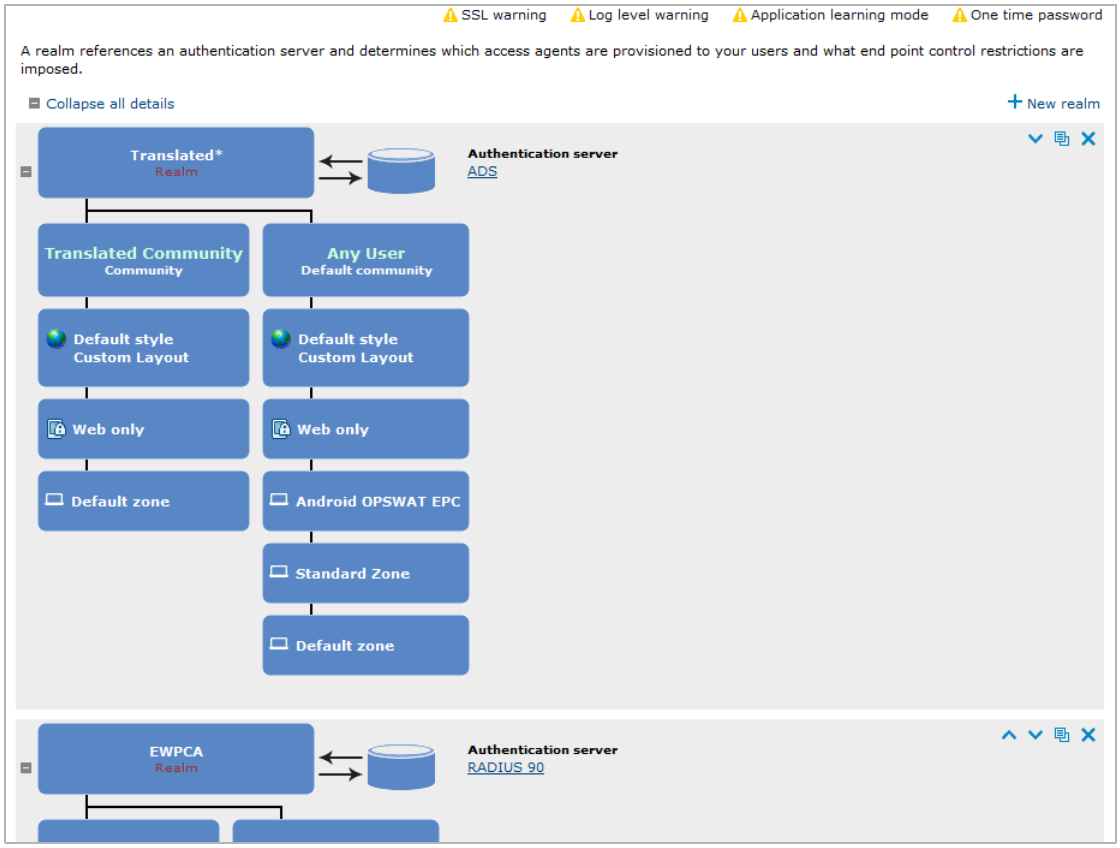
- 有効になっているレルムは青、無効になっているレルムはグレーで表示されます。レルムを無効にすると、そのレルムに対応するユーザーとグループはログインできなくなります。詳細については、レルムの有効化と無効化を参照してください。
- [**Authentication server (認証サーバ)**] エリアには、ユーザーの識別子を確認するときにレルムで使用されるサーバーの名前が表示されます。サーバーの名前をクリックすると、そのサーバーに関する [**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページが表示されます。



- レルムを作成するときに入力したオプションの説明テキストが右側に表示されます。

- 次の操作が可能です。
  - **上**および**下矢印** アイコンを使用してレルムの順序を変更します。
  - **コピー** アイコンを使用して変更するレルムのコピーを作成します。
  - **削除** アイコンを使用してレルムを削除します。
- サーバー情報の下には、レルムに関連付けられたコミュニティの一覧が表示されます。

展開表示



展開表示では、コミュニティの一覧が展開され、コミュニティとそのレイアウト、設定、ゾーンがグラフィカルに表示されます。

次の方法を選択できます。

- ページの上部にあるすべての詳細を展開またはすべての詳細を折りたたむアイコンをクリックして、すべてのレルムを展開または折りたたみます。
- 以下をクリックして、単一のレルムを展開または折りたたみます。
  - **プラス記号** (+) で詳細を表示します。
  - **マイナス記号** (-) で詳細を省略します。

2 コミュニティを使用すると、さまざまなセキュリティ要件に基づいて、レルムのメンバーをグループ化できます。コミュニティに所属しているメンバーは、ポインタをコミュニティ名に重ねるとすぐに確認できます。

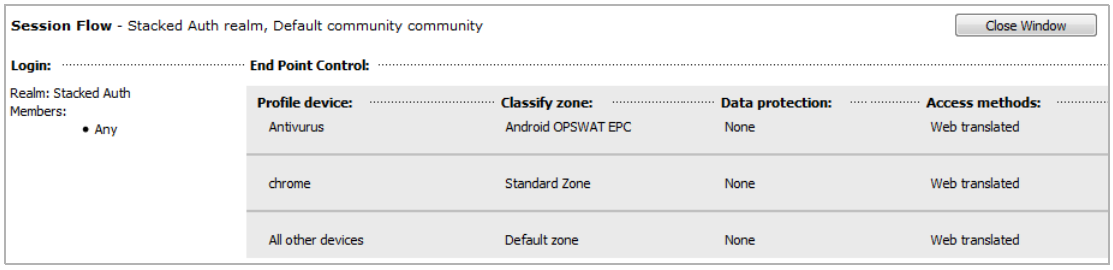
3 次のようにして関連するページにアクセスできます。

- デフォルト スタイル : WorkPlace ポータルの外観は、設定可能なスタイルとレイアウトで制御されます。例えば、モバイル デバイス ユーザーのコミュニティがある場合は、外観をコンパクトにし、レイアウトをそれに合わせたいと考えるでしょう。
- アクセス方式 : コミュニティに対するブラウザ アクセス方式を一覧表示します。
- セキュリティ ゾーン : デバイス プロファイルを使用してアクセスを許可/禁止するために使用されます。特定のゾーンで使用されているデバイス プロファイルは、そのゾーン名にポインタを重ねるとすぐに確認できます。

4 AMC のこのページでは、コミュニティ レベルの多数の構成変更を行えます。まずコミュニティ名にカーソルを重ねます。

コミュニティ名にポインタを重ねたときに表示される制御アイコンを使用して、以下を実行できます。

- **追加** (+) または**削除** (X) アイコンで、コミュニティを追加または削除します。
- **右** (>) または **左** (<) **矢印**アイコンで、コミュニティを左右に移動させて、ユーザーがグループ化されている順序を変更します。
- セッションのワークフローを表示するには、コミュニティ名にポインタを重ねて**セッション フロー** アイコンをクリックします。



5 表示されているすべてのレルムの一覧である [**Default realm (デフォルト レルム)**] ドロップダウン メニュー (ページ下部) からデフォルト レルムを指定します。デフォルト レルムは、ユーザー ログイン画面であらかじめ選択されています。

デフォルト、表示、非表示のレルム

ユーザー認証時には、ユーザーが所属しているレルムをアプライアンスで認識されている必要があります。有効なレルムが 1 つしかない場合、アプライアンスは自動的にそのレルムを使用します。一方、複数のレルムが有効になっている場合は、どのレルムを使用するかアプライアンスに認識させる必要があります。

ユーザーはログインするときに、通常、適切なレルムをリストから選択します。ただし、AMC でデフォルト レルムを定義することで、レルムを簡単に選択できるようにすることも可能です (詳細についてはデフォルト レルムの指定を参照)。デフォルト レルムが定義されている場合、レルム選択フィールドに、デフォルト レルムが自動的に表示されます。アクセス方式固有の動作については、このセクションで概説します。

重要：SonicWall ではデフォルト レルムを指定しておくことを強く推奨しています。

また、ユーザーに提示されるレルム名を選択することもできます。レルムが表示されていない場合、ユーザーはそのレルム名を把握しておき、ログインのときに手動で入力する必要があります。例えば、さまざまなサプライヤー用のレルムを作成しているとします。サプライヤー同士が互いを知らない状態が望ましい場合、このようなレルム名を非表示にしておくことができます。その際、各サプライヤーは、アプライアンスにログインするときにレルム名を入力する必要があります。

さまざまなレルム構成の場合に、ユーザーによる通常のログイン時の操作がどう変動するかは、さまざまなレルム構成におけるユーザーによる通常のログイン時の操作の変動を参照してください。

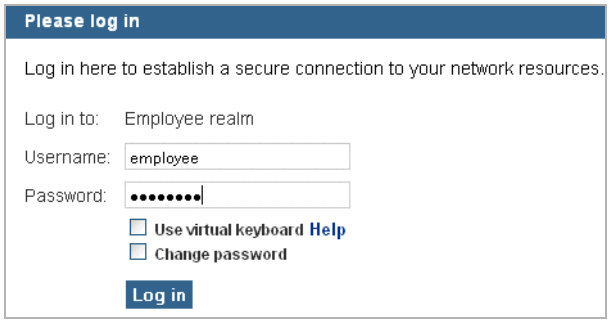
さまざまなレルム構成におけるユーザーによる通常のログイン時の操作の変動

有効なレルム	デフォルト レルムの構成	非表示レルムの構成	ユーザーのログイン時の操作
1 つ	該当なし	該当なし	ユーザーはログイン プロセスでレルムを選択する必要がありません。認証の際には、有効なレルムが自動的に使用されます。
複数	はい	なし	ユーザーはリストからレルムを選択します。[**Realm (レルム)**] フィールドにはデフォルト レルムが表示されます。
複数	いいえ	なし	ユーザーはリストからレルムを選択します。[**Realm (レルム)**] フィールドには最初のレルム (アルファベット順にソートされている) が表示されます。
複数	はい	はい	ユーザーはリストからレルムを選択します。[**Realm (レルム)**] フィールドにはデフォルト レルムが表示されます。ログイン時に非表示レルムが使用される場合、ユーザーは [**Other (その他)**] を選択して、2 番目のフィールドにレルム名を入力します。

ユーザーが初めて Secure Mobile Access WorkPlace にアクセスする際には、1 ページまたは複数のログイン ページが表示されます。1 つのレルムのみが有効な場合、ユーザー クレデンシャルを要求するページのみが表示されます。複数のレルムが有効な場合、ユーザーはログイン ページでドロップダウン リストから適切なレルムを選択します。[**User Access > Realms (ユーザー アクセス > レルム)**] ページで選択されているデフォルトのレルムが、あらかじめ選択されたレルムとしてドロップダウン メニューに表示されます。非表示レルムが 1 つ以上ある場合、ユーザーはログイン ページでレルム名の入力を求められます。

メモ：ユーザーによる選択が可能なレルムとして、最大 200 個のレルムを定義できます。また、手動での選択を回避するために、それぞれに一意のレルムを構成した WorkPlace サイトをセットアップできます。デフォルトの WorkPlace サイト数は **200** ですが、制限はありません。

[**Next (次へ)**] をクリックすると、ユーザー名とパスワードで認証するユーザーの場合、クレデンシャルを入力するためのページが表示されます。



デフォルト レルムの指定

複数の認証レルムを指定する場合は、いずれかのレルムをデフォルトとして指定する必要があります。ユーザー認証時には、ユーザーが所属しているレルムをアプライアンスで認識されている必要があります。有効なレルムが 1 つしかない場合、アプライアンスは自動的にそのレルムを使用します。一方、複数のレルムが有効になっている場合は、どのレルムを使用するかアプライアンスに認識させる必要があります。ユーザーは、適切なレルムをリストから選択できますが、AMC でデフォルト レルムを指定しておけば、ユーザーのプロセスが簡単になります(レルムを 1 つしか構成していない場合でもそれをデフォルトとして指定する必要があります。指定しないと [**Realms (レルム)**] ページに「`There is no default realm selected`（レルムが選択されていません）」という警告メッセージが表示されます)。

デフォルト レルムを指定するには

1 メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックします。

2 AMC ページの下部にある **Default realm (デフォルト レルム)** リストから、デフォルト レルムにする認証レルムを選択します。このリストには、有効かつ表示対象として構成されているレルムのみが表示されます。

レルムの有効化と無効化

アプライアンスは、複数のレルムの同時使用をサポートしています。レルムの有効/無効を切り替えることにより、アクティブにするレルムを制御できます。レルムを無効にすると、そのレルムに対応するユーザーとグループはログインできなくなります。また、有効な認証レルムがない場合、ユーザーはネットワークにアクセスできなくなります。

認証レルムを有効化または無効化するには

1 メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックして、定義されているレルムのリストを表示します。有効化されているレルムは、[**Enabled (有効)**] 列のインジケータ アイコンが緑色になっています。無効化されているレルムは、インジケータ アイコンがグレーになっています。

2 有効または無効にするレルムの名前をクリックします。この操作により、そのレルムに対する [**Configure Realm (設定レルム)**] ページが表示されます。

3 [**General (一般)**] エリアで、そのレルムの [**Status (ステータス)**] について [**Enabled (有効)**] または [**Disabled (無効)**] を選択します。

4 [**Save (保存)**] を選択します。

レルム定義におけるベスト プラクティス

レルムを定義する際は、ユーザーのログイン時の操作を軽減するため、以下のベスト プラクティスを実行します。

- ユーザーがログイン時にレルム名を選択するため、レルム名を定義するときは、ユーザー グループを明確に表す名前にします。例えば、すべての社内従業員を含むレルムの場合は「employees」などの名前を使用し、外部のサプライヤーを含むレルムの場合は「suppliers」などとします。

  モバイル デバイス ユーザーから参照されるレルムの場合は、モバイル デバイスで文字がすべて表示されるようにレルム名を短くします。例えば、標準的なテキスト サイズを使用する Pocket PC デバイスは、通常 30 文字程度の長さの名前を表示できますが、スマート フォンでは表示できません。
- 一部のユーザーが非表示のレルムにログインするような場合、そのユーザーは、レルム名と入力方法 (レルムのリストから [**Other (その他)**] を選択してフィールドにレルム名を入力) を把握しておく必要があります。
- 複数のレルムを有効にするのは、必要な場合だけにします。有効なレルムが 1 つだけであれば、ユーザーはログイン プロセスでレルムを選択する必要がなくなります。テスト環境から実稼働環境に移行するときは、テスト レルムがすべて削除されていることを確認してください。

レルムおよびコミュニティの構成

トピック:

- レルムの作成
- レルムへのコミュニティの追加
- コミュニティの作成と構成
- ネットワーク トンネル クライアントの構成
- デフォルト コミュニティの使用
- レルムでコミュニティがリストされる順序の変更
- レルムでの RADIUS アカウンティングの構成
- RADIUS アカウント レコードをファイアウォールに送信するように SMA アプライアンスを設定する

レルムの作成

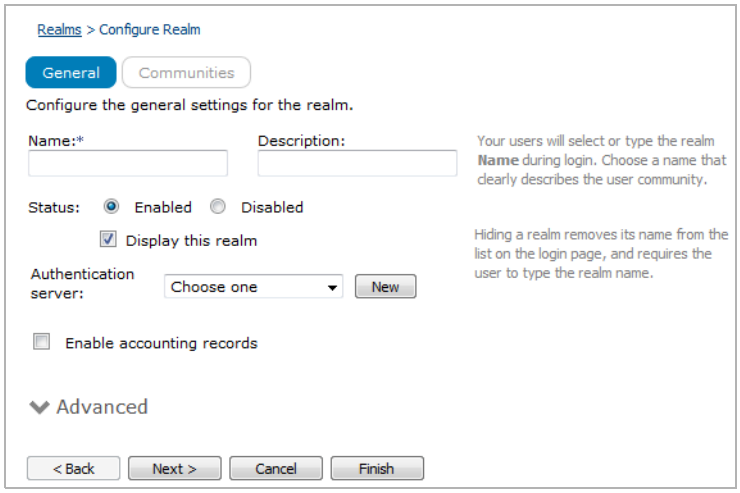
複数のレルムを作成する場合は、いずれかのレルムをデフォルトとして指定する必要があります。

レルムを作成し、これを外部認証サーバーと対応させたら、1 つまたは複数のコミュニティをレルムに追加するか、構成済みのデフォルト コミュニティを使用できます。コミュニティを割り当てずにレルムを作成し保存した場合、そのレルムにはデフォルト コミュニティが自動的に割り当てられます。デフォルト コミュニティの使用に加え、AMC でのオブジェクトの追加、編集、コピー、削除も参照してください。

レルムを作成するには

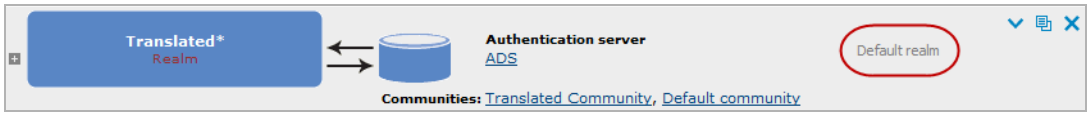
1 ナビゲーション ペインの [**User Access (ユーザー アクセス)**] で、[**Realms (レルム)**] を選択します。

2 [**+ New realm (新規レルム)**] をクリックします。[**Configure Realm (設定レルム)**] ページの [**General (一般)**] 設定が表示されます。



3 [**Name (名前)**] フィールドに、わかりやすいレルム名を入力します。ユーザーが VPN へのログイン時にレルム名を選択しなければならない場合は、必ずユーザー グループを明確に表す名前にします。

4 [**Description (説明)**] フィールドに、レルムの説明を入力します。コメントを入れるのは必須ではありませんが、VPN で複数の認証レルムを使用する場合などに便利です。このフィールドに入力されたテキストは、レルムのリストに表示されます。



5 適切な [**Status (状況)**] を選択することによって、レルムを有効または無効にします。詳細については、レルムの有効化と無効化を参照してください。

6 ユーザーに提示されるリストにこのレルムを含める場合は (ほとんどの場合これが推奨される)、[**Display this realm (このレルムを表示)**] チェックボックスを選択します。

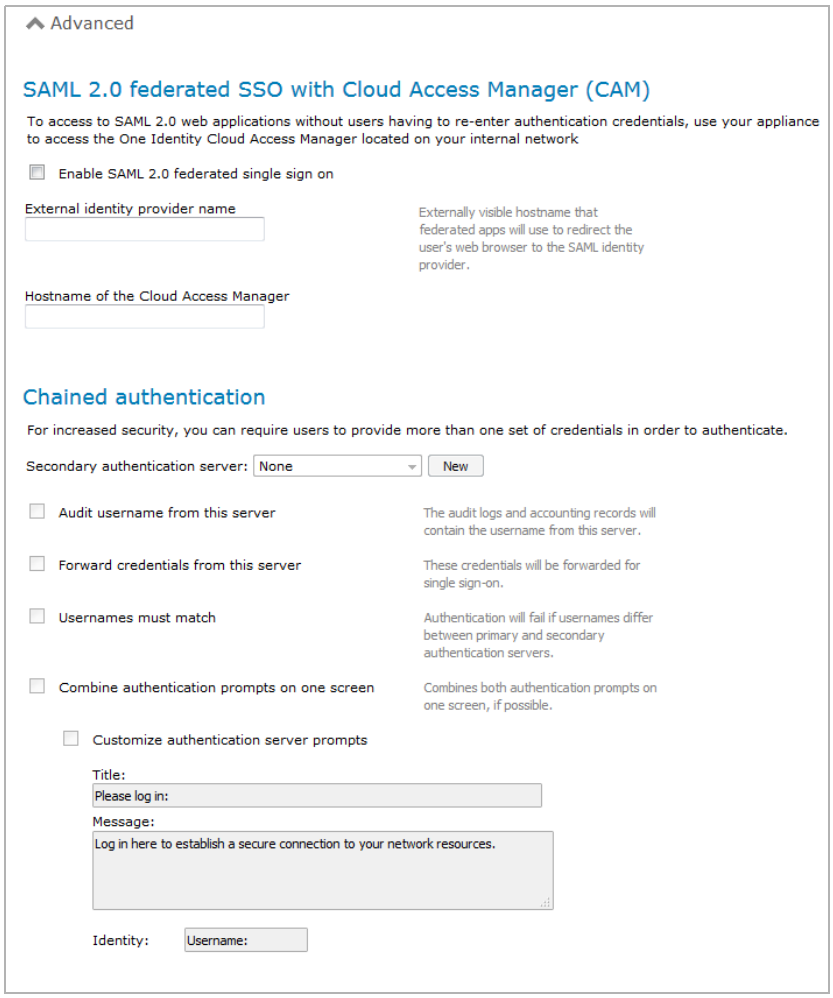
7 [**Authentication server (認証サーバー)**] ドロップダウン メニューで、ユーザーの識別子を確認するために使うレルムを選択します。サーバーを選択する必要があります。

△ **注意：[Authentication server (認証サーバ)] を [None (なし)] に設定すると、このレルムおよびそのリソースに対して、認証されていないオープンなアクセスが有効になります。このような状況を望んでいる場合以外は、この設定にしないでください。**

8 また、新しい認証サーバーを構成してレルムで参照する場合は、[**New (新規)**] をクリックして [**Authentication Servers > New Authentication Server (認証サーバー > 新規認証サーバー)**] ページを表示することもできます。詳細については、認証サーバーの構成を参照してください。

9 このレルムについてのアカウンティング情報を保存したい場合、[**Enable accounting records (アカウンティング レコードの有効化)**] チェックボックスを選択します。これを選択すると、すべての RADIUS、Syslog、およびルーティング変更が保存されます。

10 [**Advanced (詳細設定)**] をクリックして、詳細設定を表示します。



11 ユーザーが認証クレデンシャルを再入力せずに SAML 2.0 Web アプリケーションにアクセスできるようにするには、[**SAML 2.0 federated SSO with Cloud Access Manager (CAM) (Cloud Access Manager (CAM) による SAML 2.0 フェデレーション SSO)**] セクションで、

a [**Enable SAML 2.0 federated single sign on (SAML 2.0 フェデレーション シングル サイン オンの有効化)**] チェックボックスをオンにします。

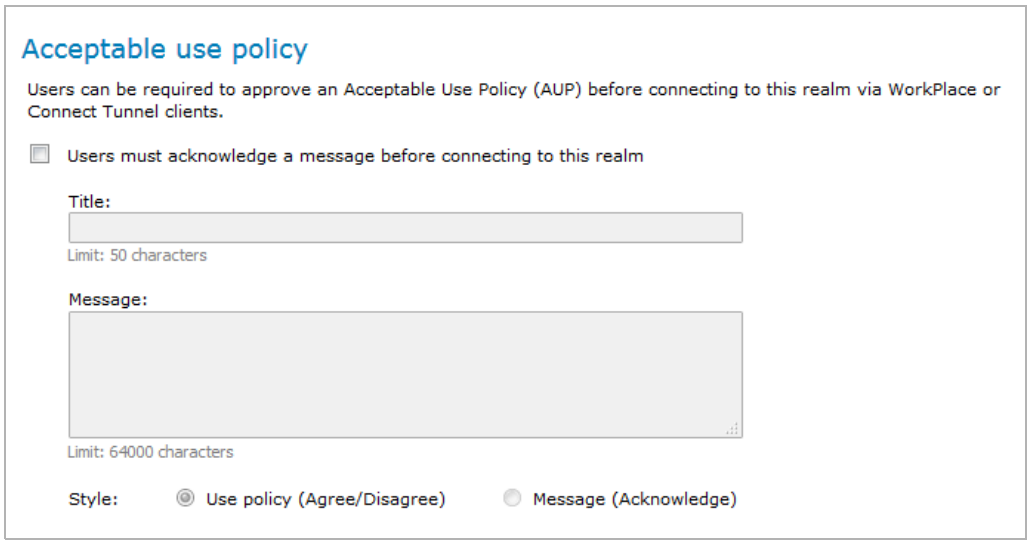
b [**External identity provider name (外部 ID プロバイダ名)**] フィールドに、フェデレーション アプリケーションがユーザーを SAML ID プロバイダにリダイレクトするために使用する、外部から見えるホスト名を入力します。

c [**Cloud Access Manager (Cloud Access Manager)**] フィールドに One Identity ホスト名を入力します。

12 2 番目の認証サーバーを使用するようアプライアンスをセットアップできます。また、AUP (Acceptable Use Policy: 使用規定に同意する) のカスタマイズも可能です。2 番目の認証サーバーをセットアップする場合には 2 通りの方法があります。

- [**Chained authentication (連鎖式認証)**]: ユーザーは複数のクレデンシャル セットが必須になります。連鎖式認証の構成を参照してください。
- [**Enable group affinity checking (グループ関連付けチェックを有効化)**]: 2 番目の認証リポジトリに照会します。詳細については、レルムでのグループ アフィニティ チェックの有効化を参照してください。

13 ユーザーがレルムにログインする際に AUP に同意するよう求める場合は、[**Acceptable Use Policy (規約の承諾)**] エリアで、[**Users must acknowledge a message before connecting to this realm (このレルムに接続する前にメッセージへの同意が必要)**] チェックボックスを選択します。



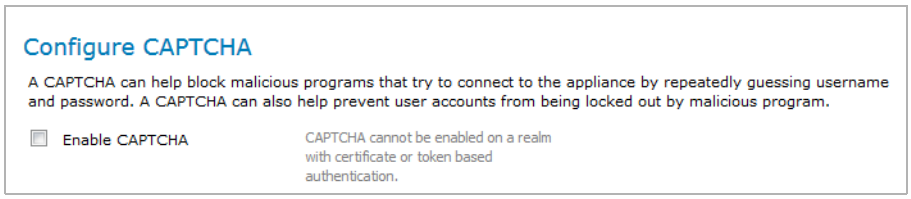
14 [**Title (タイトル)**] フィールドに、AUP のタイトルを 50 文字以下で入力します。

15 [**Message (メッセージ)**] フィールドには、ユーザーに同意を求める使用規定の文章を 64,000 文字以下で入力します。

16 [**Style (スタイル)**] 設定では、以下のラジオ ボタンのいずれかを選択します。

- [**Use policy (Agree/Disagree) (ポリシーを使用 (同意する/同意しない))**] : ユーザーに使用規定が表示され、接続を続行するには [**Agree (同意する)**] ボタンのクリックが必要になります。[**Disagree (同意しない)**] ボタンがクリックされると、セッションは終了します。
- [**Message (メッセージ)**]: ユーザーに使用規定が表示され、接続を続行するには [**OK**] ボタンのクリックが必要になります。

17 [**Configure CAPTCHA (CAPTCHA 設定)**] エリアでは、[**Enable CAPTCHA (CAPTCHA を有効化)**] チェックボックスをオンにして、WorkPlace ユーザーがログイン時にユーザー名とパスワードに加えて CAPTCHA 文字を入力するように要求します。ここで CAPTCHA が有効になっている場合のみ、CAPTCHA プロンプトが WorkPlace ログイン ページに表示されます。



CAPTCHA は、パスワード システムに対する攻撃のうち、次のようなプログラムによるタイプの悪質な攻撃の防止に有効です。

- 可能性のあるパスワードの辞書を繰り返し利用しながら、ユーザ名とパスワードを推測してログインを試みるボット
- 失敗に終わる一連の大量ログイン試行を強制的に実行して、ユーザのアカウントをロックアウトさせようとするボットからのサービス拒否 (DoS) 攻撃

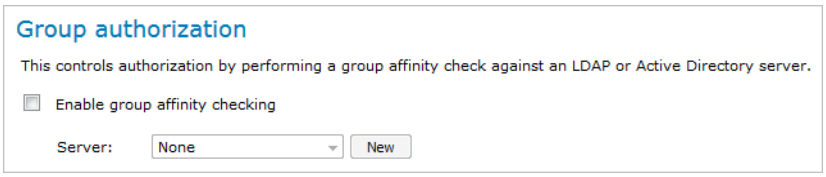
メモ： `setMicroInterrogationResult()` API で **captchaCapable** オプションが有効になっている場合のみ、このプロンプトが表示されて CAPTCHA を有効化することができます。

CAPTCHA は、すべての WorkPlace アクセス方式とすべての認証サービス構成 (ローカル Auth、LDAP、Active Directory、RADIUS) で、レルム レベルで構成されます。CAPTCHA は大文字と小文字を区別しない 6 文字の英数字で構成されています。

CAPTCHA を使用する場合は、以下の点に注意してください。

- 連鎖式認証モードでは、CAPTCHA はプライマリ認証でのみ表示されます。
- トークンベースまたは証明書ベースの認証のレルムでは、CAPTCHA を有効にすることはできません。このような場合、CAPTCHA 設定セクションは無効になります。

18 [**Group authorization (グループ認証)**] エリアで、[**Enable group affinity checking (グループ アフィニティ チェックの有効化)**] チェックボックスをオンにし、[**Server (サーバー)**] ドロップダウン メニューからサーバーを選択して、LDAP または Active Directory サーバーに対してグループ アフィニティ チェックを行います。



新しい認証サーバーを追加するには、[**New (新規)**] ボタンをクリックして、認証サーバーの構成の説明に従って新しいサーバを設定します。

19 [**Save (保存)**] を選択します。

レルムにユーザー コミュニティを追加できます（レルムへのコミュニティの追加参照）。コミュニティを割り当てずにレルムを作成し保存した場合、そのレルムにはグローバル デフォルト コミュニティが自動的に割り当てられます。詳細については、デフォルト コミュニティの使用を参照してください。

メモ：コミュニティの編集方法、コピー方法、削除方法の詳細については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

レルムへのコミュニティの追加

レルムを作成したら、そのレルムに 1 つ以上のコミュニティを対応させる必要があります。レルム内のすべてのユーザーを同じように扱うのであれば、定義する必要があるコミュニティは 1 つだけです。ユーザーを細分化したい場合には、追加のコミュニティを作成します。例えば、リモート従業員に、ローカル従業員と異なるアクセス方式と End Point Control 制約を割り当てたい場合などがこれに該当します。それぞれのコミュニティについて以下を定義します。

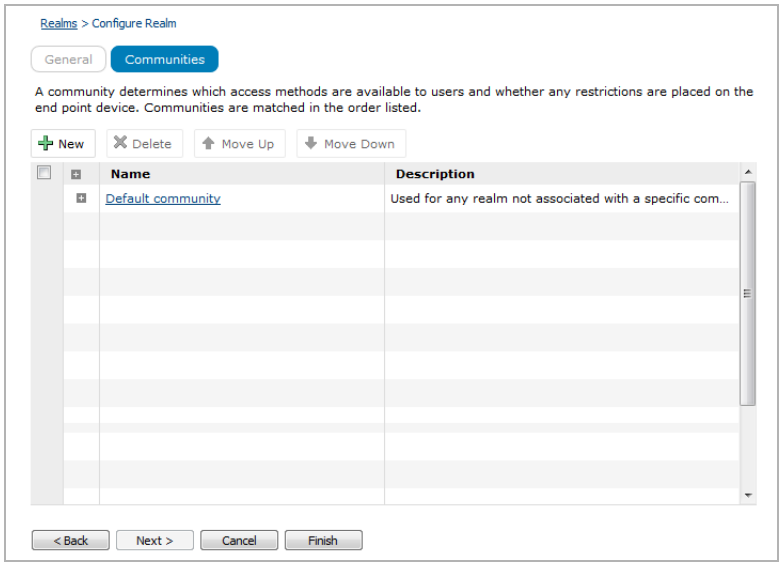
- レルム内のユーザーのサブセット
- レルムにログインするときにユーザーが使用できるアクセス方式
- そのエンド ポイント デバイスに設定される制約 (存在する場合)

アプライアンスの各レルムでは、1 つ以上のコミュニティを参照する必要があります。複数のコミュニティを使用すると、ユーザー グループを効率的に分割できます。その結果、特定のユーザーに個別のアクセス エージェントを割り当てたり、コミュニティのメンバーが使用する特定タイプのデバイスについて End Point Control の制約を設定したりすることができます。

構成済みのデフォルト コミュニティを使用するか (デフォルト コミュニティの使用を参照)、別のコミュニティをレルムに対応させることができます。時間の経過とともにユーザー アクセス要件やセキュリティ ポリシー要件が変化するのに合わせて、レルムへのコミュニティの追加、レルムが参照するユーザー コミュニティの変更、コミュニティの削除を行えます。

コミュニティをレルムに追加するには

1 [**Configure Realm (レルムの設定)**] ページの [**General (一般)**] タブでレルムを作成したら、[**Next (次へ)**] ボタンをクリックして [**Communities (コミュニティ)**] ページに移動します。[**Communities (コミュニティ)**] タブが選択された状態で、[**Configure Realm (レルムの設定)**] ページが表示されます。



2 既存のコミュニティを変更せずにそのまま使用する場合は、必要に応じて、コミュニティがリストで表示される順序を変更します。レルムでコミュニティがリストされる順序の変更を参照してください。

3 これを行うには、次の手順に従います。

- レルムの新しいコミュニティを作成するには、[**New (新規)**] をクリックします。
- 既存のコミュニティを編集するには、そのリンクをクリックします。

[**Configure Community (コミュニティの設定)**] ページが表示されます。コミュニティの作成と構成で説明されている手順に従います。

コミュニティの作成と構成

コミュニティを作成するときは、次の基本手順を実行します。

- コミュニティへのメンバーの割り当て
- コミュニティに対するアクセス方式の選択
- (オプション) コミュニティに対する End Point Control 制約の指定
- WorkPlace ポータルのスタイルとレイアウトの指定

トピック:

- コミュニティへのメンバーの割り当て
- コミュニティに対するアクセス方式の選択
- コミュニティでの End Point Control 制約の使用
- WorkPlace の外観の構成

コミュニティへのメンバーの割り当て

コミュニティ作成の最初の手順では、どのユーザーをメンバーにするかを指定します。デフォルトでは、コミュニティは、対応している認証レルムのすべてのユーザーを含むよう構成されています。ただし、レルム内の特定ユーザーまたは特定ユーザー グループのみにアクセスを限定するよう、コミュニティを構成することもできます。

これは例えば、従業員用のコミュニティと、ビジネス パートナー用のコミュニティにレルムを分割したい場合などに使用すると便利です。こうしておくと、それぞれのコミュニティに適切なアクセス エージェントを割り当てたり、セキュアでないコンピュータからログインする場合に End Point Control 制約を課したりすることができます。コミュニティは、リソースへのアクセスを許可または拒否するために、アクセス制御ルールから参照することもできます。

既存のコミュニティにメンバーを割り当てるには、

1 メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックします。

2 レルム内で、構成したいコミュニティに対するリンクをクリックします。[**Members (メンバー)**] タブが選択された状態で、[**Configure Community (設定コミュニティ)**] ページが表示されます。

3 [**Members (メンバー)**] メニューで、どのユーザーまたはグループがこのコミュニティに所属するかを指定します。ユーザーやグループをリストから選択する場合は、[**Edit (編集)**] をクリックします。ユーザーやグループが指定されない場合、このフィールドの値はデフォルト値の「**Any (すべて)**」になります。これは、このコミュニティを参照するすべての認証レルムのユーザーがこのコミュニティに属することを表しています。

4 [**Maximum active sessions (最大アクティブ セッション)**] フィールドでは、このコミュニティの各メンバーが一度にアクティブにできるセッション数を制限できます。例えば、モバイル ユーザーの場合、セッション数を 1 に制限する場合があります。セッションごとにユーザー ライセンスが 1 つ使用され、モバイル ユーザーが複数のアクティブなセッションを利用することは不可能です。自宅と会社を行き来する従業員など、その他のコミュニティの場合、許可されるセッション数は比較的多く設定されると考えられます。詳細については、ライセンスの計算方法を参照してください。

5 コミュニティのメンバーに提供するアクセス方式を選択するため、[**Access Methods (アクセス方式)**] タブをクリックします。詳細については、コミュニティに対するアクセス方式の選択を参照してください。

6 クライアント デバイスのセキュリティに基づいてユーザー アクセスを制限するため、[**End Point Control restrictions (End Point Control 制約)**] タブをクリックして、このコミュニティのユーザーにどのゾーンを提供するかを指定します。コミュニティでの End Point Control 制約の使用を参照してください。

7 [**Save (保存)**] を選択します。

コミュニティに対するアクセス方式の選択

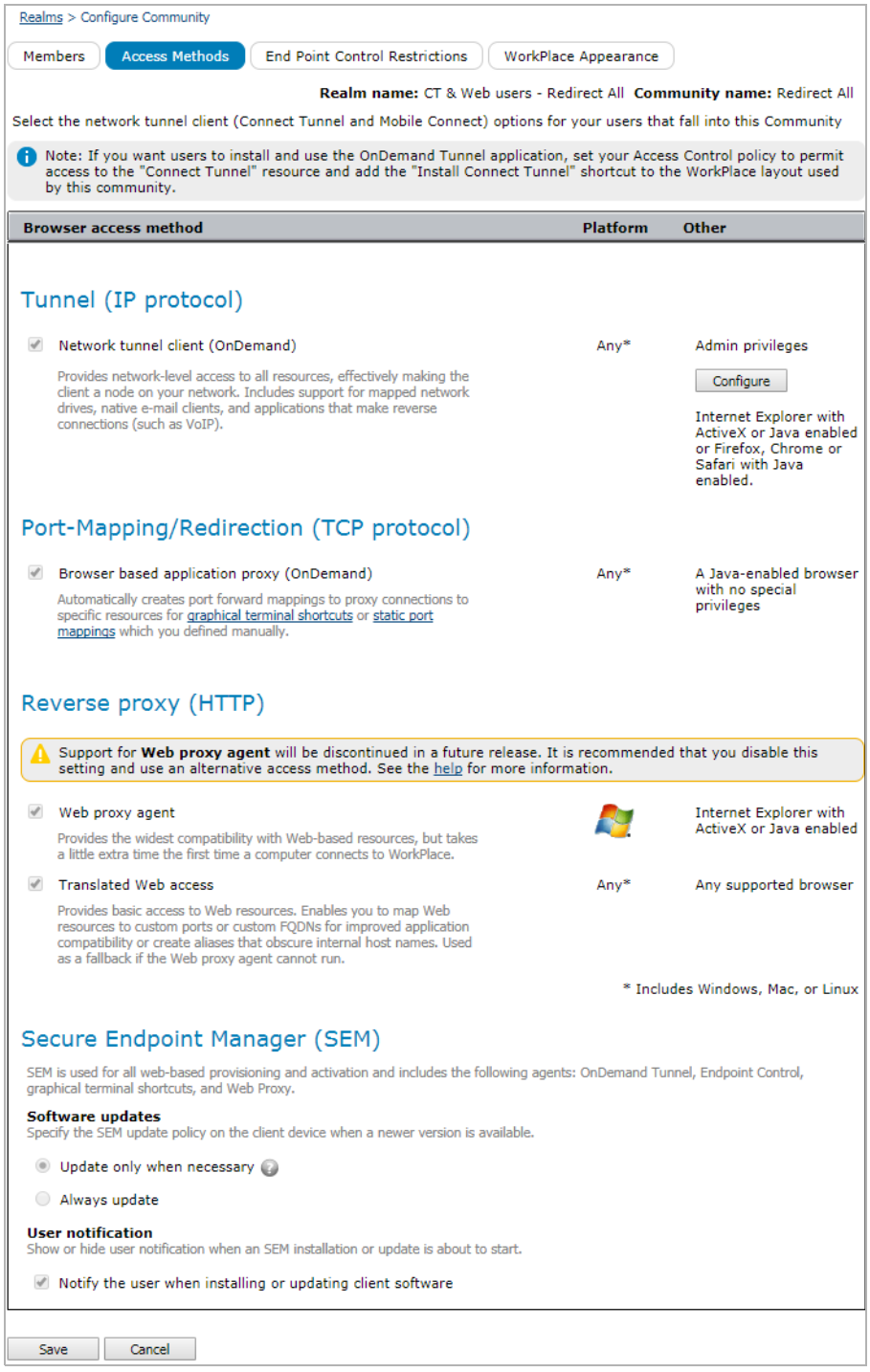
コミュニティ作成の 2 番目の手順は、コミュニティのメンバーがアプライアンスへの接続とネットワーク リソースへのアクセスの際にどのアクセス方式を使用できるようにするか決定することです。ユーザーの環境と互換性があるアクセス方式については、ユーザー アクセス コンポーネントを参照してください。

コミュニティのメンバーが使用できるアクセス方式を指定するには、

1 メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックします。

2 構成したいコミュニティに対するリンクをクリックします。

3 [**Access Methods (アクセス方式)**] をクリックするか、[**Next (次へ)**] をクリックします。



4 コミュニティのメンバーが、ネットワークのリソースに接続する際にブラウザで使用できるアクセス方式を選択します。アプライアンスは、選択されたアクセス エージェントを、ユーザーのシステムの機能に基づいて有効にします。さまざまなアクセス エージェントの機能とシステム要件については、ユーザー アクセス コンポーネントおよびサービスを参照してください。

5 ネットワーク トンネル クライアントのアクセス権をコミュニティのメンバーに付与したい場合は、次のように選択します。

- トンネル アクセス エリアで [**Network tunnel client (ネットワーク トンネル クライアント)**] を選択します。ユーザーが WorkPlace のリンクから Connect Tunnel クライアントをダウンロードしてアクティブ化するようにしたい場合は、組み込みのリソースまたはショートカットを使用できます。
- Web ベースのプロキシ アクセスの場合:

  a) [**Client/server proxy agent (OnDemand) (クライアント/サーバー プロキシ エージェント (オンデマンド))**] を選択します。

  b) [**Auto-activate from WorkPlace (WorkPlace からの自動起動)**] をクリックします。これによって、ユーザーが WorkPlace に接続するときに、Web ベースの OnDemand Tunnel エージェントがプロビジョニングまたはアクティブ化されます。
- Web アクセス (HTTP) エリアで、以下を選択します。
  - Windows クライアントの大部分の Web ベース リソースにクライアントレス アクセスできるようにするには、[**Web proxy agent (Web プロキシ エージェント)**] を選択します。
  - アプリケーションの互換性を向上させるためにカスタム ポートまたはカスタム FQDN にマッピングされているか、エイリアスを使用して内部ホスト名を遮へいする Web リソースにクライアントレス アクセスできるようにするには、[**Translated Web access (変換 Web アクセス)**] を選択します。[Translated Web access] は、デフォルトの Web プロキシ エージェントが実行できない場合のフォールバックとして使用できます。Web アクセスのさまざまなタイプについては、Web アクセスを参照してください。また、Web ベースのリソースの追加については、リソースの追加を参照してください。

  メモ：Web プロキシ エージェントは、将来のリリースで廃止される予定です。

6 ネットワーク トンネル クライアントをユーザーに展開するには、最初に、コミュニティで使用できる IP アドレス プールを 1 つ以上作成する必要があります。デフォルトの場合、構成されているすべての IP アドレス プールがコミュニティで使用可能になっていますが、必要であれば特定の IP アドレス プールを選択することもできます。ネットワーク トンネル クライアントの構成を参照してください。

7 ユーザーが WorkPlace にログインするとき、ネットワーク リソースに対するアクセスを許可する前に、Secure Mobile Access エージェントまたはクライアントをインストールするよう求めることもできます。[**Require agent in order to access network (ネットワークにアクセスするにはエージェントを必要とする)**] を選択すると、エージェントを必要とするアプリケーションの互換性を向上させることができます。結果的にユーザーのアクセスが広範囲になり、ヘルプ デスクの呼び出しも少なくなります。

この設定を無効にすると、WorkPlace にログインするユーザーが、エージェントをインストールせずに、変換 Web アクセス、カスタム ポートがマッピングされた Web アクセス、カスタム FQDN がマッピングされた Web アクセスのいずれかに進むことができるようになります。この場合ユーザーは、コミュニティの構成方法に応じて、[**Default (デフォルト)**] ゾーンまたは [**Quarantine (隔離)**] ゾーンに割り当てられます。

8 コミュニティに対するアクセス方式を選択したら、[**Next (次へ)**] をクリックします。[**End Point Control restrictions (End Point Control 制約)**] エリアが表示されます。ここで、クライアント デバイスのセキュリティに基づいて、コミュニティのメンバーのアクセス権限を制約できます。コミュニティでの End Point Control 制約の使用を参照してください。

9 このコミュニティに対して、End Point Control を採用したくない場合は、[**Finish (完了)**] をクリックします。

メモ：特定のコミュニティで、ネットワーク トンネル クライアント オプションが有効になっていない場合でも、それまで Connect Tunnel クライアントにアクセスしているユーザーは、これを使用してアプライアンスにアクセスできます。

コミュニティが、変換 Web アクセスのみを提供するよう構成されている場合、クライアント PC は独自のアプリケーション プロトコルにアクセスするために必要なネットワーク転送を使用できないため、ターミナル リソースは使用できなくなります。グラフィカル ターミナル エージェントの構成の詳細については、アクセス サービスの管理を参照してください。

コミュニティでの End Point Control 制約の使用

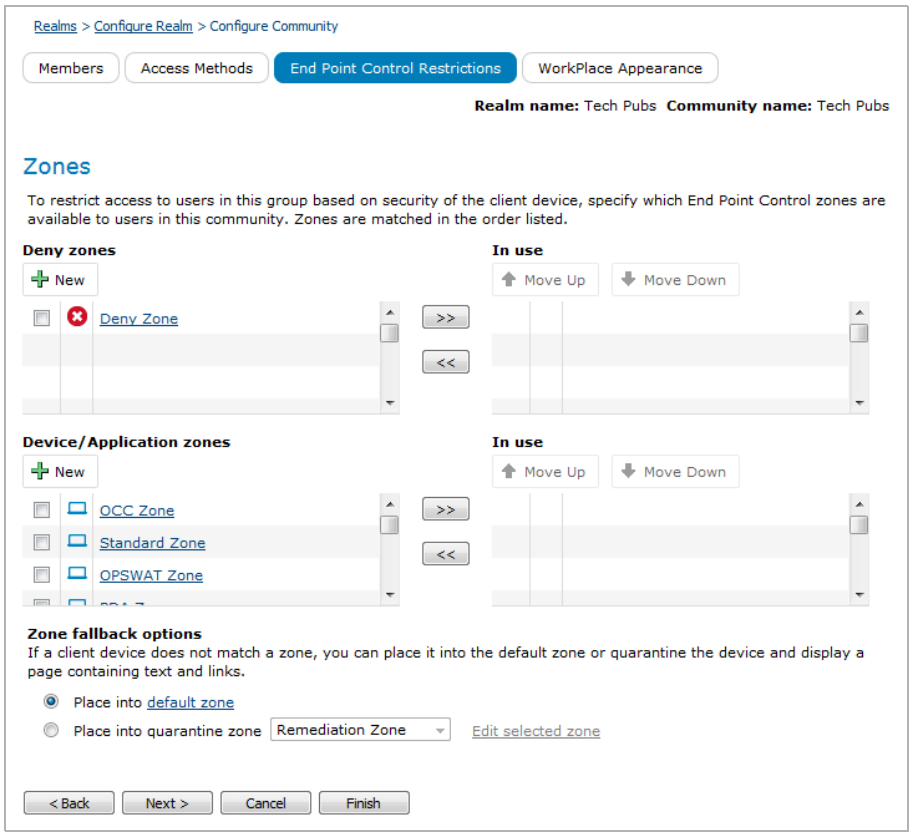
コミュニティを作成するとき、クライアント デバイスのセキュリティに基づいて、ユーザーのアクセスを制約できます。そのために、このコミュニティのユーザーが、どの End Point Control ゾーンを使用できるようにするか指定します。ゾーンには、拒否、標準、隔離、デフォルトの 4 つのタイプがあります。ゾーンの作成方法と構成方法、および接続要求の分類のために使用するデバイス プロファイルについては、ゾーンおよびデバイス プロファイルによる EPC の管理を参照してください。

また、ユーザーが Connect Tunnel クライアントを使用してアプライアンスにアクセスする場合、コミュニティで End Point Control ゾーンを使用していなくても、非アクティブ タイマーを設定できます。

コミュニティに End Point Control 制約を適用するには、

1 メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックします。

2 構成したいコミュニティに対するリンクをクリックし、[**End Point Control restrictions (End Point Control 制約)**] タブをクリックします。



3 お使いの導入環境に受け入れられないデバイス プロファイルがある場合、拒否ゾーンを使用します。例えば、PC に Google Desktop をインストールしたユーザーからの接続があった場合、そのユーザーのアクセスを拒否したい状況がこれに当たります。[**Deny zones (禁止ゾーン)**]リストでエントリを選択 (または作成) し、[>>] ボタンをクリックします。この操作により、このゾーンが [**In use (使用中)**]リストに移動します。拒否ゾーンが最初に評価されます (該当するユーザーはログオフされます)。

   新しい EPC ゾーンを作成し、それをリストに追加する場合は、[**New (新規)**] ボタンをクリックします。ゾーンの作成方法については、ゾーンの定義を参照してください。

4 コミュニティに End Point Control 標準ゾーンを 1 つまたは複数割り当てることができます。このゾーンは、コミュニティにアクセスできるデバイスを決定するときに使用します。ゾーンを選択しない場合、コミュニティのメンバーには、デフォルト ゾーンが割り当てられます。その場合、アクセス ポリシーに基づいて、リソースに対するアクセスの制限や拒否が決定されます。[**Standard zones (標準ゾーン)**] リストで、ゾーンに対するチェックボックスを選択して、[>>] ボタンをクリックします。この操作により、このゾーンが [**In use (使用中)**] リストに移動します。

5 コミュニティが複数のゾーンを参照する場合、[**Move Up (上に移動)**] と [**Move Down (下に移動)**] を使用して、リスト内のゾーンの順序を変更します。ゾーンはリストの順序で処理されるため、それぞれのゾーンでどのデバイスに許可を与えるか慎重に検討する必要があります。最も狭い範囲のゾーンをリストの先頭に配置するようにします。

6 クライアント デバイスがゾーンと一致しない場合、[**Zone fallback options (ゾーン フォールバック オプション)**] エリアの設定を使用して、それをデフォルト ゾーンに入れるか、そのデバイスを隔離して (オプションで) テキストとリンクを含むカスタマイズ ページを表示します。詳細については、隔離ゾーンの作成を参照してください。

7 コミュニティ メンバーに対して非アクティブ タイマー (キーボードやマウスが動作していない場合にトリガーされる) を設定するため、[**End inactive user connections (非アクティブ ユーザー接続の終了)**] リストから ([**After 3 mins (3 分後)**] から [**After 10 hours (10 時間後)**] までの) 時間制限を選択します。これは、ネットワーク トンネル クライアントで使用される Windows のみの設定です。

8 [**Save (保存)**] をクリックして、コミュニティの構成を終了します。

> **メモ**：アプライアンスでは、EPC インタロゲーションを使用して、クライアント上の特定のデバイス プロファイル属性についてチェックし、それに従ってデバイスを分類します。隔離ゾーンがフォールバック オプションの場合、EPC インタロゲーションで何らかのエラーが発生すると通常であれば隔離されるデバイスがデフォルト ゾーンに入れられる可能性があります。

WorkPlace の外観の構成

コミュニティごとに、WorkPlace ポータルのコンテンツ ページに適用するスタイルとレイアウトを割り当てることができます。

WorkPlace のスタイルはページを表示する際に使用する色、フォント、画像を決定し、レイアウトはページ コンテンツ、コンテンツの配置方法、ポータルでの移動方法を決定します。ログイン、エラー、通知のページのスタイルについては、サイトのセットアップ時に指定します。

コミュニティのスタイルとレイアウトを作成するには、

1 メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックします。

2 構成したいコミュニティに対するリンクをクリックし、[**WorkPlace Appearance (WorkPlace の外観)**] タブをクリックします。

3 既存スタイルを選択します。または、[**Manage styles (スタイルの管理)**] をクリックして既存スタイルを変更するか、スタイルを新たに作成します。WorkPlace のスタイルの構成については、WorkPlace スタイルの作成または編集を参照してください。

4 既存レイアウトを選択します。または、[**Manage layouts (レイアウトの管理)**] をクリックして既存レイアウトを変更するか、レイアウトを新たに作成します。WorkPlace のレイアウトの構成については、WorkPlace レイアウトの作成または編集を参照してください。

5 このコミュニティのレイアウトは、自動的に小型のデバイスに収まるよう変更されます。例えば、[**Intranet Address (イントラネット アドレス)**] フィールドがレイアウトに含まれている場合、上級モデルのモバイル デバイスには表示されますが、基本モデルには表示されません。

この表示方法を許容できない場合は、[**Small form factor devices (小型携帯端末)**] エリアで、さまざまなデバイス クラスに合わせて異なるレイアウトを指定できます。コミュニティ作成時には、そのコミュニティの WorkPlace ポータルがモバイル デバイスでどのようにデフォルト表示されるかを確認してから、必要に応じて新しいレイアウトを作成するか、既存レイアウトを変更することをお勧めします。

ネットワーク トンネル クライアントの構成

このセクションでは、Connect Tunnel クライアントおよび OnDemand Tunnel エージェントの設定を構成する方法について説明します。

- IP アドレスの割り当て
- セッションの持続性
- リダイレクション モード
- プロキシ サーバー リダイレクション
- UDP トンネル モード
- 安全なネットワークの検出
- Windows Tunnel クライアントの自動クライアント更新
- セッションの終了
- トンネル クライアント設定の構成

IP アドレスの割り当て

ネットワーク トンネル クライアントからの TCP/IP 接続を管理するようネットワーク トンネル サービスを構成するには、IP アドレスをクライアントに割り当てるための IP アドレス プールをセットアップする必要があります。アドレス プールの設定は、通常、ネットワーク トンネル サービスを構成するときに行います。IP アドレス プールを最初に設定する方法については、IP アドレス プールの構成を参照してください。

ネットワーク トンネル クライアントをユーザーに展開するコミュニティを作成するとき、コミュニティのメンバーがどの IP アドレス プールを使用できるようにするかを指定する必要があります。デフォルトの場合、構成されているすべてのアドレス プールが使用可能になっていますが、必要であれば特定の IP アドレス プールを選択することもできます。

セッションの持続性

トンネル クライアントは、ノート型 PC のドッキングを解除して会議に持ち込む場合や、外出時にセルラー ネットワーク境界をまたぐ場合など、(特にモバイル ユーザーにおいて) 頻繁に発生する接続の中断に自動的に対処します。このような一時的な中断が発生しても、ユーザーは再認証なしでセッションを再開できます。

ユーザーの IP アドレスが変わっても (オフィスから自宅に移動した場合など) セッションが自動的に再確立されるようにするには、EPC ゾーンの設定時に [**Allow user to resume session from multiple IP addresses (複数の IP アドレスからのリモート セッションを許可)**] チェックボックスを選択します。詳細については、デバイス ゾーンの作成またはデフォルト ゾーンの構成を参照してください。

この設定が無効になっている場合や、以下のいずれかに該当する場合は、再認証が必要になります。

- アプライアンスでのユーザーのセッションの期限が切れている
- 提示したクレデンシャル (SmartCard など) が、一時停止/再開時に持続しない

リダイレクション モード

ネットワーク トンネル クライアントを構成するとき、リダイレクション モードを指定し、クライアント トラフィックがアプライアンスにリダイレクトされる方法を決定する必要があります。ネットワーク トンネル サービスでは、以下のリダイレクション モードをサポートしています。

- Split tunnel mode (スプリット トンネル モード)
- Redirect All Mode (リダイレクト オール モード)

Split tunnel mode (スプリット トンネル モード)

Split tunnel mode (スプリット トンネル モード)では、AMC で定義されているリソースにバインドされたトラフィックがトンネル経由でリダイレクトされ、他のトラフィックはすべて通常どおりにルーティングされます。これは、「リダイレクト オール モード」よりも安全性は低いですが、インターネット アクセスを妨げないため、ユーザーにとっては利便性が高くなります。

インターネット接続 (トンネル分割を行って再ルーティングすることによりネットワーク リソースに到達する可能性がある) を介して、ユーザーのコンピュータに対し許可されていないアクセスが行われるのを防止するために、ユーザーのコンピュータでパーソナル ファイアウォールやウイルス対策機能が動作するよう求める End Point Control 制約の使用についても考慮します。

また、ユーザーがローカルのプリンタやファイル共有にもアクセスできるようにする場合は、[**Split tunnel, with cacess to local network (スプリット トンネル、ローカル ネットワークへのアクセス付き)**] を選択します。

アプライアンスがスプリット トンネル モードのいずれかに構成されている場合は、ローカルとリモートのネットワーク アクセスのどちらを優先するかをユーザーが決定できるように設定することが可能です。例えば、アドレスが `192.168.230.1` のホスト リソース (Web サーバー) があるとします。出張先にいるユーザーの使いたいプリンタが会議場のローカル ネットワーク上にあり、プリンタも同じアドレスを使用していることが判明した場合、AMC で [**Allow users to indicate which split tunnel redirection mode to use on the client (クライアントで使用するスプリット トンネル リダイレクション モードのユーザーによる指定を許可する)**] オプションが選択されていれば、ユーザーはネットワーク競合がある場合にローカル リソース (この場合はプリンタ) を優先させることができます。この選択は、クライアント上で、Connect Tunnel の [**Connect Tunnel Properties (Connect Tunnel のプロパティ)**] ダイアログの [**Advanced (詳細設定)**] タブで行います。

Redirect All Mode (リダイレクト オール モード)

Redirect all mode (リダイレクト オール モード) では、AMC でリソースがどのように定義されているかにかかわらず、トラフィックがトンネル経由でリダイレクトされます。このオプションは、セキュリティを強化しますが、ユーザーはトンネル セッション時にネットワーク デバイスにアクセスできなくなります。しかもネットワークの構成によっては、インターネット アクセスも阻害されます。

「リダイレクト オール モード」は、「スプリット トンネル モード」よりも安全です。Connect Tunnel を「リダイレクト オール モード」で開始した後でも、ユーザーはルーティング テーブルを変更できますが、アプライアンスからクライアントに送信されたリダイレクション リストに一致しないトラフィックはすべて即座にドロップされます。これによってユーザーは、アプライアンスをバイパスしネットワークに戻る独自のトンネル分割接続を作成するために、コンピュータ上のルーティング テーブルを変更できなくなります。ルーティング テーブルが Connect Tunnel クライアントによって変更された後にルーティング テーブルを変更しても効果はありません。詳細については、ネットワーク トンネル サービスの構成を参照してください。

すべてのトラフィックをアプライアンス経由でリダイレクトしつつ、ユーザーがローカルのプリンタやファイル共有にもアクセスできるようにするには、[**Redirect all, with access to local network (リダイレクト オール、ローカル ネットワークへのアクセス付き)**] を選択します。例えば、在宅勤務するリモート従業員のコミュニティがある場合、このリダイレクション モードを使用すれば、セキュリティを最大限に高めながら、プリンタなど自宅のネットワークのリソースも利用できるようにすることが可能です。

プロキシ サーバー リダイレクション

オプションで、VPN 接続がアクティブな場合に、インターネットへのトラフィックを内部プロキシ サーバー経由でリダイレクトするよう構成することもできます。これは、HTTP プロキシ サーバーを使用して、インターネット リソースへのリモート ユーザーのアクセスを制御したい場合に使用すると便利です。このオプションは、「リダイレクト オール モード」が有効な場合に限り使用できます。この設定の構成方法については、トンネル クライアント設定の構成を参照してください。

メモ：リダイレクション モードとして、ローカル ネットワーク アクセスを含むリダイレクト オールを選択した場合、ユーザーはローカルのファイル共有とプリンタにアクセスできます。ただし、リモート プロキシに.pac ファイルを使用している場合は、そのリダイレクション ルールが、WinINet ネットワーキング ライブラリ (Internet Explorer、Media Player、Instant Messenger など) 経由でルーティングされるすべてのトラフィックで優先されます。例えば、ユーザーは、ローカル ネットワークにあるサーバーであればその Web アプリケーションにアクセスできると考える可能性がありますが、実際にはリモート プロキシ経由で要求がリダイレクトされます。

トンネル クライアントとプロキシ自動構成ファイル (Linux プラットフォーム)

プロキシ サーバーがインターネットへのアウトバンド アクセスに使用されている環境において、OnDemand Tunnel または Connect Tunnel が Linux プラットフォームで開始されると、SMA アプライアンスではブラウザのプロキシ自動設定 (`.pac`) ファイルにリダイレクション設定が追加されます。このような変更が有効なのはセッションの間だけであり、ユーザーがログアウトしているときは元のブラウザ設定が使用されます。このプラットフォームとクライアントの組み合わせに関しては、次のような既知の問題があります。

- ユーザーのセッションの間に、ブラウザの `.pac` ファイルへの変更許可を求める確認メッセージが 1 つ以上表示される場合があります。WorkPlace にログインして適切な機能を使用するためには、この `.pac` ファイルへの変更を受け入れる必要があります。

- サーバーの .pac ファイルが更新されたら、ユーザーは OnDemand Tunnel または Connect Tunnel クライアントで接続して変更を取り込むか、手動で元のプロキシ設定に戻す必要があります。
- Connect Tunnel の起動時にユーザーの Firefox ブラウザのウィンドウが開いていると、その開いているブラウザ ウィンドウには、(適切に接続をリダイレクトするために) アプライアンスでブラウザの .pac ファイルに加える必要がある変更内容が適用されません。

  ユーザーはウィンドウを閉じてから Firefox をもう一度開くか、ブラウザのプロキシ設定を手動でリロードする必要があります。

UDP トンネル モード

ネットワーク アドレス変換 (NAT) により、複数のプライベート ネットワーク アドレスで 1 つのパブリック IPv4 アドレスを共有できます。ただし、アドレス変換が実行されるということは、VoIP やテレビ会議といったクライアント間のネットワーク アプリケーションが適切に動作しないということも意味します。このようなネットワーク アプリケーションにおいて信頼できる接続を確立して維持するには、ユーザーの IP アドレスが必要になります。

ESP (Encapsulating Security Payload) とは、UDP ラッパー (ポート 4500) 内部でパケットのカプセル化およびカプセル化解除を行って NAT をトラバースさせるためのプロトコルです。ESP を使用すると、VoIP などの UDP ストリーミング用アプリケーションのパフォーマンスを向上させることができます。ESP の詳細については、RFC 2406 および 3948 を参照してください。

http://www.ietf.org/rfc/rfc2406.txt

http://www.ietf.org/rfc/rfc3948.txt

ESP によるカプセル化は、新規定義されるコミュニティのデフォルト設定になります。UDP ポート 4500 は、アプライアンスの外部 IP アドレスと仮想 IP アドレスに対して送受信されるトラフィック向けにネットワーク ファイアウォールで開放されている必要があります。外部のアプライアンス トラフィックが NAT の対象となる場合は、UDP ポート 4500 用に NAT を構成する必要があります。また、まれですが、PMTU 検出が適切に実装されていない (RFC 1191 を参照) ネットワーク環境では、特定のアプリケーションが非効率的に実行されるか、ESP カプセル化使用時にはまったく実行されない可能性があります。

ESP が有効なときは、クライアントと EX Series アプライアンス間で自動的に ESP の使用についてネゴシエーションされます。ESP をすべてのトラフィックで使用することも、UDP トラフィックに限定して使用することもできます。ESP が失敗した場合やクライアントでサポートしていない場合は、代わりに SSL トンネルが自動的に使用されます。AMC の [**User Sessions (ユーザ セッション)**] ページには、使用されているトンネルのタイプが示されます。

ログ ファイルにも、使用されたトンネルが示されます。ログ メッセージの場合は、UDP ポート 4500 パケットが ESP トラフィックに使用され、TCP ポート 443 パケットが SSL トンネル パケットに使用されることが示されます。

安全なネットワークの検出

安全なネットワークの検出 (SND) により、ユーザーは安全性の低い場所からログインするときでも自動的にトンネル接続を確立できます。クライアントは、接続されたインターフェースに対して、クライアントの DNS サフィックスとサーバーを比較することで、安全なネットワークにデバイスが接続しているかどうかを判断します。この比較に応じて発生することは、次のとおりです。

安全なネットワークの検出

	接続された場合...	接続されなかった場合...
DNS エントリが検出された	切断し、SND 状態で再接続	SND 状態で接続
DNS エントリが検出されなかった	接続状態を維持	ダイヤラーを使用して接続

安全なネットワークの検出 (SND) は、Connect Tunnel および Mobile Connect により提供されます。SND は、クライアントのエンドポイント デバイスから SMA アプライアンスへの安全な「常時接続」 SSL VPN セッションを可能にします。SND が有効になっているときに、ユーザーが安全ではないネットワークを使用すると、Connect Tunnel および Mobile Connect クライアントで検出され、自動的にトンネル接続が確立されます。接続ステータスは、システムトレイ上のアイコンで示されます。

システムトレイ アイコン

システムトレイ アイコン	説明
	接続済み
	切断

SND を使用する際は、以下を考慮してください。

- SND を機能させるには、EPC ゾーンのレベルで [**Allow session to resume from multiple IP addresses (複数の IP アドレスからのセッションの再開を許可)**] チェックボックスを選択しておく必要があります。
- クレデンシャル のキャッシュなしでセキュア ネットワーク検出を有効にすると、セッションが [**General Settings (一般設定)**] の最大クレデンシャル存続時間よりも長い場合、ユーザーがセキュリティ保護されたネットワークからセキュリティ保護されていないネットワークに移動する際（またはその逆）に、クレデンシャルを求められる場合があります。フォールバック サーバーとセキュア ネットワーク検出を使用しており、プライマリ アプライアンスがダウンしているか利用できないことを Connect Tunnel が検出した場合（ユーザー セッションがフォールバック アプライアンスで有効でないため）にも、クレデンシャルが求められます。
- フォールバック サーバーの問題を回避するには、ユーザーがログインしているコミュニティのクレデンシャル キャッシュとセキュリティで保護されたネットワークの検出を有効にします。これにより、ユーザーのクレデンシャルがフォールバック アプライアンスに安全に再送信され、ユーザーによる操作なしに、ユーザーのクレデンシャルが再作成されます。

  メモ：クレデンシャルのキャッシュは、ユーザー名/パスワード タイプの認証サーバーでのみ機能します。

- AMC デフォルト ゾーンのチーム ソース チェックのプロパティは、EPC が無効になっているときにアプライアンスに影響します。
- 10.7 よりも以前のバージョンを実行し、End Point Control が無効になっているアプライアンスの場合、ユーザーは複数の異なる IP アドレスからログインできます。これは、End Point Control が無効になっているときはデフォルト ゾーンの値が使用されるため、[**Allow user to resume session from multiple IP addresses (複数の IP アドレスからのセッションの再開を許可)**] のデフォルト値が true (チェックあり) に変更されたからです。

接続後スクリプティング

ネットワーク トンネル接続が確立された後、クライアントの Windows、Mac OS X、または Linux コンピュータ上で実行可能ファイルやスクリプトを起動するよう構成することもできます。例えば、ネットワーク ドライブをマップするためのコマンド スクリプトを実行する Windows `.bat` ファイルを指定できます。また、スクリプトが起動するときに動作するコマンドライン オプションも指定できます。

ただし、クライアントで単に、指定されているコマンドライン オプションを使用してスクリプトを実行するに過ぎず、アプライアンスにおいてスクリプトをユーザーにプロビジョニングするわけではありません。そのため、クライアントでスクリプトを実行するためには、指定されているスクリプトがユーザーのコンピュータ上にすでに存在している必要があります。また、指定されているスクリプトは個別に展開して管理する必要もあります。

この設定の構成方法については、トンネル クライアント設定の構成を参照してください。

Windows Tunnel クライアントの自動クライアント更新

Connect Tunnel または OnDemand Tunnel クライアントの Windows バージョン (バージョン 8.7 以降) が動作している場合、自動ソフトウェア更新を有効にすることで、最新バージョンのクライアントがインストールされるようになります。

ユーザーが Windows トンネル クライアントを起動し認証するたびに、現在のバージョンのクライアント ソフトウェアがチェックされ、アプライアンスで利用できる最新バージョンかどうかが確認されます。それよりも新しいバージョンがある場合は、アップデートをダウンロードできることがユーザーに通知されます。クライアント アップデートをインストールする場合にユーザーが選択できるオプションを (コミュニティ単位で) 構成することも可能です。

- ユーザーがアップデート プロセスを開始する時期を選択できるようにします。アップデートは無期限に延期することもできます。ただし、アップデートがインストールされないと、トンネル クライアントが起動するたびに、ユーザーにアップデートのアラートが表示されます (1 日に 1 回)。
- 必要条件にする (ユーザーが VPN リソースにアクセスする際、アップデートを受け入れなければならないようにする) か、強制する (すぐにインストール プロセスが始まりユーザーがそれをキャンセルできないようにする) ことにより、アップデートを必須条件にします。

ユーザーが、ソフトウェア アップデートのダイアログ ボックスで [**Install (インストール)**]をクリックすることにより、トンネル クライアント ソフトウェアのアップデートを受け入れると、クライアント ソフトウェア アップデートが自動的にダウンロードされ、ユーザーのコンピュータにインストールされるか (Connect Tunnel の場合)、アクティブになります (OnDemand Tunnel の場合)。インストールが終わったら、トンネル クライアントが自動的に再起動します。アップデートをインストールした後、ユーザーがコンピュータを再起動する必要はありません。

ソフトウェア アップデートの構成については、トンネル クライアント設定の構成を参照してください。

セッションの終了

デフォルトの場合、トンネル クライアントのセッションが確立したら、アプライアンスでそのセッションを終了させることはありません。ユーザーはセッションを待機状態にし、再認証なしで復帰させることができます。これがセキュリティ リスクと判断される環境の場合は、セッションを終了させて、ユーザーに再認証を要求できます。

- 手動: AMC のメイン ナビゲーション メニューから [**User Sessions (ユーザ セッション)**] をクリックしてセッションのリストを確認してから、利用可能な終了オプションのいずれかを選択します。詳細については、ユーザー セッションの終了を参照してください。

- 自動設定: ユーザーのクレデンシャルが期限切れになったらすぐに再認証を求めるメッセージをユーザーに表示するようトンネル クライアントを構成できます。トンネル クライアントの構成時に [**Limit session length to credential lifetime (セッションの長さをクレデンシャルの有効期間に制限)**] を選択すると、特定のコミュニティのセッションは終了し、[**Credential lifetime (クレデンシャル存続期間)**] ([**Configure General Appliance Options (一般装置オプションの設定)**] ページ) で指定した時間の経過後に再認証が要求されます。

  このオプションの構成方法については、トンネル クライアント設定の構成を参照してください。

トンネル クライアント設定の構成

Connect Tunnel はユーザーのデバイスにインストールされるクライアント アプリケーションであり、OnDemand Tunnel はユーザーが ActiveX または Java 対応デバイスから WorkPlace にログインするたびにアクティブ化される軽量の Web ベースのエージェントです。これら 2 つのアクセス方法は、インストールされるかアクティブ化されるかで異なりますが、どちらも同じ構成設定を使用します。

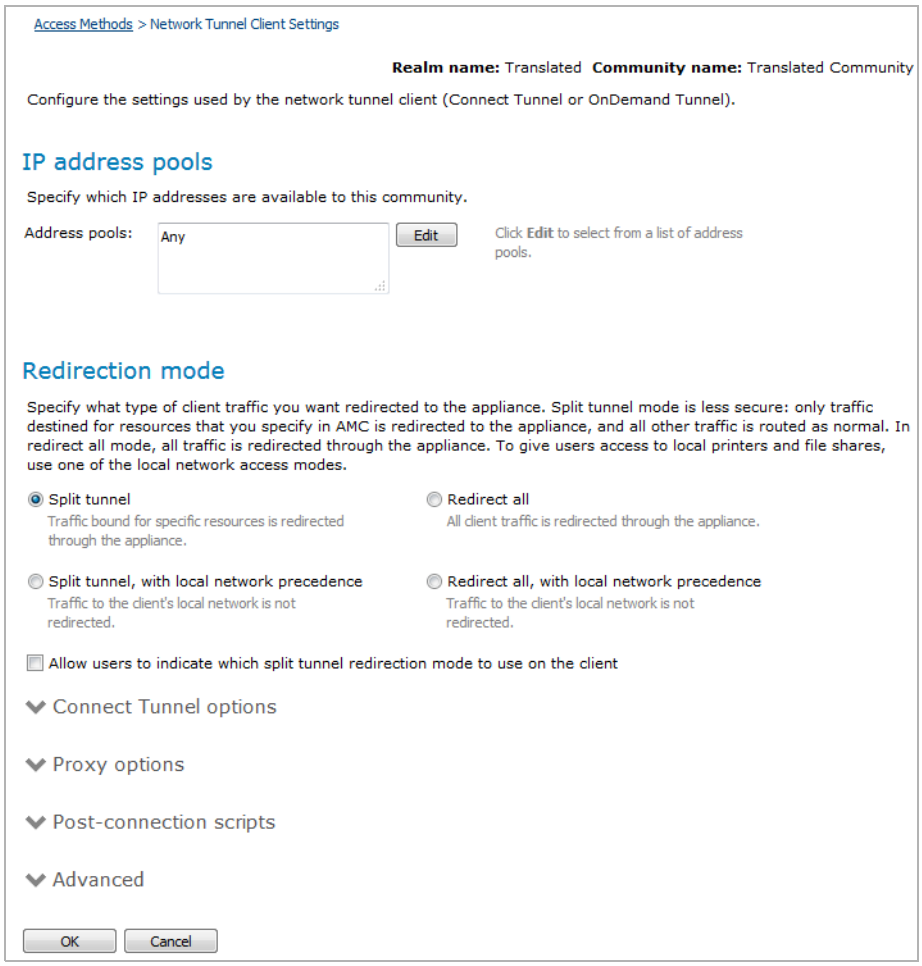
このセクションでは、トンネル クライアント設定の構成方法について説明します。この設定の詳細については、ネットワーク トンネル クライアントの構成を参照してください。

トンネル クライアントまたはエージェントの設定を構成するには、

1 選択したコミュニティの [**Access Methods (アクセス方式)**] ページで、次のアクセス方法のいずれかまたは両方を選択します。

   - **ネットワーク トンネル クライアント (OnDemand)**
   - **クライアント/サーバー プロキシ エージェント (OnDemand)**

2 [**Smart tunnel Access (Smart Tunnel アクセス)**] エリアで [**Configure (設定)**] をクリックします。[**Network Tunnel Client Settings (ネットワーク トンネル クライアント設定)**]ページが表示されます。



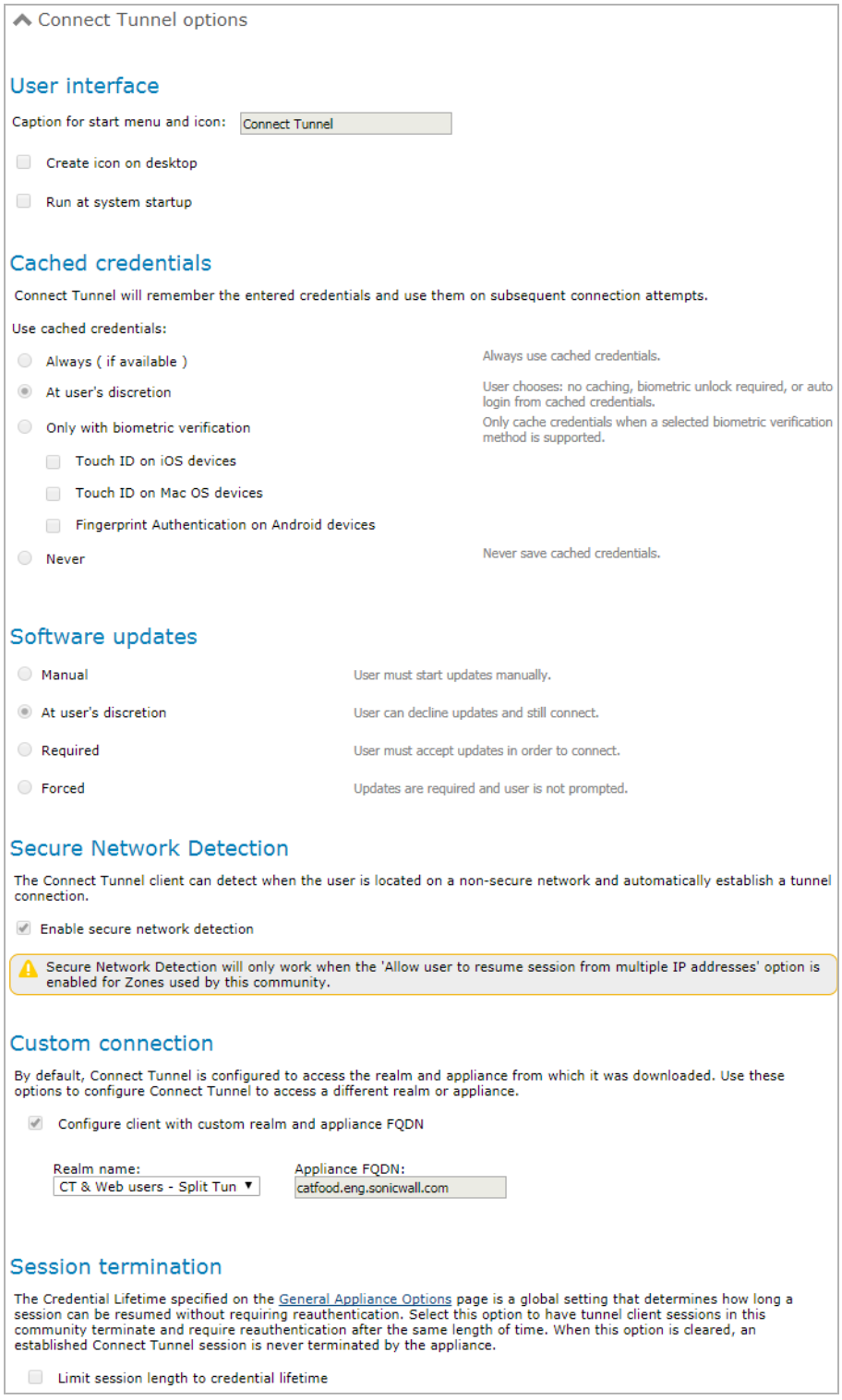
3 デフォルトでは、構成済みの IP アドレス プールがあれば、選択したコミュニティにそれが提供されます。個別の IP アドレス プールを選択するには、[**IP address pools (IP アドレス プール)**] エリアの [**Edit (編集)**] をクリックして、リストから構成済みのアドレス プールを選択します。

4 クライアント　トラフィックをアプライアンスにルーティングする際に使用するリダイレクション モードを [**Redirection mode (リダイレクション モード)**] から選択します。ネットワーク トンネル サービスでは、複数のリダイレクション モードをサポートしています。サポートされているリダイレクション モードの詳細については、リダイレクション モードを参照してください。

- [**Split tunnel (トンネルを分割する)**] : AMC で定義されているリソースにバインドされたトラフィックがトンネル経由でリダイレクトされ、他のトラフィックはすべて通常どおりにルーティングされます。
- [**Split tunnel, with access to local network (スプリット トンネル、ローカル ネットワークへのアクセス付き)**] : ユーザーがローカルのプリンタやファイル共有にアクセスできるようにします。
- [**Redirect all (リダイレクト オール)**] : AMC でリソースがどのように定義されているかにかかわらず、トラフィックがトンネル経由でリダイレクトされます。
- すべてのトラフィックをアプライアンス経由でリダイレクトしつつ、ユーザーがローカルのプリンタやファイル共有にもアクセスできるようにするには、[**Redirect all, with access to local network (リダイレクト オール、ローカル ネットワークへのアクセス付き)**] を選択します。

5 (オプション) アプライアンスがスプリット トンネル モードのいずれかに構成されている場合は、[**Allow users to indicate which split tunnel redirection mode to use on the client (クライアントで使用するスプリット トンネル リダイレクション モードのユーザーによる指定を許可する)**] を選択すれば、ローカルとリモートのネットワーク アクセスのどちらを優先するかをユーザーが決定できるようになります。詳細と例については、リダイレクション モードを参照してください。

6 (オプション) [**Connect Tunnel options (Connect Tunnel のオプション)**] をクリックして拡大します。



- [**Caption for start menu and icon (スタート メニューのキャプションとアイコン)**] フィールドには、ユーザーのデスクトップの Connect アイコンのメニューおよび下部に表示させたい Connect Tunnel クライアント用のカスタマイズ テキストを入力します。
- [**Create icon on desktop (デスクトップにアイコンを作成)**] : デスクトップに Connect Tunnel クライアントのアイコンを置きます。
- **システム起動時に実行:** オペレーティング システムがユーザーのコンピュータで起動したときに Connect Tunnel クライアントを自動的に実行します (Windows のみ)。

7 シングル サインオンを使用するには、キャッシュされたクレデンシャルを使用するタイミングを選択します。

- **常に有効:** 利用可能であれば、キャッシュされたクレデンシャルを常に使用します。
- **ユーザーの裁量:** キャッシュされたクレデンシャルを使用するタイミングはユーザーが決定します。
- **無効:** ユーザーは、キャッシュされたクレデンシャルを使用できません。

メモ： Windows システムでは、キャッシュされた *システム* クレデンシャルが Connect Tunnel で使用されます。他のシステムでも、入力されたクレデンシャルは Connect Tunnel で記憶され、以降の接続で使用されます。

8 クライアント アップデートが利用できるときにユーザーに通知する場合や、ソフトウェアを自動的に更新する場合は、[**Software updates (ソフトウェアの更新)**] オプションのいずれかを使用します。この設定は、ネットワーク トンネル クライアントが Secure Mobile Access WorkPlace からクライアントをプロビジョニングする構成になっており、バージョン 8.7 以降の場合にのみ選択できます。

- [**Manual (手動)**] : ユーザーがアップデートを手動で開始する必要があります。
- [**At user's discretion (ユーザーの裁量)**] : ユーザーがソフトウェア アップデートのインストール時期を決定できます。アップデートは無期限に延期することもできます。ただし、アップデートがインストールされないと、トンネル クライアントが起動する際に、ユーザーにソフトウェア アップデートのアラートが表示されます (1 日に 1 回)。
- [**Required (必須)**] :ユーザーがトンネル クライアント経由で VPN リソースにアクセスするためには、アップデートを受け入れる必要があります。
- [**Forced (強制)**] : 接続するためにはアップデートが必要になります。アップデート プログラムが開始され、インストールの間は進捗バーが表示されますが、プロセスの間、ユーザーにプロンプトが示されることはありません。

9 (オプション) 安全ではない場所からユーザーがログインしようとする際にトンネル接続を自動的に確立するには、[**Secure Network Detection (セキュア ネットワーク検出)**] セクションの [**Enable secure network detection (セキュア ネットワーク検出を有効化)**] チェックボックスを選択します。詳細については、安全なネットワークの検出を参照してください。

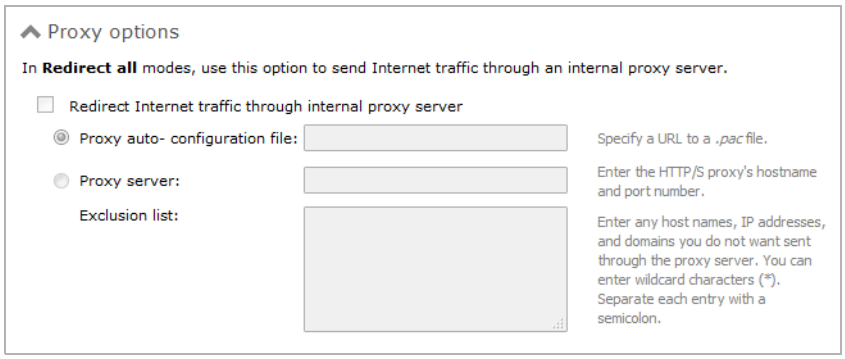
10 (オプション) デフォルトの場合、クライアントは、クライアントがダウンロードされたレルムとアプライアンス名にアクセスするよう構成されます。ただし、このデフォルト動作を上書きし、クライアントが異なるレルムやアプライアンスにアクセスするよう構成することも可能です。[**Custom connection (カスタム接続)**] エリアで、[**Configure client with custom realm and appliance FQDN (カスタム レルムとアプライアンス FQDN でクライアントを構成)**] チェックボックスを選択し、必要に応じて次のオプションを指定します。

- [**Realm name (レルム名前)**] リストからデフォルト レルムの名前をクリックします。
- [**Appliance FQDN (アプライアンス FQDN)**] フィールドに、デフォルト アプライアンスの完全修飾ドメイン名を入力します。

11 (オプション) デフォルトの場合、トンネル クライアントのセッションが確立したら、アプライアンスでそのセッションを終了させることはありません。ユーザーはセッションを待機状態にし、再認証なしで復帰させることができます。一定時間が経過したらユーザーの再認証が必要になるようにする場合は、[**Limit session length to credential lifetime (セッションの長さをクレデンシャルの有効期間に制限)**] を選択します。これで、[**Credential lifetime (クレデンシャル存続期間)**] ([**Configure General Appliance Options (一般装置オプションの設定)**] ページ) で指定した時間が経過したら、ユーザーの再認証が求められるようになります。このオプションが選択されると、セッションが非アクティブ化のしきい値に近づくとユーザーに通知され、ユーザーはマウスやキーボードで何らかの操作を行うことで切断を回避できます。

有効時間を 8 時間よりも長くするために、2 つの同一アドレス/ポートのタプル間で TCP 接続またはコンシステント UDP トラフィック フローを必要とする場合は、このオプションがチェックされていないコミュニティにユーザーを加える必要があります。[**Limit session length to credential lifetime (セッションの長さをクレデンシャルの有効期間に制限)**] チェックボックスがチェックされていない場合も、クレデンシャルの期限が切れるとユーザーはトンネル内で新しいフローを認証できなくなります。

12 (オプション) [**Redirection mode (リダイレクション モード)**] エリアで [**Redirect all (リダイレクト オール)**] を有効にしている場合、VPN 接続がアクティブなときに、インターネット トラフィックが内部プロキシ サーバー経由で送信されるよう構成できます。その場合、[**Proxy options (プロキシ オプション)**] エリアで [**Redirect Internet traffic through internal proxy server (インターネット トラフィックを内部プロキシ サーバー経由でリダイレクト)**] チェックボックスを選択して、プロキシ サーバー オプションを 1 つ選択します。



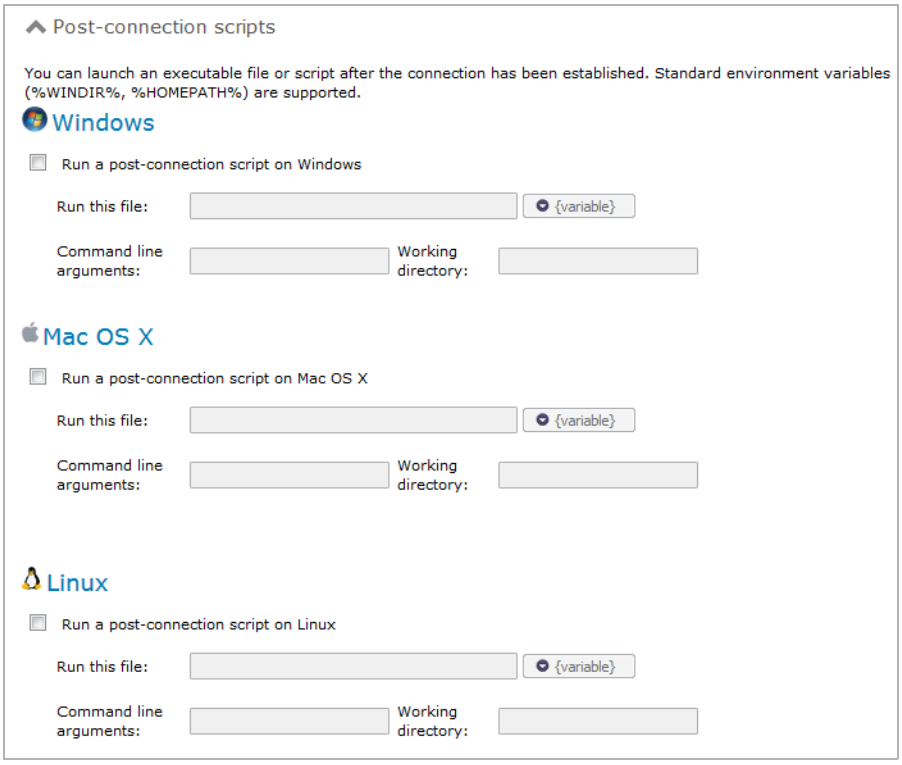
- プロキシ自動構成 (.pac) ファイルを指定するには、[**Proxy auto-configuration file (プロキシ自動構成ファイル)**] をクリックして、「http://」プロトコル識別子で始まる .pac ファイルの URL を入力します。.pac ファイルでは、ユーザーの Web ブラウザが、手動で指定した情報からではなく JavaScript ファイルからプロキシ構成設定をロードするよう構成します。JavaScript ファイルでは、どのプロキシ サーバーが使用可能で、特定の URL を特定のプロキシ サーバーにリダイレクトできるか指定します。.pac ファイルの書式については、http://en.wikipedia.org/wiki/Proxy_auto-confighttp://en.wikipedia.org/wiki/Proxy_auto-config を参照してください。
- プロキシ サーバーを手動で指定するには、[**Proxy server (プロキシ サーバ)**] をクリックして、サーバーのホスト名とポート番号を「host:port」の書式で入力します (例 : myhost:80)。オプションで、[**Exclusion list (排除リスト)**] フィールドに、プロキシ サーバーを介したリダイレクトの対象から除外したいホスト名、IP アドレス、ドメインを入力することもできます。このようなリソースを定義するときは、ワイルドカードを使用できます。また、複数のエントリをセミコロンで区切って入力することも可能です。

13 (オプション) 接続が確立したら実行可能ファイルやスクリプトを起動するよう構成するには、

a [**Post-connection scripts (接続後スクリプト)**] エリアをクリックして展開します。

b 次に、オペレーティング システムに対応する [**Run a post-connection script (接続後スクリプトの実行)**] チェックボックスをオンにします。

c 設定を行います。詳細については、安全なネットワークの検出を参照してください。



a) [**Run this file (このファイルを実行)**] フィールドに、スクリプト ファイルのパスと名前を入力します。例えば、

```
%Program Files%\ACME\remote_access.bat
```

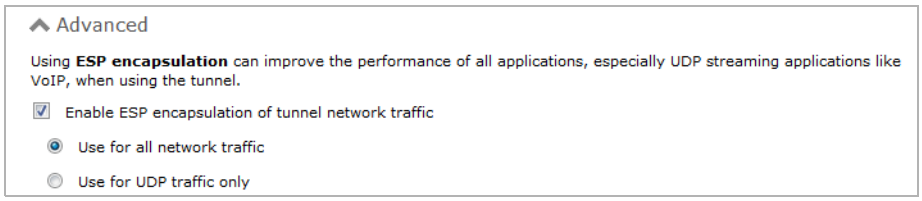
b) (オプション) [**Command line arguments (コマンドライン引数)**] フィールドに、スクリプト実行時に使用するコマンドライン引数を入力します。例えば、

```
-user=%USERNAME% -system=%OS%
```

c) (オプション) [**Working directory (作業ディレクトリ)**] フィールドに、スクリプトが実行されるディレクトリを入力します。作業ディレクトリを定義するときは、`%VariableName%` という書式で環境変数を指定できます。「`VariableName`」には実際の環境変数名を入力します。例えば、

```
%USERPROFILE%\ACME
```

14 [**Advanced (詳細設定)**] エリアでは、すべてのネットワーク トラフィック (すべてのトンネル トラフィック) に対して、デフォルトで [**Enable ESP encapsulation of tunnel network traffic (トンネル ネットワーク トラフィックの ESP カプセル化を有効にする)**] が選択されています。ESP (Encapsulating Security Payload) とは、UDP パケットの内部でカプセル化およびカプセル化解除を行って NAT (ネットワーク アドレス変換) をトラバースさせるためのプロトコルです。ESP を使用すると、特に VoIP などの UDP ストリーミング用アプリケーションのパフォーマンスを向上させることができます。



ESP トンネルを機能させるには、UDP ポート 4500 が、EX-Series アプライアンスの外部 IP アドレスと仮想 IP アドレスに対して送受信されるトラフィック向けにファイアウォールで開放されている必要があります。

ESP が有効になっていると、トンネル クライアントは ESP トンネルを確立しようとしますが、ESP トンネルの確立で問題が発生した場合は、レガシー SSL トンネルに戻ります。この問題は、ネットワーク ファイアウォールで UDP ポート 4500 が開放されていないときによく起こります。

何らかの理由で UDP ポート 4500 をファイアウォールで開放したくないために ESP を使用しない場合は、[**Enable ESP encapsulation of tunnel network traffic (トンネル ネットワーク トラフィックの ESP カプセル化を有効にする)**] チェックボックスをクリアします。コミュニティでの ESP の使用をデフォルトで無効にするには、**[Realms (レルム)] > *[お使いのトンネル レルム]* > [Communities (コミュニティ)] > *[お使いのトンネル コミュニティ]* > [Access Methods (アクセス方式)] > [Configure under Smart Tunnel Access (Smart Tunnel Access で設定)] > [Advanced (詳細設定)]** で、チェックボックスをクリアします。

15 [**OK**] をクリックします。

メモ：

- ユーザーが「リダイレクト オール モード」で OnDemand Tunnel を実行すると、変換された Web リソースへの接続が失敗し、「`Page cannot be displayed` (ページを表示できない)」というエラーが表示されます。この問題を回避するには、A (アドレス) レコードを内部 DNS サーバーに追加して、アプライアンス VIP または外部 IP をアプライアンス FQDN に割り当てます。
- [**Software updates (ソフトウェアの更新)**] エリアの[**Client software updates (クライアント ソフトウェアの更新)**] で [**At user's discretion (ユーザーの裁量)**] が有効になっている場合、ユーザーにはアップグレードの通知が表示され、Connect Tunnel クライアントはユーザーの応答を 24 時間キャッシュに保存します。それから設定を [**Required (必須)**] または [**Forced (強制)**] に変更すると、前回の応答がまだキャッシュに保存されているため、アップデートを遅らせたユーザーには、翌日になるまでメッセージが表示されないことがあります。
- 接続が確立された後に VB スクリプトを実行する場合、`.vbs` スクリプト ファイルのパスと名前を入力するだけでは実行されません。そのスクリプト ファイルを起動するために、Windows Script Host ユーティリティを使用する必要があります。これに対応するには、次のように接続後オプションを構成します。
  - [**Run this file (このファイルを実行する)**] :*<ドライブ>*:`\windows\system32\cscript.exe`
  - [**Command line arguments (コマンドライン引数)**] :*<スクリプトまでのパス>*。例えば、

    `c:\path\to\script.vbs` または `\\path\to\script.vbs`

  [**Working directory (作業ディレクトリ)**] は空白のままにしておきます。
- `.pac` ファイルの場所を指定する際には、必ずトンネル ユーザーがアクセスできるようにします。これは、リソースを定義して、アクセス ルールを作成することで行えるようになります。リソース グループの作成と管理および構成アクセス制御ルールを参照してください。

デフォルト コミュニティの使用

レルムを作成したら、そのレルムに 1 つ以上のコミュニティを対応させる必要があります。これは、アプライアンスがアクセス エージェントおよび End Point Control コンポーネントをユーザーに展開するメカニズムとして、コミュニティが使用されるためです。

コミュニティを認証レルムと対応させるための最も簡単な方法は、AMC ですでに構成されているグローバル デフォルト コミュニティを使用することです。デフォルト コミュニティには、次のような特性が自動的に割り当てられています。

- コミュニティのメンバーシップは [**Any (すべて)**] に設定されています。つまり、認証レルムのすべてのユーザーがこのコミュニティに割り当てられます。
- コミュニティのメンバー 1 人につき、最大 5 個のアクティブ セッションを利用できます。
- コミュニティのメンバーは、Web ベースのプロキシ アクセス (TCP プロトコル) と Web アクセス (HTTP) の 2 つの方法を利用できます。
- ユーザーのコンピュータには、End Point Control 制約が課せられません。

メモ：

- レルムのデフォルト コミュニティについても、他のコミュニティと同様の方法で、設定を変更できます。RADIUS アカウント レコードをファイアウォールに送信するように SMA アプライアンスを設定するを参照してください。
- また、新しくコミュニティを追加して、レルムに対応させることもできます。レルムへのコミュニティの追加を参照してください。

レルムでコミュニティがリストされる順序の変更

ユーザーが認証レルムにログインするとき、アプライアンスは、アクセス エージェントおよび EPC ポリシーを展開できるようにするため、そのユーザーが所属するコミュニティを調べます。1 つのレルムでコミュニティを 1 つしか使用しない場合、またはそれぞれのユーザーに 1 つのコミュニティしか割り当てていない場合、ログインし適切なアクセス エージェントを受け取るプロセスは単純なものになります。

ただし、あるユーザーが複数のコミュニティに所属している場合、そのユーザーに割り当てられるコミュニティは、[**Configure Realm (設定レルム)**] ページの [**Communities (コミュニティ)**] タブにリストされるコミュニティの順序で決まります。アプライアンスは、ユーザーをリストの最初のコミュニティと一致させようとします。ユーザーは、一致するリストの最初のコミュニティに割り当てられることになります。そのため、このような場合は、最も範囲が狭いコミュニティをリストの先頭に配置することをお勧めします。

レルムに対するコミュニティの順序を変更するには

1. メイン ナビゲーション メニューから [**Realms (レルム)**] をクリックします。
2. コミュニティの順序を変更する認証レルムの名前をクリックします。[**Configure Realm (設定レルム)**] ページの [**General (一般)**] タブが表示されます。
3. [**Communities (コミュニティ)**] タブをクリックします。このレルムの部分になっているコミュニティが、ここでリストされている順序で処理されます。
4. 選択しているコミュニティを上下に移動する場合は、[**Move Up (上に移動)**] または [**Move Down (下に移動)**] のリンクを使用します。
5. コミュニティが所定の場所まで移動したら、[**Save (保存)**] をクリックします。

メモ：ユーザーに割り当てられているコミュニティは、Secure Mobile Access WorkPlace ホーム ページに表示されます ([**Connection Status (接続ステータス)**] エリアの [**Details (詳細)**] をクリック)。

レルムでの RADIUS アカウンティングの構成

アカウンティング情報を収集するために RADIUS サーバーを使用する場合、AMC で RADIUS アカウンティング サーバーを構成して、レルム単位でアカウンティングを有効にできます。アプライアンスでは、ユーザー セッション、接続の時刻と時間、接続元 IP アドレスなどを示す RADIUS アカウンティング メッセージをサーバーに送信します。

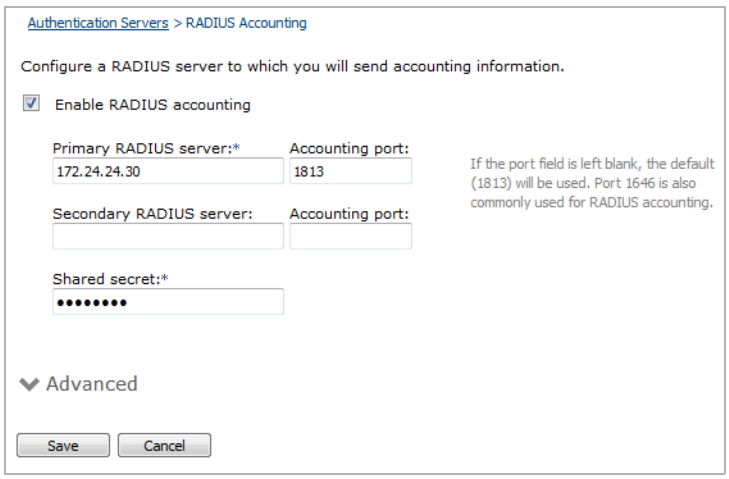
アプライアンスは、一度に 1 台の RADIUS サーバーに接続できます。AMC で 2 台の RADIUS サーバーが構成されている場合、アプライアンスはプライマリ サーバーのみにメッセージを送信し、プライマリ サーバーとの接続が失敗した場合に限り、セカンダリ サーバーと通信します。

RADIUS アカウンティング サーバーを構成するには

1 メイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

2 このページの [**Other servers (その他サーバ)**] エリアで、[**RADIUS Accounting (RADIUS アカウント)**] の横にある [**Edit (編集)**] リンクをクリックします。

3 アプライアンスが RADIUS、syslog、ルーティングの変更を保存できるようにするには、[**Enable accounting records (アカウンティング レコードの有効化)**] チェックボックスを選択します。



4 [**Primary RADIUS server (プライマリ RADIUS サーバー)**] フィールドにプライマリ アカウンティング サーバーの IP アドレスを入力します。[**Accounting port (アカウント ポート)**] ボックスには、サーバーとの通信で使用するポート番号を入力します。ここを空白のままにすると、デフォルトのサーバー ポート (**1646**) が使用されます。

5 アプライアンスとサーバー間の通信に障害が発生した場合のバックアップとして、2 台目の RADIUS アカウンティング サーバーを使用する場合は、[**Secondary RADIUS server (2 台目の RADIUS サーバー)**] フィールドにサーバーの IP アドレスを入力し、[**Accounting port (アカウンティング ポート)**] フィールドにポート番号を入力します。

6 [**Shared secret (事前共有鍵)**] フィールドに、アプライアンスが RADIUS アカウンティング サーバーと通信する上で必要な、事前に設定された秘密情報を入力します。

7 [**Advanced (詳細設定)**] エリアの [**Retry interval (再試行間隔)**] フィールドに、RADIUS サーバーからの返信を待つ時間を秒単位で入力します。この時間が経過すると、サーバーとの接続が再試行されます。

8 デフォルトの場合、アプライアンスは、そのアプライアンス名 ([**Configure Network Interfaces (ネットワーク インターフェースの設定)**] ページで設定) を使用して、RADIUS アカウンティング サーバーで認証を受けます。ただし、[**NAS-Identifier (NAS 識別子)**] ボックスや [**NAS-IP-Address (NAS IP アドレス)**] ボックスを使用することで、アプライアンスが異なる ID 情報を送信するよう設定することもできます。

9 [**Locale encoding (ロケールのエンコーディング)**] エリアで次のように設定します。

- [**Selected (選択済み)**] ドロップダウン メニューから文字セットを選択します。選択可能な文字セットのリストについては、選択可能な RADIUS 文字セットを参照してください。

- [**Other (その他)**] をクリックし、フィールドに文字セットの名前を入力します。入力できる文字セットのリストについては、サポートされているその他の RADIUS 文字セットを参照してください。

10 [**Save (保存)**] を選択します。

コミュニティの編集、コピー、削除

コミュニティの編集方法、コピー方法、削除方法の詳細については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

ユーザーおよびグループの管理

ユーザーおよびグループの管理は、継続的な作業になります。ほとんどのユーザー管理は、外部ユーザー リポジトリを介して行われますが (ユーザーとグループが直接アプライアンスに保管されることはないが参照はされる)、信頼できるアクセスを提供するためには、AMC リストで最新の状態が保持されるようにすることが必要となります。

AMC で定義されているユーザーとグループは、アプライアンスで現在構成されているディレクトリと対応しています。

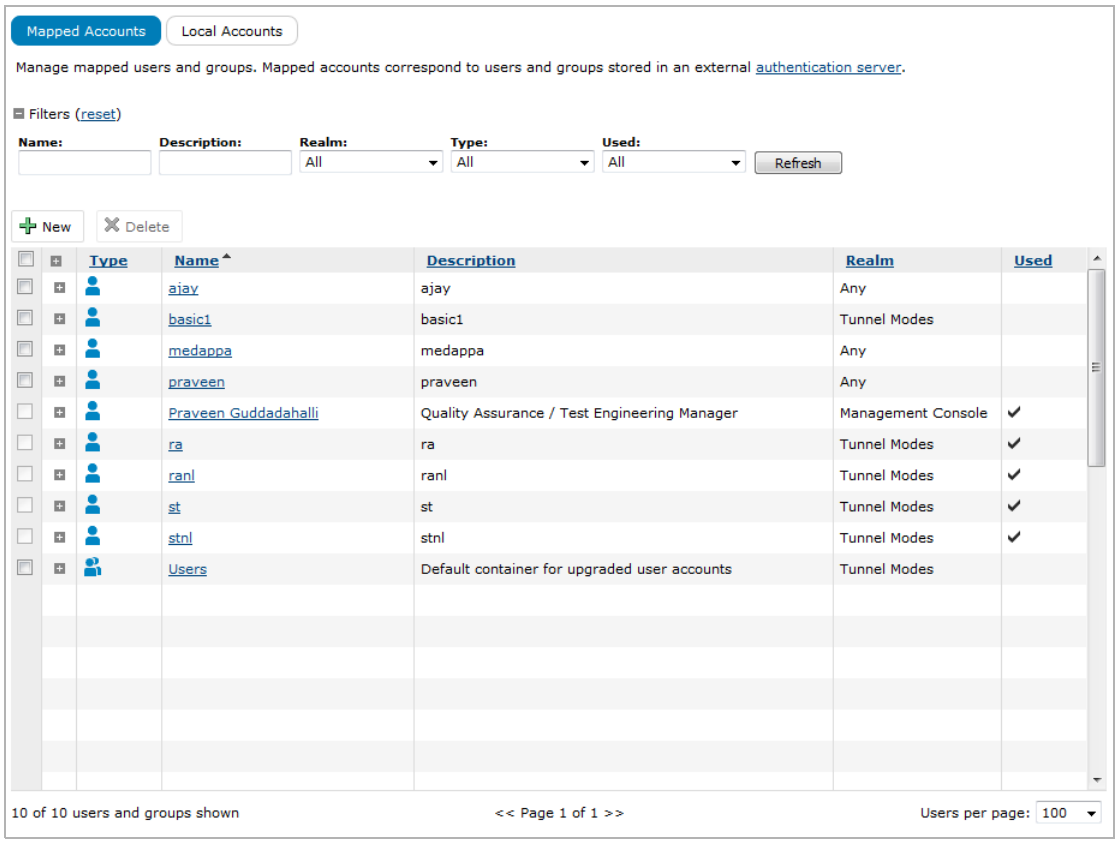
- ユーザーおよびグループの表示
- 外部リポジトリにマッピングされているユーザーおよびグループの管理
- ローカル ユーザー アカウントの管理

ユーザーおよびグループの表示

AMC で構成されているユーザーとグループは、[**Mapped Accounts (マッピングされたアカウント)**] および [**Local Accounts (ローカル アカウント)**] のページに表示されます。

ユーザーとグループを表示するには

1 メイン ナビゲーション メニューで [**Users & Groups (ユーザとグループ)**] を選択します。



2 表示するユーザー オブジェクトに対応するタブを選択します、

タブ	可能な操作
[Mapped Accounts]	外部認証サーバーに保管されたグループ情報にマッピングされているユーザー グループと個別ユーザーを管理します。 ディレクトリ情報に基づいて新しいグループを作成します。
[Local Accounts]	アプライアンスのローカル ユーザ認証リポジトリに補完されているユーザを管理します。

3 オプションの [**Filters (フィルタ)**] 設定を使用すれば、表示させるオブジェクトを絞り込むことができます。フィルターの使用方法については、フィルタを参照してください。

4 管理対象アカウント、ローカル アカウントの各リストに表示されたデータを確認します。

- チェック ボックス列は、削除するリスト項目を 1 つまたは複数選択するときに使用します。
- プラス記号 (+) の列をクリックすると、ユーザー、グループ、ローカル アカウントの情報欄が拡大されます。
- [**Type (種別)**] 列には、オブジェクトが ユーザーか グループかを示すアイコンが表示されます。
- [**Name (名前)**] 列には、ユーザー、グループ、ローカル ユーザー アカウントを作成するときに割り当てた名前が表示されます。
- [**Description (説明)**] 列には、アカウントを作成するときに入力したテキストが表示されます。

- [**Realm (レルム)**] 列には、ユーザー、グループ、ローカル ユーザー アカウントに対応するレルムが表示されます。
- [**Used (使用中)**] 列には、ユーザーまたはグループが現在使用中かどうかが示されます。

5 ある列に基づいてリストをソートする場合は、列の見出しをクリックします。

外部リポジトリにマッピングされているユーザーおよびグループの管理

ローカル ユーザー認証ストアのメンバーとして定義されていないユーザーとグループは、直接アプライアンスに保管されるわけでなく、外部ユーザー ディレクトリから参照されます。個別のユーザーを管理するのは、ほとんどの場合、グループ メンバーシップで認められているものと異なる権限を割り当てる場合に限られます。外部ディレクトリに保管されている情報を使用して、AMC でユーザーのグループを作成する場合、次の 2 種類の方法があります。

- 外部ディレクトリと同じグループ名を使用します。ほとんどのディレクトリでは、同様のユーザー アカウントをまとめるため、同様の権利や権限を与えています。ディレクトリをこのように管理する場合、アプライアンスでのユーザー管理は通常、ユーザー単位ではなく、グループ中心に行われることになります。ディレクトリに保管されているユーザー グループを参照するようアプライアンスをセットアップして、その後、アクセス制御ルールでそのグループを参照します。
- 共通の属性を使用して、外部ディレクトリを照会します。その結果を使用して、アクセス制御ルールで使用できる新しいグループ (外部ディレクトリで参照されないグループ) を作成できます。例えば、一定範囲の郵便番号の住所に居住するすべての従業員のディレクトリを照会することにより、「Local employees」という名前の新しいグループを作成できます。

Microsoft Active Directory および LDAP ディレクトリの場合、いくつかの方法でグループを追加できます (ただしこの機能は、RADIUS レルムで参照されているユーザーまたはローカル ユーザー ストアのユーザーを追加する場合は使用できません)。

- 識別名 (DN) を手動で入力
- ディレクトリの内容を検索して、リストからグループを選択
- 動的なグループ式を作成

テストや評価のために、アプライアンスでローカル ユーザーを作成することもできます。ローカル ユーザー アカウントの管理を参照してください。

トピック:

手動でのユーザーまたはグループの追加

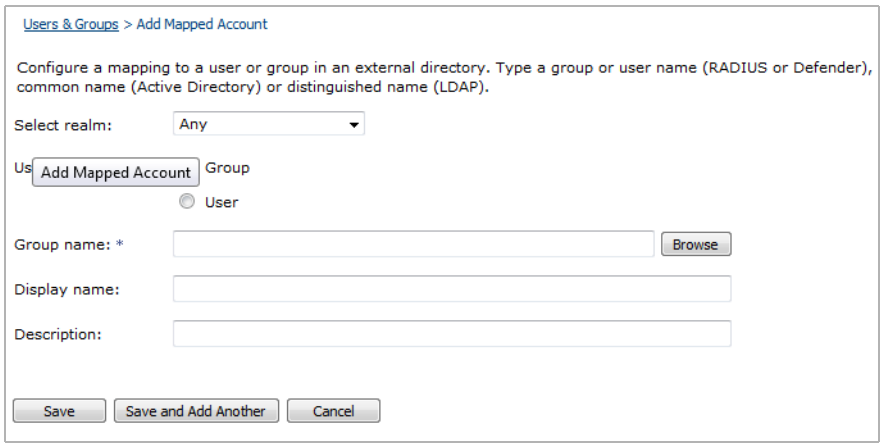
アクセス制御ルールを作成するとき、特定のルールが適用されるユーザーとグループを指定します。ただしアクセス制御ルールで指定できるようにするには、事前にユーザーを追加しておく必要があります。ユーザーは手動で追加することも、Active Directory や LDAP ディレクトリを使用して追加することもできます。ディレクトリを使用する場合は、[**Browse (検索)**] をクリックして、ディレクトリを探します。詳細については、ディレクトリの検索によるユーザーやグループの追加を参照してください。

手動でユーザーを追加するには

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Mapped Accounts (マッピングされたアカウント)**] タブをクリックして、[**New (新規)**] をクリックします。ポップアップ メニューが表示されます。

3 [**Manual entry (手動エントリ)**] を選択します。[**Add Mapped Account (マッピングされたアカウントの追加)**] ページが表示されます。



4 [**Select realm (レルムの選択)**] ドロップダウン メニューから、ユーザーが所属するレルムを選択します。ユーザーが複数のレルムに所属しており、レルムを問わずに検索したい場合は、レルムリストから [**Any (すべて)**] を選択します。

5 [**User type (ユーザー種別)**] ラジオ ボタンでは、追加するアカウントのタイプを選択します。[**Group (グループ)**] (デフォルト) または [**User (ユーザー)**]

6 グループを選択した場合は、**[Group name (グループ名)]** フィールドに、外部リポジトリに表示されるのとまったく同じグループ名を入力します(グループ名は大文字と小文字が区別されます)。この名前は、マッピング先のディレクトリのタイプによって変動します。

ディレクトリ タイプ	入力事項
LDAP	識別名 (DN) を入力します。例えば、 `cn=Sales,cn=Users,dc=example,dc=com`
Active Directory	共通名 (CN) または識別名 (DN) を入力します。CN は DN よりも簡単に入力できますが (例えば、`Sales` と入力でき、 `cn=Sales,cn=Users,dc=example,dc=com` と入力する必要はありません) ただし、CN の場合は、完全一致が保証されません。疑わしい場合は、DN を使用する方が確実です。
RADIUS	グループ名を入力します。例えば、「`Sales`」と入力します。

Active Directory または LDAP グループを指定すると、そのサブグループ (ある場合) もそれに含まれます。グループ メンバーシップの評価の対象となるネスト レベルの数は、認証サーバーのセットアップの際に構成します。詳細については、ユーザー名とパスワードを使用する LDAP の構成および ユーザー名とパスワードを使用する Active Directory の構成を参照してください。

メモ：認証に外部ディレクトリを使用している場合、AMC でユーザー グループを追加するときに、ユーザーを実際にグループ化しているわけではありません。外部ユーザー リポジトリで定義されているユーザー グループの名前を追加しているだけです。

このアプライアンスでは、ローカルのユーザーとグループもサポートしています。ローカル ユーザー アカウントの管理を参照してください。

7 [**User (ユーザー)**] を選択した場合は、**[User name (ユーザー名)]** に、外部リポジトリに表示されるのとまったく同じユーザー名を入力します。ユーザー名は大文字と小文字が区別されます。名前の選択は、ユーザーを定義するのに使用される構文を示しています。

名前の選択

ディレクトリ タイプ	入力事項
Active Directory または RADIUS	ユーザー名を入力します。例えば、「`jsmith`」と入力します。
LDAP	識別名 (DN) を入力します。例えば、 `cn=jsmith,cn=Users,dc=example,dc=com`

8 (オプション) **[Display name (表示名)]** フィールドに、AMC のページでのグループまたはユーザーの表示名を入力します。

9 (オプション) **[Description (説明)]** フィールドに、グループまたはユーザーの説明を入力します。

10 [**Save (保存)**] または [**Save and Add Another (保存して他を追加)**] をクリックします。

メモ：名前を間違って入力すると、そのユーザーはどのリソースにもアクセスできなくなります。

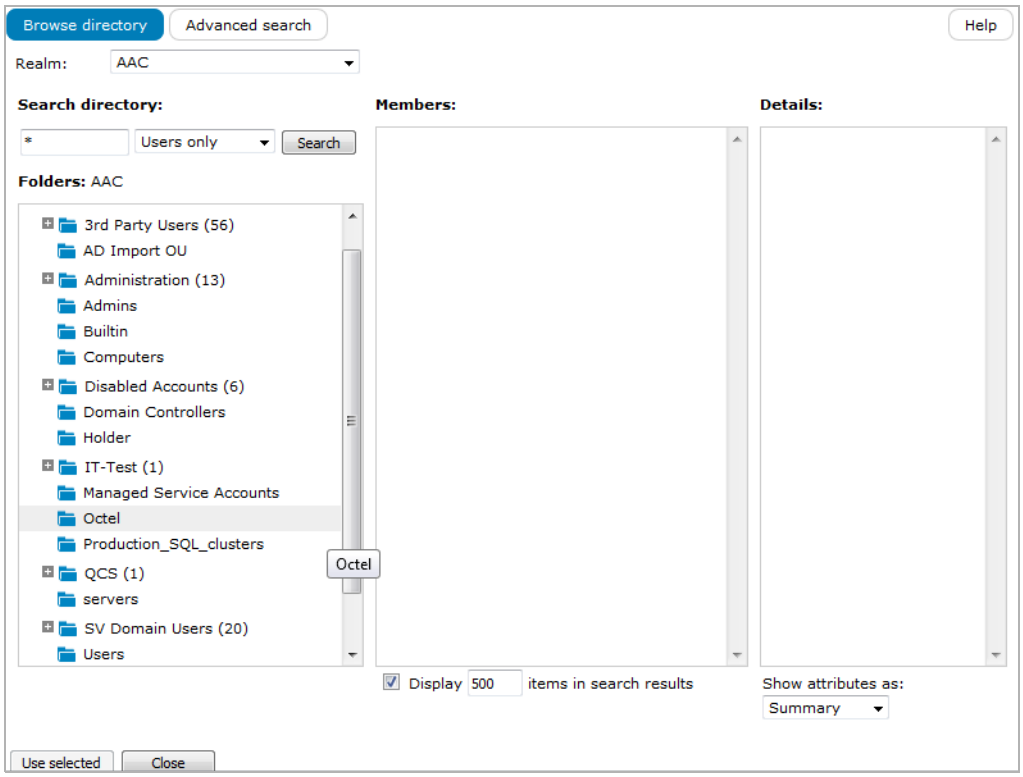
ディレクトリの検索によるユーザーやグループの追加

AMC でグループを追加する場合の最も一般的な方法は、外部ディレクトリをブラウズして、一致するグループを追加するというものです。

ディレクトリの検索によりユーザーやグループを追加するには

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Mapped Accounts (マッピングされたアカウント)**] タブで [**New (新規)**] をクリックして、[**Directory search (ディレクトリ検索)**] を選択します。[**Search Directory**] ページが表示されます。



3 検索するレルムを選択します (Active Directory、Active Directory Tree、または LDAP 認証サーバーを使用するレルムのみ選択できます)。

グループ チェックが無効になっている認証サーバーを使用するレルムを選択すると、[**Search (検索)**] フィールドはクリック不可となり、`Group checking has been disabled for this realm` (このレルムではグループ チェックが無効です) というメッセージが表示されます。詳細については、認証チェックの無効化を参照してください。

4 Active Directory Tree 認証サーバーを使用しているレルムを選択した場合は、検索するドメインも選択します。

5 検索基準を定義します。

- [**Search directory (検索ディレクトリ)**] フィールドに、ユーザー名またはグループ名のすべてまたは一部を入力します。デフォルトは「`*`」で、この場合、レルム内のすべてのレコードが返されます。ワイルドカード文字 (`*`) は、検索文字列のどの部分にも使用できます。例えば、「`j`」で始まるグループ名を検索する場合は、「`j*`」と入力します。また、「`Mary`」または「`Marty`」という名前のユーザー (ただし「`Max`」は除外) を検索するときは、「`m*y`」と入力できます。
- 検索範囲を絞り込むときは、名前を入力してドロップダウン メニューから [**Groups only (グループのみ)**] または [**Users only (ユーザーのみ)**] を選択します。例えば、ユーザーの姓を検索する場合は「`sn`」、共通名を検索する場合は「`cn`」と入力できます。
- 詳細な検索基準を指定する場合は [**Advanced (詳細設定)**] タブをクリックします。詳細については、高度な検索方法を参照してください。

6 [**Search (検索)**] をクリックします。検索基準に一致したものが 2 番目の列にすべて表示されます。

7 追加するオブジェクトを指定します。

- 結果表示ページを切り替えるときは、左下のペインにある矢印ボタン ([<] および [>]) を使用します。[<<] および [>>] を使用すると、最初のページおよび最後のページがそれぞれ表示されます。
- ユーザーまたはグループについての詳細な情報を参照するときは、その名前をクリックします。詳細な属性のリストが右側のペインに表示されます。グループがネストされている場合、サブグループをクリックすると詳細が表示されます。

  表示可能なネスト レベルの数は、認証サーバーのセットアップの際に構成します。詳細については、ユーザー名とパスワードを使用する LDAP の構成および ユーザー名とパスワードを使用する Active Directory の構成を参照してください。
- アプライアンスに追加するユーザーまたはグループの左側にあるチェックボックスを選択します。

8 選択しているユーザーまたはグループをアプライアンスに追加するには、[**Add Selected (選択したものを追加)**] ボタンをクリックします。それぞれの項目は、該当するページ ([**Groups (グループ)**] または [**Users (ユーザ)**]) のリストにアルファベット順で追加されます。

9 設定が終わったら、右上の [**Close (閉じる)**] ボタンをクリックします。この操作により、[**Search Directory (検索ディレクトリ)**] ウィンドウが閉じます。

> ⓘ **メモ**：デフォルトの場合、基本 ([basic]) 検索は、**sAMAccountName**、**cn**、**uid**、**userid** の各属性を照会することによって、ユーザーおよびグループを検索するよう構成されています。

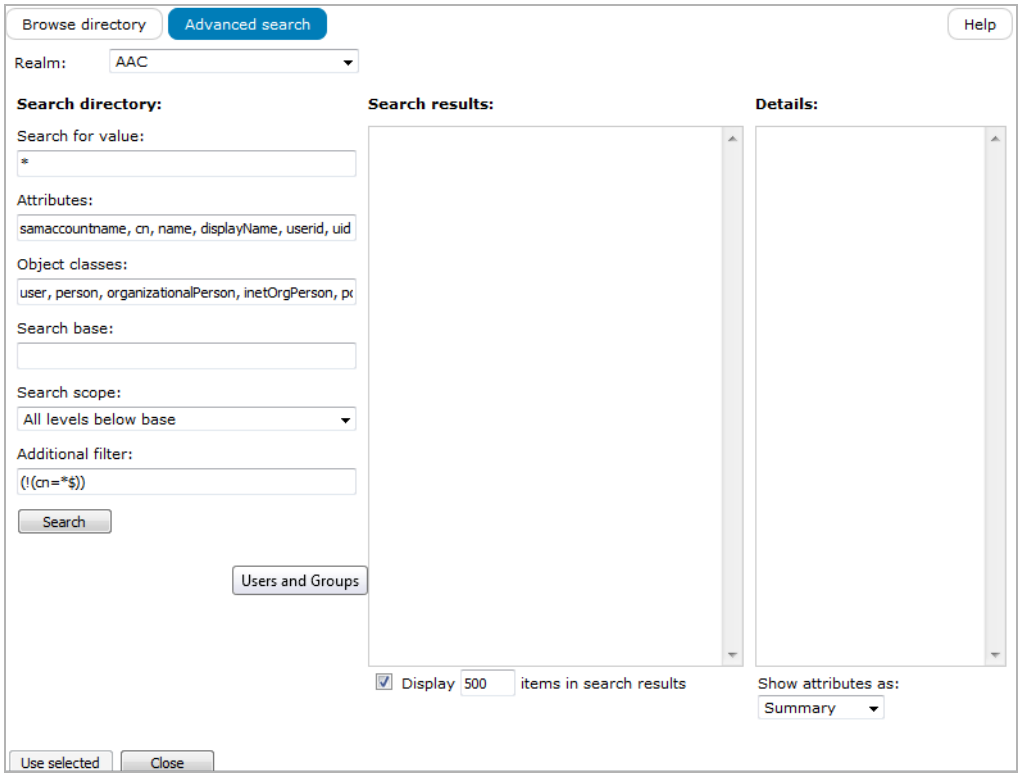
ほとんどの連鎖式認証環境では、LDAP サーバーまたは AD サーバーを (RADIUS などの) 他の認証サーバーと組み合わせて使用します。LDAP サーバーと AD サーバーを組み合わせた連鎖式認証のような特殊なケースでは、次の点について考慮しておく必要があります。

- ユーザーを検索している場合、チェーン内の最初の LDAP または AD 認証サーバーの検索結果のみが表示されます。ただし、ポリシー サーバーの場合は、チェーン内の両方のサーバーの結果が表示されます。
- グループの検索でも同じことが当てはまります (ただし、レルムでアフィニティ サーバーが構成されている場合は除きます。その場合は認証サーバーの代わりにこのサーバーが検索されます)。

例えば、連鎖式認証内の両方の LDAP サーバーまたは AD サーバーに「*Accounting*」という名前のグループがある場合、「*Accounting*」グループに限定している作成済みのアクセス制御ルールは、両方のサーバーのグループ メンバーに適用されますが、[Search Directory] ページには、チェーン内の最初のサーバーの結果のみが表示されます。

高度な検索方法

LDAP 構文に慣れている場合は、高度な検索を行うことで、照会の範囲をさらに絞り込むことができます。これは、特に大規模なディレクトリを照会する場合などに使用すると便利です。状況によっては、非標準スキーマを使用してディレクトリを照会するために、高度な検索を実行する必要があります。高度な検索を実行するには、[**Advanced search (高度な検索)**] タブをクリックします。



高度な検索基準では、高度な検索基準を指定するためのフィールドについて説明します。

高度な検索基準

フィールド	操作
検索対象の値	検索の範囲を絞り込む LDAP 検索フィルタを指定します。ユーザーまたはグループの名前の全体または一部を入力します。デフォルトは「*」で、この場合、レルム内のすべてのレコードが返されます。ワイルドカード文字 (*) は、検索文字列のどの部分にも使用できます。例えば、「j」で始まるグループ名を検索する場合は、j*」と入力します。また、「Mary」または「Marty」という名前のユーザー (ただし「Max」は除外) を検索するときは、「m*y」と入力できます。
属性	LDAP 属性を選択します。例えば、ユーザーの姓を検索する場合は [sn]、共通名を検索する場合は [cn] を選択できます。
オブジェクト クラス	ユーザーまたはグループを含むオブジェクト クラスを指定します。ユーザーの場合、これは通常「user」 または 「inetOrgPerson」になります。グループ場合は、通 常「group」、「groupOfNames」、「groupOfUniqueNames」の い ずれかになります。
検索ベース	検索を始める LDAP ディレクトリ内のポイントを入力します。通常これは、ユーザーまたはグループが含まれるディレクトリ ツリーの最下層になります。 LDAPの場合、「ou=Users,o=example.com」のように入力します。 Microsoft Active Directoryを検索するときは、 「CN=users,DC=example,DC=corp,DC=com」と指定します。

高度な検索基準

フィールド	操作
検索範囲	検索するコンテナを選択します。 [**one (1)**]: 検索ベースより 1 レベル下から情報を検索します。この範囲には、検索ベース自体は含まれません。 [**sub (サブ)**]: 検索ベースおよび検索ベースの下のすべてのレベルから情報を検索します。 [**base (ベース)**]: 検索ベースからのみ情報を検索します。検索ベースより下のコンテナは検索されません。 [**All levels below base (ベースの下のすべてのレベル)**] (デフォルト) を選択すると、ベースの下のすべてのレベルから情報を検索します。この範囲には、検索ベース自体は含まれません。
追加のフィルタ	検索の範囲を絞り込む LDAP 検索フィルタを指定します。

	構文:
	(*フィルタ* = (*演算子* (*LDAP 属性* = *値*) (. .)))
	演算子:
	• OR = |
	• AND = &
	• NOT = !
	例:
	`(cn=Sandy Cane)`
	`(!(cn=Tim Howes))`
	`(&(objectClass=Person)(|(sn=Cane)(cn=Sandy C*)))`

メモ：LDAP 検索フィルタの詳細については、RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt) を参照してください。

LDAP 検索構文は柔軟が高く、複数の方法を使用して同じ結果を引き出せるようになっています。例えば、あるディレクトリのすべてのグループを検索するとき、オブジェクト クラスを使用できます。

```
objectclass=group;groupOfNames
```

また、検索フィルタを使用しても、同じ結果を引き出すことができます。

```
(|(objectclass=group)(objectclass=groupOfNames))
```

ディレクトリを使用した動的グループの作成

外部の Microsoft Active Directory または LDAP ディレクトリを使用している場合、独自のディレクトリクエリーを構築して、AMC グループを構成できます。また LDAP 構文に慣れている場合は、独自のディレクトリ構文を記述することも可能です。アクセス制御ルールでこの動的グループが参照されると、外部ディレクトリが照会され、結果が 30 分間キャッシュされます。

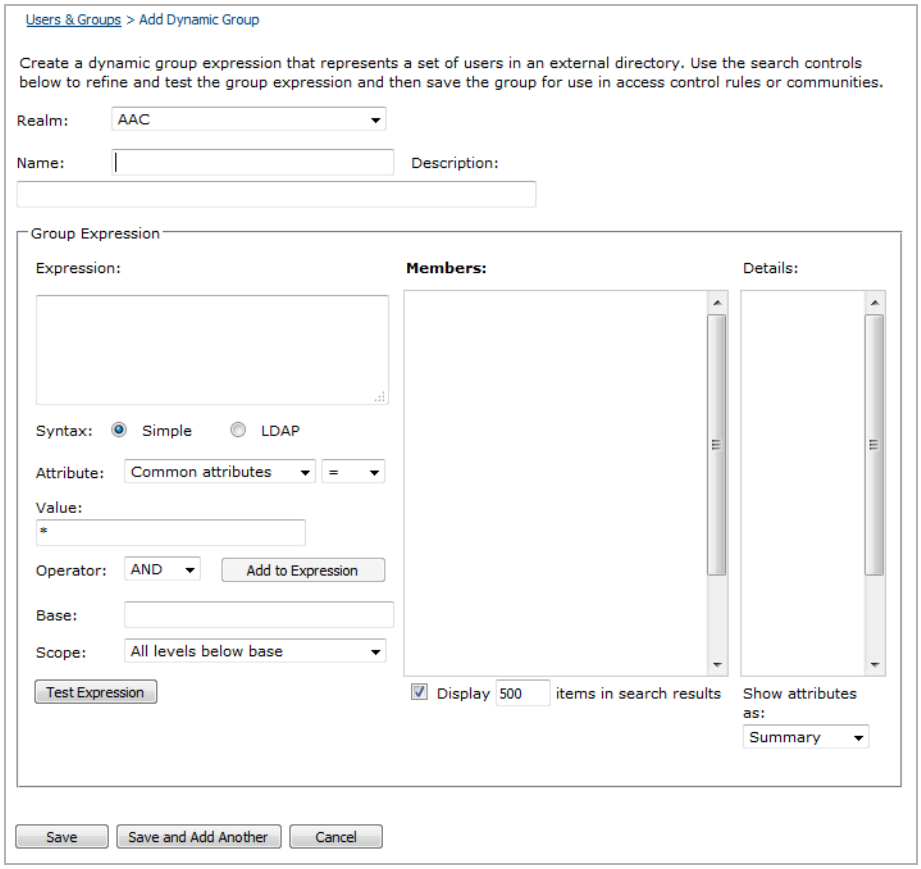
動的グループは、外部ディレクトリで定義されていないグループに適用されるポリシーを作成したい場合に使用すると便利です。例えば、「*Operations (Seattle)*」という名前のグループを作成できます。外部ディレクトリには「*Operations*」という名前のグループが存在している可能性もありますが、こうすることで、シアトルに拠点を置くメンバーのみに範囲を絞ることができます。

外部ディレクトリを使用して動的グループを追加するには、

重要：LDAP または AD ディレクトリに対して複数値のクエリーを実行するとき、クエリー対象グループの完全修飾ドメイン名を指定する必要があります。

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Mapped Accounts (マッピングされたアカウント)**] タブで [**New (新規)**] をクリックして、[**Dynamic group (動的グループ)**] を選択します。[**Add/Edit Dynamic Group (動的グループの追加/編集)**] ページが別途開きます。



このページで作成または記述する式と一致するユーザーが動的にこのグループに入れられます。後で追加したユーザーがこの式と一致した場合も、自動的にこのグループに入れられます。

3 この新しいグループが所属するレルムを [**Realm (レルム)**] ドロップダウン メニューから選択します。Active Directory または LDAP サーバー (シングルまたは連鎖式認証) で構成されているレルムのみ選択できます。

4 (オプション) この動的グループの名前を [**Name (名前)**] に入力します。

5 オプションで、説明を [**Description (説明)**] に入力します。これらは、特定のグループにのみ適用するアクセス ルールを作成する際に使用できます。

6 [**Simple (シンプル)**] または [**LDAP**] のいずれかの構文を選択します。[**Expression (式)**] フィールドで (必要に応じて) クエリーを編集できるよう、よく理解している方の構文を使用します。

7 [**Expression (式)**] エリアの各フィールドを使用して、クエリーを作成します (LDAP クエリーの構文については、高度な検索方法を参照してください)。

フィールドの使用法

設定	説明
[Expression]	ここには、以降のフィールドを使用して作成するクエリーが表示され、必要に応じて編集できます。
項目	定義されている属性のリストを取得するため、最初のクエリーが外部ディレクトリ サーバーに送信されます(このリストが正しくない場合は、[**Realm (レルム)**] リストで選択したレルムの名前を確認してください)。
[Filter operators]	LDAP または Active Directory サーバーから返された値をフィルタリングするための、一般的に使用される LDAP 検索演算子 (=、!=、>=、<=) のメニュー。
値	ユーザーが入力する値。ワイルドカード (*) を使用することもできます。例えば、[**Attribute (属性)**] で [*ZipCode*] を使用する場合、[**Value (値)**] に「`98*`」と入力することで、ワシントン州に居住するすべての従業員を照会できます。
演算子	一般的な論理演算子 (**AND**、**OR**)。
式に追加	現在の属性、値、演算子を [**Expression (表現)**] テキスト エリアに追加します。クエリーを調整するため、(必要なだけ何度でも) [**Attribute (属性)**]、[**Value (値)**]、[**Operator (演算子)**] に戻って、追加の属性、値、演算子を定義できます。追加したらそのたびに [**Add to Expression (式に追加)**] をクリックします。
[Base]	(オプション) AD/LDAP 認証サーバーのベース。クエリーを始める LDAP ディレクトリ内のポイントを指定します。例えば、Microsoft Active Directory 内のユーザーを検索する場合は、次のようにと入力します。 `CN=users, DC=engineering, DC=sonicwall, DC=com` ベースを入力しないと、認証サーバーを検索ベースにしてクエリーが実行されます。
スコープ	クエリーのレベルの深さ。[**All levels below base (ベースの下のすべてのレベル)**] (デフォルト) を選択すると、ベースの下のすべてのレベルから情報を検索します。検索ベース自体から情報を検索するには、[**One level below base (ベースの 1 レベル下)**] を選択します。検索ベースより下のコンテナは検索されません。

クエリーを直接 [**Expression (式)**] フィールドに入力することもできます。

8 作成した式をテストします。結果は [Members] セクションに表示され、検索範囲を広げたり絞ったりする必要があるかどうかがわかります。表示するメンバー数を制限するには、[**Display (表示)**] チェックボックスをチェックし、[**Display (表示)**] フィールドに最大項目数を入力します。

式をテストすると、[**Expression (表示)**] エリアに表示されている LDAP 検索クエリーが LDAP サーバーまたは AD サーバーに送信され、その結果 (ユーザーのリスト) が右側のペインに表示されます。結果が期待したものと異なる場合は、クエリーを変更して再度テストします。クエリーを変更するには、式を構築するか [**Expression (式)**] フィールドで直接クエリーを編集します。

ヒント：式のテストが終わるまで、新しいグループを保存しないでください。

9 ページの右下にある [**Show attributes as (属性の表示方法)**] ドロップダウン メニューを使用して、[**Members (メンバー)**] セクションで選択したメンバーについて [**Details (詳細)**] セクションに詳

細を表示します。[**Summary (概要)**] を選択するとメンバーの概要情報が表示され、[**All attributes (すべての属性)**] を選択するとメンバーのすべての属性が表示されます。

メモ：ほとんどの連鎖式認証環境では、LDAP サーバーまたは AD サーバーを (RADIUS などの) 他の認証サーバーと組み合わせて使用します。LDAP サーバーと AD サーバーを組み合わせた連鎖式認証のような特殊なケースでは、次の点について考慮しておく必要があります。

- ユーザーを検索している場合、チェーン内の最初の LDAP または AD 認証サーバーの検索結果のみが表示されます。ただし、ポリシー サーバーの場合は、チェーン内の両方のサーバーの結果が表示されます。
- グループの検索でも同じことが当てはまります (ただし、レルムでアフィニティ サーバーが構成されている場合は除きます。その場合は認証サーバーの代わりにこのサーバーが検索されます)。

例えば、連鎖式認証内の両方の LDAP サーバーまたは AD サーバーに「*Accounting*」という名前のグループがある場合、「*Accounting*」グループに限定している作成済みのアクセス制御ルールは、両方のサーバーのグループ メンバーに適用されますが、[**Search Directory (検索ディレクトリ)**] ページには、チェーン内の最初のサーバーの結果のみが表示されます。

ユーザーまたはグループの編集

外部ディレクトリで、ユーザーまたはグループの名前、識別名などが変更された場合、アプライアンスでアカウントを修正する必要があります。また、ローカルのユーザー アカウントやグループ名もアプライアンスで変更できます。ローカル アカウントの編集については、ローカル ユーザー アカウントの管理を参照してください。

ユーザーまたはグループを編集するには

1. メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。
2. [**Mapped Accounts (マッピングされたアカウント)**] タブをクリックし、編集するグループまたはユーザーの名前をクリックします。[**Add/Edit Mapped Account (マッピングされたアカウントの追加/編集)**] ページが表示されます。
3. 必要に応じて編集を行います。ユーザーやグループが Active Directory または LDAP レルムに所属している場合は、[**Browse (参照)**] をクリックしてユーザーを検索できます。
4. [**Save (保存)**] を選択します。

ユーザーまたはグループの削除

メモ：他のオブジェクトから参照されているユーザーまたはグループの場合は、削除できません。例えば、アクセス制御ルールで参照されているユーザーまたはグループを削除しようとすると、エラー メッセージが表示されます。削除する前に、あらかじめ、ユーザーまたはグループへのすべての参照を削除しておく必要があります。詳細については、参照されているオブジェクトの削除を参照してください。

外部のユーザー ディレクトリにマッピングされているユーザーまたはグループを削除すると、そのマッピングがシステムから削除されます。ユーザーやグループのマッピングを削除しても、外部ユーザー ディレクトリからそのユーザーやグループが削除されるわけではありません。ローカルのユーザーやグループの削除については、ローカル ユーザー アカウントの管理を参照してください。

ユーザーまたはグループを削除するには、

1. メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。
2. [**Mapped Accounts (マッピングされたアカウント)**] タブをクリックします。

3 削除するグループまたはユーザーの左にあるチェックボックスを選択します。

4 [**Delete (削除)**] を選択します。

ローカル ユーザー アカウントの管理

いずれかの方法を使用して、アプライアンスでローカル ユーザー アカウントを作成します。

- AMC でローカル ユーザー アカウントを手動で作成し、ローカル ユーザー認証リポジトリに保管します。
- カンマ区切り (CSV) テキスト ファイルからローカル ユーザー アカウントをインポートし、ローカル ユーザー認証リポジトリに保管します。新規ローカル ユーザーおよびグループのインポートを参照してください。

どの方法を使用しても、ローカル ユーザーはアプライアンスに保管されます。これは、外部認証リポジトリに保管されて AMC から参照される他のすべてのユーザーの場合と異なります。AMC では、アプライアンス上の個別のユーザーに対するローカル アカウントを作成、変更、削除でき、さらにユーザーのグループに対するローカル アカウントもサポートします。

トピック:

- ローカル ユーザの追加
- ローカル ユーザの編集
- ローカル ユーザーの削除
- ローカル グループの追加
- ローカル グループの編集
- ローカル グループの削除

ローカル ユーザの追加

ローカル ユーザーを追加する場合、あらかじめ、アプライアンスにローカル ユーザー認証リポジトリを作成しておく必要があります。作成方法についてはローカル ユーザー ストレージの構成を参照してください。ローカル認証レルムについては、ユーザーを追加する前に構成しておく必要はありません。

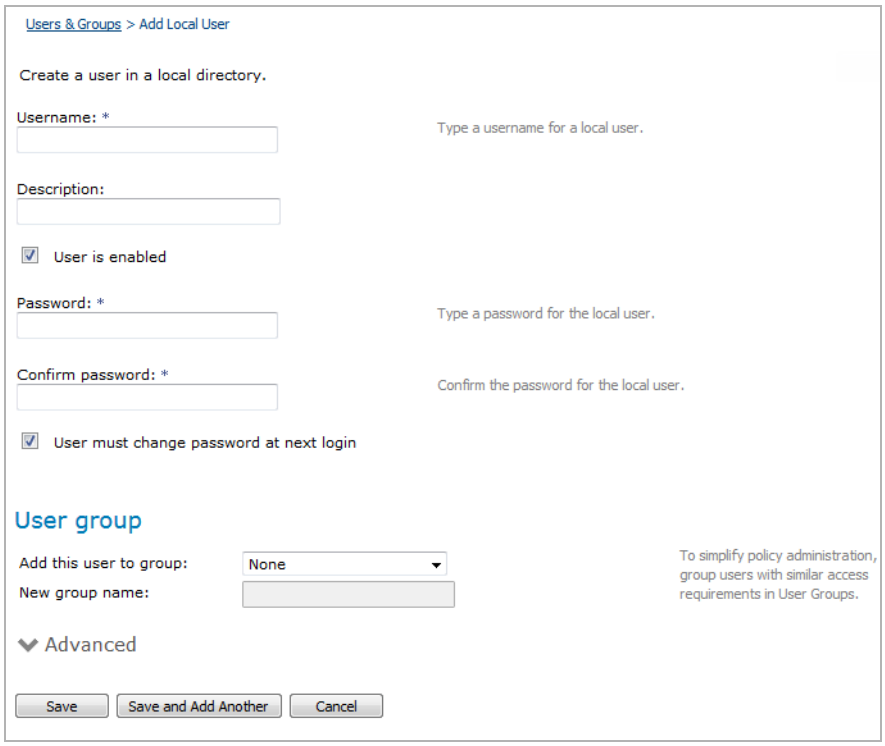
ローカル ユーザー認証リポジトリを作成したら、ローカル ユーザーをアプライアンスに追加できるようになります。

ローカル ユーザーをアプライアンスに追加するには、

1 メイン ナビゲーション メニューで [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

3 [**New (新規)**] をクリックし、[**User (ユーザ)**] を選択します。[**Add Local User (ローカル ユーザの追加/編集)**] ページが表示されます。



4 [**Username (ユーザー名)**] フィールドに、ローカル ユーザー認証リポジトリに追加するローカル ユーザーの名前を入力します。ユーザー名は、1 ～ 255 文字の長さにします。

5 [**Description (説明)**] フィールドに、ローカル ユーザーについての分かりやすいコメントを入力します。

6 ユーザーがログインできるようにするには、[**User is enabled (ユーザーは有効)**] チェックボックスを選択します。

7 [**Password (パスワード)**] フィールドに、ローカル ユーザーのパスワードを入力し、[**Confirm Password (パスワードの確認)**] フィールドに再入力します。パスワードは、ローカル認証サーバー向けに構成したパスワード ポリシーに従う必要があります。詳細については、ローカル ユーザー ストレージの構成を参照してください。

8 ユーザーの初回ログイン時にパスワード変更を必要とする場合は、[**User must change password at next login (ユーザーは次のログイン時にパスワード変更が必要)**] チェックボックスを選択します。

9 [**User Group (ユーザー グループ)**] セクションで、[**Add this user to group (このユーザーをグループに追加)**] ドロップダウン メニューからユーザーのローカル グループを選択します。選択:

- ユーザーをローカル グループに追加しない場合は、[**None (なし)**]を選択します。
- このユーザー用に新規グループを作成するには、[**(New) ((新規))**] を選択し、[**New group name (新規グループ名)**] フィールドにグループ名を入力します。

10 [**Advanced (詳細設定)**] セクションを展開し、ユーザーの電子メール アドレスまたはデバイス識別子を入力します。

11 [**Email address (電子メール アドレス)**] フィールドで、ユーザーの電子メール アドレスを構成します。このアドレスは、ユーザーにワンタイム パスワードを送信する際に使用され、デフォルトの電子メール アドレス `username@domain` を上書きします。この電子メール アドレスは、ユーザーの「**mail (メール)**」属性に割り当てられます。

12 [**Device identifier(s) (デバイス識別子)**] フィールドには、このユーザーに関連付けられているコンピュータや他のデバイスのデバイス識別子を 1 つまたはカンマで区切って複数入力します。この値は、ユーザーとデバイスのアフィニティを適用するために、デバイス識別子の終点制御機能で使用されます。これらの値は「**deviceId**」属性に割り当てられます。

13 次のどちらかをクリックします。

- [**Save (保存)**] では、ローカル ユーザー アカウントが作成され、アプライアンスのローカル ユーザー認証リポジトリに保存されます。
- [**Save and Add Another (保存して他を追加)**] では、ローカル ユーザーを保存し、さらに別のローカル ユーザーを構成します。

ローカル ユーザの編集

ローカル ユーザーの設定を変更するには、

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

3 編集するユーザーの名前をクリックします。[**Add/Edit Local User (ローカル ユーザの追加/編集)**] ページが表示されます。

4 ユーザーの設定を編集して、[**Save (保存)**] をクリックします。

ローカル ユーザーの削除

重要：他のオブジェクトから参照されているローカル ユーザーは削除できません。例えば、アクセス制御ルールで参照されているローカル ユーザーを削除しようとすると、エラー メッセージが表示されます。エラー メッセージのリンクをクリックすると、このユーザーに対する参照がすべて示されます。詳細については、参照されているオブジェクトの削除を参照してください。

ローカル ユーザーを削除するには、

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

3 削除するユーザーのチェックボックスをオンにします。

4 [**Delete (削除)**] を選択します。

ローカル グループの追加

ローカル グループを追加する場合、あらかじめ、アプライアンスにローカル ユーザー認証リポジトリを作成しておく必要があります (作成方法については、ローカル ユーザー ストレージの構成を参照してください)。ローカル認証レルムについては、グループを追加する前に構成しておく必要はありません。

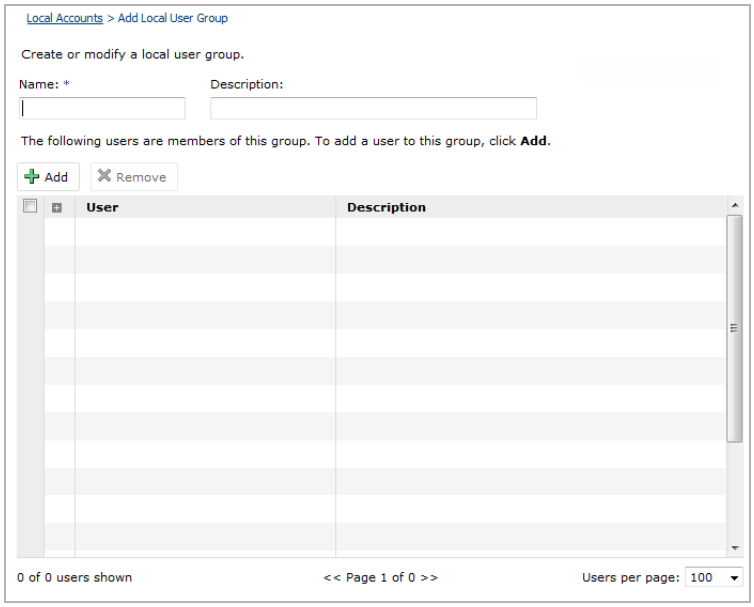
ローカル ユーザー認証リポジトリを作成したら、ローカル グループをアプライアンスに追加できるようになります。ローカル グループを手動で追加するか、グループをインポートします。インポートの詳細については、ローカル アカウントのインポートおよびエクスポートを参照してください。

ローカル グループをアプライアンスに追加するには、

1 メイン ナビゲーション メニューで [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

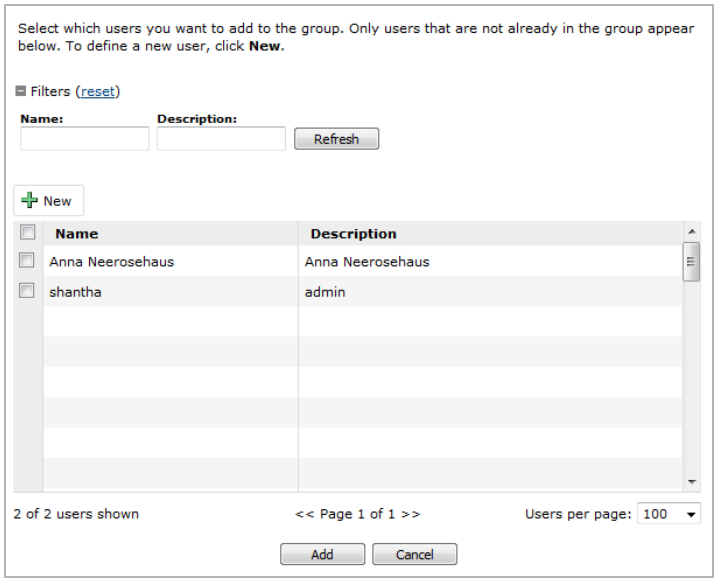
3 [**New (新規)**] をクリックし、[**Group (グループ)**] を選択します。[**Add Local User Group (ローカル ユーザ グループの追加)**] ページが表示されます。



4 [**Name (名前)**] フィールドに、ローカル ユーザー認証リポジトリに追加するローカル グループの名前を入力します。

5 [**Description (説明)**] フィールドに、ローカル グループについての分かりやすいコメントを入力します。

6 ユーザーをグループに追加するには、[**Add (追加)**] ボタンをクリックします。[**Add User to Group (ユーザーをグループに追加)**] ページが開きます。



7 グループに追加する各ユーザーの横にあるチェックボックスを選択します。

8 [**Add (追加)**] を選択します。選択したグループに含まれていないユーザーのみが表示されます。

9 新規ユーザーを作成するには、[**New (新規)**] ボタンをクリックします。[**Add User (ユーザーの追加)**] ページが表示されます。フィールドの説明については、ローカル ユーザの追加を参照してください。

10 次のどちらかをクリックします。

- [**Save (保存)**] では、ローカル ユーザー グループが作成され、アプライアンスのローカル ユーザー認証リポジトリに保存されます。
- [**Save and Add Another (保存して他を追加)**] では、ローカル グループを保存し、さらに別のローカル ユーザーを構成します。

ローカル グループの編集

ローカル グループの設定を変更するには、

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

3 編集するグループの名前をクリックします。[**Add/Edit Local Group (ローカル グループの追加/編集)**] ページが表示されます。

4 グループの設定を編集します。

5 [**Save (保存)**] を選択します。

ローカル グループの削除

重要：他のオブジェクトから参照されているローカル グループは削除できません。例えば、アクセス制御ルールで参照されているローカル グループを削除しようとすると、エラー メッセージが表示されます。エラー メッセージのリンクをクリックすると、このグループに対する参照がすべて示されます。詳細については、参照されているオブジェクトの削除を参照してください。

ローカル グループを削除するには、

1 メイン ナビゲーション メニューから [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

3 削除するグループのチェック ボックスを選択し、[**Delete (削除)**] をクリックします。

ローカル アカウントのインポートおよびエクスポート

SMA アプライアンスでは、CSV ファイルを使用して、ユーザーおよびグループの情報をインポート/エクスポートできます。ユーザーおよびグループの情報は、CSV ファイルがガイドライン (CSV ファイルの作成を参照) に従っていれば、新規および既存のユーザー アカウントにインポートできます。インポートの詳細については、新規ローカル ユーザーおよびグループのインポートおよび既存ローカル ユーザーのデータのインポートを参照してください。

Export (エクスポート)を実行すると、ローカル ユーザー認証リポジトリのすべてのローカル ユーザーを含む CSV ファイルが `LocalUsers.csv` という名前で作成されます。ガイドライン (ローカル ユーザー アカウントのエクスポートを参照) に従って、エクスポート ファイルを作成してください。

トピック:

- 新規ローカル ユーザーおよびグループのインポート
- 既存ローカル ユーザーのデータのインポート
- 新規グループのインポート
- ローカル ユーザー アカウントのエクスポート
- インポートおよびエクスポートに関するエラー メッセージ

新規ローカル ユーザーおよびグループのインポート

ローカル ユーザーおよびグループを容易に追加または編集するには、ローカル ユーザー情報をカンマ区切り (CSV) テキスト ファイルからアプライアンス構成にインポートします。これは、時間を節約できるため、特に大量のローカル ユーザーをアプライアンスに追加する必要がある新規のお客様に役立つ機能です。ユーザーのインポートは、既存ユーザーの 1 つまたは複数のプロパティを更新する必要がある場合にも非常に役立ちます。例えば、新規グループを作成する際に、新規グループを複数のユーザーにすぐに追加できます。詳細については、既存ローカル ユーザーのデータのインポートを参照してください。

ローカル ユーザーおよびグループをインポートする場合は、あらかじめアプライアンスにローカル ユーザー認証リポジトリを作成しておく必要があります (作成方法についてはローカル ユーザー ストレージの構成を参照してください)。ローカル ユーザー認証リポジトリを作成したら、ローカル ユーザーおよびグループをアプライアンスにインポートできるようになります。

メモ：ローカル認証レルムについては、ローカル ユーザーおよびグループをインポートする前に作成しておく必要はありません。

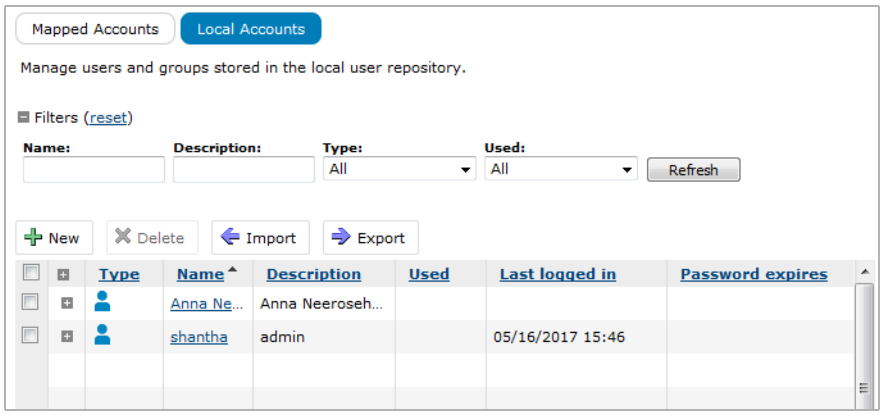
ローカル ユーザーおよびグループをアプライアンスにインポートするには、

1 インポートする CSV ファイルがローカル コンピュータにあり、ガイドライン (CSV ファイルの作成を参照) に従っていることを確認します。

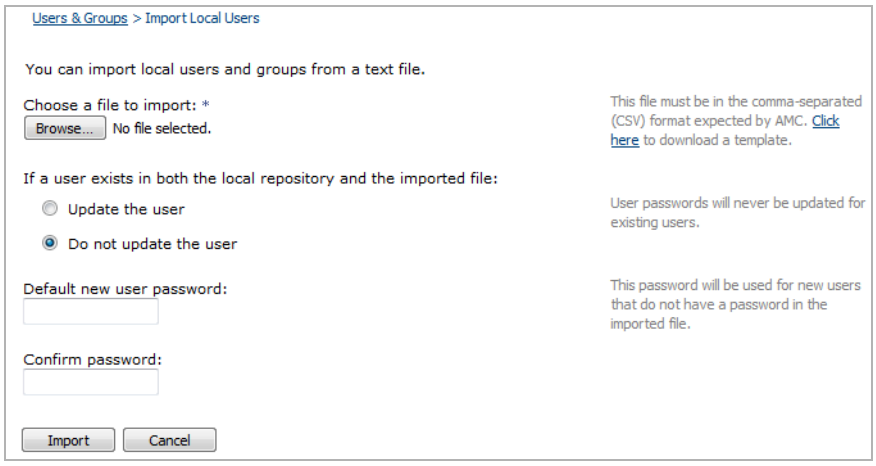
重要：CSV ファイルに何らかのエラーがあった場合、データはインポートされません。

2 [**Security Administration (セキュリティ管理)**] の下のメイン ナビゲーション メニューで [**Users & Groups (ユーザとグループ)**] を選択します。

3 [**Local Accounts (ローカル アカウント)**] タブをクリックします。



[**Import (インポート)** Import] ボタンをクリックします。[**Import Local Users (ローカル ユーザーのインポート)**] ページが表示され、ここでローカル ユーザーを CSV ファイルからローカル ユーザー認証リポジトリにインポートします。



[**Local Accounts (ローカル アカウント)**] ページを変更できるアクセス権を持ち、ローカル ユーザー認証リポジトリを利用できる状態になっている必要があります。

4 [**Choose a file to import (インポートするファイルの選択)**] フィールドで、[**Browse (参照)**] をクリックし、インポートするファイルを特定します。ファイルをインポートする前に、CSV ファイルの作成に記載されている要件を満たしていることを確認します。

5 ローカル ユーザー認証リポジトリと、インポートされるファイルの両方に含まれるユーザー アカウントがあった場合の処理方法を選択します。

選択	宛先
ユーザの更新	インポートされる CSV ファイルのユーザー レコードに一致するように、ローカル ユーザー認証リポジトリ内の重複ユーザー データを更新する
[Do not update the user]	CSV ファイル内の重複ユーザー レコードを無視し、ローカル ユーザー認証リポジトリ内のユーザー データは変更しない

この設定に関係なく、既存ユーザーのパスワードは更新されません。ただし、新規ユーザーのパスワードはインポートされます。

6 [**Default new user password (デフォルトの新規ユーザー パスワード)**] フィールドに、CSV ファイルでパスワードが定義されていない新規ローカル ユーザーをインポートする場合に共通で使用するパスワードを入力します。パスワードは、ローカル認証サーバー向けに構成したパスワード ポリシーに従う必要があります。新規ユーザーは、初回ログイン時にこのデフォルト パスワードを使用します。

7 デフォルト パスワードを [**Confirm password (パスワードの確認)**] フィールドに再入力します。

8 [**Import (インポート)**] ボタンをクリックして、ローカル ユーザー アカウントをローカル ユーザー認証リポジトリに追加します。

CSV ファイルの作成

アプライアンスへのユーザー アカウントのインポートに使用する CSV ファイルは、CSV ファイルのフィールドの順番のガイドラインに従って作成し、フィールドをこの順序で並べる必要があります。

CSV ファイルのフィールドの順番

フィールド	必須またはオプション	ガイドライン	説明
ユーザ名	必須	1 ～ 255 文字 (大文字と小文字の区別あり)	ユーザーがログイン時に入力する名前
説明	任意	許可されている文字数と文字の種類	ユーザーについての詳細情報
パスワード	任意	ローカル認証サーバー向けに構成したパスワード ポリシーに従う必要がある (新規ユーザーのインポート時のみに使用)	ユーザーがログイン時に入力するパスワード
有効	必須	`True` または `False` を含む必要がある **メモ**：大文字と小文字を区別する	ユーザーのログインを許可するかどうかを指定する
E-mail	任意	ローカル ユーザー名とドメイン名を `@` で区切る (最大 254 文字)	ユーザーにワンタイム パスワードを送信する際に使用する有効な電子メール アドレス
機器	任意	カンマ区切りリスト	ユーザーに関連付けられているデバイス ID
グループ	任意	カンマ区切りリスト (最大 255 文字) **メモ**：定義されていないグループがインポートされる場合にグループが作成されます。	ユーザーが所属しているグループのカンマ区切りリスト

この例は、ユーザーを AMC にインポートする際のファイル形式を示しています。

```
Username,Description,Password,Enabled,Email,Devices,Groups
"user0","This describes user0",,true,user0@domain.com,"abc123,def456","group0"
"user1","This describes user1",,true,user1@domain.com,"","group1,group0"
"user2","This describes user2",,false,,"",""
```

:

前述の例で示しているように、次のガイドラインにも従う必要があります。

- CSV 形式では、1 行目が列見出しとして使用されされるため、ファイルの 1 行目は無視します。
- 文字列の値は、通常二重引用符 (“) で囲みます。
- カンマを含む文字列の値は囲む必要があります。

- 文字列の値に引用符が含まれる場合は、さらに二重引用符を使用することで、引用符をエスケープする必要があります (例「`"The group name is ""Team1""."`」)

CSV ファイルに何らかのエラーがあった場合、データはインポートされず、エラー メッセージが表示されます。エラー メッセージについては、インポートおよびエクスポートに関するエラー メッセージを参照してください。

CSV テンプレートのダウンロード

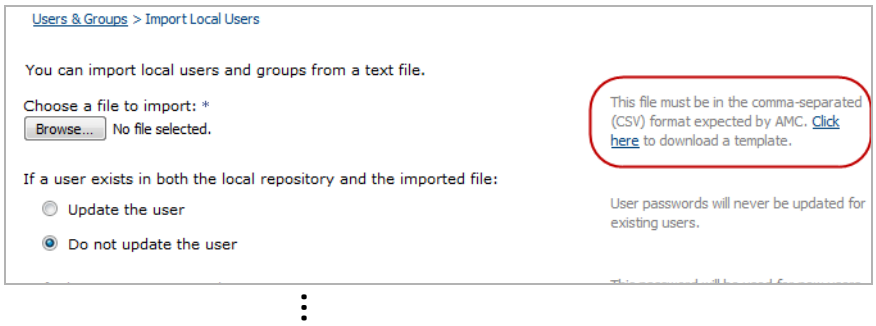
ユーザー データを含む CSV ファイルを作成するためのテンプレートをダウンロードするには、

1 [**Security Administration (セキュリティ管理)**] の下のメイン ナビゲーション メニューで [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。

3 「**Import (インポート)**」 Import ボタンを選択します。

4 [**Import Local Users (ローカル ユーザーのインポート)**] ページで、[**Click here (ここをクリック)**] リンクをクリックします。



5 Windows の [**File Download (ファイルのダウンロード)**] ダイアログが表示されたら、[**Save (保存)**] ボタンをクリックします。

6 Windows の名前を付けて保存ダイアログが表示されたら、次のいずれかを行います。

- [**Save (保存)**] ボタンをクリックして、デフォルト設定を使用します。デフォルトの場合、ファイル名は `LocalUsersTemplate.csv`、保存先は Downloads フォルダになります。
- CSV ファイルに別のファイル名と保存場所を選択します。

7 ファイルをダウンロードしたら、ローカル ユーザー認証リポジトリにインポートするユーザー データを追加するためのガイドとして使用します。

既存ローカル ユーザーのデータのインポート

ローカル ユーザー認証リポジトリにすでに含まれている複数のユーザー アカウントのプロパティを更新する必要がある場合、ユーザー アカウントを手動で編集する代わりに、ユーザーをインポートできます。例えば、新規グループを作成する際に、複数のユーザーをグループにすぐに追加できます。ユーザー アカウントを単純に CSV ファイルにエクスポートし、必要なプロパティ変更を行い、更新されたユーザー アカウントをローカル ユーザー認証リポジトリにインポートして戻します。

既存ローカル ユーザーのデータをインポートするには、新規ローカル ユーザーおよびグループのインポートの説明に従ってください。ただし、次の点に注意してください。

- ユーザーのデータを更新するかどうかを選択する際には、[**Update the User (ユーザの更新)**] を選択します。

  パスワードは、新規ユーザーの場合のみインポートされます。この設定に関係なく、既存ユーザーのパスワードは更新されません。
- 新規ユーザーをインポートする際に使用する CSV ファイルと同じ形式を使用します。CSV ファイルの作成を参照してください。ただし、インポートされるのは、次のプロパティだけです。
  - 説明
  - 電子メール アドレス
  - デバイス ID
  - グループ
- ユーザーをインポートする際には、プロパティの追加は可能ですが、削除はされません。

新規グループのインポート

新規または既存のローカル ユーザーをインポートする際には、グループ メンバーシップもインポートされます (インポートされる CSV ファイルで用意されている場合)。AMC では、明示的にローカル グループをインポートしません。ただし、ユーザーが所属しているグループが AMC で構成されていない場合は、新規ローカル グループが作成され、そのユーザーはグループのメンバーとして追加されます。

注意：CSV ファイルに含めるグループ名は間違えないようにしてください。間違えると、不要なグループが作成されることになります。

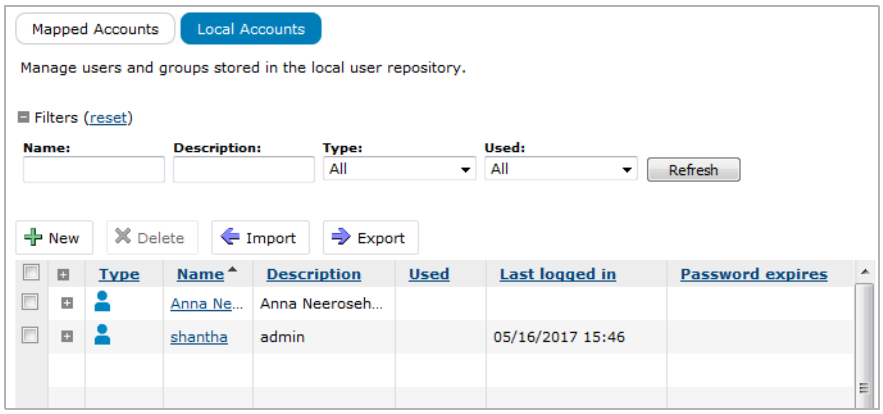
ローカル ユーザー アカウントのエクスポート

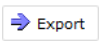
AMC では、ローカル ユーザー認証リポジトリで現在定義されているローカル ユーザー アカウントおよび関連するグループ情報をエクスポートすることで、CSV 形式のテキスト ファイルを作成できます。この CSV ファイルは、ユーザー データを任意のデータベースにインポートするのに使用できます。

ローカル ユーザー アカウントをエクスポートするには

1 [Security Administration (セキュリティ管理)] の下のメイン ナビゲーション メニューで [**Users & Groups (ユーザとグループ)**] を選択します。

2 [**Local Accounts (ローカル アカウント)**] タブをクリックします。



3 [] **Export (エクスポート)**] ボタンをクリックします。[**Windows File Download (Windows のファイルのダウンロード)**] ダイアログが表示されます。

4 [**Save (保存)**] ボタンをクリックします。

5 **Windows の名前を付けて保存**ダイアログが表示されたら、次のいずれかを行います。

- [**Save (保存)**] ボタンをクリックして、デフォルト設定を使用します。デフォルトの場合、ファイル名は `LocalUsers.csv`、保存先は Downloads フォルダになります。
- CSV ファイルに別のファイル名と保存場所を選択します。

インポートおよびエクスポートに関するエラー メッセージ

CSV ファイルのインポートまたはエクスポートを実行する際に、次のエラー メッセージが表示される場合があります。インポート時にエラーが発生すると、データはインポートされません。このため、ファイルをインポートするには、エラーを解決する必要があります。

重複するユーザー名	CSV ファイルの複数のレコードに同一ユーザー名 (大文字と小文字の区別なし) が存在する場合は、そのユーザー名と、重複するユーザー名がある行番号がエラー メッセージで示されます。
間違った数のデータ列	レコードに無効な列数が含まれていると、データが無効であることと、そのレコードの行番号がエラー メッセージで示されます。
不正なメールアドレス	レコードに含まれている電子メール アドレスが無効なアドレスの場合は (例: 「`useratdomain.com`」)、ユーザー名、無効なアドレス、無効なアドレスがある行番号がエラー メッセージで示されます。
不正な既定のパスワード	デフォルト パスワードが、ローカル認証サーバーで構成されているパスワード基準を満たしていない場合は、その基準がエラー メッセージで示されます。例えば、パスワードには大文字も記号も含まれていないが、そのいずれかまたは両方を含めることが必須となっている場合は、どちらも含まれていないことがエラー メッセージで示されます。
不正な「有効」値	Enabled 列の値が、「`true`」でも「`false`」でもない場合は、その問題の説明とレコードの行番号がエラー メッセージで示されます。
ユーザ名が無効です	ユーザー名が無効の場合は (255 文字を超えている場合など)、その問題の説明とレコードの行番号がエラー メッセージで示されます。
不正なグループ名	グループ名が無効の場合は (255 文字を超えている場合など)、その問題の説明とレコードの行番号がエラー メッセージで示されます。
存在しないユーザー名	ユーザー名が存在しないエントリの場合、その問題の説明とレコードの行番号がエラー メッセージで示されます。
パスワードなし (かつ新規ユーザーの既定のパスワードが指定されていない)	新規ユーザーのエントリにパスワードがなく、さらにデフォルトのパスワードが設定されない場合は、その問題の説明とレコードの行番号がエラー メッセージで示されます。
不正なユーザー パスワード	新規ユーザーのエントリに含まれているパスワードが、ローカル認証サーバーで構成されたパスワード ポリシーに従っていない場合は、パスワードがポリシーに従っていないことと、問題が生じている行番号がエラー メッセージで示されます。

SMA アプライアンスと SonicWall ファイアウォールとの統合

ファームウェア バージョン 12.1 以上を実行する Secure Mobile Access (SMA) 1000 シリーズ アプライアンスは、ファームウェア バージョン SonicOS 5.9.X 以上を実行する SonicWall TZ、NSA、および SuperMassive シリーズのファイアウォールで動作するように統合できます。

これらのデバイスを統合して、SonicOS シングル サインオン (SSO) 機能を使用してセッション情報を共有することができます。SonicWall TZ、NSA、または SuperMassive シリーズのファイアウォールは、RADIUS アカウンティング サーバとして機能し、Secure Mobile Access (SMA) 1000 シリーズ アプライアンスから RADIUS アカウンティング レコードを受信するように設定できます。

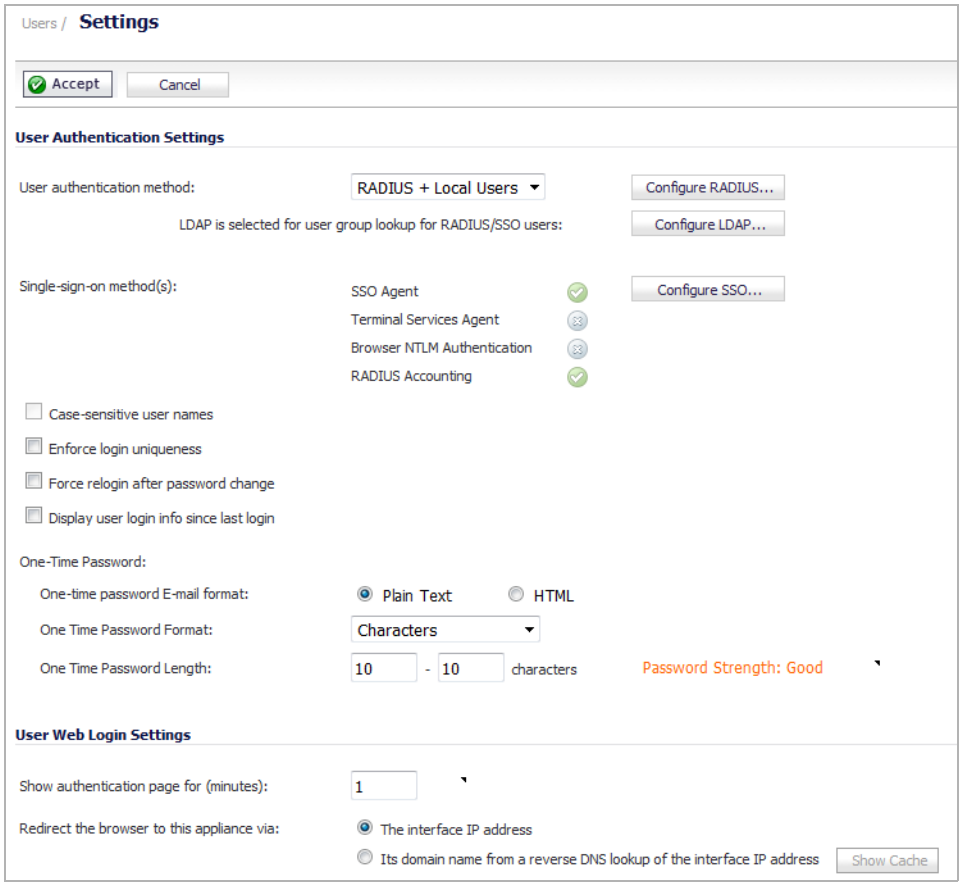
トピック:

- SMA アプライアンスから RADIUS アカウント レコードを受信するようにファイアウォールを設定する
- RADIUS アカウント レコードをファイアウォールに送信するように SMA アプライアンスを設定する
- ファイアウォール上の SMA ユーザーの表示

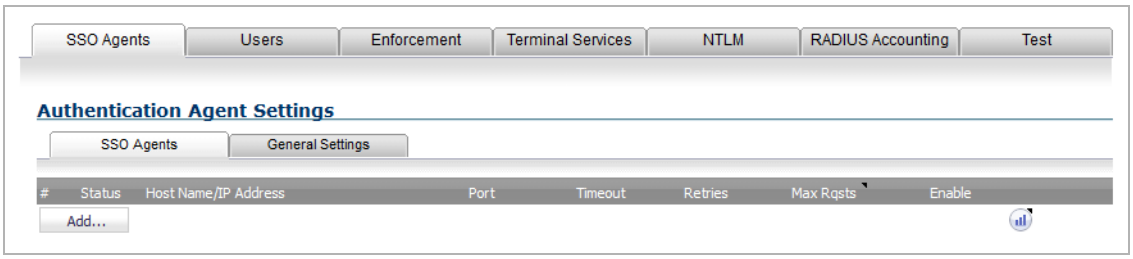
SMA アプライアンスから RADIUS アカウント レコードを受信するようにファイアウォールを設定する

SMA アプライアンスから RADIUS アカウント レコードを受信するようにファイアウォールを設定するには、

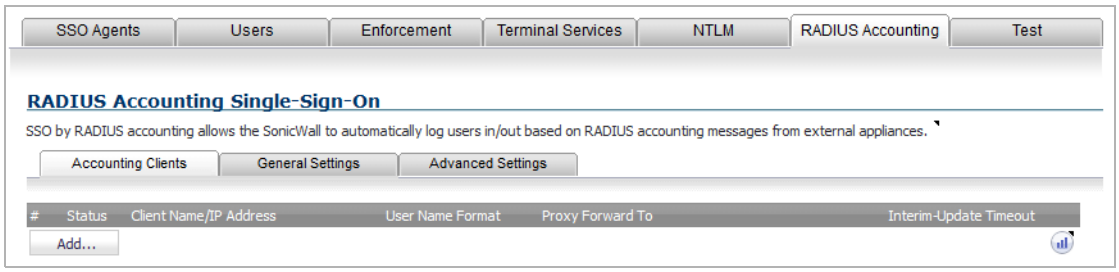
1 ファイアウォールで、[**Users > Settings (ユーザー > 設定)**] ページを開きます。



2 [**Configure SSO (SSO の設定)**] をクリックします。[**SonicWall SSO Authentication Configuration (SonicWall SSO 認証設定)**] ページが表示されます。

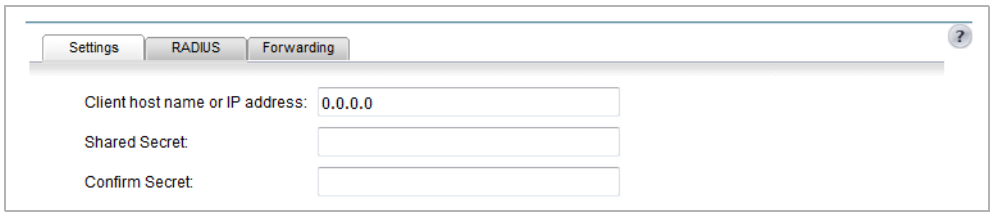


3 [**RADIUS Accounting (RADIUS アカウント)**] タブを選択します。



4 [**Accounting Clients (アカウント クライアント)**] タブを選択します。

5 [**Add (追加)**] を選択します。[**Settings (設定)**] タブが表示されます。



6 [**Client host name or IP address (クライアント ホスト名または IP アドレス)**] フィールドに、ファイアウォール (RADIUS サーバー) に接続されている SMA アプライアンス (RADIUS クライアント) の内部インターフェースの IP アドレスまたはホスト名を入力します。

7 [**Shared Secret (事前共有鍵)**] を入力します。

> **メモ：**[**Shared Secret (事前共有鍵)**] は、RADIUS クライアントと RADIUS サーバー間のパスワードとして機能するテキスト文字列です。[**Shared Secret (事前共有鍵)**] のこのインスタンスは、RADIUS サーバーとして機能するファイアウォール用です。この [**Shared Secret (事前共有鍵)**] は、SMA アプライアンスを設定するときに入力します。

8 [**Confirm Secret (事前共有鍵の確認)**] フィールドに [**Shared Secret (事前共有鍵)**] を再度入力します。

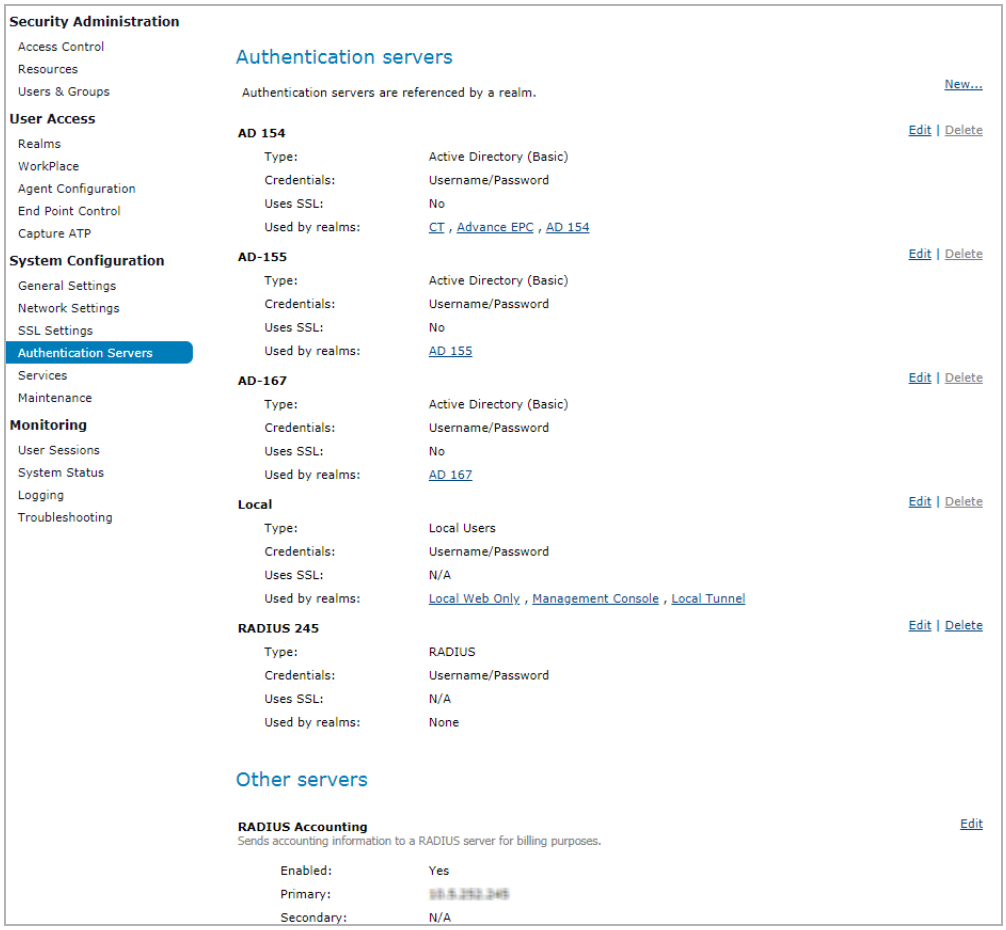
9 [**Apply (適用)**] を選択します。

10 [**OK**] を選択します。

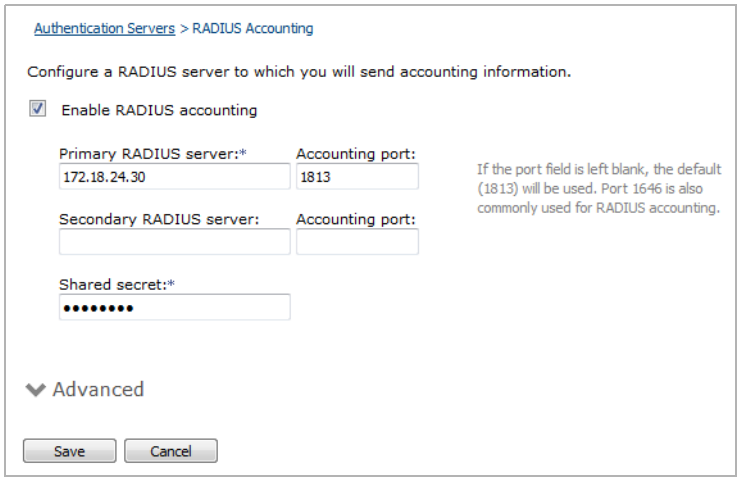
RADIUS アカウント レコードをファイアウォールに送信するように SMA アプライアンスを設定する

RADIUS アカウント レコードをファイアウォールに送信するようにSMA アプライアンスを設定するには、

1 SMA アプライアンスで、[**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページに移動します。



2 [**Other servers (その他のサーバ)**] で、[**RADIUS Accounting (RADIUS アカウント)**] の [**Edit (編集)**] アイコンをクリックします。[**RADIUS Accounting (RADIUS アカウント)**] ダイアログが表示されます。



3 [**Enable RADIUS Accounting (RADIUS アカウントの有効化)**] チェックボックスをオンにします。

4 [**Primary RADIUS server (プライマリ RADIUS サーバ)**] フィールドに、SMA アプライアンスと SonicWall ファイアウォールとの統合で設定したファイアウォールの IP アドレスを入力します。

   a [**Accounting port (アカウンティング ポート)**] フィールドに、使用するポート番号を入力します。ポート フィールドを空白のままにすると、既定のポート (**1813**) が使用されます。ポート 1646 は、RADIUS アカウンティングにもよく使用されます。

5 [**Secondary RADIUS server (セカンダリ RADIUS サーバ)**] フィールドに、SMA アプライアンスと SonicWall ファイアウォールとの統合で設定したファイアウォールの IP アドレスを入力します。

   a [**Accounting port (アカウンティング ポート)**] フィールドに、使用するポート番号を入力します。ポート フィールドを空白のままにすると、既定のポート (**1813**) が使用されます。ポート 1646 は、RADIUS アカウンティングにもよく使用されます。

6 [**Shared secret (事前共有鍵)**] フィールドに、SMA アプライアンスと SonicWall ファイアウォールとの統合のファイアウォールで設定したのと同じ [**Shared Secret (事前共有鍵)**] を入力します。

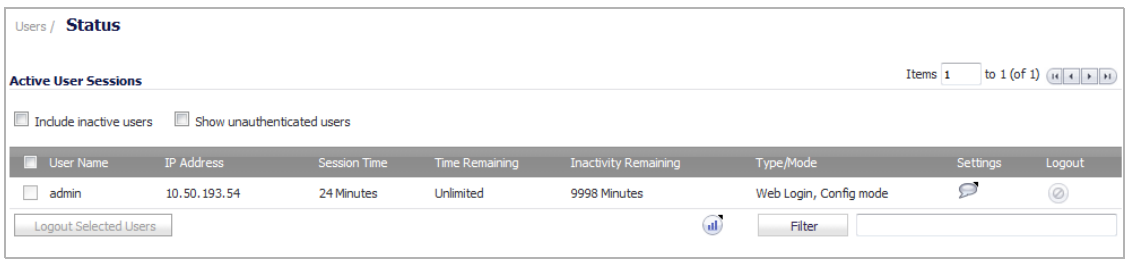
7 [**Save (保存)**] を選択します。

ファイアウォール上の SMA ユーザーの表示

SonicWall ファイアウォールが VPN クライアント経由で SMA アプライアンスに接続されている場合、ファイアウォール上で SMA ユーザーを表示できます。

ファイアウォール上の SMA ユーザーを表示するには、

1 ファイアウォールで、[**Users > Status (ユーザー > 状況)**] ページを開きます。



2 [**Include inactive users (無動作ユーザを含める)**] チェックボックスをオンにします。SMA ユーザーがリストに表示されます。

SMA ユーザーがファイアウォールの外部にあるデバイスにログインすると、ファイアウォールはそれらのユーザー セッションを停止中として扱います。このページに表示されている SMA ユーザーを確認するには、[**Include inactive users (無動作ユーザを含める)**] のチェックボックスをオンにする必要があります。ファイアウォールが SMA アプライアンスから RADIUS アカウンティング情報を受信するように設定され、SMA アプライアンスによって正常に認証されると、すぐにこのリストにユーザが自動的に追加されます。SMA セッションが終了すると、自動的に削除されます。

4

アプライアンス管理コンソールの操作

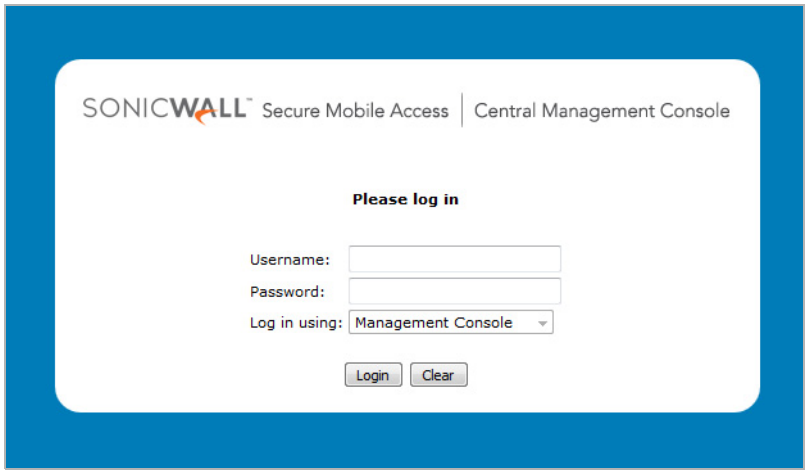
AMC へのログイン

この節では、アプライアンスを管理するための Web ベースのインターフェース、アプライアンス管理コンソール (AMC) について説明します。

AMC にログインする前に、Setup Tool を使用して初期セットアップを行ったときに内部インターフェースで入力したホスト名または IP アドレスを用意しておく必要があります。

AMC にログインするには、

1 Web ブラウザを起動し、URL「`https://<ipaddress>:8443/console`」を入力します。ただし、*<ipaddress>* は、Setup Tool または Setup Wizard の実行時に指定した内部インターフェースのアドレスです。

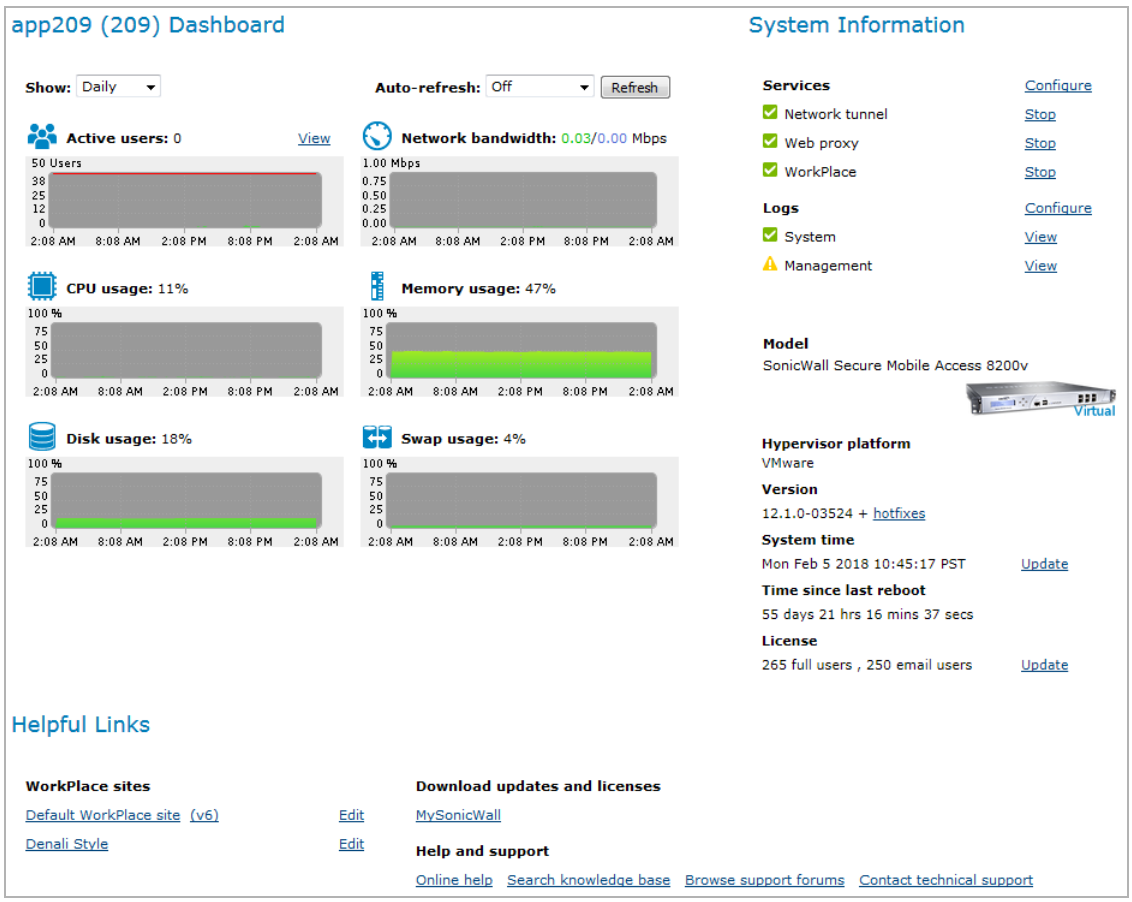


2 [**Username (ユーザ名)**] テキスト フィールドに「`admin`」と入力します。

3 [**Password (パスワード)**] テキスト フィールドに、Setup Tool を使用して作成した root パスワードを入力します。

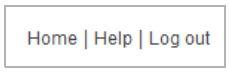
4 [**Log in using (ログインに使用)**] ドロップダウン メニューを使用して、[**Management Console (管理コンソール)**] を選択します。

5 「**ログイン**」を選択します。AMC のホーム ページが表示されます。



6 システム統計を見直し、右側にある機能を使用してシステムの構成およびメンテナンスを実行します。

7 アプライアンスの設定の詳細については、上部の [**Help (ヘルプ)**] をクリックしてください。



AMC パスワードの変更方法については、管理者アカウントの編集を参照してください。

メモ：複数の管理者が AMC で同時に変更しないようにしてください。詳細については、複数管理者の構成ファイルの衝突の回避を参照してください。

ログアウト

AMC 管理者アカウントのセキュリティを維持することが重要です。AMC での作業が終了したら、画面の右上にある [**Log out (ログアウト)**]をクリックします。Web ブラウザを閉じてセッションを終了した場合、そのセッションは、タイムアウトする (使用しない状態で 15 分経過する) までアクティブな状態です。このルールには、重要な例外があります。詳細については、アプライアンス セッションを参照してください。

AMC の基礎

このセクションでは、AMC の操作方法の基礎を説明します。AMC とブラウザの間でやり取りされるすべての構成データは SSL を使用して暗号化されるため、データは安全な状態に保たれます。セキュリティを強化したい場合は、信頼できるネットワーク (ファイアウォールの内側の内部ネットワーク) で AMC を使用してください。詳細については、証明書の使用に関するよくある質問を参照してください。

- AMC インターフェース クイック ツアー
- AMC でのオブジェクトの追加、編集、コピー、削除
- ヘルプの表示

AMC インターフェース クイック ツアー

AMC インターフェースは、同様の Web ベース セキュリティ管理アプリケーションを使用したことがあれば、容易に使いこなすことができます。このセクションでは、AMC の操作に関する基本事項を説明します。

トピック:

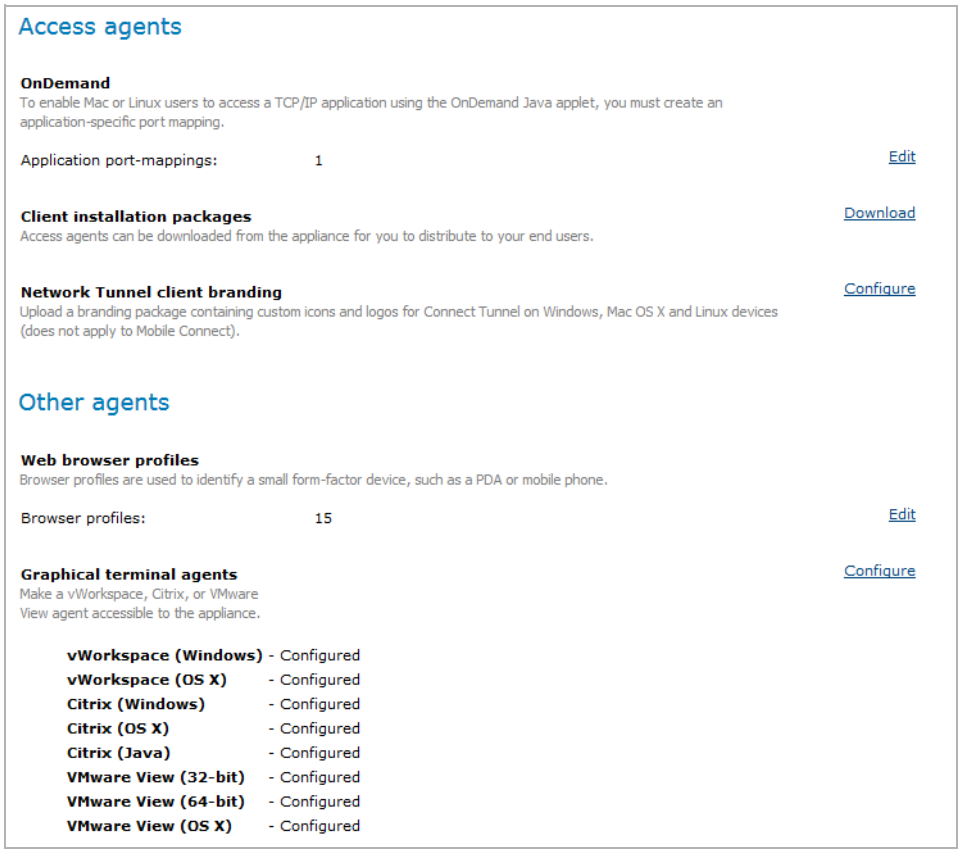
- サマリー ページ
- 表とタブ
- フィルタ
- ページ リンク
- オブジェクトの編集
- ページ ビューの変更
- リスト詳細の展開されたビュー
- 必須フィールドとエラー
- 名前と説明の割り当て
- ページの変更の保存
- AMC ステータス エリア
- バージョン番号と製品シリアル番号

サマリー ページ

AMC の最上位のページはサマリー ページで、下位の構成ページにここから迅速にアクセスし、主要な構成設定やステータス情報を表示できます。次のサマリー ページがあります。

- エージェント設定
- 一般設定
- ネットワーク設定
- SSL 設定
- 認証サーバー
- サービス

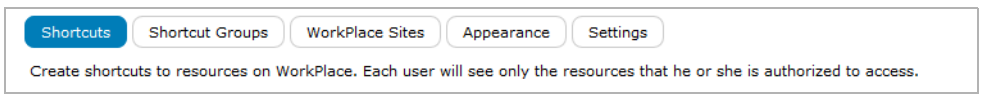
例えば、[**Agent Configuration (エージェント設定)**] ページには、End Point Control エージェント、Secure Mobile Access アクセス エージェント、およびその他のエージェントを構成するページへのリンクがあります。また、このサマリー ページでは、それぞれのエージェントが有効または無効のどちらになっているかがすぐにわかります。



表とタブ

多くの AMC ページでは、表形式のレイアウトを使用して、管理対象のオブジェクトが提示されます。表にはスクロール バーが付いており、長いリストであっても、ページの主要な要素 (ナビゲーション バー、ヘッダ、フッタなども含む) をいつでも簡単に表示できます。一部の表では、下線付きの列見出しをクリックして、表示されているデータを並べ替えることもできます。

状況によっては、タブを使用してモードを切り替えることができます。例えば、タブを使用して、管理リソース、リソースのグループ、およびリソースの定義で使用されている変数を切り替えます。



フィルタ

大規模構成で何ページにもなる項目のリストが含まれる AMC のページでは、フィルタを使用すると、探している項目を簡単に見つけられます。フィルタは、フィルタを含むページの AMC ページで使用できます。

フィルタを含むページ

セキュリティ管理

- アクセス制御
- リソース
- リソース > リソース グループ
- ユーザとグループ
- ユーザとグループ > ローカル アカウント

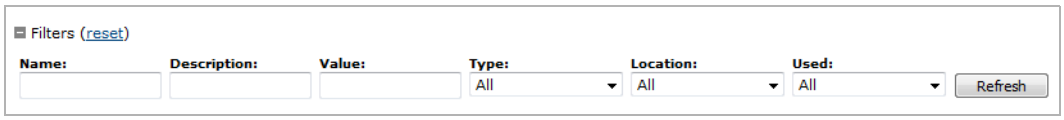
ユーザー アクセス

- WorkPlace
- WorkPlace > ショートカット グループ

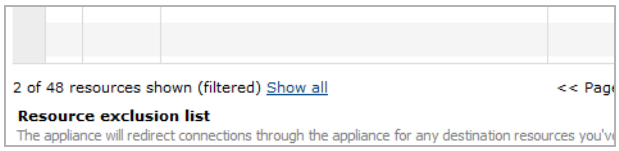
監視

- ユーザ セッション
- ログ

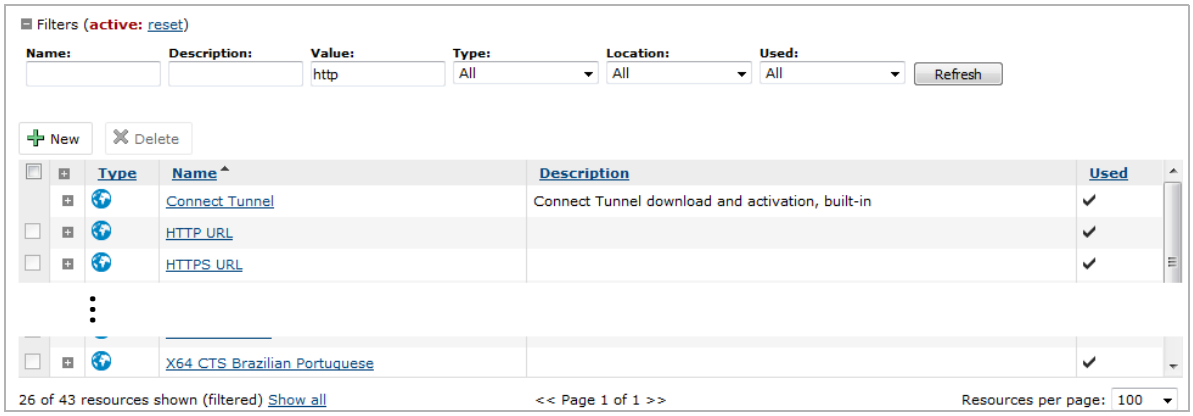
実際のフィルタはページごとに多少異なりますが、次の機能はどのページでも同じです。



- [**reset (リセット)**] リンクは、フィルタ フィールドをデフォルト値にリセットします。
- 赤の [**active (動作)**] インジケータは、そのページがフィルタを使用してロードされたことを表します。すなわち、構成されているすべての項目がページに表示されていない可能性があります。
- [**Refresh (再表示)**] ボタンは、指定したフィルタを適用してページをリロードします。
- フィルタが保管され、次回のページのロードでは、最後に適用されたのと同じフィルタ使用されます。フィルタはセッションをまたいで保管されるため、ログアウトした後にまたログインしたとしても、同じフィルタが使用されます。
- リストに下にあるフッタに、表示されている項目の数とリスト内の項目の合計数が表示されます。フィルタがアクティブである場合、**(filtered)** というインジケータと、フィルタをリセットする [**Show all (すべて表示)**] リンクが表示されます。



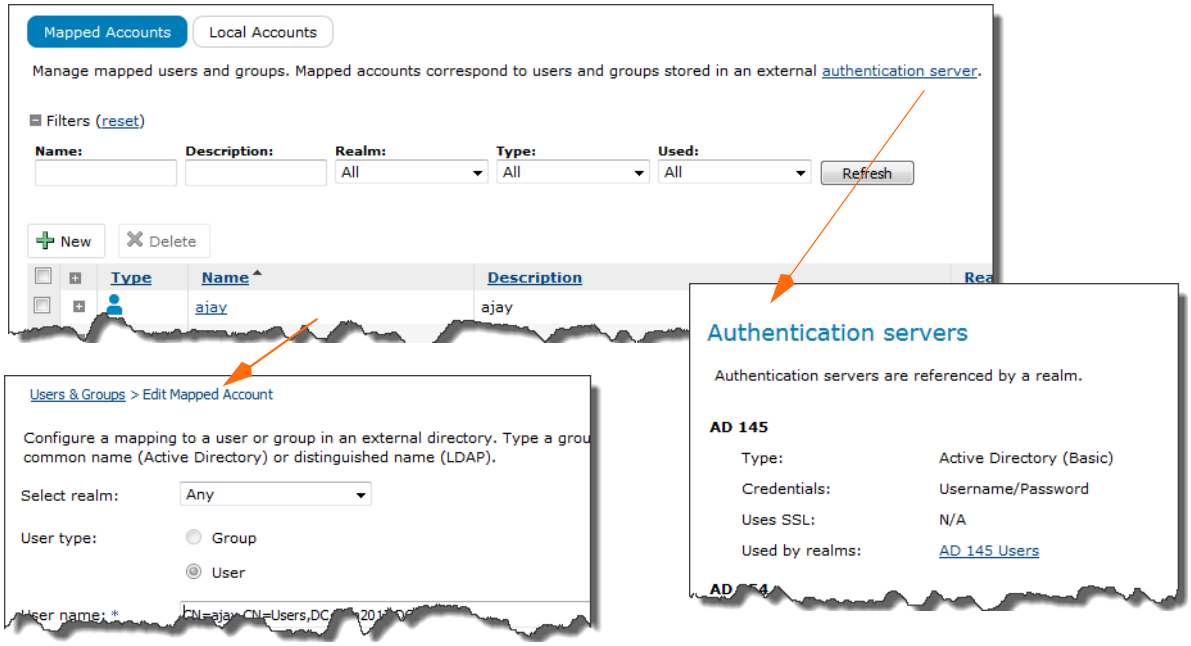
このリンクをクリックすると、フィルタがデフォルトにリセットされ、ページが更新されてリストにすべての項目が表示されます。一般的に、利用可能なフィルタがリストに表示される列にマッピングされます。[**Resource Groups (リソース グループ)**] や [**Shortcut Groups (ショートカット グループ)**] などの場合は、リストの列ではないグループのメンバーに基づいて、リストをフィルタできます。あるいは、[**Resources (リソース)**] ページの場合であれば、列ではなく、リスト内の項目を展開すると表示される **Value (値)** 属性の何らかの条件に基づいて、リストをフィルタできます。



この機能のカスタム フィルタでの 1 つの使用方法として、関連する項目の [**Description (説明)**] フィールドにカスタム文字列を追加して独自の「タグ」を作成する場合が考えられます。例えば、いくつかのリソースがすべて 1 つのお客様の 1 つの部門によって使用されている場合、それらのリソースの [Description] にキーワードまたはタグを追加すると、フィルタ機能を使用して、そのキーワードまたはタグが含まれるリソースだけを迅速に表示できます。

ページ リンク

他のページへのリンクは青色で表示され、下線が引かれています。リンクを選択すると、そのページが表示されます。



オブジェクトの編集

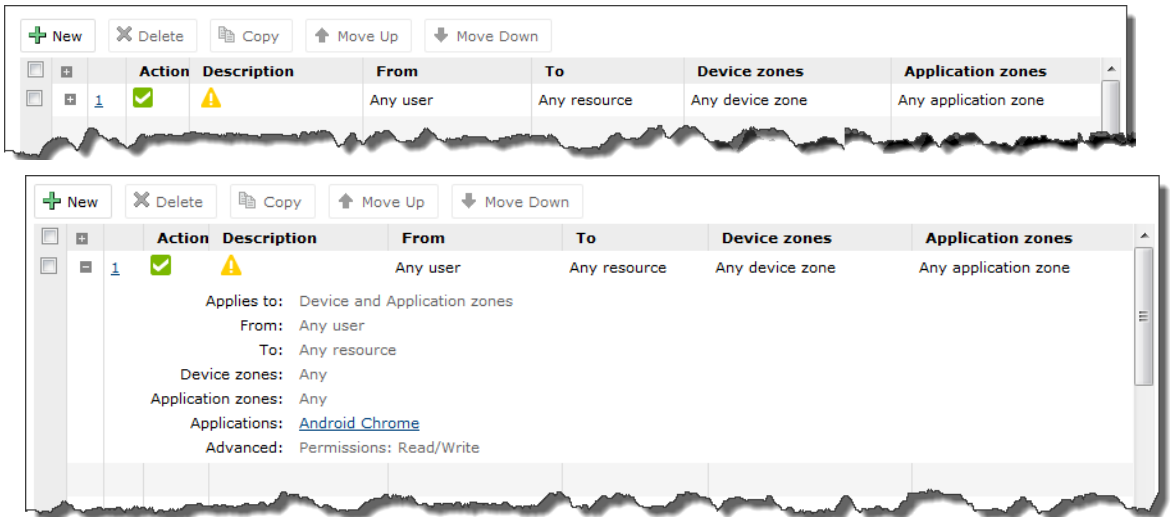
オブジェクトのリストの表示に使用するほとんどの表では、名前フィールド ([**Access Control (アクセス制御)**] ページの場合はルール番号) にハイパーリンクが設定されています。オブジェクトを編集するには、対応するハイパーリンクをクリックします。

ページ ビューの変更

AMC の長い複雑なページでは、高度な機能の構成に使用する編集コントロールが表示されないものもあります。こうすることで、最も重要な構成オプションに集中できるようになっています。非表示のオプションを表示するには下矢印をクリックし、上矢印をクリックすると非表示に戻ります。

リスト詳細の展開されたビュー

[**Access Control (アクセス制御)**] ページなどのオブジェクトのリストを表示する AMC ページでは、2 列目のプラス記号 (+) をクリックすることで、そのオブジェクトの詳細を表示できます。1 行表示に戻すには、マイナス記号 (-) をクリックします。



必須フィールドとエラー

AMC では、必須フィールドにはアスタリスクが表示されます。必須フィールドに値を入力せずに [**Save (保存)**]をクリックすると、そのフィールドの下に、必須であることを示す赤のメッセージが表示されます。エラー メッセージも赤で表示されます (例えば、無効な値を入力した場合)。

名前と説明の割り当て

AMC での作業のほとんどは、次の 3 種類のオブジェクトの管理に関連するものです。

- アクセス制御ルール
- リソース
- ユーザーとグループ

AMC でこれらのオブジェクトを作成する場合、名前を必ず入力します。オプションで説明を入力できます。

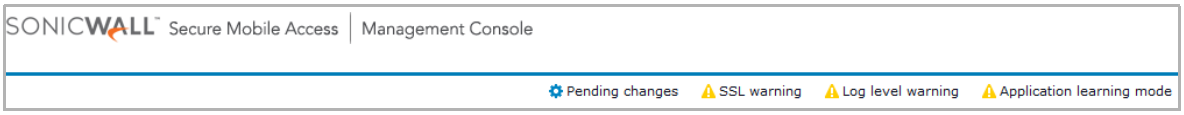
必須ではありませんが、アクセス ルールの目的やサブセット範囲にどのリソースがあるといったわかりやすい説明を付けると、管理するオブジェクトの重要な情報を思い出すのに役立ちます。オブジェクトのグループを管理する場合、わかりやすい説明が特に便利です。例えば、AMC に後で戻って大量のネットワーク リソースを管理するような場合、そのグループにどのようなオブジェクトがあるかを思い出せるような説明があると役に立ちます。

ページの変更の保存

一部の AMC ページでは、変更を保存 ([**Save (保存)**]) するかキャンセル ([**Cancel (キャンセル)**]) できます。[**Cancel (キャンセル)**] をクリックしたり、ブラウザの [**Back (戻る)**] ボタンを使用したりすると、変更は保存されません。

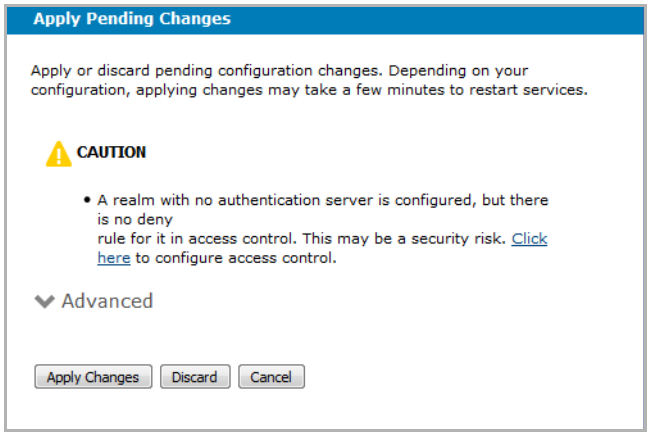
AMC ステータス エリア

ステータス エリアは、SonicWall Secure Mobile Access バナーのすぐ下にあり、重要な情報が表示されます。

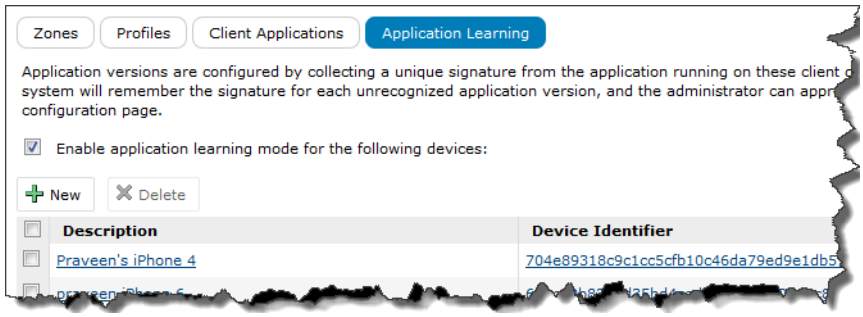


各メッセージには情報の重要度を示すインジケータがあります。例えば、黄色の警告サインです。これらのメッセージのそれぞれは、次のいずれかを表示するリンクです。

- [**Pending changes (保留中の変更)**] をクリックする場合など、詳細情報を含むダイアログが表示されます。



- [**Application learning mode (アプリケーション学習モード)**] をクリックすると、[**End Point Control > Application Learning (エンド ポイント コントロール > アプリケーション学習)**] が表示されるなど、関連するページが表示されます。



バージョン番号と製品シリアル番号

現在のシステム ソフトウェアのバージョンと製品シリアル番号は、AMC の各ページの左側にあるナビゲーション バーの下部に表示されます。

[**System Status (システム状況)**] ページと [**Maintenance (メンテナンス)**] ページには、バージョン番号以外に、適用されたホット フィックスのリストも表示されます。バージョン番号とホット フィックス情報は、システム アップデートを計画する場合に利用できる他に、SonicWall テクニカル サポートにお問い合わせいただく際にも必要になります。

AMC でのオブジェクトの追加、編集、コピー、削除

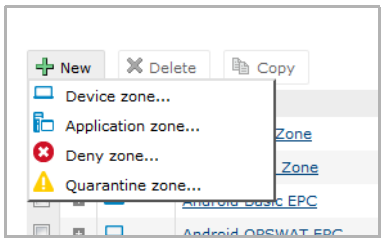
AMC には、標準化されたインターフェースが搭載されており、リソース、アクセス制御ルール、ユーザー、コミュニティ、End Point Control ゾーン、デバイス プロファイル、および VPN を編成して動作させるための、その他のアイテムなどのほとんどのオブジェクトを管理できます。

AMC でオブジェクトを追加、編集、コピー、削除する際の基本手順を以下に記載します。ただし、対象となるオブジェクトや使用する AMC ページによっては手順が少し異なることがあります。この例では、[**End Point Control Zones (End Point Control ゾーン)**] ページを使用しています。

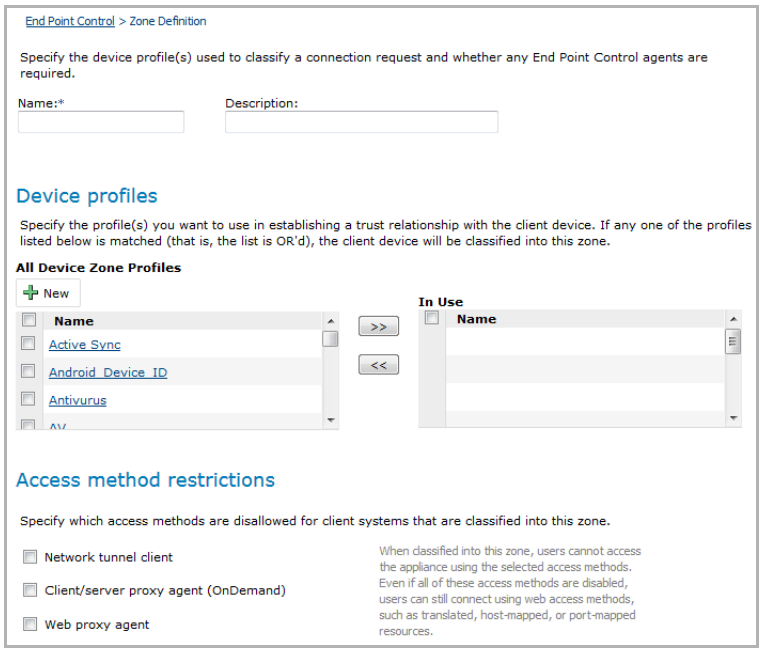
AMC で新しいオブジェクトを追加するには、

1 作成するオブジェクト タイプが表示されているページで [**New (新規)**] をクリックします。

2 作成のオプションを選択します。この例では、[**Device zone... (デバイス ゾーン...)**] が使用されています。



[**Zone Definition - Device Zone (ゾーン定義 - 機器ゾーン)**] ページが表示されます。



3 オブジェクトに対応する情報を入力します。

4 画面の下部にある [**Save (保存)**] ボタンをクリックします。

AMC でオブジェクトを編集するには、

1 編集するオブジェクトが表示されているページで、変更するオブジェクトの名前 (場合によっては数値) のリンクをクリックします。オブジェクトの簡単な説明を参照できる展開 (+) ボタンを、ほとんどのリストで使用できます。

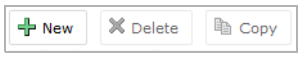
2 オブジェクトの情報を変更します。

3 [**Save (保存)**] を選択します。

AMC でオブジェクトをコピーするには、

1 コピーするオブジェクトが表示されているページで、オブジェクトの左にあるチェックボックスを選択します。

2 [**コピー**] をクリックします。



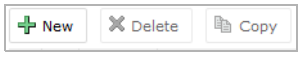
3 コピー元のオブジェクトの情報を変更し、新しい名前を割り当てます。

4 [**Save (保存)**] を選択します。

AMC でオブジェクトを削除するには、

メモ：あるオブジェクトが他のオブジェクトにまだ関連付けられている場合、そのオブジェクトは削除できません。詳細については、参照されているオブジェクトの削除を参照してください。

- 削除するオブジェクトが表示されているページで、オブジェクトの左にあるチェックボックスを選択します。
- [**Delete (削除)**] を選択します。



ヘルプの表示

どの AMC ページにも [**Help (ヘルプ)**] ボタンがあり (ページの右上)、このボタンをクリックすると、コンテキストに応じたオンライン ヘルプが新しいブラウザ ウィンドウで表示されます。

[**Help (ヘルプ)**] ウィンドウには、ナビゲーション ペインが左側に、ヘルプ コンテンツが右側に表示されます。ナビゲーション ペインでアイテムをクリックすると、そのアイテムのヘルプ コンテンツが表示されます。

管理者アカウント

ここでは、以下の方法を説明します。

- 管理者アカウントを管理
- 複数の管理者がアプライアンスを管理している場合に発生する問題の回避

トピック:

- 管理者アカウントと役割の管理
- 複数管理者の構成ファイルの衝突の回避

管理者アカウントと役割の管理

AMC では、異なるユーザー名とパスワードの複数の管理者を作成できます。その上で、役割を管理者に割り当て、使用できる AMC の機能やアクセスのレベルを指定できます。

AMC にはデフォルトで、AMC のすべての領域にフル アクセスできるプライマリ管理者の役割が構成されています。プライマリ管理者のみが、他の管理者アカウントを追加、編集、削除できます。

トピック:

- 管理者アカウントの追加
- 管理者アカウントの編集
- レガシー ローカル管理者アカウントの追加/編集
- 管理者の役割の定義
- 認証サーバーの追加
- 管理者の役割の編集

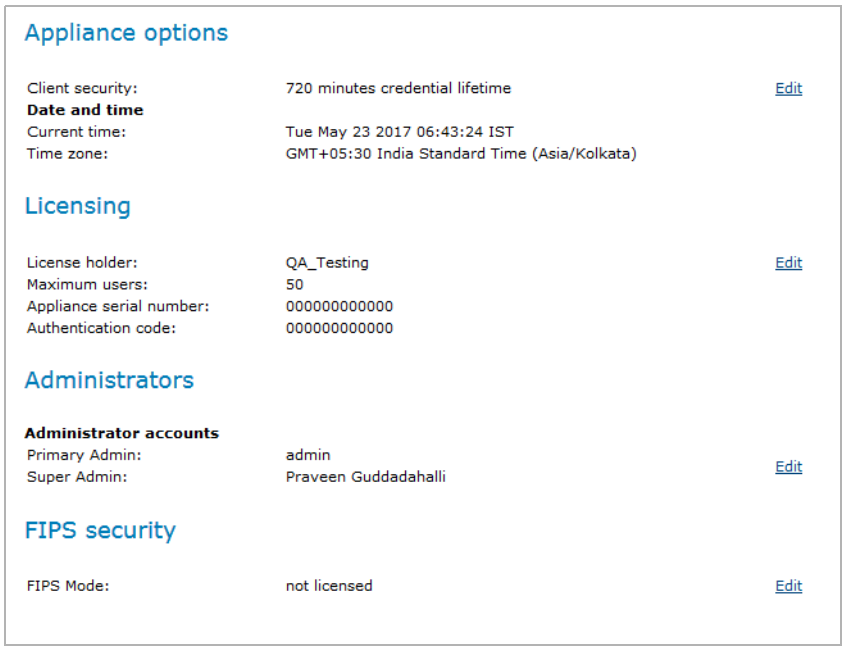
管理者アカウントの追加

ポリシー管理の管理者が複数いて、それぞれの管理者に独自のログイン クレデンシャルを与える場合、追加の管理者アカウントを作成できます。セカンダリ管理者アカウントを作成、変更、削除できるのは、「プライマリ」管理者 (デフォルト名は「*admin*」で、この名前は変更できません) だけです。

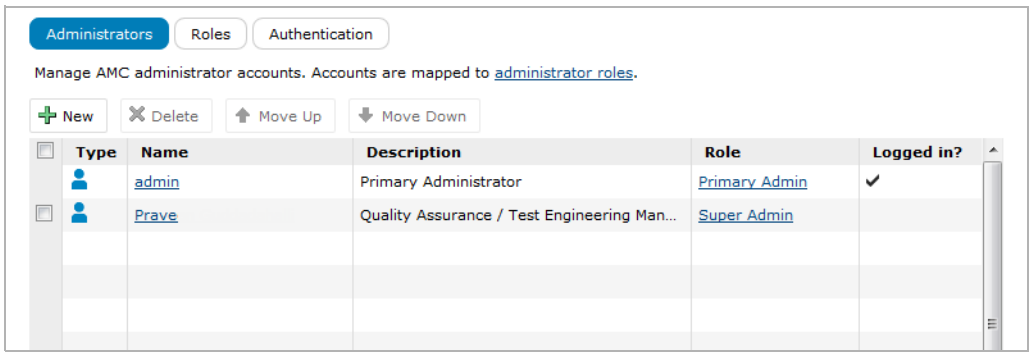
デフォルトでは、構成済みの役割には、あらゆる形式のセッション データの表示とセッションの終了が許可されています。詳細については、ユーザー セッションの表示とユーザー セッションの終了を参照してください。

管理者アカウントを追加するには、

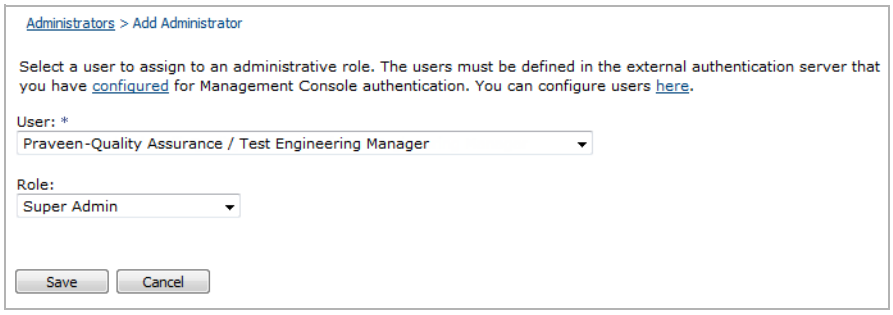
1 メイン ナビゲーション メニューから、[**General Settings (一般設定)**] をクリックします。



2 [**Administrator accounts (管理者アカウント)**] エリアの [**Edit (編集)**] をクリックします。[**Manage Administrator Accounts (管理者アカウントを管理)**] ページが表示されます。



3 [**New (新規) > Administrator...(管理者...)**] をクリックします。[**Add/Edit Administrator (管理者の追加/編集)**] ページが表示されます。



4 [**User (ユーザー)**] ドロップダウン メニューからユーザーを選択します。

5 [**Role (役割)**] ドロップダウン メニューから管理者の役割を選択します。AMC には、構成済みの役割の説明に示す役割が構成済みで、[**Add/Edit Administrator Role (管理者の役割の追加/編集)**] ページで定義されています。これらの構成済みの役割を変更することも、新しい役割を作成することもできます (管理者の役割の定義を参照してください)。

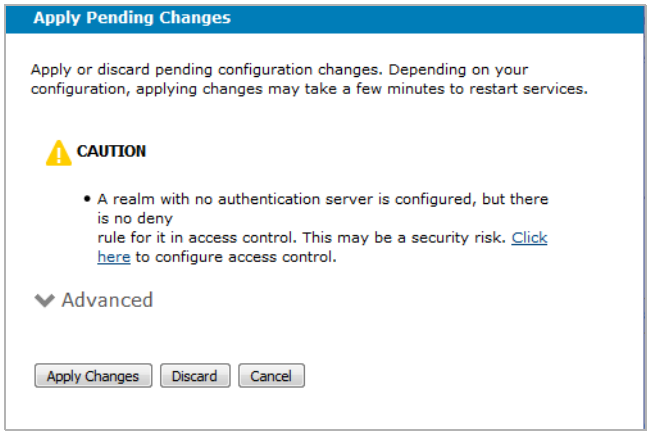
> **メモ**：デフォルトでは、構成済みの役割には、あらゆる形式のセッション データの表示とセッションの終了が許可されています。詳細については、ユーザー セッションの表示とユーザー セッションの終了を参照してください。

構成済みの役割の説明

構成済みの役割	説明
Super Admin	AMC のすべてのページに対して読み取り/書き込みアクセスが許可されています
Security Admin	AMC のセキュリティ管理とモニタリングのページに対する読み取り/書き込みアクセスと、システム設定に対する参照アクセスが許可されています
System Admin	AMC のシステムとモニタリングのページに対する読み取り/書き込みアクセスと、セキュリティ ページに対する参照アクセスが許可されています

6 [**Save (保存)**] を選択します。

7 ページの上部にある [**Pending Changes (保留中の変更)**] をクリックします。[**Apply Pending Changes (保留中の変更を適用)**] ダイアログが表示されます。



8 [**Apply Changes (変更を適用)**] を選択します。

管理者アカウントの編集

メモ：管理者アカウントの削除については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

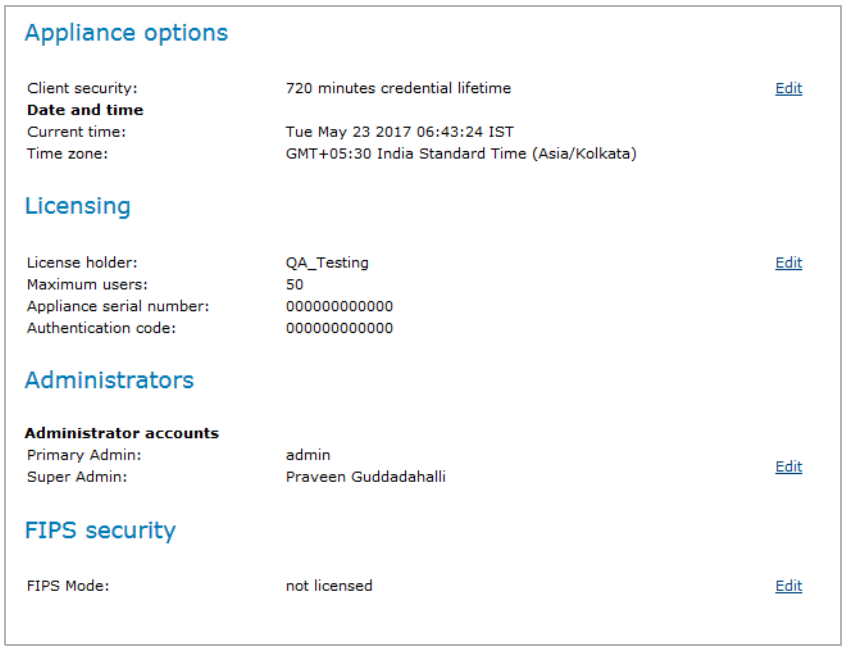
AMC パスワードを安全な状態に保つためには、パスワードを随時変更する必要があります。それぞれの管理者は、自分のアカウントを編集して、パスワードを変更したり、説明を更新したりできます。プライマリ AMC 管理者 (ユーザー名が「*admin*」) は、他の管理者のアカウント設定を編集できます。

パスワードは 8 ～ 20 文字で指定し、大文字と小文字を区別します。大文字と小文字、および数字を組み合わせて強力なパスワードを作成することが推奨されます。また、辞書に載っているような単語は避けてください。

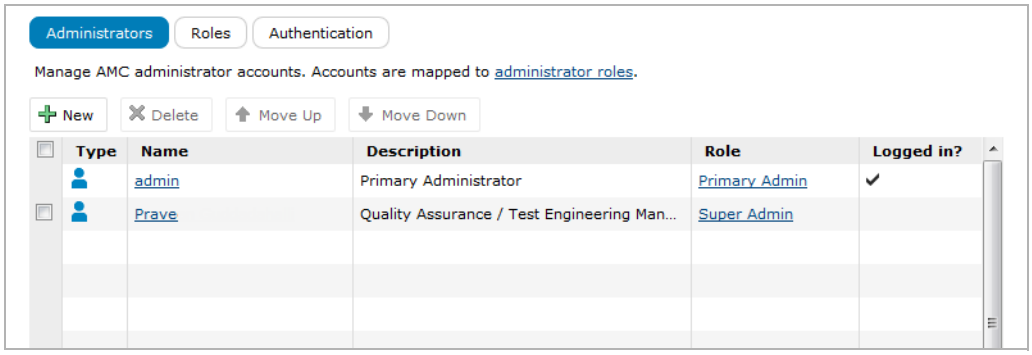
パスワードを変更したら、何らかの形で記録し、安全な場所に保管します。セカンダリ管理者のパスワードを変更した場合は、該当する管理者にそのパスワードを忘れずに通知します。

管理者アカウントを編集するには、

1 メイン ナビゲーション メニューから、[**General Settings (一般設定)**] をクリックします。



2 [**General Settings (一般設定)**] ページで、[**Administrators (管理者)**] エリアの [**Edit (編集)**] をクリックします。

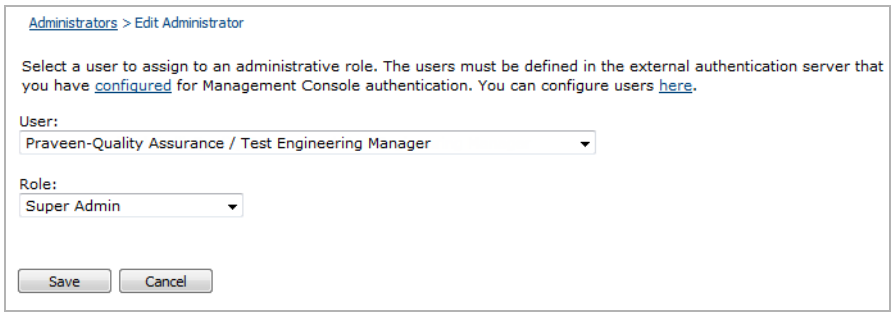


3 [**Manage Administrator Accounts (管理者アカウントを管理)**] ページの [**Name (名前)**] 列で、編集するアカウントの管理者の名前をクリックします。

重要：プライマリ管理者 (ユーザー名が *admin*) のパスワードが変更されると、アプライアンスに (*root* として) 直接ログインするためのパスワードも変更されます。

メモ：プライマリ管理者やレガシー ローカル管理者のユーザー名や役割は変更できません。

4 [**Add/Edit Administrator (管理者の追加/編集)**] ページで、説明テキスト、ログイン パスワード、または役割を変更します。



レガシー ローカル管理者アカウントの追加/編集

後方互換性のみの目的でサポートされているレガシー ローカル管理者アカウントを、作成または変更できます。ローカル管理者の構成には、ローカル認証サーバーにユーザーを作成し、そのユーザーを管理者の役割にマッピングする方法を推奨します。以前のバージョンでは、管理者を認証サーバーには定義できず、アプライアンスにのみローカルで定義できていました。

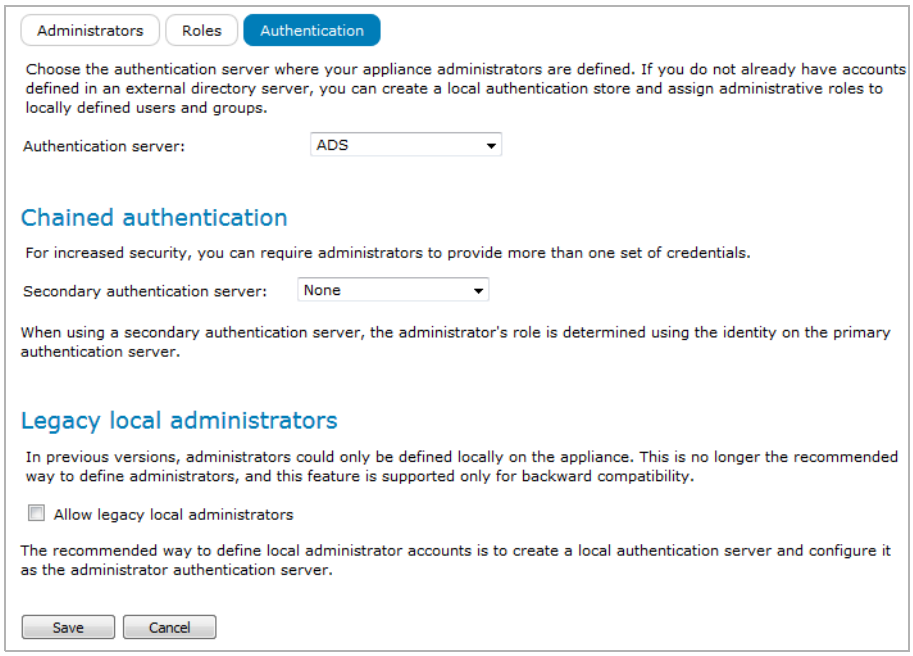
管理者アカウントの削除については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

レガシー ローカル管理者アカウントを追加または編集するには、

1 メイン ナビゲーション メニューから、[**General Settings (一般設定)**] をクリックします。

2 [**Administrators (管理者)**] エリアで管理者アカウントの [**Edit (編集)**] をクリックします。[**Manage Administrator Roles (管理者の役割を管理)**] ページが表示されます。

3 レガシー ローカル管理者を追加する場合は、[**Authentication (認証)**] をクリックします。



a [**Legacy local administrators (レガシー ローカル管理者)**] エリアで、[**Allow legacy local administrators (レガシー ローカル 管理者の許可)**] チェックボックスをオンにします。

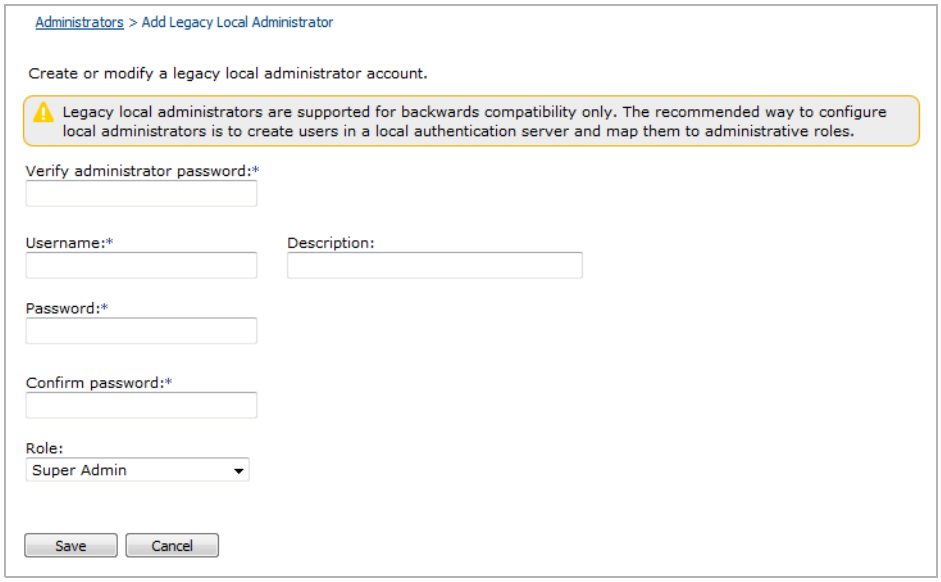
b [**Save (保存)**] を選択します。

4 [**Administrator (管理者)**] エリアで [**Edit (編集)**] をクリックします。[**Manage Administrator Accounts (管理者アカウントを管理)**] ページが表示されます。

5 これを行うには、次の手順に従います。

- レガシー ローカル管理者アカウントを追加するには、[**New > Legacy Local Administrator... (新規 > レガシー ローカル管理者...)**] をクリックします。
- 既存のレガシー ローカル管理者アカウントを編集するには、編集する管理者の名前をクリックします。

[**Add/Edit Administrator (管理者の追加/編集)**] ページが表示されます。



6 [**Verify administrator password (管理者パスワードの検証)**] フィールドに、管理者のパスワードを入力します。

7 [**Username (ユーザ名)**] フィールドに、レガシー ローカル管理者のユーザー名を入力します。

8 [**Description (説明)**] フィールドに、レガシー ローカル管理者アカウントの説明を入力します。

9 [**Password (パスワード)**] フィールドに、レガシー ローカル管理者のパスワードを入力します。

10 [**Confirm password (パスワードの確認)**] フィールドに、レガシー ローカル管理者のパスワードをもう 1 度入力します。

11 [**Role (役割)**] ドロップダウン メニューから管理者の役割を選択します。AMC には、構成済みの役割の説明に示す役割が構成済みで、[**Add/Edit Administrator Role (管理者の役割の追加/編集)**] ページで定義されています。これらの構成済みの役割を変更することも、新しい役割を作成することもできます (管理者の役割の定義を参照してください)。

12 [**Save (保存)**] を選択します。

13 ページの上部にある [**Pending Changes (保留中の変更)**] をクリックします。

14 [**Apply Changes (変更を適用)**] を選択します。

管理者の役割の定義

役割ベースの管理により、プライマリ管理者は、セカンダリ AMC 管理者に対して、一定の制約付きで管理制御権限を付与できます。

管理者の役割の定義では、AMC の機能が 4 つに分類されています。カテゴリごとに、役割に付与する権限を指定する必要があります。AMC の管理者権限の 4 つのカテゴリを、管理者権限で説明します。それぞれのカテゴリの権限レベルは、権限レベルのように設定できます。

管理者権限

種別	管理者権限
セキュリティ管理	アクセス制御ルール、リソース、ユーザーおよびグループ、WorkPlace、OnDemand、End Point Control の各ページに対する管理者のアクセスを制御します。
システムの設定	ネットワーク設定、一般アプライアンス設定、SSL 設定、アクセスおよびネットワーク サービス、認証サーバー、レルムの各ページに対する管理者のアクセスを制御します。
システム メンテナンス	アプライアンスの終了や再起動、システム ソフトウェアの更新やロールバック、構成データのインポートやエクスポートに対する管理者の権限を制御します。
システム 監視	[**View (表示)**] アクセスでは、管理者がシステム ログやグラフを表示したり、アクティブ ユーザーを表示したり、トラブルシューティング ツールを実行したりできます (ネットワーク トレースの開始、停止、ダウンロード、削除など)。[**Modify (変更)**] アクセスでは、ユーザー セッションの終了とログ設定の変更の権限がさらに追加されます。

権限レベル

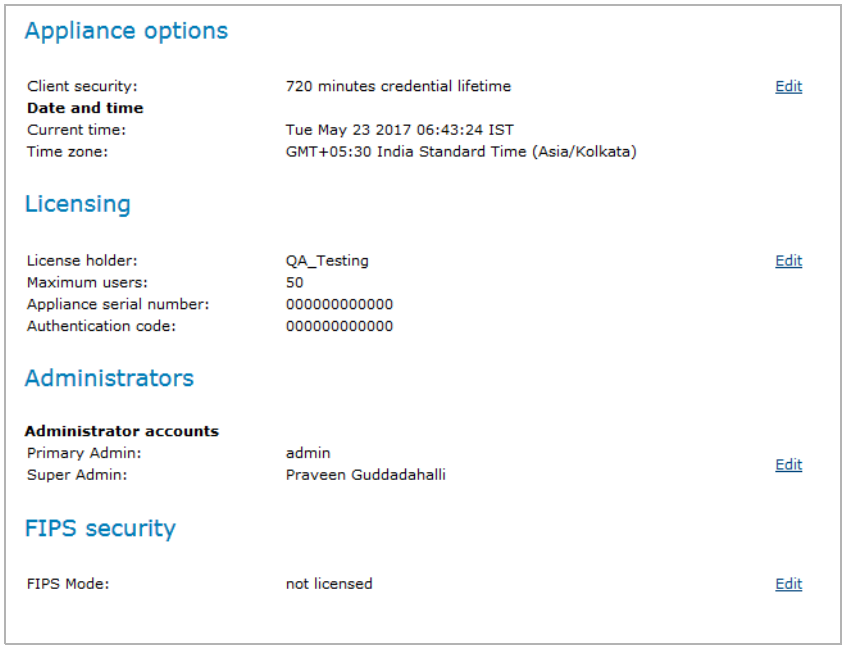
権限レベル	説明
変更	カテゴリ内の読み取り/書き込みアクセスを許可します。

権限レベル

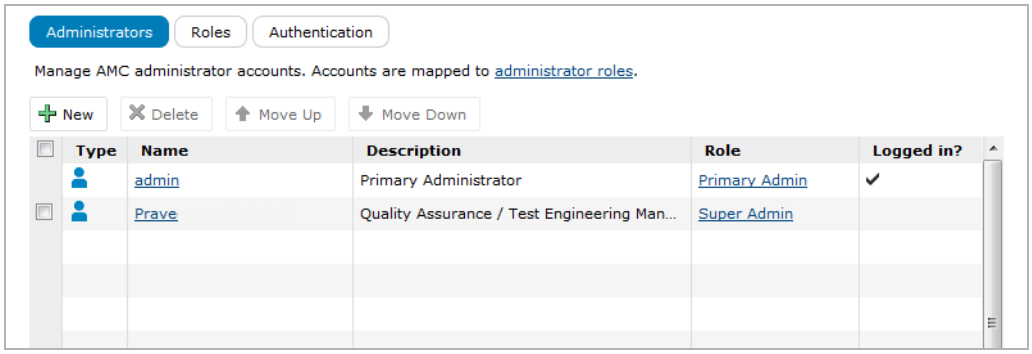
権限レベル	説明
表示	カテゴリ内の読み取り専用アクセスを許可します。
なし	カテゴリ内の関連 AMC ページへのアクセスを禁止します。あるカテゴリの権限レベルに [**None (なし)**] を選択すると、AMC では、そのカテゴリ内のページが表示されず、それらのページにリンクするメイン ナビゲーション メニュー コマンドも表示されません。

管理者の役割を作成するには、

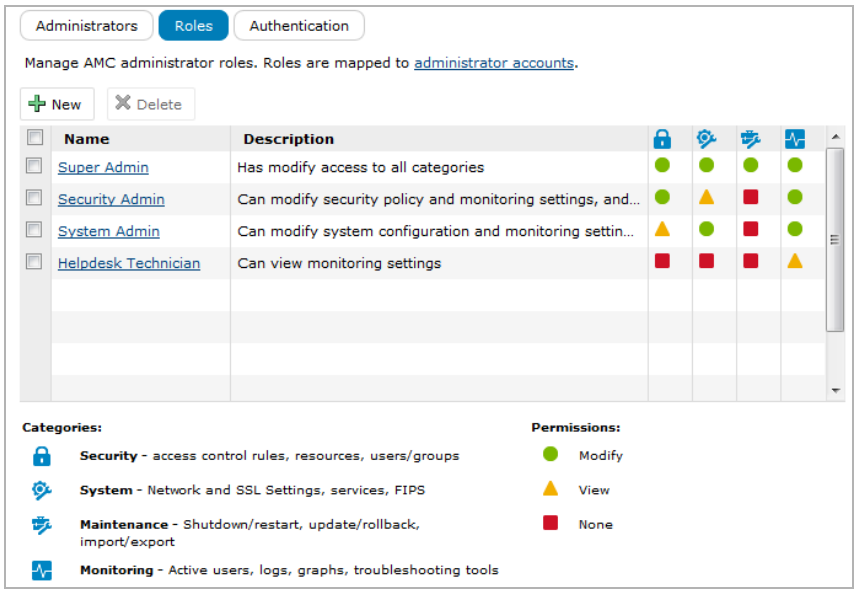
1 メイン ナビゲーション メニューから、[**General Settings (一般設定)**] をクリックします。



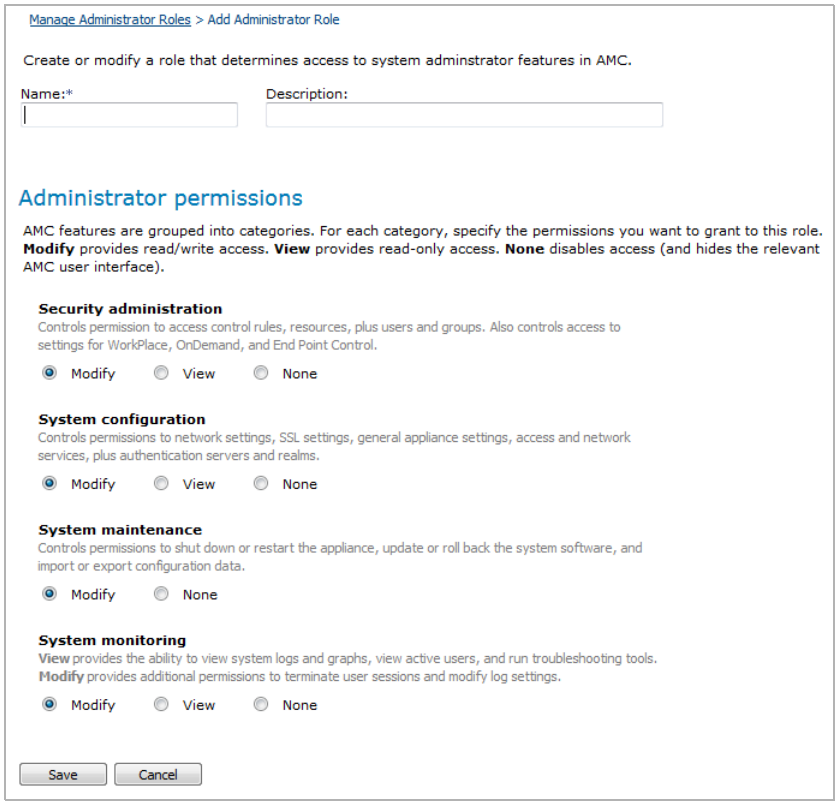
2 [**Administrators (管理者)**] エリアで管理者アカウントの [**Edit (編集)**] をクリックします。[**Manage Administrator Roles (管理者の役割を管理)**] ページが表示され、管理者と役割の一覧が表示されます。



3 [**Roles (役割)**] タブをクリックします。



4 [**New (新規)**] **をクリックします。**[**Add Administrator Role (管理者の役割の追加)**] ページが表示されます。



5 [**Name (名前)**] フィールドに、管理者の役割の名前を入力します。

6 オプション。[**Description (説明)**] フィールドに、役割の説明を入力します。

7 [**Administrator permissions (管理者権限)**] エリアから、役割に付与する権限のカテゴリを 1 つ以上選択します。

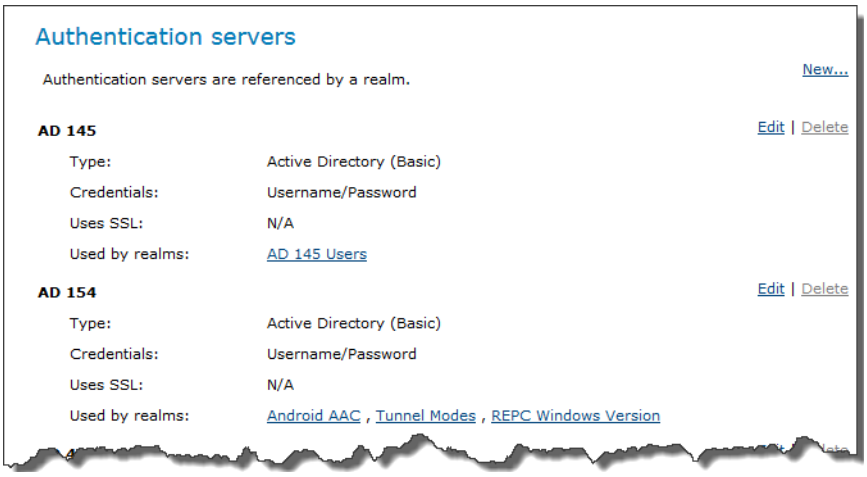
8 [**Save (保存)**] を選択します。

認証サーバーの追加

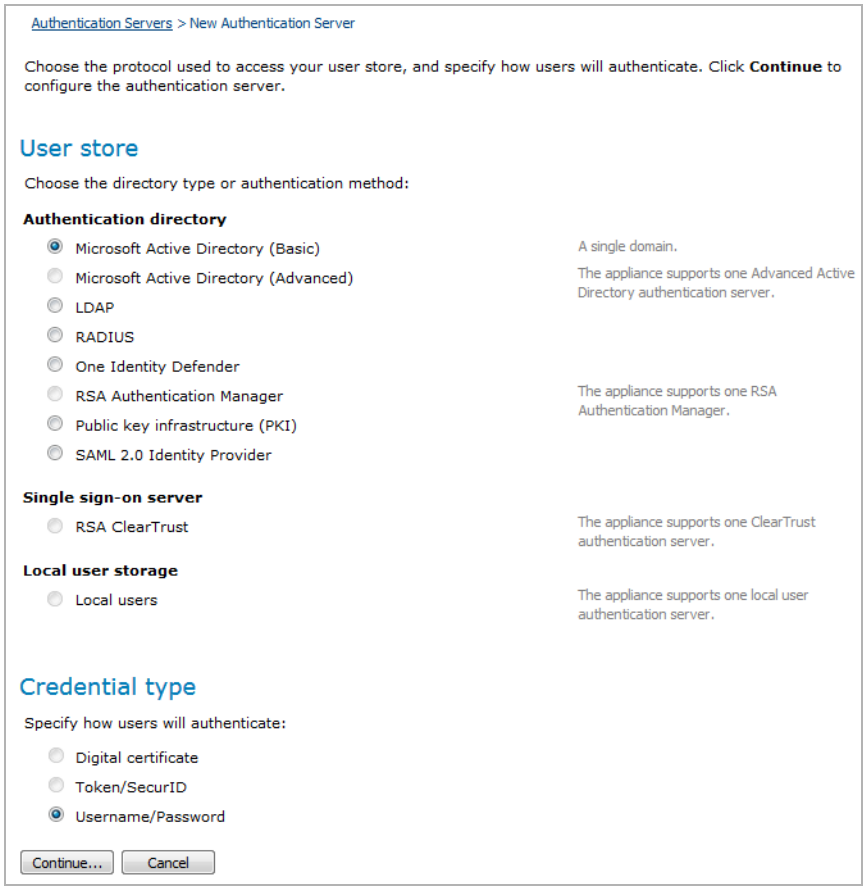
Secure Mobile Access では、アプライアンス管理者を定義する認証サーバーを選択できます。アカウントが外部ディレクトリ サーバーにすでに定義されている場合、ローカル認証ストアを作成し、管理者の役割をローカルに定義されたユーザーやグループに割り当てることができます。

認証サーバーを追加するには、

1 メイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

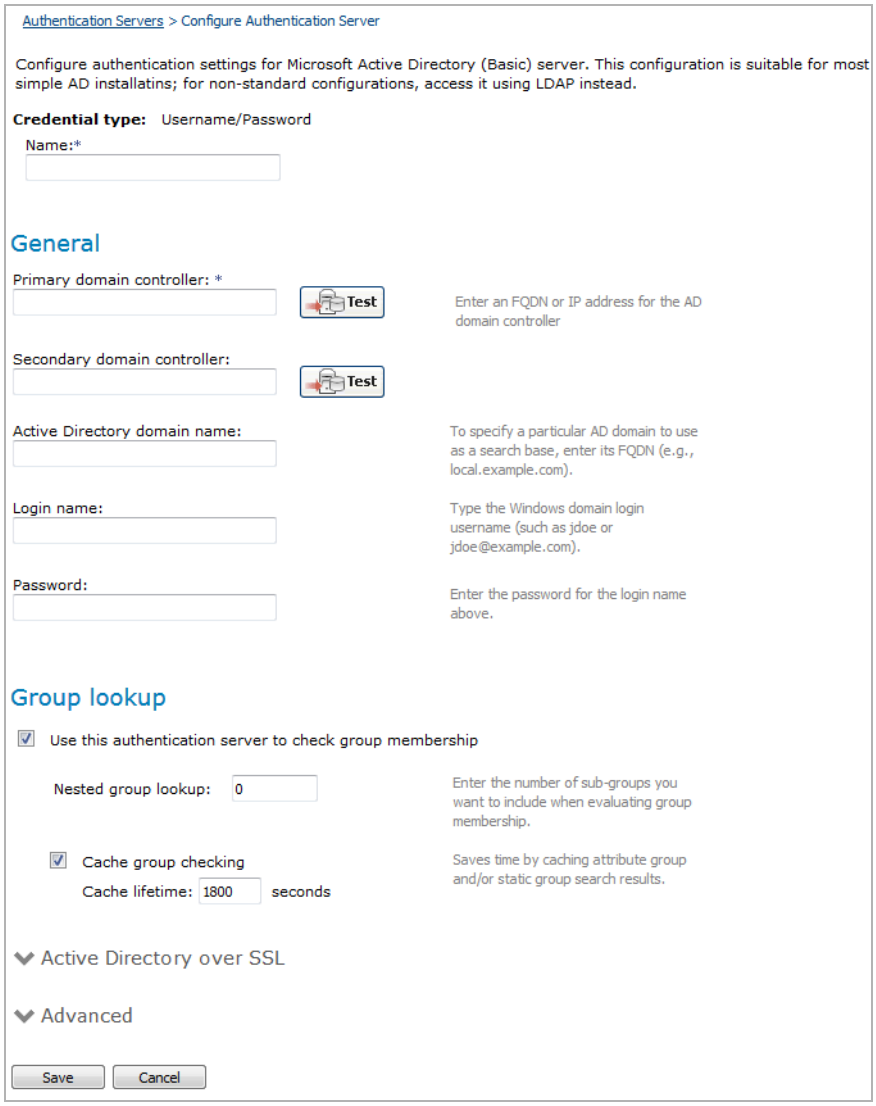


2 [**New...(新規...)**] をクリックします。[**New Authentication Server (新しい認証サーバー)**] ページが表示されます。



3 設定を入力し、

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



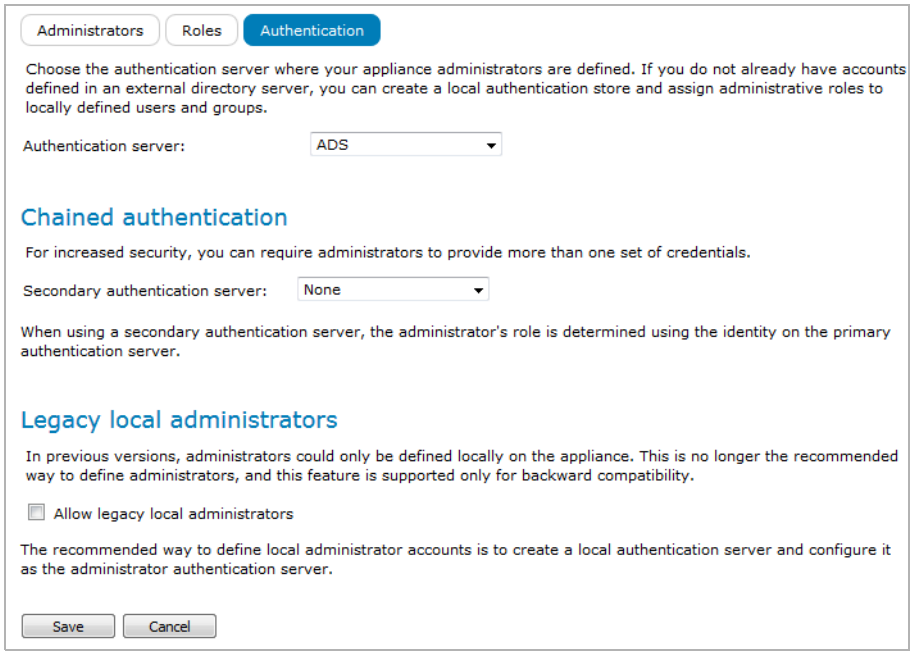
5 構成設定を入力します。

6 [**Save (保存)**] を選択します。

7 [**General Settings (一般設定)**] に移動します。

8 [**Administrators (管理者)**] エリアで管理者アカウントの [**Edit (編集)**] をクリックします。

9 [**Authentication (認証)**] タブをクリックします。



10 [**Authentication server (認証サーバー)**] ドロップダウン メニューから、ステップ 2で追加した認証サーバーを選択します。

11 それ以外のオプションはすべて、デフォルトのままにします。

12 [**Save (保存)**] を選択します。

13 ページの右上にある [**Pending Changes (保留中の変更)**] をクリックします。

14 [**Apply Changes (変更を適用)**] を選択します。

管理者の役割の編集

プライマリ AMC 管理者は、セカンダリ管理者の役割を変更して権限レベルを変更でき、セカンダリ管理者の役割を削除することもできます。詳細については、管理者の役割の定義を参照してください。

複数管理者の構成ファイルの衝突の回避

複数の管理者がアプライアンスを管理する場合、AMC を同時に使用しないようにする必要があります。複数の管理者が同じオブジェクトを変更した場合、AMC は最後の変更を保存します。そのため、意図しない結果になることがあり、アクセス制御ルールが矛盾して変更されると、セキュリティの問題が発生する可能性があります。

複数の管理者が AMC にログインしている場合、AMC の右上のリンクで警告が表示されます。

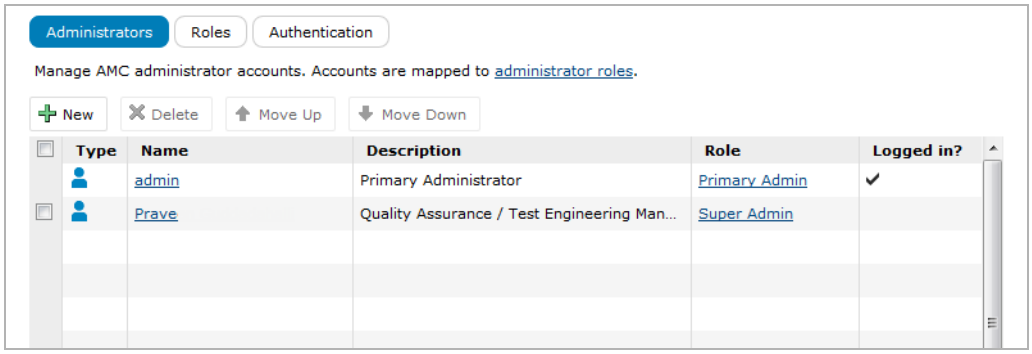
AMC にログインしているすべての管理者のユーザー名と IP アドレスのリストを参照するには、このリンクをクリックします。[**Administrator Sessions (管理者セッション)**] ページが別ウィンドウに表示されます。管理者が Web ブラウザの複数のインスタンスを使用して AMC にログインしている場合、管理者のユーザー名と IP アドレスが複数表示されます。

他の管理者に連絡してお互いの活動を調整することで、構成ファイルの衝突を回避する必要があります。

AMC 管理者の全リストを表示するには、

1 AMC のメイン ナビゲーション メニューから [**General Settings (一般設定)**] をクリックします。

2 [**Administrator accounts (管理者アカウント)**] エリアの [**Edit (編集)**] をクリックします。[**Manage Administrator Accounts (管理者アカウントを管理)**] ページにすべての管理者のリストが表示され、現在どの管理者がログインしているかも表示されます。



管理コンソールの監査ログには、管理者による AMC 構成のあらゆる変更が記録されます。管理監査ログを参照してください。

AMC セッションを終了する場合は [**Log Out (ログアウト)**]をクリックする必要があります。Web ブラウザを閉じてセッションを終了すると、タイムアウト (デフォルトでは 15 分) するまでの間、アクティブ セッションとしてリストに表示されます。

複数の Secure Mobile Access アプライアンスの管理

SMA アプライアンスは、中央管理サーバー (CMS) で管理する必要があります。

重要：SMA 12.1 では GMS はサポートされていません。

中央管理サーバー (CMS) は、すべての VPN アプライアンスを管理できる単一の管理ユーザー インターフェースです。CMS は、総運用コストを削減し、エンタープライズ企業向けの複数の VPN アプライアンスの管理を簡素化する仮想マシンです。

中央管理サーバー (CMS)

VPN 管理者は、中央管理サーバー (CMS) の中央管理コンソール (CMC) を使用して、世界中の場所に関係なくすべての VPN アプライアンスを管理します。CMS と管理対象アプライアンスは、ネイティブ通信チャネルを介して緊密な統合が行われています。中央管理:

- 企業の顧客が分散 VPN インフラストラクチャを管理するためのダッシュボードを提供します。
- 複数のアプライアンスの管理に関連する総運用コスト (TCO) およびオペレータのエラーを削減します。
- アプライアンスを構成、保守、監視するための中央管理コンソール (CMC) を提供します。
- 集中管理されたライセンスでライセンス管理を簡素化するため、アプライアンスごとのライセンスは不要です。

- ライセンスの使用を最適化します。つまり、ユーザーの負荷に基づいてアプライアンスにライセンスを動的に割り当てます。
- コンソール ダッシュボードと SNMP トラップを介して、集中アラートを容易にします。
- 専用のアプライアンスまたはハードウェアは必要ありません (中央管理サーバーは仮想マシンです)。

CMC のこのダッシュボード ビューには、すべての管理対象アプライアンスの概要が表示されます。

管理アプライアンスに CMC から共通の設定を適用できます。統合された監視とレポートにより、管理者は管理対象のすべてのアプライアンスの概要を確認できます。

構成データの操作

このセクションでは、構成の変更を AMC に保存して有効にする方法について説明します。

トピック:

- 構成変更のディスクへの保存
- 構成変更の適用
- 保留中の構成変更の破棄
- 保留中の変更のスケジュール

構成変更のディスクへの保存

AMC での変更が終了して [**Save (保存)**] をクリックすると、変更がディスクに保存されます。[**Cancel (キャンセル)**] をクリックしたり、ブラウザの [戻る] ボタンを使用したりすると、変更は保存されません。

構成変更をディスクに保存するには、

1 AMC で構成を変更します。

2 ページの下部にある [**Save (保存)**]ボタンをクリックします。

構成変更はディスクに保存されますが、アクティブな構成には適用されません。AMC のステータス エリアに、変更が保留になっていてアプライアンスに適用する必要があることを示すメッセージが表示されます。

詳細については、構成変更の適用を参照してください。

構成データを管理する方法には、いくつかのオプションがあり、例えば、エクスポートする、アプライアンスに保存する、リストアするなどの方法があります。詳細については、構成データの管理を参照してください。

構成変更の適用

アプライアンスの構成を変更すると、ディスクには保存されますが、すぐに適用されるわけではありません。このような変更は、有効にするか (このセクションで説明)、破棄できます (詳細については、保留中の構成変更の破棄を参照してください)。

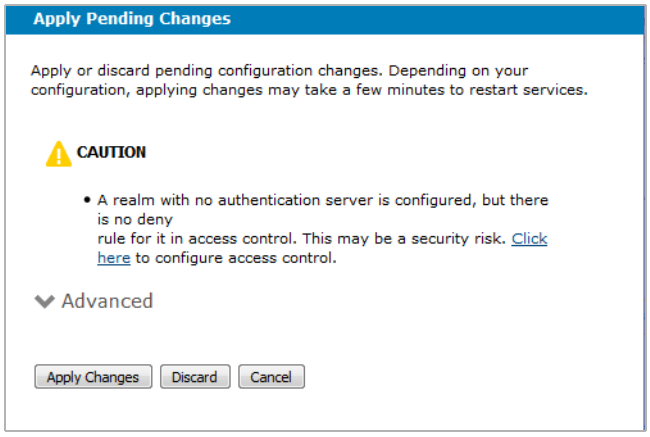
構成変更を有効にするには、変更を適用する必要があります。ほとんどの構成変更は、ユーザーへのサービスを中断することなく適用でき、新しい接続では新しい構成が使用されます。低レベルの構成

変更 (例えば、IP アドレスの変更) はやや面倒で、ネットワーク サービスが自動的に再起動し、ユーザー接続が停止し、ユーザーには再認証が要求されます。可能であれば、オフピーク時 (保守期間など) にこのような構成変更を適用し、ユーザーに事前に通知しておきます。

サービスを手動で再起動する必要がある場合は、Secure Mobile Access サービスの停止と開始を参照してください。

変更を適用するには、

1 ページの上部にあるメッセージの一覧から、[**Pending Changes (保留中の変更)**] をクリックします。保留中の変更を適用ダイアログが表示されます。



2 [**Apply Changes (変更の適用)**] ページのメッセージを参照して、変更の適用の影響を評価します。

警告メッセージ	説明
• 変更を適用すると、すべてのサービスが再起動し、すべてのユーザー接続が停止します。 • 変更を適用すると、既存の TCP/IP ユーザー接続が停止します。 • 変更を適用すると、既存の HTTP ユーザー接続が停止します。	このような変更を適用すると、既存のユーザー接続が停止します。 **注意：ユーザーの再認証が必要になるため、データが失われる可能性があります。**
変更には AMC の再起動が必要となります。再起動すると、現在の管理セッションは終了します。リクエストが完了したら、新しいブラウザを開き、再度 AMC にログインします。	現在のセッションが終了すると、AMC を使用できなくなります。ブラウザを閉じて AMC に再ログインしてください。
認証レルムは有効化されません。そのため、ユーザーはリソースにアクセスできません。	ユーザーがリソースにアクセスできるようにするには、1 つ以上の認証レルムが有効である必要があります。認証レルムが有効でないと、ユーザーがアプライアンスに対して認証できません。

3 [**Apply Changes (変更の適用)**] をクリックして、構成変更を適用します。

構成変更を WorkPlace に適用すると、AMC がサービスの再起動を実行します。ユーザーは WorkPlace に再認証する必要はありませんが、ネットワーク共有にアクセスするために Windows ログイン クレデンシャルを提供している場合、WorkPlace の再起動時に再入力が要求されます。

変更の適用時にすでに存在していた接続では、その接続が終了するまで、古い構成が引き続き使用されます。Web 接続は短いため、Web リソースにアクセスするほとんどのユーザーには、構成変更が短時間で適用されます。一方で、クライアント/サーバー接続は長時間継続する可能性があります。

新しい構成をロードできない場合、既存の接続がそのまま有効になりますが、新しい接続の試行は失敗します。このような状況での対処の詳細については、AMC の問題を参照してください。

保留中の構成変更の破棄

AMC での構成変更はディスクに保存されますが、構成変更の適用で説明したように、適用するまで有効になりません。AMC ログ ファイルを使用すると、どの変更が保留になっているかを確認でき、AMC の [**Apply Changes (変更の適用)**] ページに移動して破棄できます。保留中の変更はグループ単位でのみ破棄でき、個別には破棄できません。

保留中の変更を破棄するには、

1 (オプション) 管理コンソールの監査ログ ファイルで、保留中の変更のリストを確認できます。

   a メイン ナビゲーション メニューから [**Logging (ロギング)**] をクリックし、[**Log file (ログ ファイル)**] リストから [**Management Console audit log (管理コンソール監査ログ)**] を選択します。

   b [**Applied configuration changes message (適用された構成変更メッセージ)**] が最後に表示されたとき以降に追加された [**Info (情報)**] レベルの項目を、破棄できます。

   詳細については、管理監査ログを参照してください。

2 メイン ナビゲーション ページから、[**Maintenance (メンテナンス)**] をクリックします。

3 [**Apply Changes (変更の適用)**] をクリックします。

4 [**Apply Changes (変更の適用)**] ページで、[**Discard (破棄)**] をクリックします。保留中の変更を破棄でリストアされる構成のタイムスタンプと日付スタンプが表示されます。

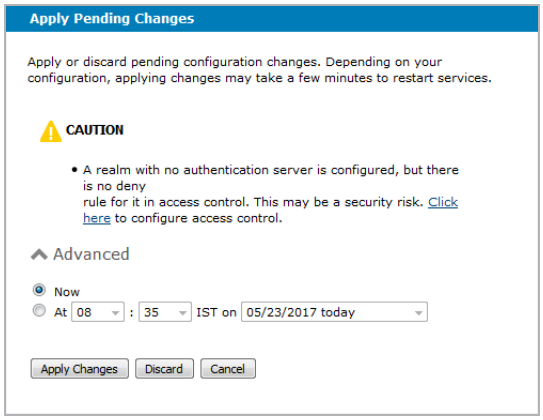
5 **OK** をクリックして、変更の破棄を確定します。

保留中の変更のスケジュール

変更をスケジュールするには

1 AMC の右上にある [**Pending changes (保留中の変更)**] リンクをクリックするか、[**Maintenance (メンテナンス)**] ページの [**Apply Changes (変更の適用)**] ボタンをクリックして、[**Apply Pending Changes (保留中の変更を適用)**] ダイアログを表示します。

2 [**Advanced (高度な設定)**] 見出しの右にある下矢印をクリックして、[**Advanced (高度な設定)**] セクションを展開します。



3 保留中の変更を後で適用するようスケジュールするには、[**At (時刻)**] ラジオ ボタンをクリックし、適用する時刻と日付を選択します。

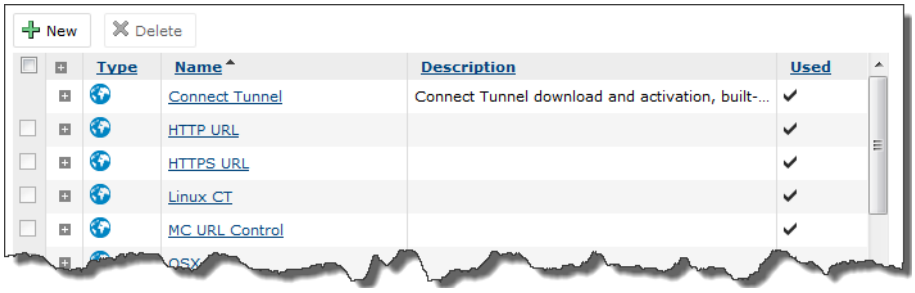
[**Now (現在)**] ラジオ ボタンを選択すると保留中の変更が直ちに適用され、[**Discard (破棄)**] をクリックすると保留中の変更が破棄されます。

4 [**Apply Changes (変更を適用)**] **を選択します。**次に [**Pending Changes (保留中の変更)**] をクリックすると、スケジュールされたアクションが表示されます。

スケジュールされた時刻の前であれば、このダイアログで、いつでもスケジュールを変更したり、破棄したりできます。

参照されているオブジェクトの削除

あるオブジェクト (リソースやユーザーなど) が他のオブジェクトによって参照されていると、そのオブジェクトは削除できません (AMC でそのオブジェクトの隣のチェックボックスを選択できません)。次の例では、リソース「*Connect Tunnel* 」は削除できません。



Web ショートカット、WorkPlace レイアウト、またはアクセス ルールなどの他のオブジェクトが使用しているオブジェクトを削除するには、使用している側のオブジェクトを最初に特定する必要があります。そのためには、オブジェクトの隣にあるプラス (+) をクリックして、リスト項目を展開します。この例では、「*DFS*」という名前の WorkPlace シュートカットがリソースを使用しているため、WorkPlace ショートカットを削除しないと、このリソースを削除できません(このリソースは「**Default Resources**」という名前のリソース グループの一部でもありますが、それが唯一の参照である場合には削除できます)。

他のオブジェクトから参照されていると削除できないオブジェクト タイプに、他のオブジェクトから参照されていると削除できないオブジェクト タイプを記載します。

他のオブジェクトから参照されていると削除できないオブジェクト タイプ

オブジェクト タイプ...	このオブジェクト タイプが参照するオブジェクト...
リソース	アクセス制御ルール、リソース グループ、WorkPlace Web ショートカット
リソース グループ	アクセス制御ルール
ユーザー	アクセス制御ルール
ユーザー グループ	アクセス制御ルール
レルム	ユーザー、ユーザー グループ
認証サーバー	レルム
コミュニティ	レルム
Web アプリケーション プロファイル	リソース

他のオブジェクトから参照されていると削除できないオブジェクト タイプ

オブジェクト タイプ…	このオブジェクト タイプが参照するオブジェクト…
End Point Control ゾーン	アクセス制御ルール、コミュニティ
デバイス プロファイル	End Point Control ゾーン

第 4 部

認証

- ネットワークと認証の構成

5

ネットワークと認証の構成

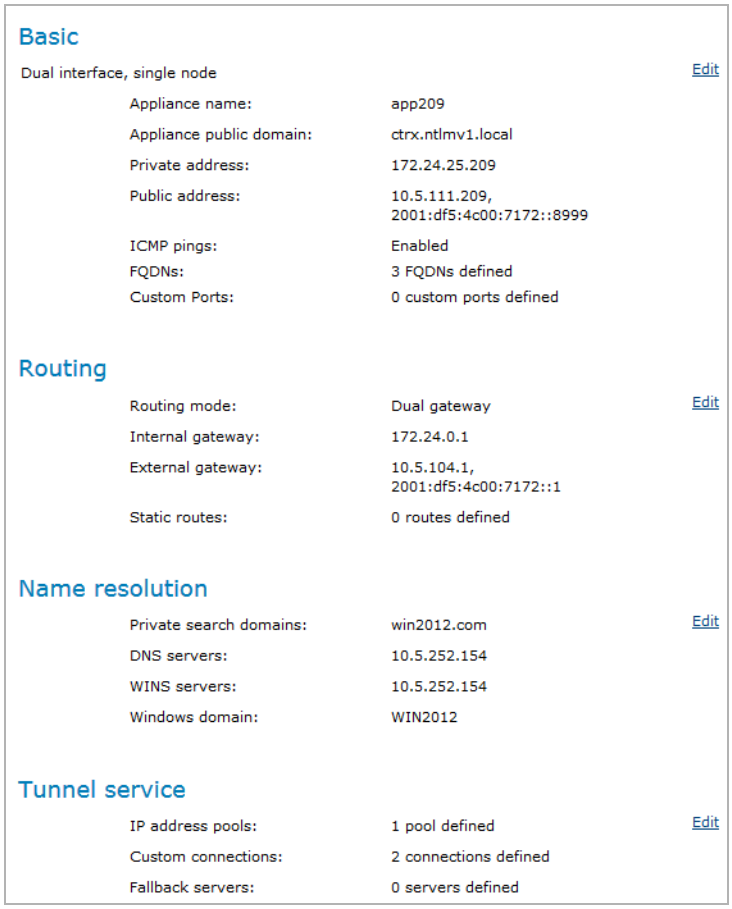
ネットワークの設定について

このセクションでは、基本的なネットワーク構成作業、つまり、ネットワーク インターフェースの構成、ルーティング モードの選択、ネットワーク ゲートウェイの構成、静的ルートの定義、名前解決などについて説明します。また、SSL および CA 証明書の管理やユーザー認証の構成の方法についても説明します。

ここで説明するのは、アプライアンスを動作させる上で必要な最小限のネットワーク構成です。NTP、SSH、ICMP、syslog などのこれ以外のサービスの構成については、システム管理を参照してください。

基本ネットワーク設定の構成

IP インターフェース、ルーティング、および名前解決などのすべての基本ネットワーク設定は、AMC で構成できます。AMC でネットワーク オプションを構成する場合、最初に [**Network Settings (ネットワーク設定)**] ページを使用します。



トピック:

- システム ID の指定
- ネットワーク インターフェースの設定
- ICMP の構成
- 完全修飾ドメイン名とカスタム ポートの表示
- Connect Tunnel のフォールバック サーバーの設定

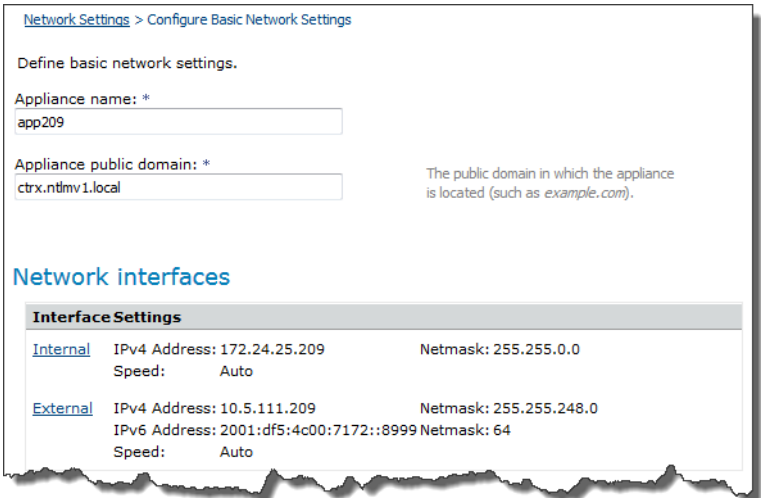
システム ID の指定

アプライアンスに名前を付け、そのアプライアンスを置くドメイン名を指定する必要があります。

システム ID を指定するには、

1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Basic (基本)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Basic Network Settings (基本ネットワーク設定の設定)**] ページが表示されます。



3 [**Appliance name (アプライアンス名)**] のアプライアンス名は、さまざまなコンテキスト (特に、複数のアプライアンスが実行中である場合) でアプライアンスを区別するのに役立ちます。

- SMA アプライアンスのコマンド プロンプトに表示されます。
- ログ ファイルに保存されるため、どのログ メッセージがどのアプライアンスに関するものであるのかを特定できます。
- アプライアンスの構成ファイルを (AMC の [**Maintenance (メンテナンス)**] ページで) エクスポートすると、この**Appliance name (アプライアンス名)**がファイル名の先頭に付加されます。

この名前はユーザーに提示されることはありません。

4 [**Default Domain (既定のドメイン)**]フィールドに、アプライアンスが置かれているドメインの名前 (例えば、`yourcompany.com`) を入力します。この名前で、アプライアンスがアクセスするホストを識別するのに使用する DNS ネームスペースが定義されます。

ネットワーク インターフェースの設定

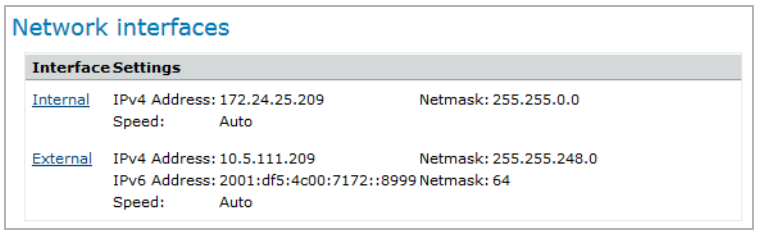
ネットワーク インターフェースを構成するには、IP アドレス、サブネット マスク、およびインターフェース速度を指定します。内部と外部の両方のインターフェースを使用するか (デュアル ホーム構成)、またはオプションで内部のインターフェースだけを使用して (シングル ホーム構成)、アプライアンスを実行できます。インターフェース構成オプションの詳細については、ネットワークのアーキテクチャを参照してください。

ネットワーク インターフェースを構成するには、

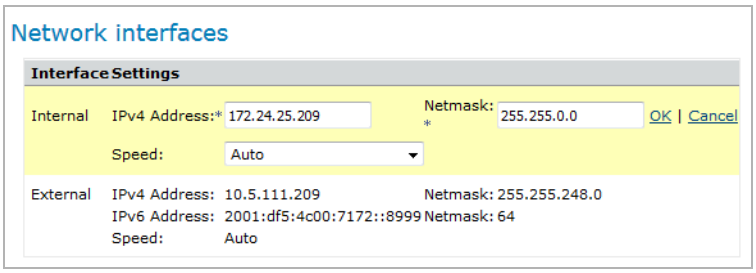
1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Basic (基本)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Basic Network Settings (基本ネットワーク設定の設定)**] ページが表示されます。

3 [**Network interfaces (ネットワーク インターフェース)**] エリアで、内部 (またはプライベート) ネットワークに接続する内部インターフェースの設定を構成します。



a [**Internal (内部)**]をクリックします。表示が編集可能になります。



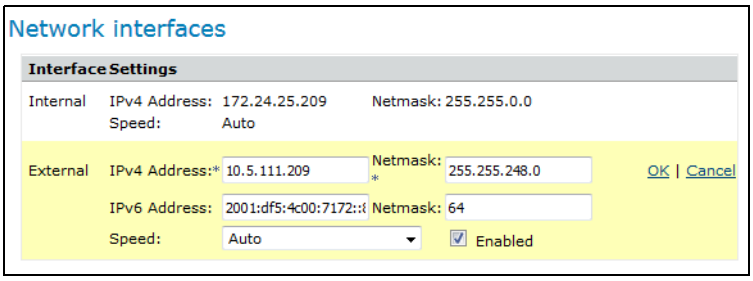
b インターフェースのアドレスとネットワークをそれぞれ [**Address (アドレス)**] と [**Netmask (ネットマスク)**] を入力します。

c リストから該当する**インターフェース速度**を選択します (デフォルトは[**Auto (自動)**])。

d [**OK**] を選択します。

4 外部ネットワーク (またはインターネット) に接続されているインターフェースを設定します。

a [**External (外部)**]をクリックします。表示が編集可能になります。



b インターネットから SMA アプライアンスへの接続に使用するアドレスとネットマスクの設定をそれぞれ[**Address (アドレス)**]と[**Netmask (ネットマスク)**]に入力します。外部の IPv4 または IPv6 アドレスは、パブリックにアクセスできるものである必要があります。

c リストから該当する**インターフェース速度**を選択します (デフォルトは[**Auto (自動)**])。

d [**Enabled (有効)**]チェックボックスをオンにします。

e [**OK**] を選択します。

5 [**Save (保存)**] を選択します。

6 [**Pending changes (保留中の変更)**]をクリックします。

7 変更を適用します (詳細については、構成変更の適用を参照してください)。

アプライアンスを内部と外部の両方のインターフェースを使用するよう構成する場合、ルーティング設定を確認して、内部インターフェースへのネットワーク ルートが存在することを確認します。アプライアンスが AMC へのアクセスに使用するコンピュータと異なるネットワークに存在する場合は、ルーティングをセットアップして (トラフィックを内部ルーターに渡す内部デフォルト ネットワーク ゲートウェイを構成するか、アプライアンスがインストールされているネットワークへの静的ルートを定義します)、ネットワーク構成の変更を適用した後も AMC へのアクセスが維持されるようにする必要があります。詳細については、ルーティングの設定を参照してください。

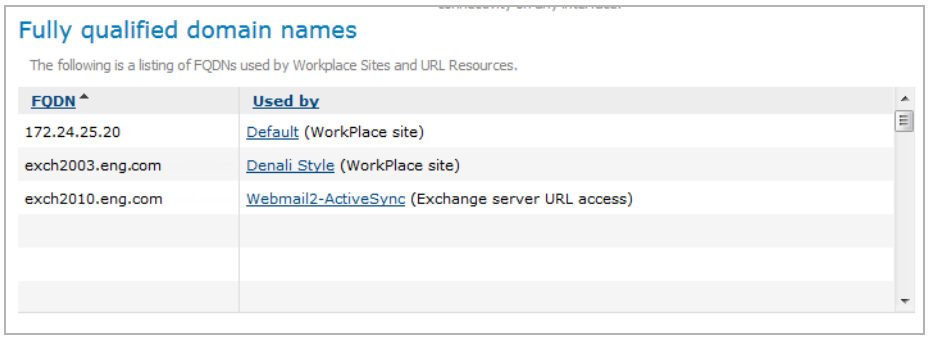
ICMP の構成

ICMP (Internet Control Messaging Protocol) を有効にすると、ping コマンドを使用して IPv4 または IPv6 のインターフェースへのネットワーク接続をテストできます。

ping を有効にするには、[**Enable ICMP pings (ICMP Ping を有効にする)**]チェック ボックスを選択します。Ping を無効にする場合は、このチェックボックスをオフにします。

完全修飾ドメイン名とカスタム ポートの表示

ページの[**Fully qualified domain names (完全修飾ドメイン名)**]セクションには、IPv4 または IPv6 アドレス、FQDN、および WorkPlace サイトとそれらが使用する URL リソースの表が表示されます。任意の列の見出しのリンクをクリックすると、その列の昇順または降順にリストを並べ替えることができます。



[**Used by (使用先)**] の下にリンクとして表示される WorkPlace サイト名または URL リソース名をクリックすると、AMC のそのページに移動し、設定を編集できます。

[**Custom ports (カスタム ポート)**] セクションには、カスタム ポート番号と、カスタム ポートを使用するよう構成されているすべての URL リソースに対してそのポートを使用する URL リソースの表が表示されます。[**Used by resource (リソースが使用)**]の下にリンクとして表示される URL リソース名をクリックすると、**[Resources (リソース)] > [Edit Resource (リソースを編集)]**ページに移動し、リソース設定を編集できます。

Connect Tunnel のフォールバック サーバーの設定

自然災害などの計画外の停止によって、プライマリ アプライアンスを使用できなくなった場合に備え、Connect Tunnel ユーザー向けに 1 つ以上のフォールバック サーバーを設定できます。設定するフォールバック サーバーの名前をユーザーが知っている必要はなく、フォールバック サーバーが指定されているアプライアンスにいつでもクライアントが正しく接続でき、フォールバック サーバーのリストがクライアントに転送されて保存されます。

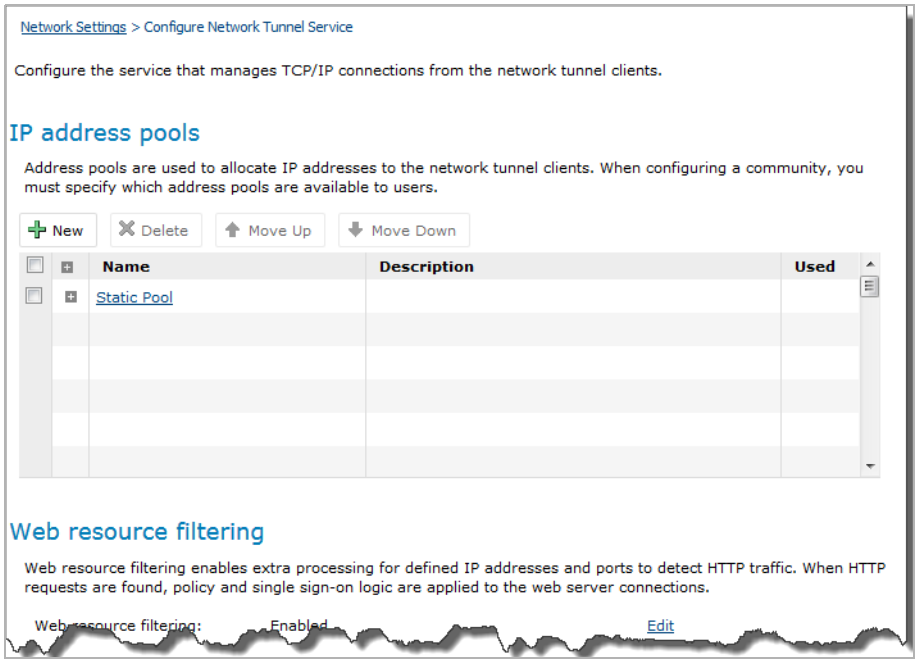
トピック:

- フォールバック サーバーとユーザー環境
- セッション リミット

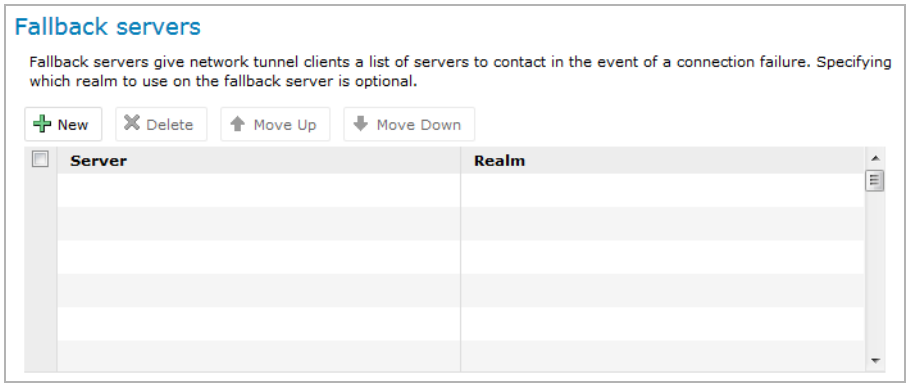
Connect Tunnel ユーザーのフォールバック サーバーを指定するには、

1 メイン ナビゲーション メニューから、[**Network Settings (ネットワーク設定)**] をクリックします。

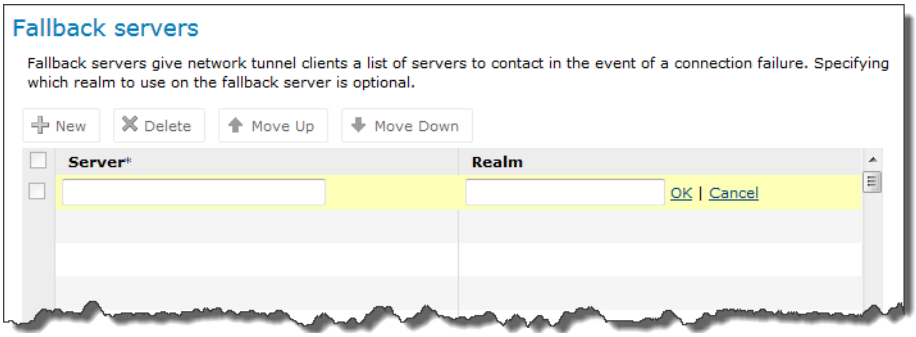
2 [**Tunnel service (トンネル サービス)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Network Tunnel Service (設定ネットワーク トンネル サービス)**] ページが表示されます。



3 [**Fallback servers (代替サーバー)**] エリアの [**New (新規)**] をクリックします。



4 サーバフォールバック **Server (サーバー)**をホスト名または IP アドレスで指定します。



5 [**Realm (レルム)**]フィールドを次のいずれかに設定します。

- 何も入力しない: プライマリ サーバーが利用可能になる前にユーザーがログインしたレルムの場合、同じレルム名がこのフォールバック サーバで使用されます。
- レルムを指定する: ユーザーがこのサーバーに接続する場合に、特定のレルムへのログインを強制します。

6 [**OK**] を選択します。

フォールバック サーバーとユーザー環境

プライマリ サーバーに接続しようとして失敗すると、Connect Tunnel クライアントが自動的に、指定されたフォールバック サーバーへの接続を試行します。この機能は、Windows、Macintosh、または Linux オペレーティング システムで実行中の Connect Tunnel クライアントで利用できます。接続が試行されるために最初に 20 秒程度の一時停止が発生することと、バックアップ ホストに接続されることを示すステータス メッセージが出力されることを除けば、フォールバック サーバーに接続されることをユーザーが認識することはありません。

フォールバック サーバーが使用されるのは、ユーザーが手動で (ダウンしている) プライマリ アプライアンスへの新たな接続を開始したときだけです。アクティブ セッション中にプライマリ サーバーを利用できなくなった場合は、セッションが終了し、ユーザーが新しいセッションを開始する必要があります。

セッション リミット

ユーザーのログイン認証情報に一定期間だけ有効な PIN またはその他のパラメータが含まれている場合は、セッション リミットがどの位であるかを認識しておいてください。例えば、[**Credential lifetime (クレデンシャル存続期間)**]が 30 秒と短く設定されていて、クライアントが接続しようとして何回かフォールバック サーバーとやり取りすると、サーバーの候補のリストを検査し終わる前にユーザーの PIN またはその他のパラメーターがタイムアウトする可能性があります。

いくつかの設定によって、再認証なしでセッションを再開できる時間が決定されます。

- [**Credential lifetime (クレデンシャル存続期間)**]は、[**Configure General Appliance Options (一般装置オプションの設定)**] ページ (メイン ナビゲーション ページで [**General Settings (一般設定)**] をクリックしてから、[**Appliance options (装置オプション)**] エリアの [**Edit (編集)**] をクリックします) で指定されたグローバル設定です。
- [**Limit session length to credential lifetime (セッションの長さをクレデンシャルの有効期間に制限)**] は、コミュニティごとに設定される設定です。選択したコミュニティのトンネル クライアント

セッションは、**Credential lifetime (クレデンシャル存続期間)** で指定した時間の経過後に終了し、再認証が必要になります。

メモ：

- クライアントがフォールバック サーバーに接続し、(AMC で設定された) 要求されたレルムを利用できないと、認証エラーで接続が失敗します。
- 高可用性ペアに接続しているユーザーは、ペアのどのメンバーが最初の接続先であるかにかかわらず、同じフォールバック情報で動作します。
- サーバーに 1 度コンタクトすると、ログイン試行が失敗した場合も、フォールバックは継続しません。
- サーバーのフォールバック　リストがあるアプライアンスから別のアプライアンスに手動で変更すると、2 つ目のサーバーは、ユーザーがそのホストに対して選択した最後の既知のレルムが表示されます。

ルーティングの設定

SMA アプライアンスを、ネットワーク ゲートウェイまたは静的ルートを使用してトラフィックをルーティングするよう構成できます。これらのルーティング方法は、別々に、または組み合わせて使用できます。

トピック:

- ルーティングについて
- ネットワーク ゲートウェイの構成
- ネットワーク ゲートウェイ オプションの選択
- デュアルホーム環境におけるネットワーク ゲートウェイの構成
- シングルホーム環境におけるネットワーク ゲートウェイの構成
- インターネットへのルートの有効化
- 構成静的ルート

ルーティングについて

- アプライアンスが内部と外部の両方のインターフェースを使用するよう構成する場合は、ルーティングの設定に内部インターフェースに対するネットワーク ルートがあることを確認します。アプライアンスが AMC へのアクセスに使用するコンピュータと異なるネットワークに存在する場合は、ルーティングをセットアップして (トラフィックを内部ルーターに渡す内部デフォルト ネットワーク ゲートウェイを構成するか、アプライアンスがインストールされているネットワークへの静的ルートを定義します)、ネットワーク構成の変更を適用した後も AMC へのアクセスが維持されるようにする必要があります。詳細については、ルーティングの設定を参照してください。
- AMC のルーティング情報は、次のようにソートされています。
  - プライマリ キーは [**Netmask (ネットマスク)**] で、エントリは降順 (最大から最小) にソートされます
  - セカンダリ キーは [**IP address (IP アドレス)**] で、エントリは昇順 (最小から最大) にソートされます

- 内部ネットワークに連続するアドレス空間がある場合、静的ルートの作成時に正しいサブネット マスクを指定することで、複数の静的ルートを 1 つのエントリにまとめることができます。複数の静的ルートの組み合わせ に、サブネット マスクを使用して 1 つの静的ルート エントリから複数のネットワークへと内部トラフィックをルーティングする 2 つの例を示します。

複数の静的ルートの組み合わせ

トラフィックをルーティングするネットワーク	指定する IP アドレス	指定するサブネット マスク
192.168.0.0 192.168.1.0 192.168.2.0 192.168.3.0	192.168.0.0	255.255.252.0
192.168.*.* (192.168 の範囲のすべてのネットワーク)	192.168.0.0	255.255.0.0

必要があれば、他のサブネットの静的ルートを明示的に追加して作成でき、その場合には、ルーティング テーブルでネットマスクを広い範囲から狭い範囲へと検索されます。

ネットワーク ゲートウェイの構成

ネットワーク ゲートウェイとは、他のネットワークへのアクセスのポイントとして機能するルーターのアドレスのことです。ネットワーク ゲートウェイのオプションは、使用するネットワーク アーキテクチャによって異なり、アプライアンスをデュアルホーム (内部と外部の両方のインターフェースが有効) またはシングルホーム (内部インターフェースだけが有効) のどちらで構成したかによっても異なります。詳細については、ネットワークのアーキテクチャを参照してください。

トピック:

- ネットワーク ゲートウェイ オプションの選択
- デュアルホーム環境におけるネットワーク ゲートウェイの構成
- シングルホーム環境におけるネットワーク ゲートウェイの構成

ネットワーク ゲートウェイ オプションの選択

ネットワーク ゲートウェイをデュアルホーム環境で設定する場合、次の 4 つのルーティング モード オプションから選択できます。

- [Dual gateway]
- [Single gateway, restricted]
- [Single gateway, unrestricted]
- [No gateway]

これらのシナリオを参考にして、どのオプションが使用環境に最適なオプションであるかを判断します。

- シナリオ 1: 内部ルーターとインターネット ルーターを使用する
- シナリオ 2: クライアント要求を静的ルートで管理する

- シナリオ 3: クライアント要求を指定したゲートウェイに転送する
- シナリオ 4: テスト設定でアプライアンスを評価する
- シナリオ 5:「リダイレクト オール モード」でのネットワーク トンネル クライアントの展開

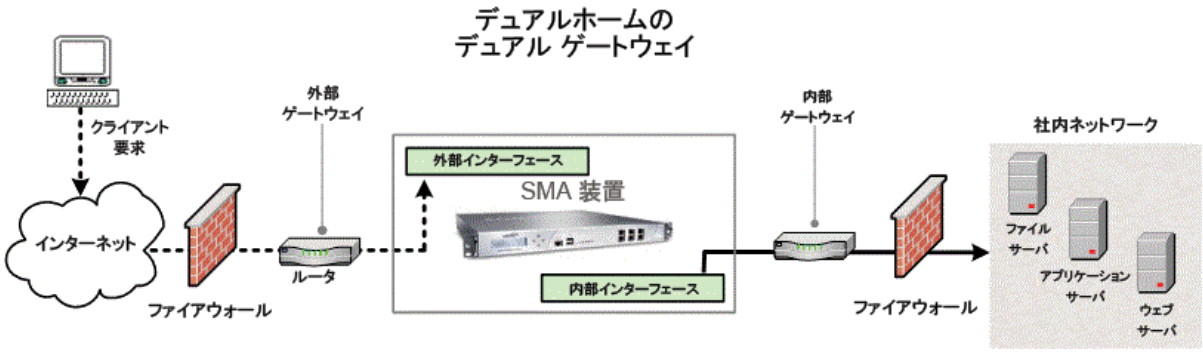
シナリオ 1: 内部ルーターとインターネット ルーターを使用する

内部ルーターとインターネット ルーターを使用する場合、[**Dual gateway**] オプションを使用します。内部リソースへのアクセスには、内部ルーターを利用できます。

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。アプライアンスが [Dual gateway] ルーティング モードに設定されていると、企業ネットワークの内部リソースに対するクライアント要求が内部ルーターに送信されるようにできます。内部ルーターとインターネット ルーターの使用を参照してください。

内部ルーターとインターネット ルーターの使用

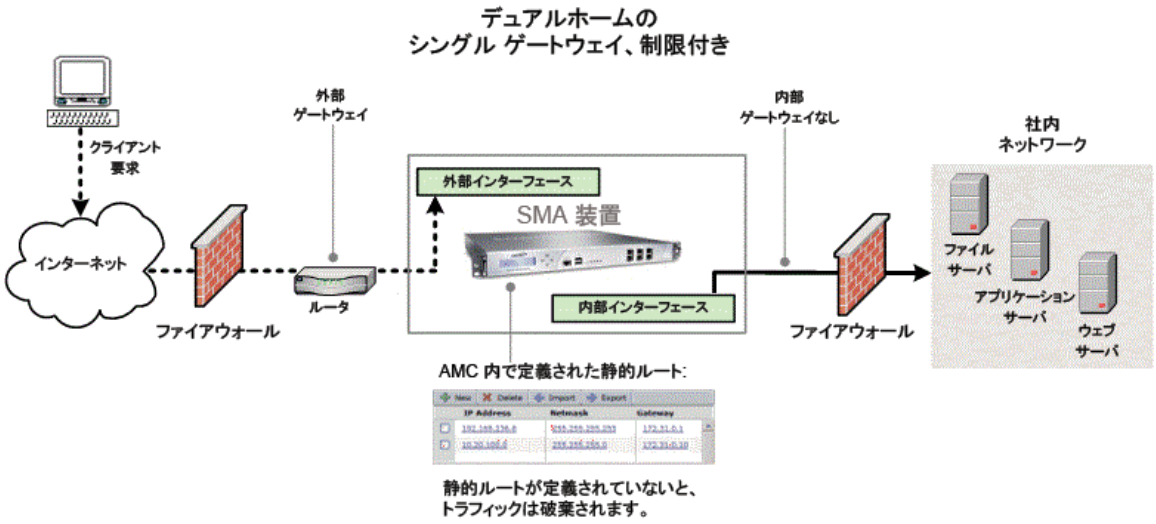


シナリオ 2: クライアント要求を静的ルートで管理する

内部ルーターを使用していない、またはアプライアンスのルーティングを管理したい場合、[*Single gateway, restricted*] オプションを使用します。このシナリオでは、すべてのクライアント要求に静的ルートを定義する必要があります。静的ルートが定義されてないクライアント要求は、アプライアンスによって破棄されます。このオプションでは、必要な作業が多くなりますが、インバンド トラフィックを細かく制御できます。

サンプル シナリオ

B 社は、使用する内部リソースが多くないため、ルーティング情報をアプライアンスで管理したいと考えています。そのため、VPN ユーザーがアクセスするそれぞれのリソースに静的ルートを作成します。VPN ユーザーがアプライアンスのルーティング テーブルに定義されていないアドレスにアクセスしようとすると、トラフィックは破棄されます。クライアント要求を静的ルートで管理するを参照してください。



シナリオ 3: クライアント要求を指定したゲートウェイに転送する

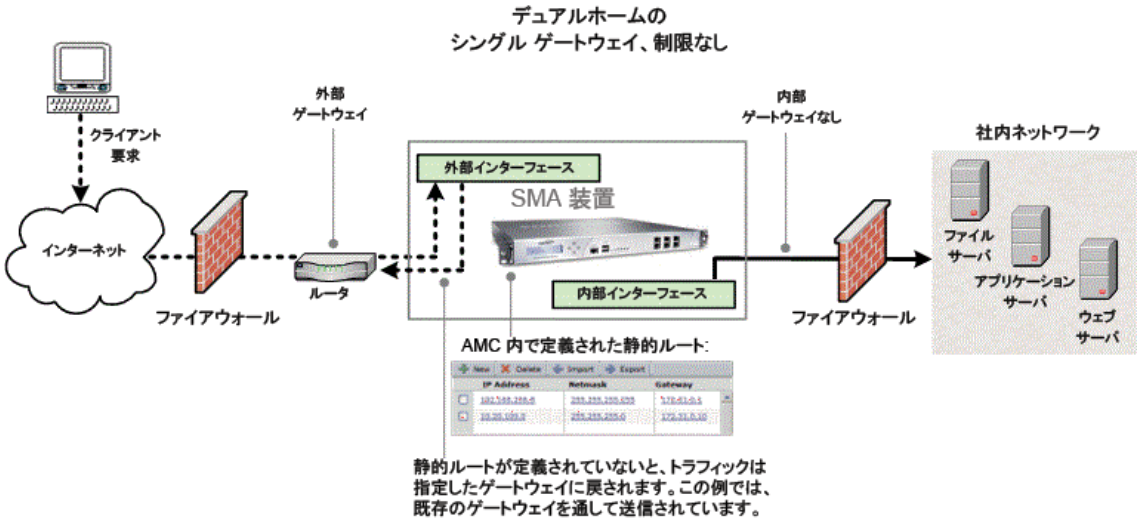
[**Single gateway, unrestricted**] オプションを使用すると、アプライアンスは、静的ルートに一致しないすべてのクライアント要求を、指定したゲートウェイ (アプライアンスの内部または外部のいずれかのインターフェース) に転送します。このオプションでは、インフラストラクチャのフィルタリングやルーティングのポリシーによっては、インターネット ルーターとネットワークの外部にトラフィックが渡される可能性があるため、セキュリティが低下します。この設定は、メンテナンスも難しくなります。

サンプル シナリオ

B 社と同様、C 社も、ルーティング情報をアプライアンスで管理したいと考えているため、VPN ユーザがアクセスする必要があるそれぞれのリソースに静的ルートを作成しました。ただし、同社の一部のユーザーは、インターネット リソースにもアクセスする必要があるため、このトラフィックがアプライアンスからリダイレクトされるようにする必要があります。例えば、ある企業のユーザーが、登録済みの IP アドレスが必要なパブリック Web サーバーにアクセスする必要があるとします。クライアント要求を指定したゲートウェイに転送するを参照してください。

その場合、ユーザーは最初に、アプライアンスとの VPN セッションを確立する必要があり、その後に要求がアプライアンスの外部ゲートウェイへとリダイレクトされます。

クライアント要求を指定したゲートウェイに転送する



シナリオ 4: テスト設定でアプライアンスを評価する

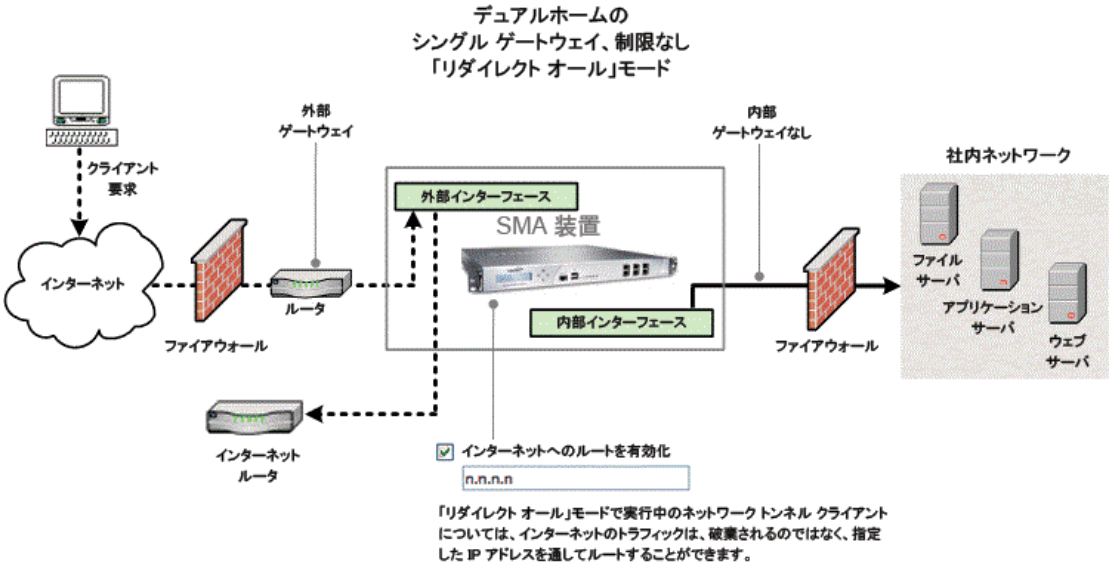
インターフェースをテスト ネットワークに接続し、ルーティングを必要としない場合は、[**No gateway**] オプションを使用して評価します。

シナリオ 5: 「リダイレクト オール モード」でのネットワーク トンネル クライアントの展開

ネットワーク トンネル クライアントを「リダイレクト オール モード」で展開する予定の場合、ネットワーク トンネル ユーザーが内部ネットワークとインターネットの両方にアクセスできるようにする必要があります (詳細については、リダイレクション モードを参照してください)。これには、次のいずれかのオプションを使用します。

- [**Dual gateway**] オプションを使用し、内部ゲートウェイ ルーターにインターネットへのルートが構成されていることを確認します。「リダイレクト オール モード」でのネットワーク トンネル クライアントの展開を参照してください。
- [**Single gateway, unrestricted**] オプションを使用し、インターネットへのルートを使用するようにアプライアンスを構成します。手順については、インターネットへのルートの有効化を参照してください。

「リダイレクト オール モード」でのネットワーク トンネル クライアントの展開



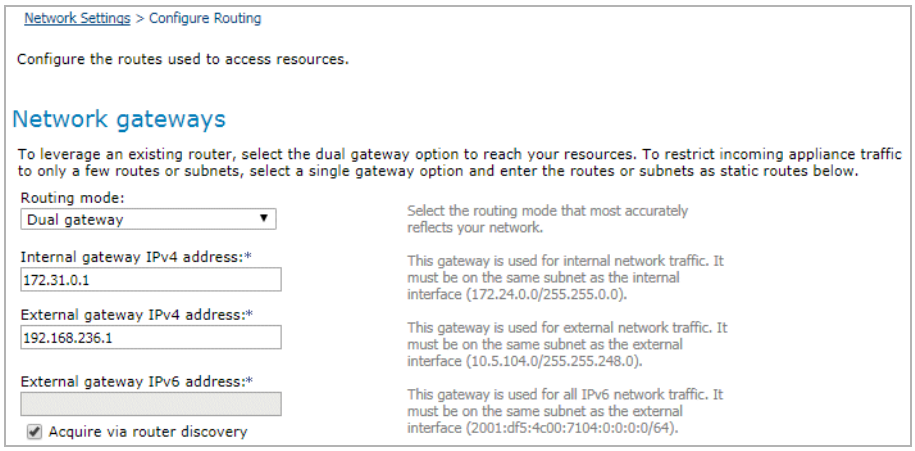
デュアルホーム環境におけるネットワーク ゲートウェイの構成

以下の手順で、内部と外部の両方のインターフェースが有効なデュアルホーム環境で、ネットワーク ゲートウェイをセットアップします。

ネットワーク ゲートウェイをデュアルホーム環境で構成するには、

1 メイン ナビゲーション メニューから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Routing (ルーティング)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Routing (設定ルーティング)**] ページが表示されます。



3 トラフィックをネットワーク ゲートウェイにルーティングするには、次のオプションからルーティング モードを選択します。

- [**Dual gateway**] : 外部と内部の両方のゲートウェイの IP アドレスを指定します。クライアント要求に対して生成されるネットワーク トラフィックは、外部ゲートウェイに送信されます。静的ルートが定義されていないそれ以外のすべてのトラフィックは、内部ゲートウェイに送信されます。

- [**Single gateway, restricted**] : 外部ゲートウェイに対する IP アドレスのみを指定します。静的ルートが定義されていないそれ以外のすべてのトラフィックは、破棄されます。
- [**Single gateway, unrestricted**] : 外部と内部の両方のゲートウェイとして使用する IP アドレスを指定します。静的ルートと一致しないネットワーク トラフィックは、外部ゲートウェイに送信されます。
- [**No gateway**] : アプライアンスが受け取ったものの、静的ルートと一致しないネットワーク トラフィックは、破棄されます。

4 [**Save (保存)**] を選択します。

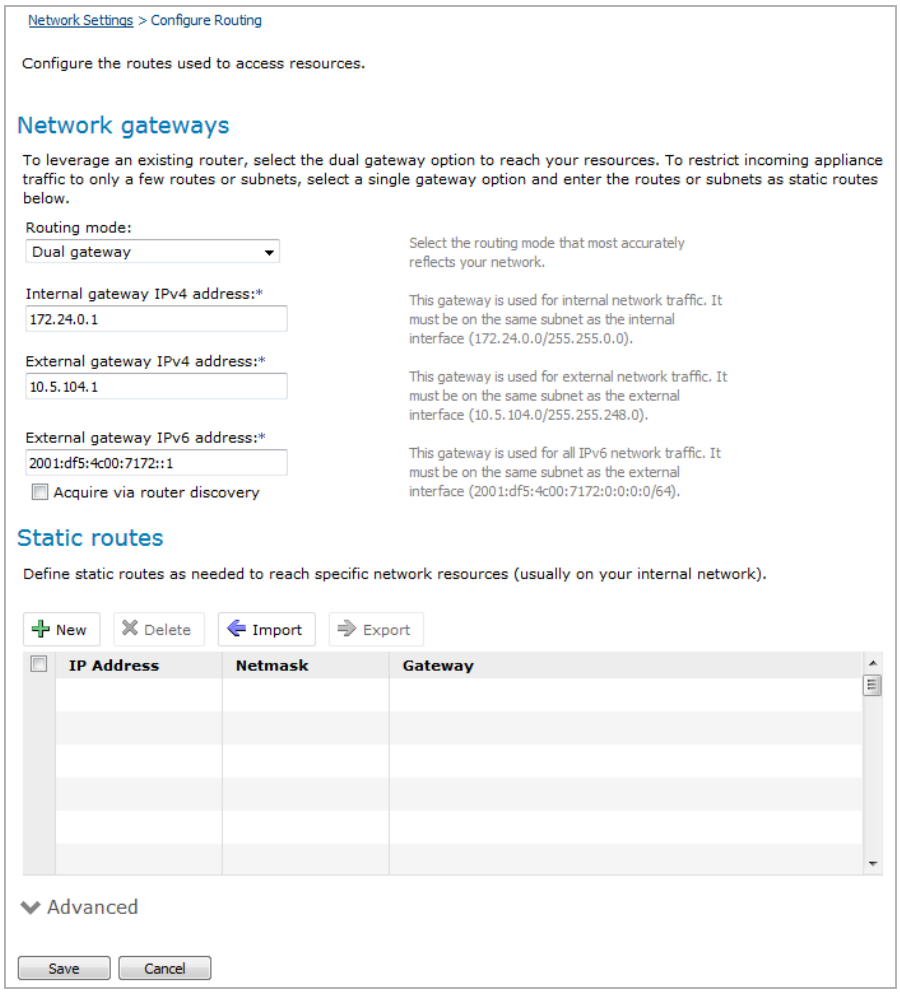
シングルホーム環境におけるネットワーク ゲートウェイの構成

以下の手順で、内部インターフェースだけが有効なシングルホーム環境でネットワーク ゲートウェイをセットアップします。この設定は、デュアルホーム構成よりも一般的ではありません。

ネットワーク ゲートウェイをシングルホーム環境で構成するには、

1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Routing (ルーティング)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Routing (設定ルーティング)**] ページが表示されます。



3 トラフィックをネットワーク ゲートウェイにルーティングするには、次のいずれかのルーティング モードを選択します。

- [**Default gateway**] : デフォルト ゲートウェイの IP アドレスを指定します。アプライアンスが受け取ったものの、静的ルートと一致しないネットワーク トラフィックは、このアドレスに送信されます。
- [**No gateway**] : アプライアンスが受け取ったものの、静的ルートと一致しないネットワーク トラフィックは、破棄されます。

4 [**Save (保存)**] を選択します。

インターネットへのルートの有効化

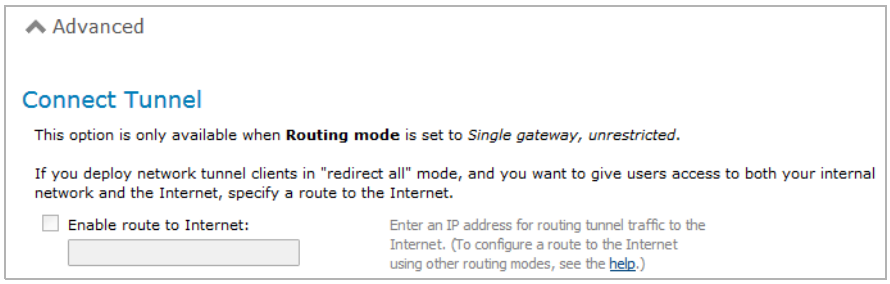
[**Routing mode (ルーティング モード)**]が[**Single gateway, unrestricted (シングル ゲートウェイ、制限なし)**]に設定されている場合も、アプライアンスがデュアルホーム (内部と外部の両方のインターフェースが有効) で構成されていれば、ネットワーク トンネル クライアントでのインターネットへのルートが有効になります。[**Enable route to Internet (インターネットへのルートの有効化)**]が設定されていると、クライアントを起点とし、インターネットを宛先とするすべてのトンネル トラフィック (「リダイレクト オール モード」で動作) は、破棄されずに、指定した IP アドレスにルーティングされます。

インターネットへのルートを有効にするには:

1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Routing (ルーティング)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Routing (設定ルーティング)**] ページが表示されます。

3 [**Advanced (詳細)**]エリアを展開します。[**Connect Tunnel (トンネルを接続)**]エリアが表示されます。



4 [**Enable route to Internet (インターネットへのルートを有効化)**]チェックボックスを選択し、インターネット ルーターの IP アドレスを入力します。

5 [**Save (保存)**] を選択します。

構成静的ルート

静的ルートは、インターネット インターフェースから到達できるネットワークのエントリとして、ルーティング テーブルに追加されます。静的ルート テーブルの管理は、特に大規模サイトにおいては面倒な作業を伴うことがあります。その場合は、AMC を使用せずにルーティング情報をカンマ区切り値 (CSV) テキスト ファイルとして作成、編集してから、AMC にインポートする方法もあります。AMC にインポートする静的ルート情報は、ASCII テキスト ファイルで作成し、各エントリを新しい行に記述し (前のエントリとの区切りに CR/LF を使用)、3 つの値:IP アドレス、ネットマスク、および

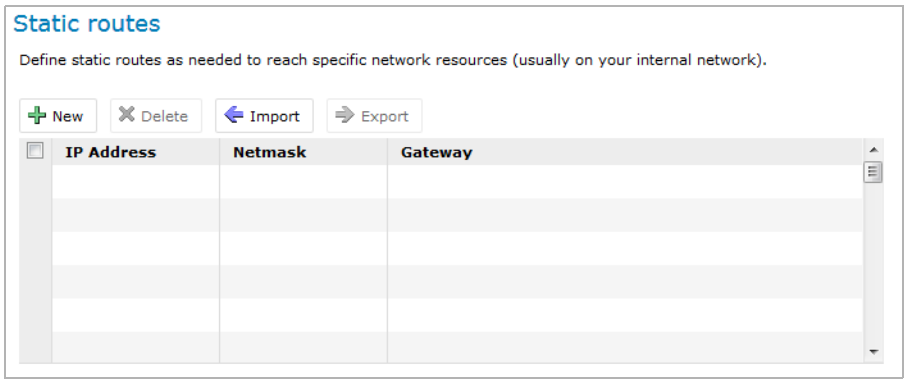
ゲートウェイをカンマで区切ります。IP アドレス、ネットマスク、およびゲートウェイ。ファイルをインポートすると、AMC で現在指定されているすべての静的 ルートが完全に置き換えられます。

静的ルーティング情報を構成するには、

1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Routing (ルーティング)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Routing (設定ルーティング)**] ページが表示されます。

3 [**Static routes (静的ルート)**] エリアで、リストのエントリを単独またはグループとして追加または変更できます。



- [**New (新規)**]をクリックし、[**IP address (IP アドレス)**]、[**Netmask (ネットマスク)**]、および[**Gateway (ゲートウェイ)**]フィールドにルート情報を入力すると、単一のエントリが追加されます。リストのエントリを変更するには、リンクをクリックして変更します。エントリを追加または変更したら、[**OK**] をクリックします。
- [**Import (インポート)**] をクリックして、インポートする静的ルート テーブルを選択します。静的ルート情報は、CSV 形式の ASCII テキスト ファイルである必要があります。各エントリを新しい行に記述し (前のエントリとの区切りに CR/LF を使用)、3 つの値:IP アドレス、ネットマスク、およびゲートウェイをカンマで区切ります。IP アドレス、ネットマスク、およびゲートウェイ。ファイルをインポートすると、AMC で現在指定されているすべての静的 ルートが完全に置き換えられます。
- 既存のルートのリストを変更するには、変更したいリスト項目をクリックするか、リスト全体をエクスポートし、内容を変更してインポートする必要があります。

4 変更が終了したら、[**Save (保存)**] をクリックします。

静的ルートを削除するには、

1 [**Configure Routing (設定ルーティング)**] ページで、削除する静的ルートの左にあるチェック ボックスを選択し、[**Delete (削除)**] をクリックします。

2 [**Save (保存)**] を選択します。

名前解決の設定

アプライアンスは、DNS サーバーにアクセスして、ホスト名を IP アドレスに解決する必要があります。WorkPlace を使用して Windows ネットワークを参照する場合は、WINS (Windows Internet Name Service) サーバーと Windows ドメイン名も指定する必要があります。

トピック:

- Domain Name Service の構成
- Windows ネットワーク名前解決の構成

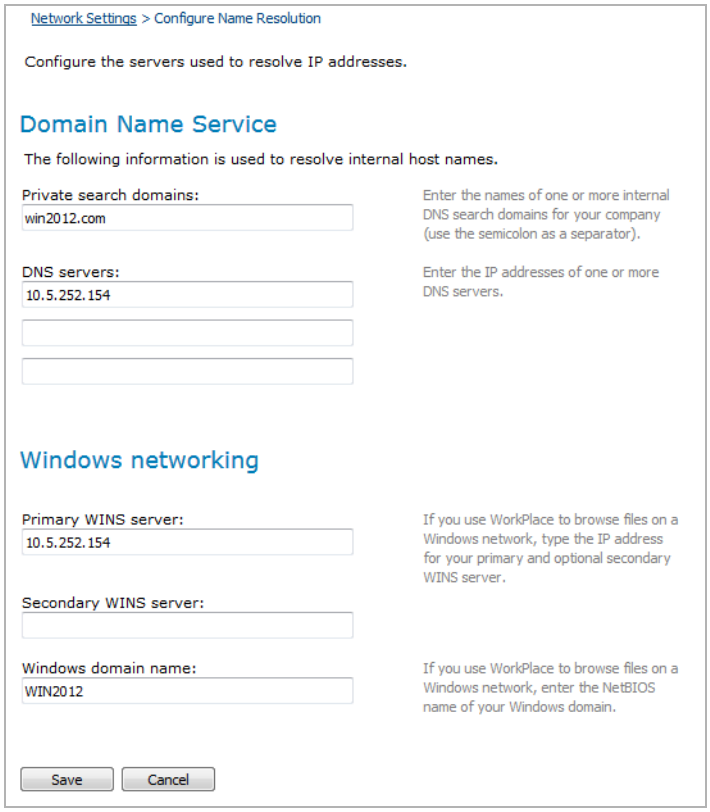
Domain Name Service の構成

DNS サーバーを構成すると、アプライアンスがホスト名を正しく解決できるようになります。DNS を正しく構成することで、アプライアンスがネットワーク リソースへのアクセスを提供できるようになります。

DNS 名前解決を構成するには、

1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Name resolution (名前解決)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Name Resolution (設定名前解決)**] ページが表示されます。



3 [**Private search domains (プライベート検索ドメイン)**]フィールドに、セミコロン (;) 区切り記号（`example.com; sales.example.com` など）を使用して、会社の 1 つ以上の DNS ドメイン名を入力します）。このドメイン名が非修飾ホスト名に付加され、解決されます。最大 6 つのドメイン名をセミコロンで区切って入力できます。

4 [**DNS servers (DNS サーバー)**]フィールドに、プライマリと (ある場合は) バックアップの DNS サーバーの IP アドレスを入力します。プライマリ サーバーを使用できない場合に、バックアップ サーバーが使用されます。

5 [**Save (保存)**] を選択します。

Windows ネットワーク名前解決の構成

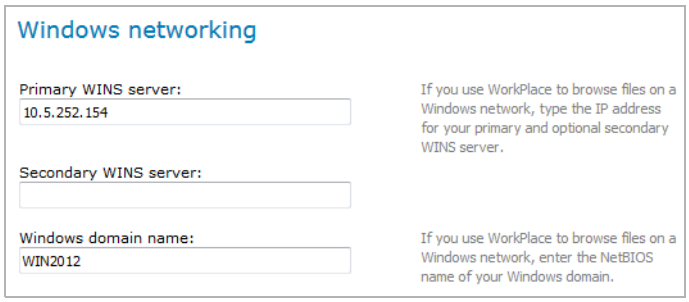
WorkPlace を使用して Windows ネットワークのファイルを参照する場合は、WINS (Windows Internet Name Service) サーバーと Windows ドメイン名を指定する必要があります。WorkPlace は、名前解決を実行したりユーザーが参照するリソースのリストを構築したりする場合に、この情報を使用します。

Windows ネットワーク名前解決を構成するには、

1 AMC のメイン ナビゲーション ページから、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Name resolution (名前解決)**] エリアの [**Edit (編集)**] をクリックします。[**Configure Name Resolution (設定名前解決)**] ページが表示されます。

3 [**Windows networking (Windows ネットワーク)**] エリアに次の情報を入力します。



- プライマリと (ある場合は) セカンダリの WINS サーバーの IP アドレス
- NetBIOS 構文を使用した **Windows domain name (Windows ドメイン名)** (例えば `mycompany`)

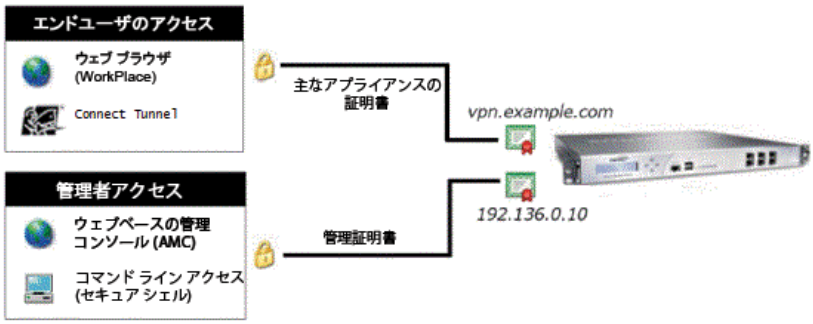
4 [**Save (保存)**] を選択します。

証明書

SMA アプライアンスは、SSL 証明書を使用して、クライアント コンピュータからサーバーに送信される情報を保護したり、接続するユーザに対してアプライアンスの ID を評価したりします。証明書の使用方法を参照してください。少なくとも 2 つの SSL 証明書が必要です。

- Secure Mobile Access サービスは、証明書を使用して、Web ブラウザから WorkPlace へ、および Connect クライアントからアプライアンスへのユーザ トラフィックを保護します (複数の WorkPlace サイトを使用する場合は、複数のサイトに 1 つのワイルドカード証明書を使用するか、サイトごとに異なる証明書を使用するように対応させることができます。どちらの場合も、サイトで異なるホストやドメイン名を使用できます。詳細については、WorkPlace サイトの追加を参照してください)。
- AMC は、管理トラフィックの保護に個別の証明書を使用します。これは一般的に、自己署名証明書です。

証明書の使用方法



サブジェクト代替名 (SAN) 証明書は、WorkPlace、WorkPlace サイト、および接続トンネルでサポートされています。これらの証明書は、一連のクライアントと複数の異なる SSL または TLS のサービスとの間の通信チャネルを安全に暗号化するために使用されます。

SAN 証明書は、一般的な導入環境で必要とされる、IP アドレス/ホスト名/証明書のセットを簡素化します。1 つの SAN 証明書、1 つの IP アドレスで、複数の異なる SSL または TLS で保護された Web やクライアント/サーバーのサービスを使用でき、追加の IP アドレスを構成する必要はありません。また、SAN を同じ IP アドレスの異なるホスト名にも使用できるため、SSL 証明書の共通名を 1 対 1 で FQDN にマッピングする必要はありません。

メモ：SAN 証明書と CSR (証明書署名要求) では、IPv4 アドレスのみをサポートしています。

以下の点が改善されました。

- SAN 関連の機能を、アプライアンスの外部からではなく、AMC で生成できます。
  - SAN を使用する CSR
  - SAN エントリを使用する自己署名証明書
- WorkPlace サイト、カスタム FQDN URL リソース、および ActiveSync リソースを、既存の SAN 証明書を使用して作成できます。
- WorkPlace サイトが専用の IP アドレスを使用しているか、または Default Workplace サイトと 1 つの IP アドレスを共有しているかにかかわらず、アプライアンスは、IP アドレス、FQDN、または SSL 証明書の組み合わせを使用する WorkPlace サイトへの Web 接続をシームレスに処理します。
- Workplace への Connect Tunnel または Mobile Connect の接続を使用する場合は、Workplace サイトが専用の IP アドレスで定義されておらず、Default Workplace サイトの IP アドレスを共有していることを確認してください。例えば、`vpn.mycompany.com` の Default Workplace サイトが `192.168.200.160` にバインドされていて、SSL 証明書 `*.mycompany.com` が使用されている場合に、新しい Workplace サイトを `contractors.mycompany.com` に追加するには、[New Workplace Site] 構成ページに完全修飾ドメイン名 (FQDN) を追加するだけで済み、別の IP アドレスを指定するわけではありません。これにより、Web または Tunnel の接続が `vpn.mycompany.com` または `contractors.mycompany.com` のいずれかに接続できるようになり、アプライアンスでの構成は必要ありません。

Administrator は、SAN 証明書を生成、インポート、処理したり、その SSL 証明書を Workplace、ActiveSync、カスタム FQDN URL マッピング、または Tunnel ベースのアクセス サービスに使用したりできます。

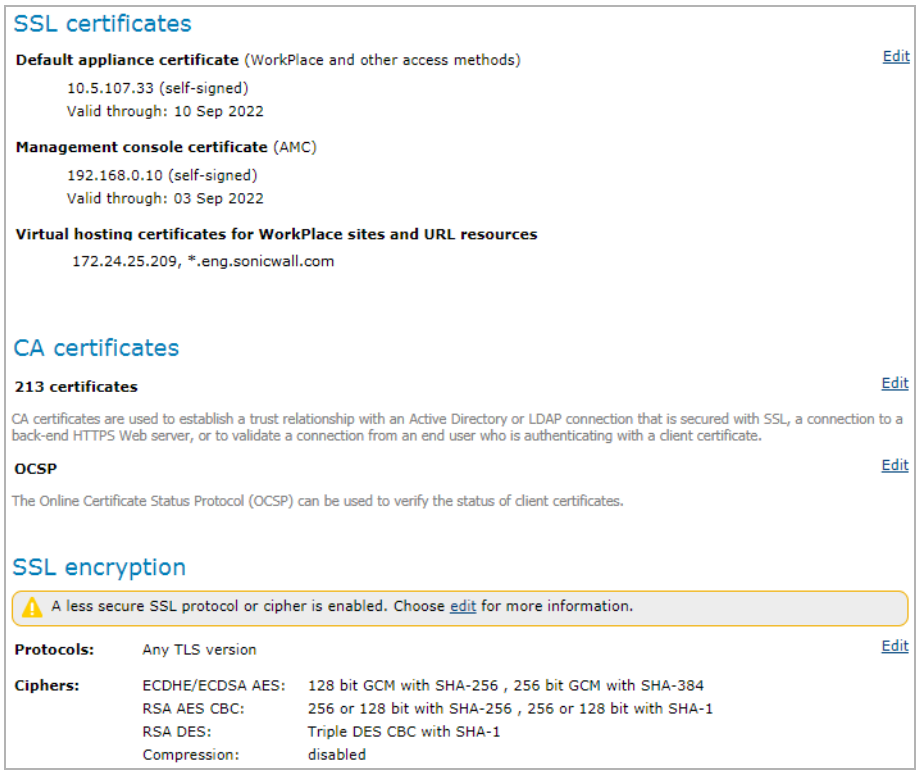
CA 証明書は、バックエンド サーバーへの接続やクライアント証明書を使用する認証の保護にも使用できます。詳細については、CA 証明書のインポートを参照してください。

トピック:

- サーバ証明書
- CA 証明書
- 証明書の使用に関するよくある質問

サーバ証明書

WorkPlace および AMC へのアクセスに使用する SSL サーバー証明書を管理するには、AMC のメイン ナビゲーション メニューから [**SSL Settings (SSL 設定)**] をクリックします。



このページで、SSL および CA 証明書を表示、インポート、削除します。

- 証明書の計画
- 商用 CA からの証明書の取得
- 自己署名証明書の作成
- AMC 内のサーバー証明書の管理

証明書の計画

証明書には、次の 2 種類があります。

- **commercial CA (商用 CA)** は、会社の ID を保証し、CA が署名する証明書の提供することで、その会社の ID を証明します。CA は、商用認証局や第三者機関である必要はなく、企業がその企業自身の CA になることもできます。商用証明書は、Symantec (http://www.symantec.com/ssl-certificates) などの CA から購入するもので、通常は 1 年間有効です。

- **self-signed SSL certificate (自己署名 SSL 証明書)**の場合は、証明書の持ち主が自分自身であることを証明します。対応するプライベート キー データがパスワードを使用して暗号化されます。自己署名証明書は、ワイルドカード証明書にもなるため、IP アドレスと証明書が同じであれば、FQDN が違っていても、複数のサーバーで使用できます。

  この種類の証明書は安全ですが、自己署名証明書はブラウザの CA リストに入っていないため、接続するたびにユーザーに同意を要求するメッセージが表示されます。次のようないくつかの方法で、この要求メッセージが表示されないようにできます。

  - Secure Mobile Access クライアントを構成して、証明書のルート ファイルを使用するようにする。
  - Web ブラウザで、ユーザーの信頼できるルート認証局リストに自己署名証明書を追加する。
  - デフォルトで、広く信頼されている商用 CA を使用する。

どの種類の証明書をサーバーに使用するかを決定する場合は、どのようなユーザがアプライアンスに接続し、それらのユーザがネットワークのリソースをどのように使用するかを考慮します。

- ビジネス パートナーがアプライアンス経由で Web リソースに接続する場合は、取引を実行したり、機密情報を提供したりする前に、相手の ID がある程度保証されていることを期待するでしょう。このような場合は、アプライアンスに商用 CA の証明書を取得するとよいでしょう。

  これに対し、Web リソースに接続する従業員であれば、自己署名証明書を信頼できます。その場合にも、サードパーティの証明書を取得すれば、従業員が接続するたびに自己署名証明書を受け入れなくて済むようになります。

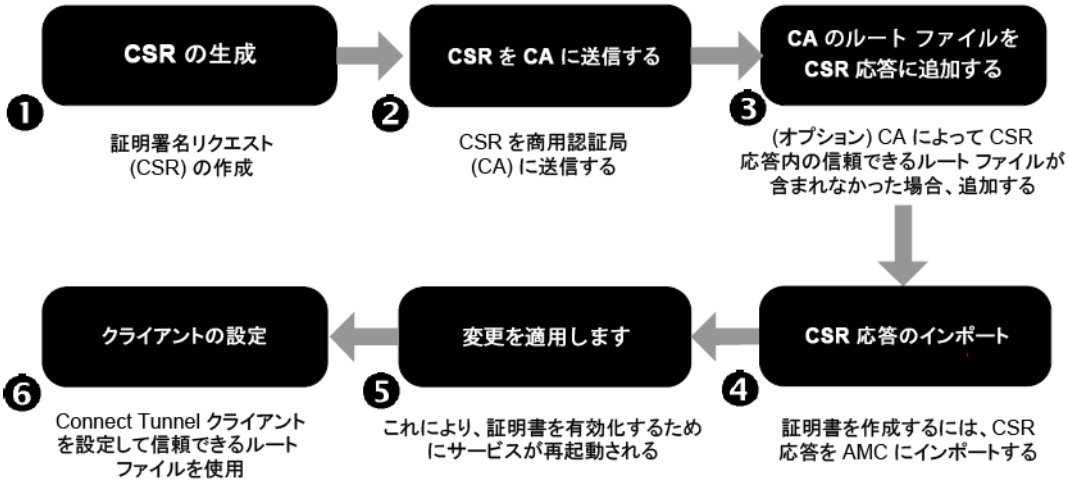
- 小型携帯端末からアプライアンスに接続するユーザーに対応するには、主要 CA (VeriSign など) の証明書を使用するようアプライアンスを構成するか、使用している CA のルート証明書をユーザーの小型携帯端末にインポートします。

> △ **注意：アプライアンスが無名の CA の証明書または自己署名証明書を使用するよう構成されている場合、多くの小型携帯端末では、エラー メッセージが表示されるか、ログインできません。例えば、Windows Mobile 対応デバイスの場合、ルート ファイルで、VeriSign、CyberTrust、Thawte、および Entrust のみが構成されています。小型携帯端末の詳細については、WorkPlace と小型携帯端末を参照してください。**

商用 CA からの証明書の取得

商用 CA から証明書を取得すると、アプライアンス経由でネットワークに接続するユーザーの ID を確認できるようになります。CA 証明書の取得で示されている通り、商用 CA から証明書を取得して構成するには、いくつかの手順を実行する必要があります。

CA 証明書の取得



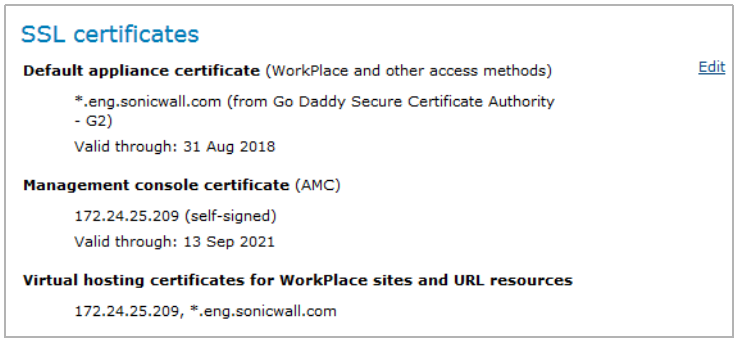
- ステップ1: 証明書署名要求を生成する
- ステップ2: CSR を商用 CA に送信する
- ステップ 3: CSR 応答を確認し、CA のルート証明書を追加する
- ステップ 4: CSR 応答を AMC にインポートする
- ステップ 5: 変更を適用します

ステップ1: 証明書署名要求を生成する

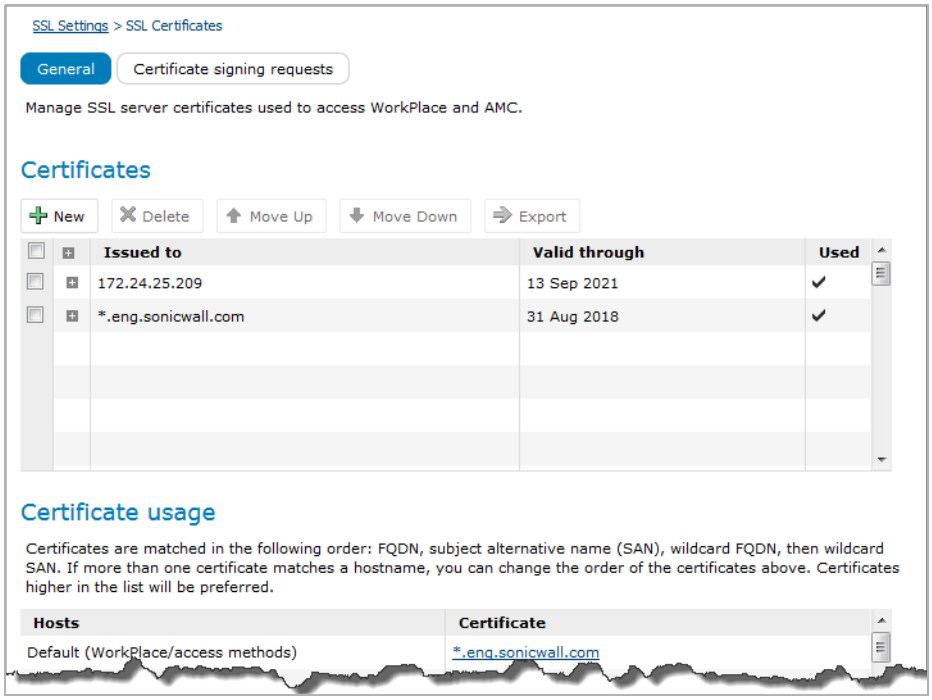
AMC を使用して、証明書署名要求 (CSR) を生成できます。このプロセスでは、サーバー情報や、パブリック キーや ID 情報が含まれる CSR を保護するのに使用される RSA キーのペアが作成されます。ここで指定した情報は、商用 CA が証明書を作成するときに使用され、アプライアンスに接続するユーザーに提示されます。

CSR を生成するには:

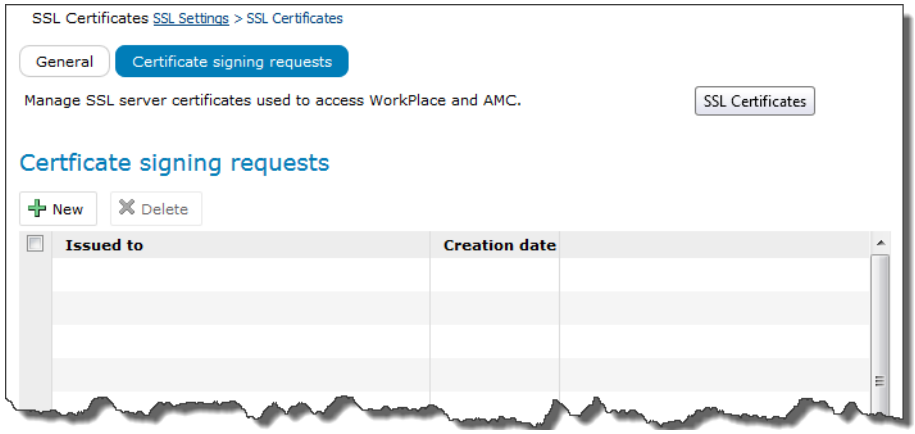
1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。



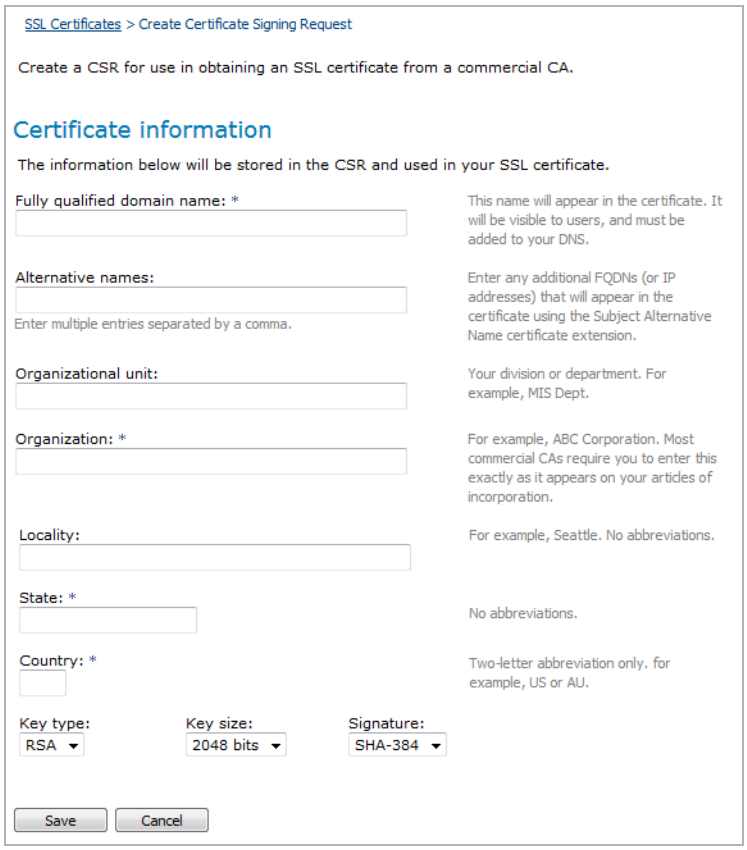
2 [**SSL certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。[**SSL Certificates (SSL 証明書)**] ページが表示されます。



3 [**Certificate signing requests (証明書署名リクエスト)**]タブをクリックします。



4 [**Certificate signing requests (証明書署名リクエスト)**]エリアで[**New (新規)**]をクリックします。[**Create Certificate Signing Request (証明書署名リクエストの作成)**] ページが表示されます。



5 ここで入力した証明書情報は、CSR に保存され、証明書の生成時に商用 CA によって使用され、アプライアンスに接続するユーザーに提示されることがあります。

> **メモ**：一部の商用 CSR では、「&」や「!」などの SHIFT キーを押したときに生成される文字が含まれる CSR の読み取りで、問題が発生することがあります。例えば、会社名やその他の情報を指定する際に「&」を使用していたのであれば、それを「*and*」として記述します。

a [**Fully qualified domain name (完全修飾ドメイン名)**]フィールドに、証明書に記載するサーバー名を入力します。このサーバー名は、「共通名 (CN)」とも呼ばれ、一般的にはホスト名とドメイン名で構成され、例えば、「`vpn.example.com`」と入力します。

Web ベースのクライアントを使用するユーザーは、この名前を使用してアプライアンスにアクセス (言い換えれば、WorkPlace にアクセス) するため、覚えやすい名前を使用します。TCP/IP リソースにアクセスできるように Connect や OnDemand のコンポーネントを構成する場合も、この名前を参照します。ユーザーがアプライアンスにアクセスできるようにするには、この名前を外部 DNS に追加する必要があります。

証明書署名要求を、複数の FQDN または IP アドレスで作成できます。**[SSL Settings (SSL 設定)] > [SSL Certificate (SSL 証明書)] > [Create Certificate Signing Request (証明書署名リクエストの作成)]** ページに、複数の FQDN や IP アドレスをカンマ区切りで入力します。任意の数の SAN を証明書に追加できますが、テキスト入力フィールドの最大文字数は 1,000 です。ワイルドカードを使用できます。CSR 内で、入力した FQDN と IP アドレスは証明書の SAN (Subject Alternative Name) 拡張領域でエンコードされ、証明書 FQDN は追加 SAN エントリとしてエンコードされます。

b [**Alternative name (代替名)**]フィールドに、証明書の SAN (Subject Alternative Name) 拡張領域を使用して証明書に記載すべき追加の FQDN または IP アドレスを入力します。複数の代替名や IP アドレスは、カンマ区切りで入力します。

c [**Organizational unit (組織ユニット)**]フィールドに、部門や部署 (例えば[MIS Dept]) を入力します。

d [**Organization (組織)**]フィールドに、SSL 証明書に記載する会社名または組織名を入力します。

e [**Locality (住所)**]フィールドに、市または町の名前を入力します。省略形は使用しないでください。

f [**State (州)**]フィールドに、州または都道府県名を入力します。省略形は使用しないでください。

g [**Country (国)**]フィールドに、国を表す 2 文字の略語を入力します。有効な国コードのリストについては、国際標準化機構 (ISO) の Web サイト (http://www.iso.org) にアクセスし、ISO 3166-1 を検索してください。

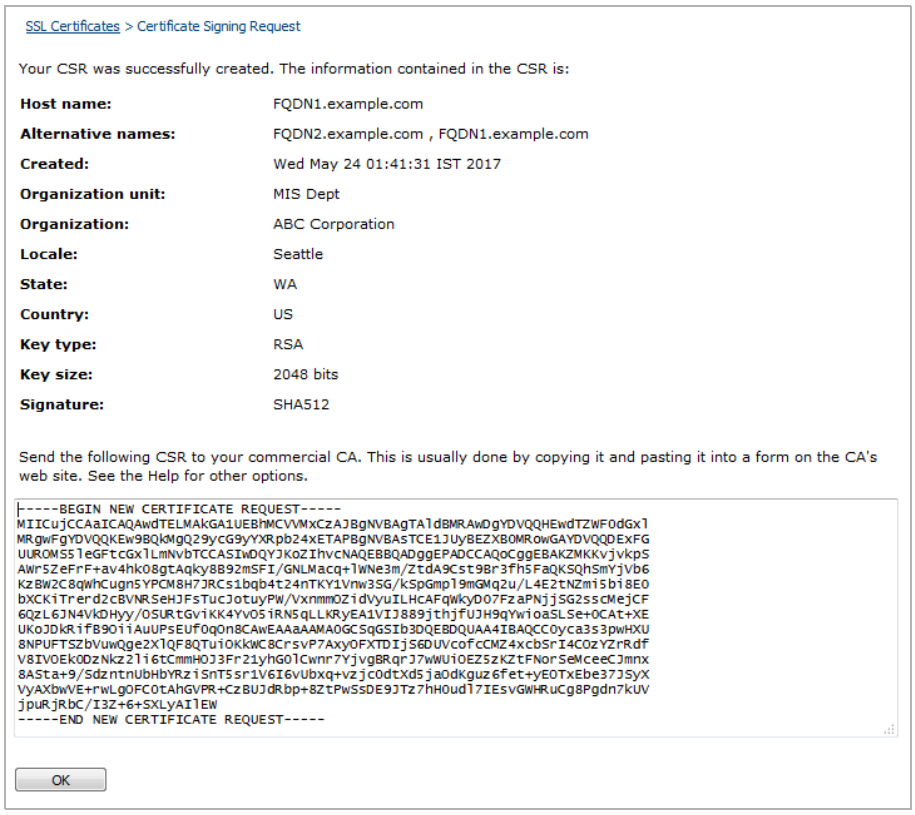
h [**Key length (キー長)**]ドロップダウン メニューで、キーに使用するキー長を選択します。**512**、**768**、**1024**、**1280**、**1536**、**2048** (既定)、または **3072**。キーが長いほどセキュリティは向上しますが、アプライアンスの処理速度は遅くなります。ほとんどのインストール環境に、キー長 2048 を推奨します。

6 [**Key type (キー タイプ)**]ドロップダウン メニューからキー タイプを選択します。既定値は **RSA** です。

7 [**Signature (シグネチャ)**]ドロップダウン メニューから、証明書に使用されているアルゴリズムを選択します。

8 情報を見直して正しく入力されていることを確認します。

9 [**Save (保存)**]をクリックして CSR を生成します。[**Certificate Signing Request (証明書署名リクエスト)**]ページが、入力した CSR 情報とともに再表示されます。



10 CSR テキストの内容を AMC からクリップボードまたはテキスト ファイルにコピーします。

11 [**OK**] を選択します。

ステップ2: CSR を商用 CA に送信する

CSR を送信するプロセスは、選択した商用 CA によって異なります。

CSR を商用 CA に送信するには、

1 証明書署名要求の内容を、AMC の [**Create Certificate Signing Request (証明書署名リクエストの作成)**] ページからコピーします。

2 これを指定された方法で CA に送信します (通常は、CSR テキストをコピーして CA の Web サイトにペーストするか、電子メールのメッセージに添付します)。

CA の指定によって、すべてのテキストをペーストする場合と、`BEGIN NEW CERTIFICATE REQUEST` と `END NEW CERTIFICATE REQUEST` のバナーの間のテキストだけ (バナーそのものも含む) をペーストする場合があります。どの方法なのかがよくわからない場合は、CA にお問い合わせください。

3 商用 CA による ID の確認が終了するのを待ちます。会社の ID を証明する 1 つ以上のドキュメントを作成するよう要求されることがあります (会社の営業許可や定款など)。

メモ：CSR を 1 度だけ送信します。2 回以上送信すると、CA から二重に課金されることがあります。この操作で、内部プライベート キーも変更され、CA からの応答を利用できなくなります。

ステップ 3: CSR 応答を確認し、CA のルート証明書を追加する

CSR への送信後は、CA が会社の ID を確認するのを待つ必要があります。このプロセスの完了後に、CA から証明書の返信が送信されます。返信は通常、次のいずれかの形式です。

- **電子メールのメッセージの添付ファイル。**この場合は、ファイルをローカル ファイル システム (AMC にアクセスするファイル システム) に保存し、AMC にインポートできます。
- **電子メールのメッセージに埋め込まれたテキスト。**この場合は、テキストをコピーし、AMC のテキスト ボックスにペーストします。必ず、`BEGIN CERTIFICATE` と `END CERTIFICATE` のバナーが含まれるようにします。

CA から CSR 応答で完全な証明書チェーンが提供されない場合 (一般的な方法) は、CSR 応答のインポート時に AMC が証明書を完成させようとします。証明書チェーンを完成させることができないと、AMC はエラー メッセージを表示します。その場合は、CA のルート証明書または中間公開証明書をアプライアンスにアップロードする必要があります。自分の会社が CA の役割も果たす場合は、おそらくこの手順を実行する必要があります。

証明書チェーンを完成させるには、

1 信頼できるルート証明書または中間公開証明書を CA から取得します。ほとんどの外部商用 CA は、Web サイトでこの証明書を提供しています。

2 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

3 [**SSL certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。

4 [**Certificate signing requests (証明書署名要求)**] リストで、該当する証明書に対応する [**Process CSR response (CSR 応答を処理)**] リンクをクリックします。[**Import CSR Certificate (CSR 証明書をインポート)**]ページが表示されます。

5 証明書のアップロード:

- 証明書がバイナリ形式の場合、[**Browse (参照)**]をクリックして、証明書の返信をローカル ファイル システム (つまり、AMC にログインしたコンピュータ) からアップロードします。
- 証明書が base-64 エンコード (PEM) テキスト形式の場合は、[**Certificate text (証明書テキスト)**]をクリックして、証明書をフィールドにペーストします。必ず、`BEGIN CERTIFICATE` と `END CERTIFICATE` のバナーが含まれるようにします。

6 [**Import (インポート)**] をクリックして [**CA Certificates (CA 証明書)**] ページに戻ります。

7 証明書が正しくアップロードされたことを確認するには、[**CA Certificate (CA 証明書)**] をクリックします。新しい証明書が [**CA Certificates (CA 証明書)**] ページに表示されます。

ステップ 4: CSR 応答を AMC にインポートする

証明書を作成するには、CSR 応答を AMC にインポートします。

証明書の返信をインポートするには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**SSL certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 [**Certificate signing requests (証明書署名要求)**] リストで、該当する証明書に対応する [**Process CSR response (CSR 応答を処理)**] リンクをクリックします。

4 [**Import CSR Certificate (CSR 証明書のインポート)**] ページで証明書をアップロードします。

- 証明書がバイナリ形式の場合、[**Browse (参照)**] をクリックして、証明書の返信をローカル ファイル システム (つまり、AMC にログインしたコンピュータ) からアップロードします。
- 証明書が base-64 エンコード (PEM) テキスト形式の場合は、[**Certificate text (証明書テキスト)**] を選択して、証明書をテキスト ボックスにペーストします。必ず、`BEGIN CERTIFICATE` と `END CERTIFICATE` のバナーが含まれるようにします。

5 [**Used by (使用先)**]ドロップダウン メニューで、[**AMC**]または[**WorkPlace/access methods (WorkPlace/アクセス方法)**] を選択します(後で選択する証明書のリストを構築する場合は[**None (なし)**]を選択します)。デフォルトの WorkPlace サイト以外に追加の WorkPlace サイトを定義した場合は、その名前がこのリストに表示されます。

6 [**Save (保存)**] を選択します。

7 証明書が正しくアップロードされたことを確認するには、[**SSL Certificates (SSL 証明書)**] ページで、その証明書の隣にあるプラス記号 (+) をクリックします。

ステップ 5: 変更を適用します

新しい証明書の使用を開始するには、構成の変更を適用する必要があります。詳細については、構成変更の適用を参照してください。

変更を適用すると、アプライアンスが新しい証明書を検査し、すべての新しい接続にその証明書を使用します。アプライアンスが証明書を正しく処理できないと、失敗したことを示すメッセージが表示され、失敗に関する情報がイベント ログに記録されます。一般的には、証明書がない、証明書の有効期限が切れた (またはまだ有効ではない)、または暗号化されたパスワード ファイルにキャッシュされているパスワードが正しくない場合に、このような状況が発生します。

メモ：ユーザーがデジタル証明書を認証に使用する場合は、サーバーとクライアントの両方で信頼できるルート ファイルを構成する必要があります。クライアント証明書失効の構成を参照してください。

自己署名証明書の作成

自己署名 SSL 証明書を (商用 CA から証明書を取得せずに) 使用する場合、AMC を使用して作成できます。証明書とホストは 1 対 1 にマッピングされていないため、証明書に対してホストは選択されません。ワイルドカード証明書を使用すると、1 つの証明書を複数のホストにマッピングできます。また、自己署名 SSL 証明書を、複数の FQDN または IP アドレスで作成できます。

自己署名証明書を作成するには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**SSL certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 [**New...(新規...)**] をクリックします。

4 メニューから[**Create self-signed certificate (自己署名証明書を生成)**]を選択します。

5 [**Fully qualified domain name (完全修飾ドメイン名)**]フィールドに `*.domainname.com` などのワイルドカード ドメイン名を入力するか、証明書に記載する個々のサーバー名を入力します。

- メインのアプライアンス証明書の場合、ワイルドカード証明書を使用するか、「`vpn.example.com`」のように入力します。ユーザーがアプライアンスにアクセスできるようにするには、この名前を外部 DNS に追加する必要があります。

  これは、ユーザーがネットワーク上の Web ベースのリソースにアクセスする際に入力する名前になります。ワイルドカード証明書の場合、「*」は特定のサーバー名のように、ピリオドまでの任意の文字列と一致します。TCP/IP リソースにアクセスできるように Connect クライアントを構成する場合も、この名前を参照します。

- この証明書を (WorkPlace ではなく) AMC で使用する場合は、`amc.example.com` のように入力します。多くの場合に、この名前を内部 DNS に追加すると、AMC に簡単にアクセスできるようになります。

- 任意の数の SAN を証明書に追加できますが、テキスト入力フィールドの最大文字数は 1,000 です。複数の FQDN あるいは IPv4 または IPv6 のアドレスは、カンマ区切りで入力します。SAN には、ワイルドカード エントリ (`*.example.com`、`*.access.example.com`)、一意の FQDN (`access.example.com`、`vpn.example.com`)、および IP アドレスを使用できます。

  証明書内で、入力した FQDN と IP アドレスは証明書の SAN (Subject Alternative Name) 拡張領域でエンコードされ、FQDN は CSR の追加 SAN 名としてエンコードされます。SAN が IP アドレスの場合は、SAN 拡張領域で、DNSName ではなく、IPAddress としてエンコードされます。

6 [**Alternative names (代替名)**]フィールドに、証明書の SAN (Subject Alternative Name) 拡張領域を使用して証明書に記載すべき追加の FQDN または IP アドレスを入力します。複数の代替名や IP アドレスは、カンマ区切りで入力します。

7 [**Organization (組織)**]フィールドに、SSL 証明書に記載する会社名または組織名を入力します。

8 [**Country (国)**]フィールドに、国を表す 2 文字の略語を入力します。有効な国コードのリストについては、国際標準化機構 (ISO) の Web サイト (http://www.iso.org) にアクセスし、ISO 3166-1 の情報を検索してください。

9 [**Key size (キー サイズ)**]リストで、キーに使用するキー長を選択します。キーが長いほどセキュリティは向上しますが、アプライアンスの処理速度は遅くなります。ほとんどのインストール環境に、*1024 ビット*または *2048 ビット*のキーの長さを推奨します。

10 [**Signature (シグネチャ)**] リストから、証明書に使用されているアルゴリズムを選択します。

11 [**Save (保存)**] を選択します。

12 [**Pending changes (保留中の変更)**] をクリックして、変更を適用します (詳細については、構成変更の適用を参照してください)。

自己署名証明書に対する信頼できるルート ファイルの作成

自己署名証明書を使用する場合は、信頼できるルート ファイルをユーザーに提供できます (提供しないと、ログインのたびにセキュリティ プロンプトが表示されます)。

メモ：

- Setup Tool によって、AMC 用の自己署名証明書が作成されます。ほとんどの導入環境では、この自己署名証明書で十分であり、商用 CA から証明書を取得する必要はありません。ただし、信頼できるネットワーク内で AMC を使用することが重要です。自己署名証明書は、受動的な傍受の防止策にはなりますが、能動的な攻撃からの防止策にはなりません。
- Apple Macintosh システムで Microsoft Internet Explorer を使用するユーザー向けに OnDemand を展開する場合は、商用 SSL 証明書を取得する必要があります。Macintosh Java Virtual Machine (JVM) は未知の CA からの署名証明書を受け付けないため、自己署名証明書が機能しません。

自己署名証明書に対する信頼できるルート ファイルを作成するには、

1 アプライアンスにログインします。

2 `/usr/local/extranet/etc` にある `server.cert` ファイルのコピーを作成します。

3 コピーしたファイルをテキスト エディタで開き、ルート証明書以外のすべてを削除します。ファイルに、1 つ以上の証明書とプライベート キーが含まれた状態になります。ルート証明書は、このファイルの、バナーを含む最後の証明書ブロックです。次の例では、最初の証明書ブロックとプライベート キー ブロックを削除します。

削除後のファイルは次のようになります。

```
-----BEGIN CERTIFICATE-----
MIIDTjCCAvigAwIBAgIBADANBgkqhkiG9w0BAQQFADCBqDELMAkGA1UEBhMCVVMx7Vkfwp
/zfKMBawQicc+/SK60AXCuYT2Kc5X1GDnY01Hjxw==
-----END CERTIFICATE-----
```

4 このファイルをユーザーに配布します。こうすることで、セキュリティが向上し、ユーザーが接続するたびに SSL 証明書を受け入れるよう要求されることもなくなります。CA 証明書のインポートを参照してください。

Web ベースのユーザーのセキュリティを向上させるには、このファイルをこれらのユーザーのブラウザにインポートします。

AMC 内のサーバー証明書の管理

トピック:

- 他のコンピュータからの既存の証明書のインポート
- SSL 証明書のエクスポート

他のコンピュータからの既存の証明書のインポート

商用 CA から証明書をすでに取得している場合、その証明書とプライベート キーをアプライアンスに転送することもできます。証明書をインポートすると、サーバーがその証明書を使用して、アプライアンスのユーザー トラフィックを保護できます。

証明書とホストは 1 対 1 にマッピングされていないため、証明書に対してホストは選択されません。ワイルドカード証明書を使用すると、1 つの証明書を複数のホストにマッピングできます。

アプライアンスは証明書を PKCS #12 形式で保管します。証明書が異なる形式で保管されている場合は、インポート前に PKCS #12 形式に変換します。変換の実行後に、PKCS #12 ファイルに完全な証明書チェーンが含まれていることを確認してください。

既存の証明書をアプライアンスに転送するには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**SSL certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 [**New (新規)**] をクリックし、メニューから [**Import certificate (証明書のインポート)**] を選択します。

4 [**Import Certificate (証明書のインポート)**] ページで [**Browse (参照)**] をクリックして、証明書をローカル ファイル システム (つまり、AMC にログインしたコンピュータ) からアップロードします。

5 [**Password (パスワード)**]ファイルで、プライベート キーの暗号化に使用したパスワードを入力します。

6 [**Save (保存)**] を選択します。

構成の変更を適用するまでは、アプライアンスは、以前の証明書を使用します。

SSL 証明書のエクスポート

アプライアンスのユーザー トラフィックの保護に使用している SSL 証明書をエクスポートできます。この証明書にはプライベート キーが含まれ、PKCS #12 形式で保存されます。

SSL 証明書をアプライアンスからエクスポートするには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**SSL certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 エクスポートする証明書の隣にあるチェックボックスを選択し、[**Export (エクスポート)**]をクリックします。[**Export Certificate (証明書のエクスポート)**] ページが表示されます。

4 [**Password (パスワード)**]フィールドに、プライベート キーの暗号化に使用するパスワードを入力します。

5 [**Save (保存)**] をクリックし、証明書をローカル ファイル システム (すなわち、AMC にログインしたコンピュータ) にダウンロードします。

6 [**OK**] を選択します。

CA 証明書

どの CA にも、デジタル証明書を要求するエンティティがその CA を「信頼」できるようにするための証明書が必要です。クライアントが CA 証明書を信頼している場合、その CA から発行された他のすべての証明書も自動的に信用することになります。このように、CA 証明書によって、パブリック キー暗号化の基礎の 1 つが形成されます。CA 証明書は、CA 自身 (ルート証明書) またはパブリック キー インフラストラクチャの CA の階層で上位にある認証局 (中間 CA 証明書) のいずれかによって署名されます。

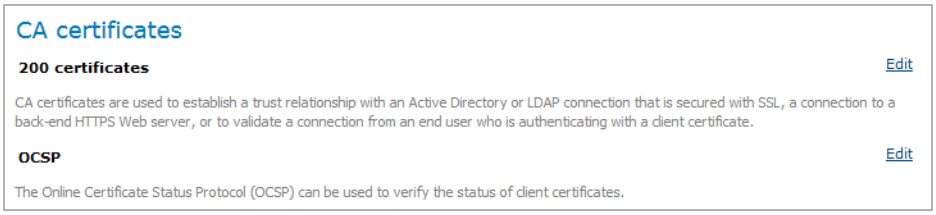
アプライアンスは、CA 証明書を使用して以下を保護します。

- バックエンド LDAP または AD 認証サーバーへの接続
- バックエンド HTTPS Web サーバーへの接続
- デバイス プロファイリング (End Point Control)。アプライアンスに接続するユーザーから送信された証明書の有効性を検証するために使用されます。詳細については、デバイス プロファイルの属性のデバイス プロファイルの属性: クライアント証明書を参照してください。

CA 証明書の使用

アプライアンスには、主要商用 CA の 100 以上のパブリック ルート証明書が含まれています。商用 CA から証明書を取得している場合、そのルート証明書または中間パブリック証明書がアプライアンスにすでにインストールされている可能性があります。ただし、自分自身が CA としての役割を果たす場合は、ルート証明書または中間パブリック証明書をアプライアンスにインポートする必要があります。

証明書のリストを表示するには、[**SSL Settings (SSL 設定)**] ページの [**CA Certificates (CA 証明書)**] エリアにある [**Edit (編集)**] をクリックします。



CA 証明書の削除もここで実行します。

トピック:

- CA 証明書のインポート
- クライアント証明書失効の構成
- CA 証明書の管理

CA 証明書のインポート

アプライアンスに必要な CA 証明書が構成されていない場合は、コピーを取得し、AMC を使用してアプライアンスにインポートする必要があります。この手順は、証明書の使用目的がバックエンド リソースへの接続の保護またはクライアント証明書によるユーザーの認証のどちらであっても同じです。

新しい証明書が [**CA Certificates (CA 証明書)**] ページのアルファベット順リストに表示されます。クライアント証明書認証で使用するために CA 証明書をアップロードすると (そして、変更を適用すると)、ネットワーク サービスは自動的に再起動され、ユーザー接続は終了し、ユーザーの再認証が強制されます。変更をオフピーク時にスケジュールすると良いでしょう。

メモ：

- 証明書を認証サーバー接続の保護に使用する場合は、AMC の [**Configure Authentication Server (設定認証サーバ)**] ページの該当する [**LDAP over SSL**] または [**Active Directory over SSL (SSL 経由の Active Directory)**] の設定が有効になっていることを確認します。
- デフォルトでは、Web プロキシ サービスはバックエンド HTTPS Web サーバーが提示するルート証明書を検証するよう構成されています。この重要なセキュリティ チェックによって、バックエンド サーバーの ID を信頼できるようになります。Web プロキシ サービスの構成を参照してください。
- [**CA Certificates (CA 証明書)**] ページに表示される CA を信頼したくない場合は、該当する CA の隣にあるチェック ボックスを選択し、[**Delete (削除)**] をクリックします。
- デバイスのプロファイルを設定する場合は、同じゾーン内のクライアント証明書を 3 回を超えてチェックしないでください。同じゾーン内のクライアント証明書に対して複数の EPC チェックが存在すると、ユーザーに対してエラー メッセージ (「An error was encountered encoding data to be sent to the Logon Server(ログオン サーバーに送信するデータのエンコード時にエラーが発生しました)」) が表示されます。

CA 証明書をアプライアンスにインポートするには、

1. 信頼できるルート証明書または中間公開証明書を CA から取得します。ほとんどの外部商用 CA は、Web サイトでこの証明書を提供しています。自分の会社が CA の役割も果たしている場合は、サーバー管理者に確認してください。
2. AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。
3. [**CA Certificates (CA 証明書)**] エリアで、**certificates (証明書)** 行の [**Edit (編集)**] をクリックします。
4. [**New...(新規...)**] をクリックします。[**Import CA Certificate (CA 証明書のインポート)**] ページが表示されます。
5. 以下のいずれかを実行します。
   - 証明書がバイナリ形式の場合、[**Choose File (ファイルの選択)**] をクリックして、証明書をローカル ファイル システム (つまり、AMC にログインしたコンピュータ) からアップロードします。
   - 証明書が base-64 エンコード (PEM) テキスト形式の場合は、[**Certificate text (証明書テキスト)**] をクリックして、証明書をテキスト ボックスにペーストします。必ず、BEGIN CERTIFICATE と END CERTIFICATE のバナーが含まれるようにします。
6. この証明書を使用して保護する接続タイプを指定します。

証明書の接続タイプ

接続種別	説明
認証サーバー接続 (LDAPS)	LDAP または Active Directory (AD) 接続を SSL で保護すると、LDAP サーバーまたは AD サーバーを装う試みを排除することで、セキュリティを強化できます。LDAP または AD over SSL を構成するには、LDAP または AD 証明書を付与した CA に対するルート証明書を、SSL の信頼できるルート ファイルに追加する必要があります。
ウェブ サーバー接続 (HTTPS)	バックエンド Web リソースを SSL で保護している (つまり、HTTP ではなく HTTPS を使用している) 場合は、Web プロキシ サービスを構成して、バックエンド サーバーが提示したルート証明書を確認するよう設定する必要があります。この重要なセキュリティ チェックによって、バックエンド サーバーの ID を信頼できるようになります。詳細については、Web プロキシ サービスの構成を参照してください。 バックエンド サーバーのルート証明書がアプライアンスに予めインストールされていない場合は、コピーを取得して AMC にインポートする必要があります。
デバイス プロファイリング（エンド ポイント制御）	EPC は、アプライアンスに接続するユーザーから送信された証明書の有効性を検証するために使用されます。ユーザーを EPC ゾーンに分類するためにクライアント証明書がデバイス プロファイルで使用されている場合は、クライアント証明書をユーザーに発行した CA に対するルート証明書または中間公開証明書をアプライアンスに構成する必要があります。 アプライアンスが指定された証明書の存在をユーザーのコンピューターに照会する際にシステム ストア (*HKLM\SOFTWARE\Microsoft\SystemCertificates*) だけが検索されるように構成することも、ユーザー ストア (*HKCU\Software\Microsoft\SystemCertificates*) も含めるようにすることもできます。
OCSP 応答の検証	OCSP 応答署名証明書は、構成されている OCSP レスポンダからの応答を検証するために使用されます。OCSP 応答署名証明書のインポート時に、**OCSP response verification (OCSP 応答の検証)**を有効にします。これは、PKI 認証サーバーで使用される OCSP レスポンダやサーバーそのものの CA 証明書とは異なる証明書です。

7 「**インポート**」を選択します。[**CA Certificates (CA 証明書)**] ページに確認メッセージが表示されます。

クライアント証明書失効の構成

クライアント デバイスにインストールされている証明書は、ユーザーまたはデバイスを認証して特定のレルムへのアクセスを許可するために使用できます。証明書は通常、有効期限が切れるまで有効ですが、期限が切れる前に無効にすることもできます。例えば、CAは、証明書が正しく発行されたかどうか、あるいは、プライベート キーが無効になっているかどうかを判断したりします。

証明書失効リスト (CRL) を参照すると、証明書の有効性をチェックできます (ロケーション - CRL 配布ポイント、つまり、CDP は通常、X.509 証明書に含まれます)。証明書が有効でないと、そのユーザーはアクセスが拒否されます。CRL は各認証局に対して発行され、その証明書の認証局が発行した証明書のみのステータスを含むことができます。そのため、信用したい CA ごとに別々の階層型 CRL サー

バーが必要です。クライアントは、それぞれの証明書とチェーン内の各レベルの CA を確認するために、チェーン内の各 CA のパブリック キーを知っている必要があります。

OCSP (Online Certificate Status Protocol) と OCSP レスポンダ サーバーを CRL サーバーの代わりに使用して、証明書のステータスをチェックできます。OCSP は、証明書をクライアントから受け取って評価し、サーバーに対して、失効済み、有効、または不明の応答を返します。CRL サーバーのリストは極めて大きくなることがあるため、大規模の組織では、OCSP によって帯域幅を節約できます。OCSP を構成して、任意の数の CA と証明書に動作するようにできます。CA の関係にかかわらず、PKI インフラストラクチャ全体に対して 1 つの OCSP サーバーを構成できます。

メモ：

- CA 証明書で CRL と OCSP の両方が有効な場合は、OCSP だけが使用されます。
- CRL から OCSP へ、または OCSP から CRL へのフォールバックはサポートしていません。

トピック:

- CRL を使用する証明書の管理
- OCSP レスポンダの構成

CRL を使用する証明書の管理

AMC の [**Manage CA Certificate** (CA 証明書の管理)] ページを使用して、個別の証明書に対する証明書失効チェックを構成し、この証明書で保護される接続タイプを判断します。

クライアント証明書の有効性を検証し、証明書失効を構成するには、

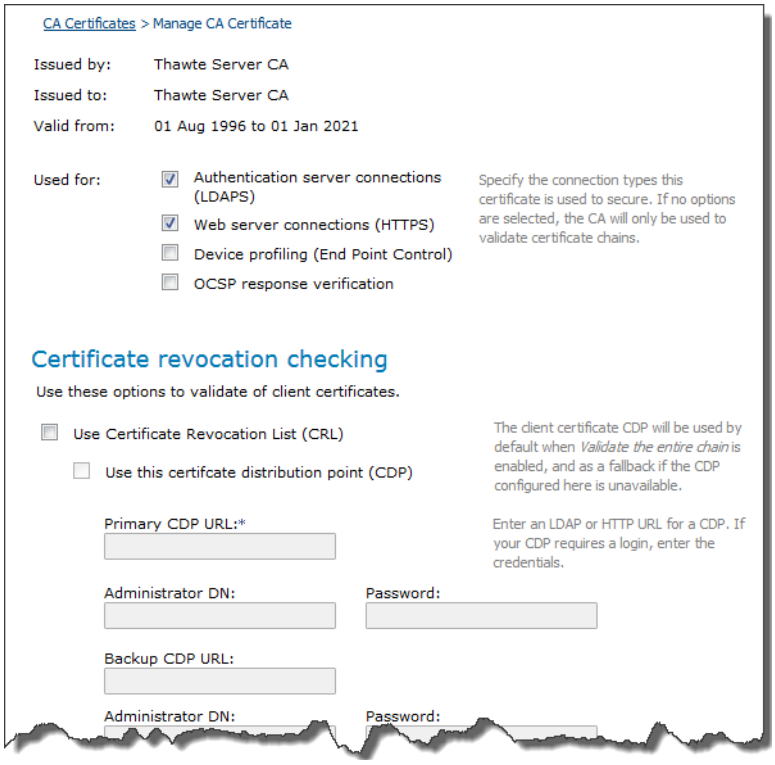
1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**CA Certificates (CA 証明書)**]で、*<番号>* **証明書**行にある[**Edit (編集)**]をクリックします。すべての証明書が表示されます。

3 証明書の詳細を表示するには、2 番目の列のプラス記号 (+) をクリックします。証明書を編集するには、そのリンクをクリックします。例えば、

a 「*Thawte Server CA*」の隣にあるプラス記号をクリックすると、Thawte Consulting の証明書の詳細が表示されます。

b リンクをクリックして編集します。[**Manage CA Certificate (CA 証明書の管理)**]ページが表示されます。



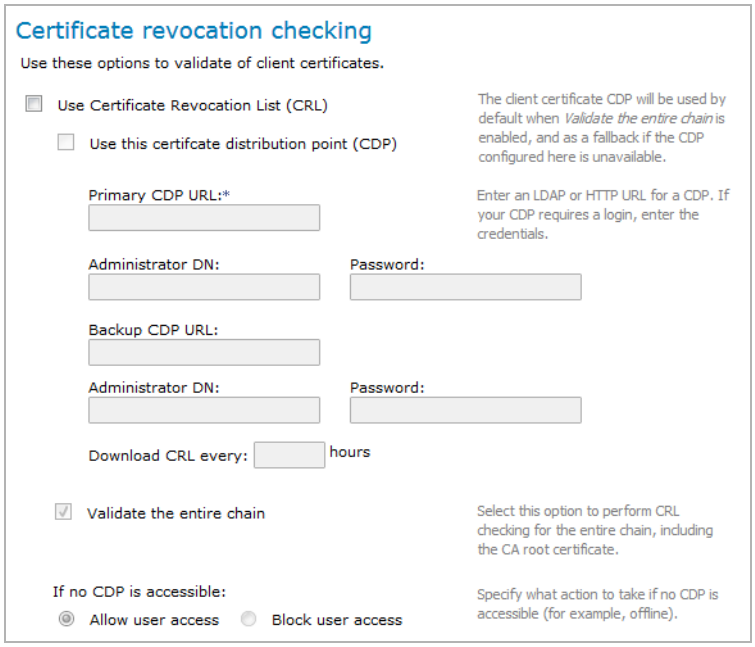
4 [**Used for (用途)**] エリアで、この証明書を使用して保護する接続タイプを指定します。

- **認証サーバー接続 (LDAPS)** : PKI 認証サーバーの構成を参照してください。
- **Web サーバー接続 (HTTPS)**: CA 証明書を参照してください。
- **デバイス プロファイリング (エンド ポイント制御)** - デバイス プロファイルの属性のデバイス プロファイルの属性: クライアント証明書を参照してください。

- **OCSP 応答検証** - 構成された OCSP 応答者からの応答を検証します。

5 CRL 設定を指定するには、[**Certificate revocation checking (証明書失効確認)**] エリアの [**Use Certificate revocation list (証明書失効リスト)**] を確認します。

> **重要**：CRL の形式は DER ベース (`.crl`) である必要があり、アプライアンスは PEM 形式で作成された CRL は使用できません。



6 アプライアンスが CRL 配布ポイント (CDP) から失効した証明書のリストを取得します。この CDP のロケーションを指定します。

- CDP は通常、証明書そのもので指定されます。デフォルトでは、アプライアンスは[**CDP from the client certificate (クライアント証明書の CDP)**]を使用します。
- URL を指定することもできます。[**Use this certificate distribution point (CDP) (この証明書配布ポイント (CDP) を使用)**]チェックボックスをチェックします。ログインが必要であれば、クレデンシャルを入力します。

7 [**Use this certificate distribution point (CDP) (この証明書配布ポイント (CDP) を使用)**]を選択した場合は、[**Download CRL every <n> hours (<n> 時間ごとに CRL をダウンロード)**]オプションを使用して、CRL を検索する頻度を指定できます。ダウンロード間隔を指定しない場合は、古い CRL の有効期限が切れたときに新しい CRL が取得されます (CRL は頻繁に更新されるため、証明書が無効になると、その情報がタイムリーに配布されます)。

8 アプライアンスが、クライアント証明書をこのリストと照会します。CA ルート証明書から開始して証明書のチェーン全体の CRL チェックを実行するには、[**Validate the entire chain (チェーン全体を検証)**]チェックボックスを選択します。

9 [**Allow user access (ユーザー アクセスを許可)**] または [**Block user access (ユーザー アクセスをブロック)**] を選択することで、CDP にアクセスできない場合にユーザーにアクセスを許可するか拒否するかを指定します。指定したリモート CDP がオフラインの可能性もあり、証明書で指定されていない場合もあります (X.509 標準では、オプション項目であり、必須項目ではありません)。

10 [**Save (保存)**] を選択します。

OCSP レスポンダの構成

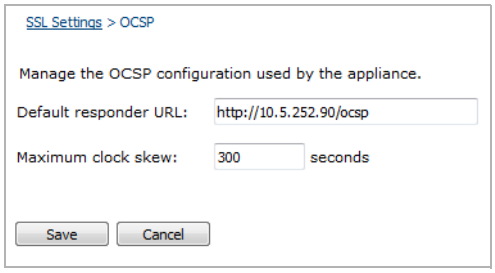
AMC の [**OCSP**] ページを使用して、OCSP レスポンダのグローバル設定を構成します。PKI 認証サーバーの構成時に、OCSP レスポンダを参照できます。

メモ：CA 証明書をインポートして OCSP を有効にするだけでは、OCSP は動作しません。使用する CA 証明書の OCSP 応答署名証明書をインポートし、インポート時に [OCSP response verification (OCSP 応答の検証)] を有効にする必要があります。CA 証明書のインポートを参照してください。

OCSP レスポンダを構成するには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**CA Certificates (CA 証明書)**] の **OCSP** 行の [**Edit (編集)**] をクリックします。[OCSP] ページが表示されます。



3 [**Default responder URL (既定応答者 URL)**] フィールドに OCSP レスポンダ サーバーの URL を入力します。

4 [**Maximum clock skew (最大クロック スキュー)**] フィールドに、OCSP の応答時間とローカル時間の許容される最大時間差を秒数で入力します。既定値は **300** 秒、最小値は 1 秒、最大値は 3600 秒です。

5 [**Save (保存)**] を選択します。

CA 証明書の管理

このセクションでは、アプライアンスでの証明書の管理に関連する作業について説明します。証明書のインポートについては、CA 証明書のインポートで説明しています。

トピック:

- CA 証明書の詳細の表示
- 証明書とホストのマッピング
- CA 証明書のエクスポート
- CA 証明書の削除

CA 証明書の詳細の表示

タイトル、発行者、開始日と終了日、シリアル番号、MD5 チェックサムなどのアプライアンス証明書の詳細データを表示できます。新しくインポートした証明書の詳細データは、構成の変更を適用するまで表示されません。

CA 証明書の詳細を表示するには、

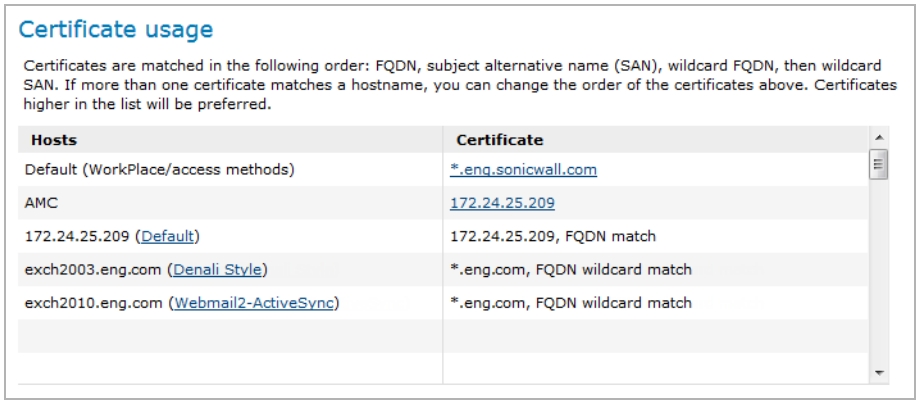
1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**CA Certificates (CA 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 詳細を表示する証明書の左にあるプラス記号 (+) をクリックします。

証明書とホストのマッピング

アプライアンスの複数のホストが 1 つのワイルドカード証明書を使用できるため、[**Certificate usages (証明書使用率)**] テーブルで 1 つの証明書を複数のホストのセットにマッピングします。ホストのセットは、同じ IP アドレスのリソースにマッピングされた 1 つ以上の WorkPlace サイト、Exchange サイト、またはカスタム FQDN として定義されます。どのホストのセットも同じワイルドカード証明書を使用する必要があるため、[**Certificate usages (証明書使用率)**] テーブルでの証明書のマッピングでは、1 つの項目として処理されます。AMC は、シングル ホーム アプライアンスの他のホストと同じ IP アドレスであったとしても、別のホストとして処理されます。



新しい証明書を 1 つのホストまたはホストのセットにマッピングするには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**SSL Certificates (SSL 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 [**Certificate usages (証明書使用率)**] テーブルの [**Certificates (証明書)**] 列で、証明書をクリックしてドロップダウンで証明書を選択し、ドロップダウンで証明書を選択できる組み込みエディターをアクティブにします。

4 証明書を選択します。ホストを個別に選択する場合は、どの証明書でも選択できます。複数のホストのセットの場合は、ワイルドカード証明書のみを選択できます。

5 [**OK**] を選択します。

CA 証明書のエクスポート

CA 証明書とそのプライベート キーをローカル コンピュータにエクスポートできます。証明書は PKCS #12 形式で保存されます。

CA 証明書をエクスポートするには、

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**CA Certificates (CA 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 エクスポートする証明書の左にあるチェックボックスを選択します。

4 [**Export (エクスポート)**] を選択します。

5 [**Password (パスワード)**]フィールドにプライベート キーを暗号化したパスワードを入力します。

6 [**Save (保存)**] を選択します。証明書は (デフォルトでは) `server_cert.p12` という名前のファイルに保存されます。

CA 証明書の削除

証明書のリストを管理しやすくするために、必要のない証明書を削除できます。

CA 証明書を削除するには

1 AMC のメイン ナビゲーション ページから、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**CA Certificates (CA 証明書)**] エリアの [**Edit (編集)**] をクリックします。

3 削除する証明書の左にあるチェック ボックスを選択します。

4 [**Delete (削除)**] を選択します。

証明書の使用に関するよくある質問

トピック:

- 証明書を非商用 CA から取得するにはどうすればよいですか。
- 証明書と CRL の有効期限はいつ切れますか。
- Secure Mobile Access はSAN 証明書をサポートしますか？
- 中間証明書はエンドユーザー証明書の検証に対応していますか？
- アプライアンスの CA 証明書にはどのようなものがあり、それぞれがどのように使用されますか。
- アプライアンスの保管できる CA 証明書の数はいくつですか。
- 他のツールで生成したプライベート キーや CSR をアプライアンスにインポートできますか。
- AMC 証明書はどこに保管されますか。
- すべての CA 証明書をアプライアンスに置いておくべきですか。または、必要なものだけを置いておくべきですか。

証明書を非商用 CA から取得するにはどうすればよいですか。

取得するプロセスは、商用 CA から証明書を取得する場合とほぼ同じですが、非商用 CA (Microsoft Self-Signed Certificate Authority など) の場合は CSR に送信する必要があります。この手順については、ステップ2: CSR を商用 CA に送信するに概要が記載されています。

証明書と CRL の有効期限はいつ切れますか。

自己署名証明書は 5 年間有効です。サードパーティの証明書の場合は、証明書の発行者によって有効期限が異なります。詳細については、CA にお問い合わせください。証明書失効リスト (CRL) の有効期限はこれよりはるかに短く、数日、場合によっては数時間です。

証明書と CRL を使用する場合は、アプライアンスのクリックが正確であることが重要です。クロックは、これらの有効期限が切れる時期を判断する際に使用されます。

Secure Mobile Access はSAN 証明書をサポートしますか？

サブジェクト代替名 (SAN) 証明書は、WorkPlace、WorkPlace サイト、および接続トンネルでサポートされています。証明書 (UCC--ユニファイド コミュニケーション証明書とも呼ばれます) は、一連のクライアントと複数の異なる SSL または TLS のサービスとの間の通信チャネルを安全に暗号化するために使用されます。

SAN 証明書は、一般的な導入環境で必要とされる、IP アドレス/ホスト名/証明書のセットを簡素化します。1 つの SAN 証明書、1 つの IP アドレスで、複数の異なる SSL または TLS で保護された Web やクライアント/サーバーのサービスを使用でき、追加の IP アドレスを構成する必要はありません。また、SAN を同じ IP アドレスの異なるホスト名にも使用できるため、SSL 証明書の共通名を 1 対 1 で FQDN にマッピングする必要はありません。

メモ：SAN 証明書と CSR (証明書署名要求) では、IPv4 アドレスのみをサポートしています。

以下の点が改善されました。

- SAN 関連の機能を、アプライアンスの外部からではなく、AMC で生成できます。
    - SAN を使用する CSR
    - SAN エントリを使用する自己署名証明書
- WorkPlace サイト、カスタム FQDN URL リソース、および ActiveSync リソースを、既存の SAN 証明書を使用して作成できます。
- グローバル ロード バランシングは、元の Web 要求を使用して、デフォルトの WorkPlace サイトではなく、ロード バランサにトラフィックを渡します。
- Connect Tunnel は、WorkPlace サイトへの接続をシームレスに処理し、WorkPlace サイトは、関連付けられている IP アドレスの数に関係なく、IP アドレス、FQDN、または SSL 証明書の組み合わせを使用します。

Administrator は、SAN 証明書を生成、インポート、処理したり、その SSL 証明書を Workplace、ActiveSync、カスタム FQDN URL マッピング、または Tunnel ベースのアクセス サービスに使用したりできます。

中間証明書はエンドユーザー証明書の検証に対応していますか？

はい。エンド ユーザーの検証で中間証明書をサポートしています。これには、PKI および LDAP 証明書の方法が含まれます。これにより、ルート認証局の信頼がなくても、中間認証局をインポートして証明書チェーンを評価できます。

クライアント マシンは、中間認証局が発行したクライアント証明書を使用できます。クライアント証明書が Windows 7 に直接インポートされる場合、クライアント証明書は個人ストアに保存され、中間証明書は中間 CA ストアにインポートされ、ルート CA 証明書はルート CA ストアにインポートされ

ます。これが推奨される方法であり、証明書が、トンネル クライアントと PKI 認証を使用する ExtraWeb クライアントで動作します。3 つの証明書すべてが個人ストアに保存されると、certmgr.msc を使用してクライアント証明書がインポートされ、Connect Tunnel にエラー メッセージが表示され、アクセスが拒否されます。そのため、この構成は推奨されません。

アプライアンスの CA 証明書にはどのようなものがあり、それぞれがどのように使用されますか。

アプライアンスの CA 証明書のリストを表示するには、メイン ナビゲーション メニューから [**SSL Settings (SSL 設定)**] をクリックし、[**CA Certificates (CA 証明書)**] エリアの [**Edit (編集)**] をクリックします。デフォルトでは、リストの任意の証明書を最大 3 種類の接続タイプ (認証サーバー、セキュア Web サーバー、クライアント証明書) の保護に使用できます。証明書をクリックして、保護する接続タイプを設定します。

アプライアンスの保管できる CA 証明書の数はいくつですか。

ルート ファイルには、必要な数の証明書を入れることができます。追加の CA 証明書のインポート方法については、CA 証明書のインポートを参照してください。

他のツールで生成したプライベート キーや CSR をアプライアンスにインポートできますか。

プライベート キーと CSR は、Setup Tool または証明書生成ツールを使用して、アプライアンスで生成する必要があります。ただし、プライベート キーや CSR を、AMC 内のサーバー証明書の管理の手順で、SMA アプライアンス間でコピーできます。コピーした証明書は、AMC で変更すると上書きされます。

AMC 証明書はどこに保管されますか。

AMC の自己署名証明書は、アプライアンスの `/usr/local/app/mgmt-server/sysconf/active/` に保存されます。

AMC の場合、ほとんどの環境では自己署名証明書で十分です。ただし、信頼できるネットワーク内で AMC を使用することが重要です。自己署名証明書は、受動的な傍受の防止策にはなりますが、能動的な攻撃からの防止策にはなりません。

すべての CA 証明書をアプライアンスに置いておくべきですか。または、必要なものだけを置いておくべきですか。

利便性のために、アプライアンスには 100 以上の CA 証明書が入っています。導入環境の安全性を向上させるために、このリストを削除し、クライアント証明書、LDAPS、HTTPS に必要な CA 証明書だけを入れることもできます。リストが短いほど、管理が容易になります。

ユーザー認証の管理

認証とは、ユーザーの ID を検証し、当人であることを確認するプロセスです(認証は許可とは異なります。認証では ID を検証し、許可はアクセス権を指定します)。このセクションでは、外部認証サーバーを参照する方法を説明します。

ユーザー認証を管理するには、AMC に 1 台以上の外部認証サーバーを定義し、それらの認証サーバーを参照するレルムをセットアップする必要があります。そして、ユーザーはこれらのレルムにログインすることになります。レルムの詳細については、レルムおよびコミュニティの使用を参照してください。テスト用に、ローカル ユーザー ストレージの構成に記載されている方法で、アプライアンスにローカル認証レポジトリを構成することもできます。

トピック:

- 中間証明書について
- 認証サーバーの構成
- マイクロソフト アクティブ ディレクトリ サーバーの設定
- LDAP と LDAPS 認証の構成
- RADIUS 認証の構成
- ユーザーがマップしたトンネルのアドレッシング
- RSA サーバー認証の構成
- PKI 認証サーバーの構成
- カスタム証明書の追加フィールド
- SAML ベースの認証サーバーの構成
- シングル サインオン認証サーバーを設定する
- CAM を使用したレガシーおよびフェデレーション型 ID SSO のサポート
- RSA ClearTrust 認証の使用
- One Identity Defender
- ローカル ユーザー ストレージの構成
- LDAP および AD 認証構成のテスト
- 連鎖式認証の構成
- レルムでのグループ アフィニティ チェックの有効化
- ワンタイム パスワードの使用によるセキュリティの強化
- 個人用機器認証の設定

中間証明書について

認証サーバーを構成することで、チェーン全体を検証することなく、中間 CA を信頼できるようになります。この方法には、複数の署名認証局で何人かがルート CA サーバーからリモートである場合の証明書配布の管理などの利点があります。そのような状況でこの方法を使用しないと、証明書を発行できません。また、いずれかの署名認証局でセキュリティが侵害されても、ネットワーク全体のセキュリティは侵害されないため、セキュリティが強化されるという利点もあります。

信頼できる中間証明書を構成する方法については、PKI 認証サーバーの構成を参照してください。

例えば、会社のネットワークに接続されていないシステムにルート証明書署名認証局を作成したとします。次に、ネットワークの複数のセクター (多くの場合は、組織や部門ごと) に展開する、信頼できる中間署名認証局証明書のセットを発行します。VPN の場合は、マシンや個人の証明書をクライアント システムに配布する方法が一般的です。

あるいは、VeriSign や Thawte などの認証局の署名証明書を取得する方法もあります。この場合、実際にはメインの CA が中間 CA です。

SSL ルールにより、チェーン全体を評価するためには、ルート CA 証明書にアクセス可能である必要があります。ところが、アプライアンスでは、CA 証明書のインポートの目的が CA 証明書を信頼するためであっても、CA 証明書をインポートして中間 CA に対して証明書チェーンを評価し、アプライアンスを信頼するためであっても、区別されません。CA 証明書のインポート時にオプションを選択しないと、CA は証明書チェーンの評価のためだけに使用されます(オプションでは、証明書を使用して保護する接続タイプ: （オプションは、証明書が保護用に使用される接続タイプです: 認証サーバー接続 (LDAPS)、Web サーバー接続 (HTTPS)、およびデバイス プロファイリング (End Point Control) を選択します)。証明書チェーンの評価のみに使用する CA 証明書はすべて、クライアント証明書の認証や EPC 証明書の強制で、信頼できる署名者とはなりません。

中間 CA が署名したクライアント証明書をエンド ユーザーが提示すると、アプライアンスは署名認証局を信頼できるものであると仮定され、ユーザーは通常通りに認証され、リソースへのアクセスが許可されます。

信頼できる中間 CA のルート CA が発行したクライアント証明書をエンド ユーザーが提示すると、管理者が信頼する目的でルート CA もインポートしていない限り、有効で信頼できる証明書がないため、エンド ユーザーの認証の試行が失敗します。

チェーン評価のみに存在する、CA が署名した証明書をクライアントが提示すると、その証明書は拒否され、結果として、認証が失敗するか、証明書の認証が失敗して証明書 EPC のデバイス プロファイルが一致しなくなります。

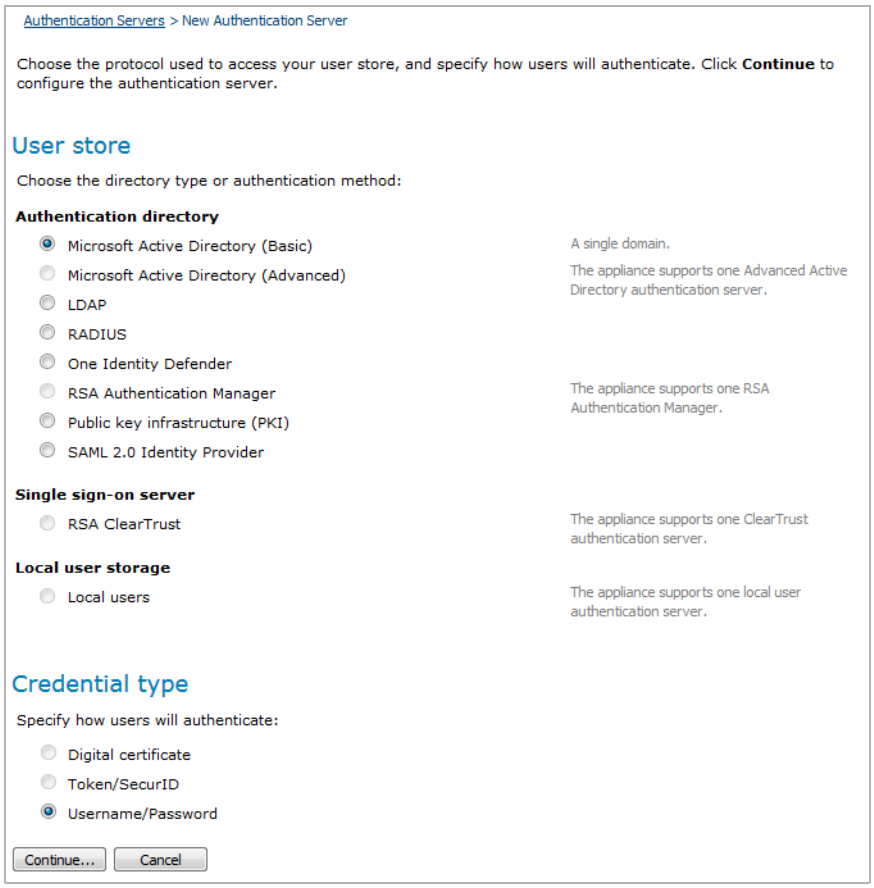
認証サーバーの構成

認証サーバーの構成認証のセットアップでは、ディレクトリ (LDAP、Microsoft Active Directory、またはアプライアンスのローカルの認証ストアなど)、認証方式 (ユーザー名/パスワード、トークンまたはスマート カード、またはデジタル証明書など)、および認証プロセスの独自の構成項目 (例えば、LDAP 検索ベース、カスタム プロンプトやメッセージの追加など) を構成します。SMA アプライアンスは、主要な認証ディレクトリや認証方式をサポートしています。

あるレルムの認証サーバーを参照し、ユーザーをレルムに対応させると、アプライアンスがユーザーのクレデンシャルを指定された認証レポジトリに保管されているクレデンシャルと比較してチェックします。また、連鎖式 (2 要素) 認証もセットアップできます。詳細については、連鎖式認証の構成を参照してください。

認証サーバーを構成するには、

1 AMC のメイン ナビゲーション ページから [**Authentication Servers (認証サーバ)**] をクリックし、[**New...(新規...)**] をクリックします。



2 [**User store (ユーザ ストア)**] エリアで、構成するディレクトリ タイプまたは認証方式を指定します。

ディレクトリ タイプまたは認証方法の選択

認証ディレクトリ	クレデンシャル タイプ	詳細情報
マイクロソフト アクティブ ディレクトリ Microsoft Active Directory ツリー	• ユーザー名/パスワード	マイクロソフト　アクティブ ディレクトリ サーバーの設定
LDAP	• ユーザー名/パスワード • デジタル証明書	LDAP と LDAPS 認証の構成
RADIUS	• ユーザー名/パスワード • トークンベースの認証 (SecurID や SoftID など)	RADIUS 認証の構成
RSA Authentication Manager Server	• トークンベースの認証 (SecurID や SoftID など)	RSA サーバー認証の構成
パブリック キー インフラストラクチャ (PKI)	• デジタル証明書 (証明書失効チェックをオプションで搭載)	PKI 認証サーバーの構成
SAML 2.0 ID プロバイダ	• ユーザー名/パスワード	SAML ベースの認証サーバーの構成

ディレクトリ タイプまたは認証方法の選択

認証ディレクトリ	クレデンシャル タイプ	詳細情報
RSA ClearTrust (シングル サインオン)	• 該当なし	シングル サインオン認証サーバーを設定する
ローカル ユーザ (ローカル ユーザー ストレージ)	• ユーザー名/パスワード	ローカル ユーザー ストレージの構成

3 [**Credential type (クレデンシャル タイプ)**] で認証サーバーのクレデンシャル タイプを選択します (選択できるタイプは、選択した [**User store (ユーザ ストア)**] によって異なります)。

4 [**Continue...(続ける...)**] を選択します。構成プロセスの次の手順については、前の [**User store (ユーザ ストア)**] で選択した項目に対応するリンクの手順に従ってください。

認証サーバーを設定した後のタスクの詳細については、以下を参照してください。

- 複数の認証サーバーの定義
- 認証チェックの無効化
- 連鎖式認証の構成
- レルムでのグループ アフィニティ チェックの有効化
- ワンタイム パスワードの使用によるセキュリティの強化

複数の認証サーバーの定義

SMA アプライアンスは、複数の認証サーバーの定義と使用をサポートしています。*レルム*は、2 つの認証サーバーのうちいずれかを参照して、ユーザーに対してどのアクセス エージェントをプロビジョニングし、どの End Point Control (ある場合) の制約を課すかを決定します。レルムの詳細については、ユーザー、グループ、コミュニティ、レルム参照してください。

次に、レルムが参照する複数の認証サーバーを使用する例を示します。

- **連鎖式認証 (2 台の認証サーバー)**

  例: トークン/SecurID を使用する RADIUS と、ユーザー名/パスワードを使用する LDAP

  レルムにログインするユーザーが 2 台のサーバーで認証されます。AMC を構成して、ユーザーにプロンプトが 1 回だけ提示されるようにすることができます。詳細については、連鎖式認証の構成を参照してください。

- **認証と許可の処理に異なるサーバーを使用する**

  例: トークン/SecurID を使用する RADIUS と、Active Directory (グループ情報)

  ユーザーが 1 つのレポジトリで認証され、ユーザーのグループ情報は 2 番目のレポジトリから渡されます。詳細については、レルムでのグループ アフィニティ チェックの有効化を参照してください。

- **複数のクレデンシャル タイプと 1 つの認証サーバー**

  例: ユーザー名/パスワードを使用する RADIUS と、トークン/SecurID を使用する RADIUS

  社員はユーザー名とパスワードでログインし、コールセンターの従業員は SecurID トークンでログインする場合などが考えられます。この場合、*employee* レルムと *callcenter* レルムを作成し、それぞれが適切なクレデンシャル タイプと RADIUS サーバーを参照するようにします。

- **同じディレクトリ/認証方式の複数のインスタンスが異なるバックエンド サーバーを使用する**

例: 異なる RADIUS サーバーを使用する 2 つの RADIUS/パスワード インスタンス

この場合、それぞれの適切なサーバー情報で 2 つの認証サーバーを定義します。

- **同じディレクトリ / 認証方式の複数のインスタンスが同じサーバーに存在し、異なる方法で構成されている**

  例: ユーザー名/パスワードを使用する LDAP の 2 つのインスタンスが同じサーバーに存在し、異なる検索ベースを使用する

  この場合、レルムごとにディレクトリ内の異なるサブツリーを検索します。例えば、相手 A がある LDAP サブツリー内にあり、相手 B が他の LDAP サブツリーにある場合です。例えば、Partner A が特定の LDAP サブツリーにあり、Partner B が別のサブツリーにあると仮定します。*partnerA* レルムと *partnerB* レルムを定義し、それぞれに適切な検索ベースを構成します。

認証チェックの無効化

認証サーバーの構成時に、認証に使用するグループ情報のクエリーをオプションで無効にできます。アクティブ ディレクトリ、アクティブ ディレクトリ Tree、および LDAP サーバーなどの、認証に使用するグループ情報を含めることができるサーバーごとに、[**Use this authentication server to check group membership (この認証サーバーを使用してグループ メンバーシップを確認する)**]チェックボックスを使用できます。

通常、ディレクトリ サーバーを認証の一部として使用する場合は、グループ情報もここに置いて、ポリシー許可で使用するようにしたいと考えるものです。ところが、場合によっては、ディレクトリ サーバーはセカンダリ認証に使用されていて、グループ情報が含まれていないことがあります。あるいは、セカンダリ認証サーバーがユーザーと同じ ID を使用していないこともあります。

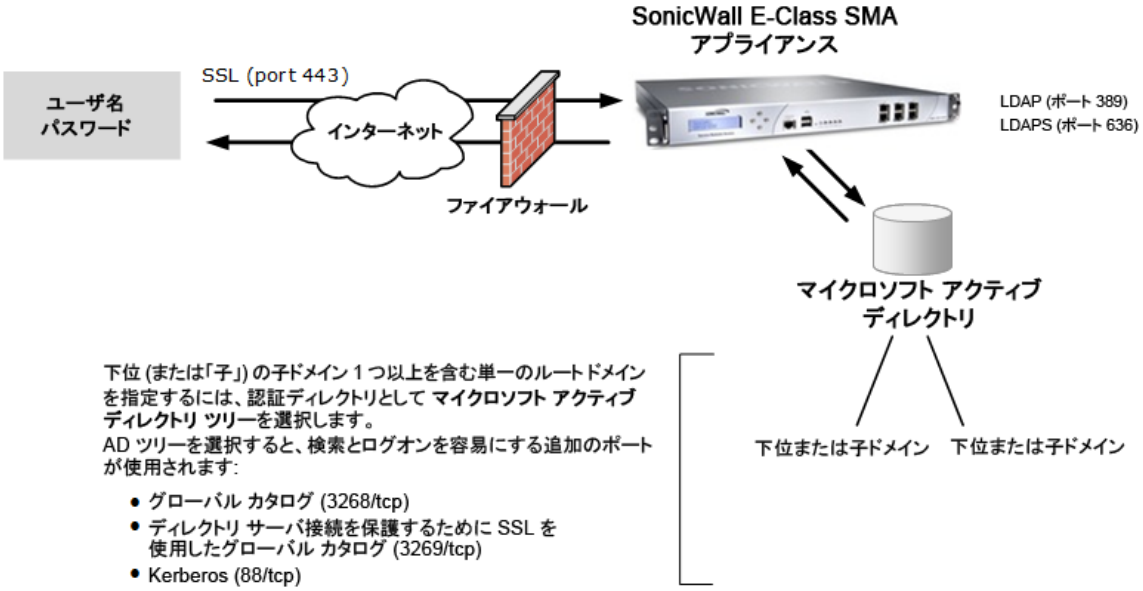
グループのクエリーをプライマリとセカンダリの両方のサーバーで実行すると、認証プロセスに時間がかかります。けれども、ユーザー名が 2 つのサーバーで異なると、プライマリ サーバーの名前を使用するグループのクエリーが、セカンダリ サーバーではエラーになります。アプライアンスのポリシーではデフォルトが常に closed であるため、このようなエラーによってエンド ユーザーに対して拒否のルールが提供されることになります。グループ許可チェックをセカンダリ サーバーで無効にすることで、これらの問題を回避できます。

グループ チェックが認証サーバーで無効になっていると、そのサーバーはレルム構成ページの利用可能なアフィニティ サーバーのリストから選択できません。これに対し、認証サーバーがいずれかのレルムでアフィニティ サーバーとして使用されていると、その認証サーバーでグループ チェックを無効にできません。詳細については、レルムでのグループ アフィニティ チェックの有効化を参照してください。

マイクロソフト アクティブ ディレクトリ サーバーの設定

アプライアンスは、シングル ルート ドメインまたは複数の下位 (子) のドメインのいずれかで構成されているマイクロソフト アクティブ ディレクトリ (AD) でユーザ名/パスワード クレデンシャルを検証できます。マイクロソフト アクティブ ディレクトリの設定オプションで、一般的なアクティブ ディレクトリの設定オプションを紹介しています。

マイクロソフト アクティブ ディレクトリの設定オプション



アプライアンスが AD サーバーと通信できるようにするために、ファイアウォールまたはルーターを変更する必要があります。アプライアンスは、標準の LDAP ポートと LDAPS ポートを使用して、Active Directory と通信します。

- LDAP (389/tcp)
- LDAP over SSL (636/tcp)

Microsoft Active Directory ツリーには、検索とログオンに利用される追加ポートがあります。

- グローバル カタログ (3268/tcp)
- SSL を使用するグローバル カタログ (3269/tcp)
- Kerberos (88/tcp)

AD サーバーの構成後に、テスト接続を確立することで、レルム構成の設定を検証できます。詳細については、LDAP および AD 認証構成のテストを参照してください。

トピック:

- ユーザー名とパスワードを使用する Active Directory の構成
- 複数の Active Directory ツリーの構成
- Active Directory 認証を行うための LDAP の構成
- Active Directory 認証のための LDAP の例

ユーザー名とパスワードを使用する Active Directory の構成

メモ：

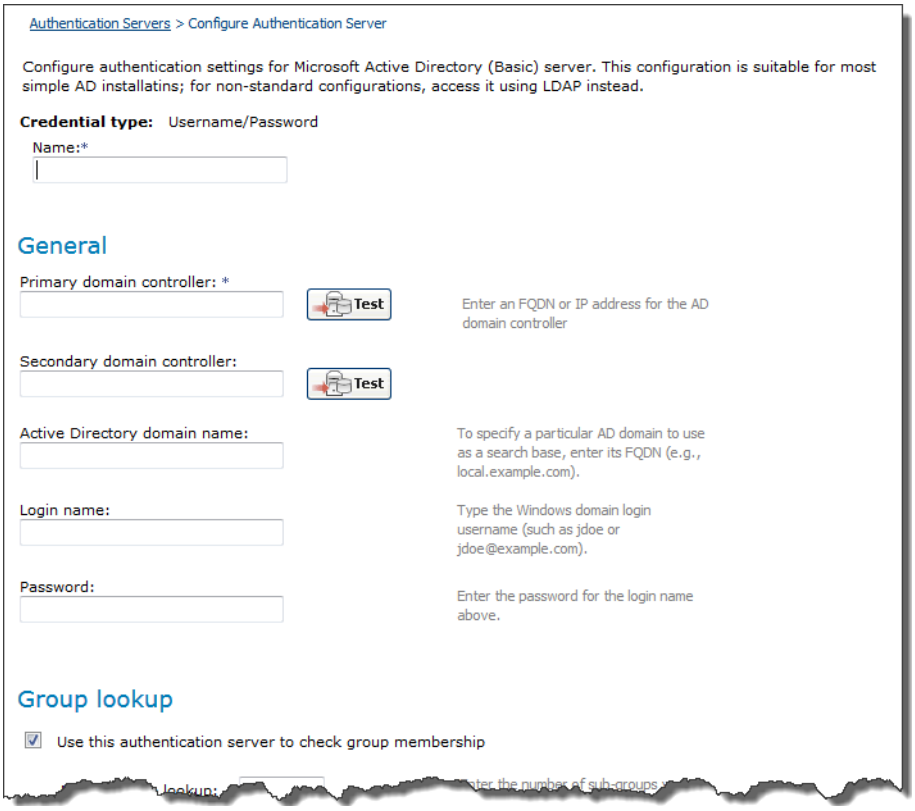
- Active Directory でデジタル証明書を使用している場合、AD を LDAP レルムとして構成する必要があります。Active Directory 認証を行うための LDAP の構成を参照してください。
- AD 認証サーバーに下位 (子) のドメインがある場合、詳細については、複数の Active Directory ツリーの構成を参照してください。

ユーザー名/パスワード検証を使用するアクティブ ディレクトリ認証サーバーを構成する場合、次の手順を実行します。

1 AMC のメイン ナビゲーション ページから [**Authentication Servers (認証サーバ)**] をクリックし、[**New...(新規...)**] をクリックします。

2 [**User store (ユーザー ストア)**]の[**Microsoft Active Directory (Basic) (マイクロソフト アクティブ ディレクトリ (ベーシック))**]をクリックします。

3 AD で選択できる唯一の **Credential type (クレデンシャル タイプ)**は**ユーザ名/パスワード**です。[**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



4 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

5 [**Primary domain controller (プライマリ ドメイン コントローラ)**]フィールドに、AD ドメインコントローラの IP アドレスまたはホスト名を入力します。フェイルオーバー サーバーを使用している場合 (オプション)、[**Secondary domain controller (セカンダリ ドメイン コントローラ)**]ボックスでそのアドレスを指定します。

AD サーバーが一般的なポート (非暗号化接続の場合は 389、SSL接続の場合は 636) 以外でリッスンする場合、コロンの後に接尾辞としてポート番号を指定できます (例えば、`ad.example.com:1300`)。

6 特定の AD ドメインを指定する場合は、[**Active Directory domain name (アクティブ ディレクトリのドメイン名)**]フィールドに入力します。ここでは、検索ベースとして使用するドメイン (つまり、適切な `cn=users` コンテナが含まれるドメイン) を指定する必要があります。例えば、*marketing* などの単一のドメインを検索したい場合は、「`marketing.example.com`」と入力します。会社のドメイン全体を検索したい場合は、「`example.com`」と入力します。ドメインを指定しないと、アプライアンスは、ドメイン コントローラで最初に見つかったデフォルト ネーミング コンテキストを検索します。

7 AD 検索を実行するには、アプライアンスが Active Directory にログインする必要があります (アノニマス検索を許可するよう AD を構成している場合を除く)。[**Login name (ログイン名)**]フィールドに、Windows ドメインへのログインに使用するユーザー名または **sAMAccountname** 属性を入力します (例えば、「`jdoe`」や「`jdoe@example.com`」)。

ログイン名は、そのドメイン コントローラの管理者などの、検索の実行とユーザー レコードの参照の権限があるユーザーのものである必要があります。これらの権限があれば、管理者ではないユーザーを指定することもできます。

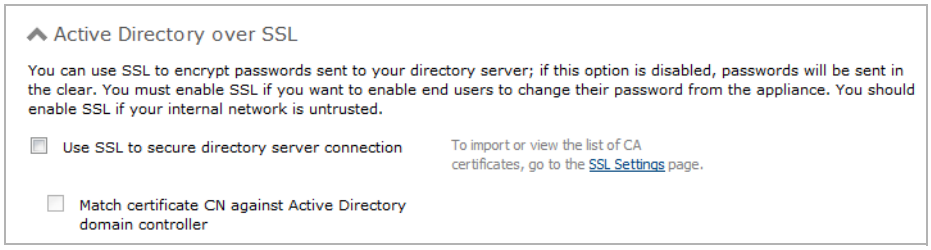
AD ドメインを指定すると、アプライアンスはそのドメインでユーザーを検索します。ドメインを指定しないと、アプライアンスは、ドメイン コントローラで最初に見つかったデフォルト ネーミング コンテキストを検索します。ユーザー情報がこれらのロケーションのいずれにも保存されていない場合は、このレルムを LDAP レルムとして構成する必要があります。Active Directory 認証を行うための LDAP の構成を参照してください。

8 **Login name (ログイン名)**に対応するパスワードを [**Password (パスワード)**] に入力します。クレデンシャルを入力した後に、指定したそれぞれのサーバーで [**Test (テスト)**] ボタンをクリックして、接続をテストします。

9 [**Group lookup (グループ ルックアップ)**] の下に表示される情報を入力します。

- このサーバーのグループ チェックを有効にするには、[**Use this authentication server to check group membership (この認証サーバーを使用してグループのメンバーシップを確認する)**] チェックボックスを選択します。このボックスを選択解除すると、グループ チェックの動作だけに適用されるため、ネストされたコントロールは無効になります。このチェックボックスを選択解除すると、LDAP、AD、または AD のツリーの認証サーバーを、許可チェックを有効にせずに構成できます。これにより、スタックド/アフィニティ認証のサポートが向上し、効率が向上します。
- 検索の深度 (検索対象にいくつのサブグループを入れるか) を指定するには、[**Nested group lookup (ネストされたグループの参照)**]チェックボックスに数値を入力します。このタイプの検索ではアクティブ ディレクトリ ツリー全体の検索が必要になるため、時間がかかる可能性があります。[**Cache group checking (グループ チェックをキャッシュ)**]をオンにすることを強く推奨します。
- ディレクトリの負荷を軽減し、パフォーマンスを向上させるには、属性グループや静的グループの検索結果をキャッシュします。[**Cache group checking (グループ チェックをキャッシュ)**]チェックボックスを選択して、[**Cache lifetime (キャッシュの持続時間)**]ボックスにキャッシュの持続時間を秒単位で入力します。デフォルト値は *1800* 秒 (30 分) です。

10 AD 接続を SSL で保護するには、[**Active Directory over SSL (SSL 経由の Active Directory)**] エリアを展開し、次の設定を構成します。

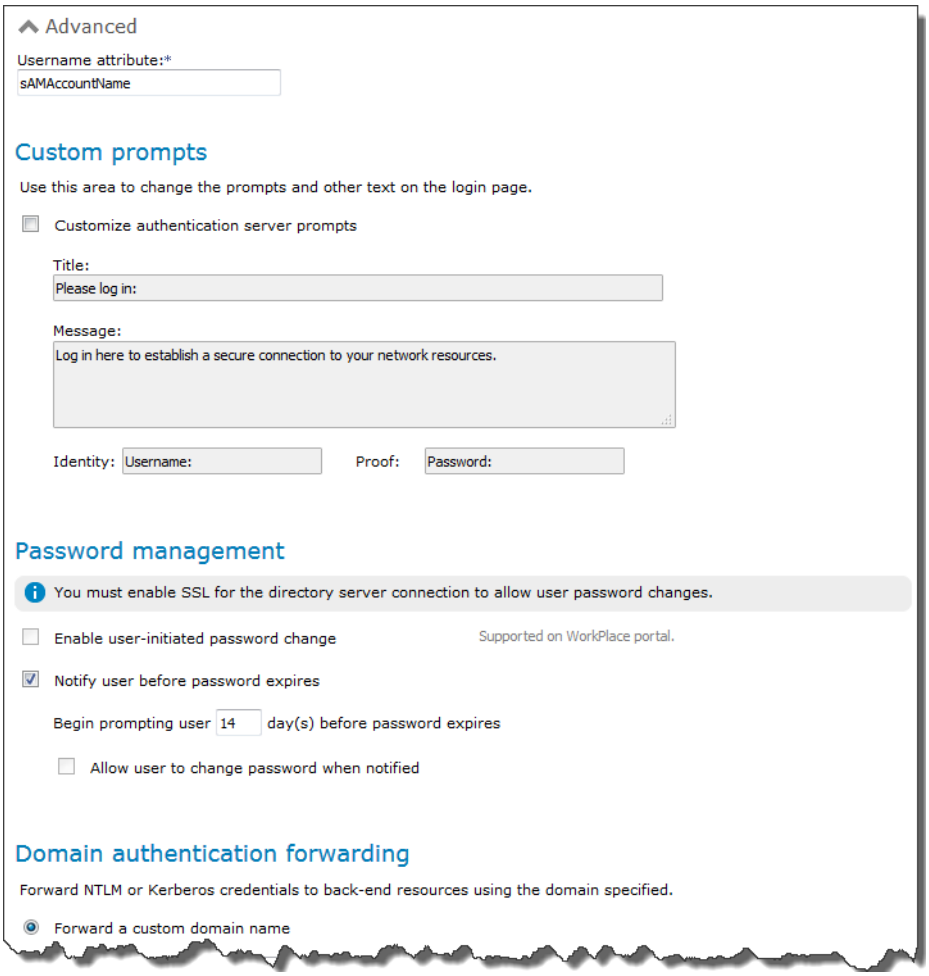


a [**Use SSL to secure Active Directory connection (SSL を使用してアクティブ ディレクトリ接続を保護)**]チェックボックスを選択します。

b 証明書の詳細を表示し、アプライアンスがルート証明書を使用できることを確認するには、[**SSL Settings (SSL 設定)**] リンクをクリックします。この操作により、クライアント証明書と SSL 証明書を発行した CA の名前 (1 つまたは複数) がリストされます。AD サーバーの CA がこのファイルにリストされていない場合や自己署名証明書を使用する場合は、証明書をこのファイルに追加する必要があります。詳細については、CA 証明書のインポートを参照してください。

c AD ドメイン コントローラのホスト名がアクティブ ディレクトリ サーバーで提示された証明書の名前と同じであることを確認するには、[**Match certificate CN against Active Directory domain controller (証明書 CN をアクティブ ディレクトリのドメイン コントローラに対して一致させる)**]チェックボックスを選択します。通常、サーバー名はデジタル証明書で指定されている名前と一致します。これが当てはまる場合は、SonicWall は実稼働環境でこのオプションを有効にすることを推奨します。こうしておくと、デジタル証明書または DNS サーバーが危険にさらされた場合でも、許可されていないサーバーが AD サーバーをマスカレードすることは困難になります。

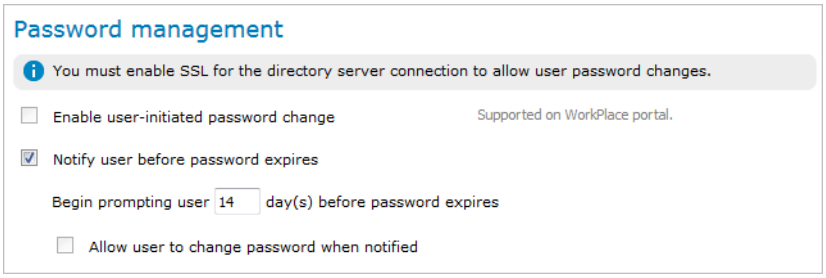
11 [**Advanced (詳細設定)**] エリアでは、ユーザー名属性の指定やカスタム プロンプトの設定が可能で、Active Directory パスワードの有効期限が切れる前にユーザーに通知するようにしたり、NTLM 認証転送オプションを構成したり、ワンタイム パスワードをセットアップしたりできます。



12 ユーザー名との一致に使用する [**Username attribute (ユーザ名属性)**] を入力します。ほとんどの AD インプリメンテーションでは、**sAMAccountName** がユーザー ID (例えば「*jdoe*」) と一致しま

す。cn を代わりに使用できますが、その場合は、ユーザー ID (「*jdoe*」) ではなく、フルネーム (「*John Doe*」) で認証しなければならなくなります。

13 認証サーバーへのログイン時に Windows ユーザーに表示されるプロンプトやその他のテキストを変更するには、[**Customize authentication server prompts (認証サーバーのプロンプトをカスタマイズする)**]チェックボックスを選択します。例えば、ユーザーが従業員 ID を使用してログインする場合、[**Identity (ID)**] プロンプトを [**Username (ユーザ名)**:] から [**Employee ID (従業員 ID)**] に変更できます (連鎖式認証を使用する場合は、ユーザーが区別しやすいため、カスタマイズしたパスワード プロンプトが特に便利です)。



14 アプライアンスと認証サーバーの間の接続が SSL で保護されている ([**Use SSL to secure Active Directory connection (SSL を使用してアクティブ ディレクトリ接続保護する)**] が有効である) 場合は、ユーザが[**Enable user-initiated password change (ユーザーが開始したパスワードの変更を有効にする)**] を選択することで、WorkPlace で自分のパスワードを変更できるようにすることができます。

△ **注意：SSL 経由の Active Directory が有効ではない場合、パスワードが暗号化されない状態で AD サーバーに転送されます。内部ネットワークが信頼されていない場合は、SSL を有効にしてください。AD サーバーでも SSL の使用を有効にする必要があります。詳細については、Microsoft AD のマニュアルを参照してください。**

ⓘ **メモ：**

- [**Login name (ログイン名)**]および[**Password (パスワード)**]フィールドは、アクティブ ディレクトリ サーバーへの接続の必須のフィールドではありませんが入力しないと (または、パスワードを指定しないと)、アプライアンスは匿名でバインドします。この場合、Active Directory がアノニマス検索を許可するように構成されていないと、検索が失敗します。
- パスワード通知期間内は、AD サーバーでユーザーが自分のパスワードを変更できる権限を与えておく必要があり、有効期限が切れた後は、管理者にユーザー パスワードを変更する権限が必要になります。これらの両方の操作では、セキュリティ上の理由から、パスワードがリセットされるのではなく、置換されるようになっています。
- 複数の Active Directory with SSL サーバーを定義する場合は、それぞれのサーバーで同じ [**Match certificate CN against Active Directory domain controller (アクティブ ディレクトリ ドメイン コントローラに対して証明書 CN を一致させる)**] 設定を指定します。(SonicWall では、実稼働環境でこのオプションを有効にすることを推奨します。)AMC では、この設定をレルム単位で構成できますが、アプライアンスは実際には、最後にロードされた ADS レルムで指定された設定を使用します。例えば、3 つのレルムでこのチェックボックスを選択し、4 つ目のレルムで選択解除すると、4 つのレルムすべてでこの機能が無効になります。

15 アクティブ ディレクトリ サーバーがユーザーにパスワードの有効期限が切れることを通知できるようにするには、[**Notify user before password expires (パスワードが期限切れになる前にユーザーに通知)**]チェックボックスを選択します。事前通知を開始する時期を指定します (デフォルトは **14** 日、最長は 30 日です)。これにより、ユーザーに表示されるパスワード プロンプトが AD サーバーによって制御されるようになります。

16 ユーザーが自分のパスワードを管理できるようにするには、[**Allow user to change password when notified (通知時にユーザーによるパスワード変更を許可)**]チェックボックスを選択します。この設定を変更できるのは、[**Active Directory over SSL (SSL 経由の Active Directory)**]エリアの[**Use SSL to secure Active Directory connection (SSL を使用してActive Directory 接続を保護)**]チェックボックスが選択されている場合だけです。パスワード管理は、Web アクセスを使用するユーザーと Connect Tunnel を使用するユーザーだけが使用できます。

17 NTLM 認証転送を有効にするには、[**NTLM authentication forwarding (NTLM 認証転送)**] オプションのいずれかをクリックします。詳細については、NTLM 認証転送を参照してください。

18 OTP を含む認証を構成するには、[**Use one-time passwords with this authentication server (この認証サーバーでワンタイム パスワードを使用)**] を有効にします。メール サーバーも構成する必要があり、OTP が外部ドメインに配信される場合 (例えば、SMS アドレスや外部 Web メール アドレス)、SMTP サーバーを構成してアプライアンスから外部ドメインにパスワードを送信できるようにする必要があります。

- OTP の文字数を [**Password contains (パスワードが次を含む)**] フィールドに入力します。デフォルトの長さは 8、最小は 4、最大は 20 です。
- OTP の文字のタイプをドロップダウン メニューから選択します。[**Alphabetic (アルファベット)**]、[**Alphabetic and numeric (アルファベットと数字)**]、または [**Numeric (数字)**] を選択します。
- [**From address (送信元アドレス)**] フィールドに、OTP の送信元の電子メール アドレスを入力します。
- [**Primary email address attribute (プライマリ電子メール アドレス属性)**] フィールドに、ワンタイム パスワードを送信する電子メール アドレスのディレクトリ属性を入力します。プライマリ属性が認証サーバーに存在する場合は、その属性が使用されます。
- [**Secondary email address attribute (セカンダリ電子メール アドレス属性)**] を指定すると、プライマリ電子メール アドレスに加えて使用されます。OTP が両方のアドレスに送信されます。

  OTP が (電子メール メッセージではなく) テキスト メッセージとして送信されるようにするには、対応する属性名を入力します (例えば、[`Mail`] または [`primaryEmail`] の代わりに [`SMSphone`])。詳細については、AD または LDAP ディレクトリ サーバーの構成を参照してください。
- [**Subject (件名)**] フィールドで、OTP 電子メールの件名をカスタマイズします。置換変数 *{password}* を使用すると、件名で実際のパスワードを表示する場所を指定できます。
- [**Body (本文)**] フィールドで、OTP メッセージの本文をカスタマイズします。置換変数 *{username}* を使用すると、メッセージでユーザーのアカウント名を表示する場所を指定できます。置換変数 *{password}* を使用すると、メッセージで実際のパスワードを表示する場所を指定できます。
- ユーザーへの OTP の配信をテストするには、OTP を受け取るユーザーの電子メール アドレスを [**Email address (電子メール アドレス)**] フィールドに入力し、[**Send test message (テスト メッセージを送信)**] ボタンをクリックします。アプライアンスがメッセージを送信できる場合は、ボタンの下に「メッセージが正常に送信されました」というステータスが表示されます。SMTP サーバーへの接続エラー、AD/LDAP サーバーとの通信エラー、指定したユーザーの AD/LDAP サーバーでの検索エラーなどのメッセージも、このボタンの下に表示されます。

19 [**Save (保存)**] を選択します。

複数の Active Directory ツリーの構成

この機能を利用すると、信頼できるフォレストと AD のフェデレーション型フォレスト内でのユーザーの認証と許可が 1 つの Active Directory (AD) ツリーから複数の AD ツリーへと拡大します。AD マルチフォレスト/マルチレルムのサポートの設定は、次の手順からなります。

1 AD フォレスト認証サーバーを構成し、現在の AD フォレストと信頼できるフォレストを有効にします。

2 複数のツリーを使用してグループを構成します。

3 信頼できるフォレストのツリーを使用してグループを構成します。

AD の複数フォレスト/複数レルムのサポートを構成すると、指定されたフォレストのユーザーの WorkPlace と Connect Tunnel での認証とログインが可能になります。

メモ：信頼できるドメインとは、ログイン時にユーザーを認証するドメインのことです。

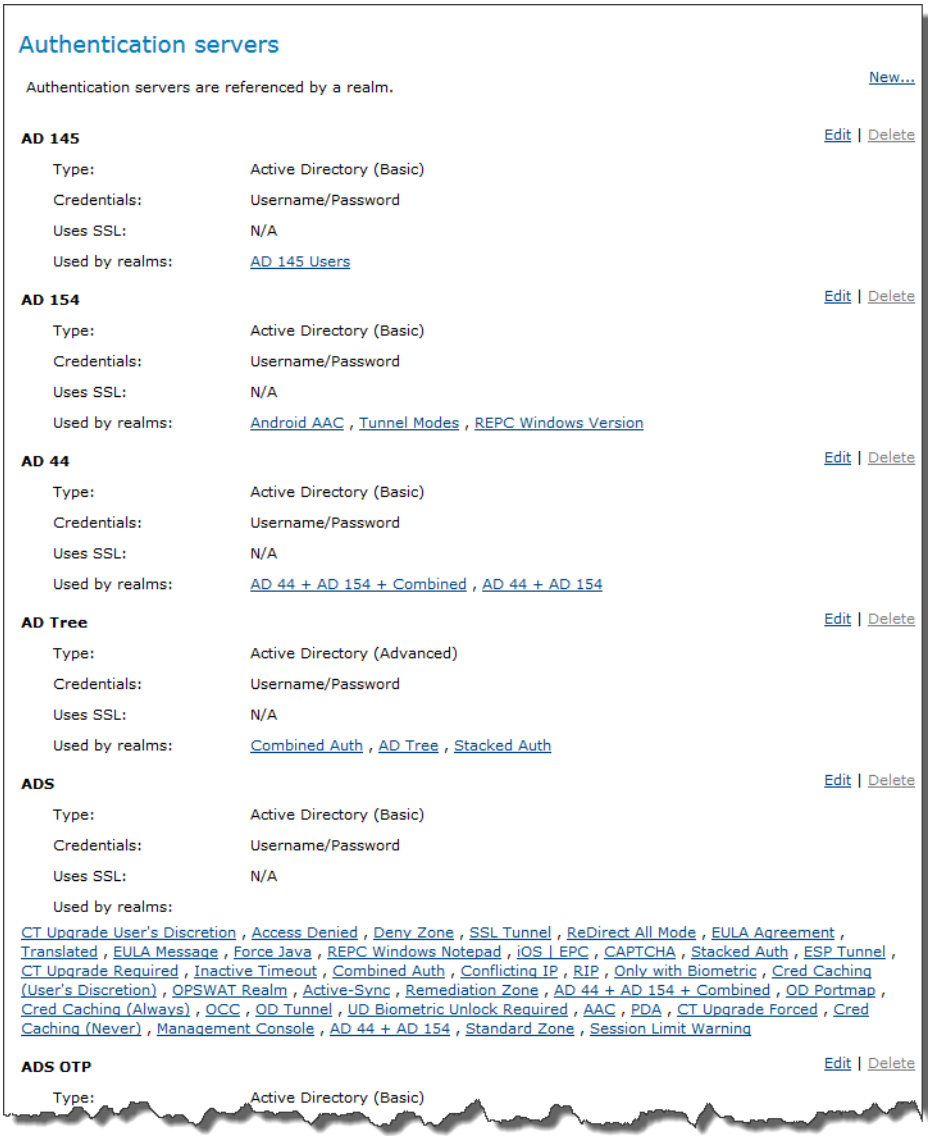
トピック:

- AD フォレスト認証サーバーを構成する
- 複数のツリーを使用してグループを構成する
- 信頼できるフォレストのツリーを使用してグループを構成する
- ユーザ ログイン

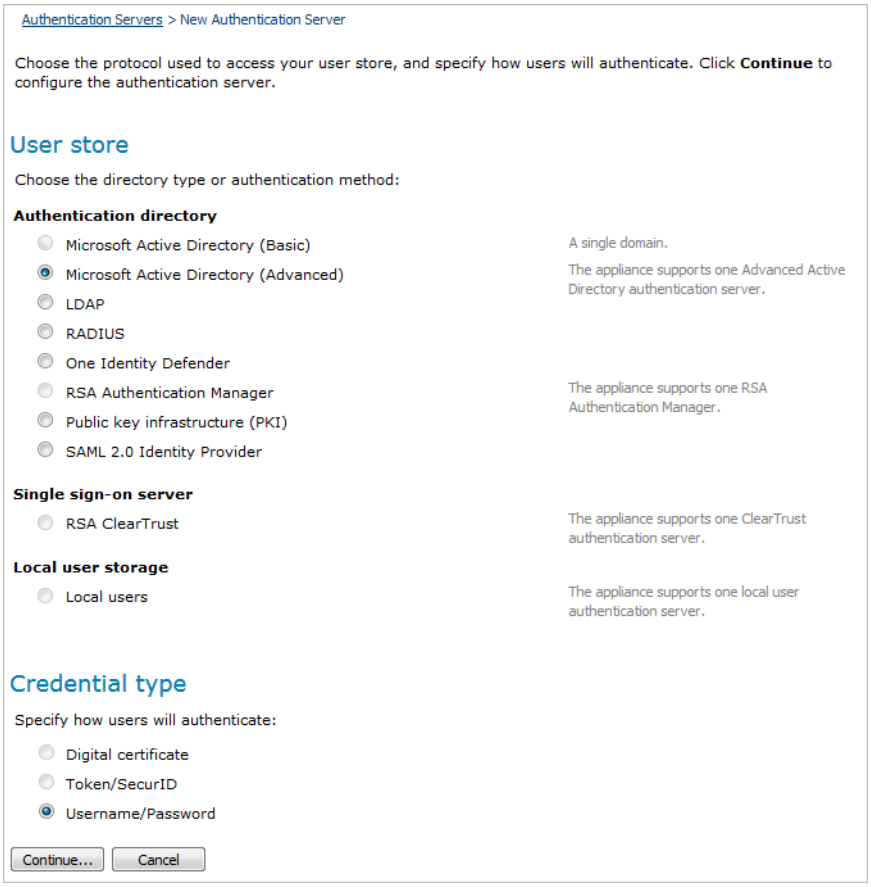
AD フォレスト認証サーバーを構成する

AD フォレスト認証サーバーを構成し、現在の AD フォレストと信頼できるフォレストの AD ドメインを有効にします。

1 メイン ナビゲーション メニューで [**Authentication Servers (認証サーバ)**] を選択し、**Authentication Servers (認証サーバ)**ーのセクションの [**New...(新規...)**] をクリックします。



2 [**New Authentication Server (新しい認証サーバー)**]ページの[**User Store (ユーザー ストア)**]セクションで、[**Microsoft Active Directory (Advanced) (マイクロソフト アクティブ ディレクトリ (高度))**]を選択します。



3 アプライアンスのその他の該当するオプションを選択し、[**Continue... (続行...)**]をクリックして[**Configure Authentication Server (認証サーバーの設定)**]ページに進みます。

4 [**Name (名前)**] フィールドに、Active Directory のツリーまたはフォレストの識別に使用する名前を入力します。

5 [**Root Domain (ルート ドメイン)**]フィールドに、フォレストの AD ルート ドメインを入力します。

6 [**Enable cross-forest trust (クロスフォレスト信頼を有効にする)**]チェックボックスを選択して、アプライアンスが他の信頼できるフォレストにアクセスできるようにします。有効になっていない場合、アプライアンスは、構成したフォレストと直接信頼関係があるフォレストだけにアクセスできます。

7 [**Login name (ログイン名)**] と [**Password (パスワード)**] フィールドに、フォレスト全体に読み取りアクセスできるユーザーのユーザー名とパスワードを入力します。

8 [**Active Directory DNS (アクティブ ディレクトリ DNS)**]セクションで、DNS と Key Distribution Center (KDC) を正しく構成します。

- [**Use DNS to lookup Active Directory domains (アクティブ ディレクトリ ドメインのルックアップに DNS を使用)**] を選択して、KDC/Kerberos レルムの DNS 検索を有効にしてから、WorkPlace に表示されるようにするドメインを選択します。[**Enable cross-forest trust (クロスフォレスト信頼を有効にする)**]が無効になっていると (チェックボックスが選択解除されていると)、構成したフォレストから取得されたドメインだけが表示されます。

- [**Use these Active Directory domains and KDCs (これらのアクティブ ディレクトリ ドメインおよび KDC を使用)**]を選択して KDC も使用するようにし、[**New (新規)**]をクリックして KDC を構成します。

複数のツリーを使用してグループを構成する

フォレストの AD ドメインからインポートしたユーザーのグループとグループを作成します。が選択解除された場合、構成したフォレストのユーザーとグループだけが含まれます。

信頼できるフォレストのツリーを使用してグループを構成する

構成したフォレストと信頼できるフォレストの AD ドメインからインポートしたユーザーのグループとグループを作成します。「クロスフォレスト信頼を有効にする」が選択された場合、構成したフォレストとすべての信頼できるフォレストのユーザーとグループが含まれます。

ユーザ ログイン

AD の複数フォレスト/複数レルムのサポートを構成すると、指定されたフォレストのユーザーの WorkPlace と Connect Tunnel での認証とログインが可能になります。

ユーザーは、次のいずれかを使用して、WorkPlace または Connect Tunnel にログインします。

- UPN 形式のユーザー名 (例: <*ユーザー名*>@KERBEROS_REALM) およびパスワード
- ユーザー名、パスワード、およびドメイン - [Domain Selection] オプションが構成されている場合
- ユーザー名とパスワード - デフォルト ドメインが構成されている場合

Active Directory 認証を行うための LDAP の構成

(例えば、AD のデフォルトを使用せずに検索ベースを指定することで) Active Directory をカスタマイズしている場合、LDAP を使用して Active Directory を認証する必要があります。LDAP サーバーを構成する手順については、LDAP と LDAPS 認証の構成に記載されています。LDAP を構成する場合は、ディレクトリの照会時に使用する属性について、特に注意してください。AD のインプリメンテーションごとに異なるため、実際の Active Directory スキーマでオブジェクト クラスと関連する属性がどのように構成されているかを知っておく必要があります。

メモ：アクティブ ディレクトリ (AD) サーバーを LDAP サーバーとして使用すると、ACL 検査を実行できません。短縮名 (SN) または共通名 (CN) は、LDAP サーバーではサポートされていません。これらは、AD サーバーでのみサポートされています。

次の表は、ユーザー名/パスワード クレデンシャルを検証するときに使用される、主要な AD 属性を示しています。属性では大文字と小文字が区別されません。

クレデンシャルの検証のための AD 属性

フィールド	説明
Login DN	Active Directory サーバーとの接続を確立するときに使用される DN。*example.com* ドメインにある汎用の AD 構成では、ユーザー名「John Doe」の DN は次のようになります。 `cn=John Doe,cn=users,dc=example,dc=com`
検索ベース	ユーザー情報の検索を始める AD ディレクトリ内のポイント。通常これは、ユーザー情報が含まれるディレクトリ ツリーの最下層になります。AD にバインドするユーザーには、このレベルでディレクトリを表示する権限が必要です。 一般的なインストールの場合、検索ベースが「`cn=users,dc=example,dc=com`」になっていると、ほとんどのユーザーが検索されます。一部のユーザーが異なるブランチに保管されている場合、高いレベルから検索することもできます (例えば、「`dc=example,dc=com`」)。
ユーザ名属性	ユーザー名との一致に使用される属性。ほとんどの AD インプリメンテーションでは、**sAMAccountName** がユーザー ID (例えば「*jdoe*」) と一致します。`cn` を代わりに使用できますが、その場合は、ユーザー ID (「*jdoe*」) ではなく、フルネーム (「*John Doe*」) で認証しなければならなくなります。

グループを参照するアクセス制御ルールを作成する場合、ユーザーは、ルールとの一致を要求する際に、グループの明示的なメンバーである必要があります。ネストされたグループのメンバーを入れる場合は、AMC で認証サーバーを構成するときに [**Nested group lookup (ネストされたグループの参照)**] を設定しておく必要があります。

例えば、*SeattleCampus* グループに *Marketing* という名前のグループが含まれていると仮定します。従業員の *John Doe* は *Marketing* グループのメンバーですが、*SeattleCampus* の明示的なメンバーではありません。この状態で[**Nested group lookup (ネストされたグループの参照)**]が「*0*」に設定されていると、*John Doe* は *SeattleCampus* グループのメンバーとして認識されませんが、「*1*」に設定されていると、メンバーとして認識されます。

Microsoft から、ディレクトリの接続、参照、変更などの LDAP 操作を簡単に実行できるグラフィカル ツールが提供されています。LDP (`ldp.exe`) という名前のこのツールは、Windows Server プラットフォームのサポート ツールから利用できます。詳細については、Microsoft の製品サポート サイトを参照してください。

Active Directory 認証のための LDAP の例

例 1 : Active Directory

アクティブ ディレクトリの構成 1

Login DN	*CN=AVtest,CN=Users,DC=testusrs,DC=example,DC=com*
検索ベース	*DC=testusrs,DC=example,DC=com*
ユーザ名属性	*sAMAccountName*

例 2 : Active Directory

アクティブ ディレクトリの構成 2

Login DN	*CN=johnDoe,CN=Users,DC=na,DC=example,DC=com*
検索ベース	*CN=Users,DC=na,DC=example,DC=com*
ユーザ名属性	*sAMAccountname*

例 3 : Domino サーバーを使用する LDAP

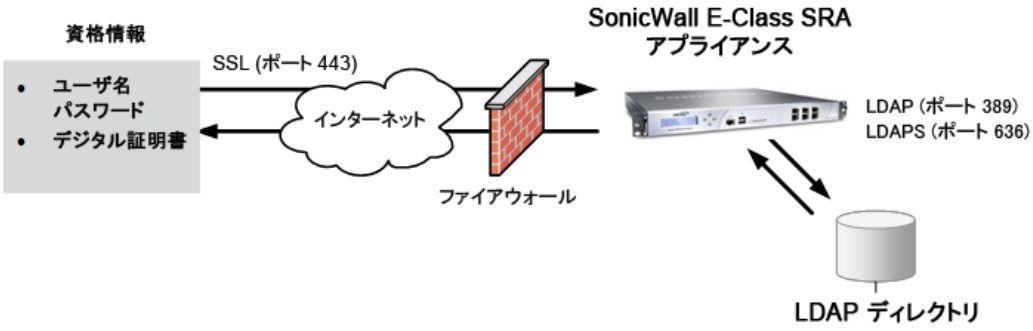
Domino サーバーを使用した LDAP 構成

Login DN	*CN=E-Class SMA,O=peoplesoft*
検索ベース	*o=peoplesoft*
ユーザ名属性	*cn*

LDAP と LDAPS 認証の構成

SMA アプライアンスは、LDAP または LDAPS (LDAP over SSL) プロトコルを使用した認証をサポートしています。どちらかのプロトコルを使用して、ユーザー名とパスワードのクレデンシャルを認証できます。LDAP および LDAPS 認証設定オプションで、一般的な LDAP の設定オプションを紹介しています。

LDAP および LDAPS 認証設定オプション



LDAP 接続を SSL で保護するには、追加の構成が必要です。LDAP 証明書を与えた CA のルート証明書を、SSL の信頼できるルート ファイルに追加する必要があります。こうして LDAP サーバーの成りすましを防ぐことで、セキュリティが強化されます。詳細については、CA 証明書のインポートを参照してください。

LDAP または LDAPS サーバーの構成後に、テスト接続を確立することで、レルム構成の設定を検証できます。詳細については、LDAP および AD 認証構成のテストを参照してください。

LDAP 認証を設定するときは、次の制限事項を考慮してください。

- **ファイアウォールおよびルータ** - アプライアンスが LDAP サーバーと通信できるようにするために、ファイアウォールまたはルータを構成する必要があります。標準 LDAP はポート 389/tcp を使用し、LDAPS はポート 636/tcp 経由で通信します。
- **LDAP アフィニティ サーバー** - すべての認証サーバに対して LDAP アフィニティ サーバーを設定することは可能ですが、アフィニティ サーバーは、RADIUS、RSA、および PKI サーバーなどのフル グループ検索機能を含まない認証サーバーのみに使用すべきです。さらに、Secure Mobile

Access は、いずれかの認証サーバーにグループ チェック機能があるスタック型認証のアフィニティ サーバーをサポートしていません。

メモ：アクティブ ディレクトリ (AD) サーバーを LDAP サーバーとして使用すると、ACL 検査を実行できません。短縮名 (SN) または共通名 (CN) は、LDAP サーバーではサポートされていません。これらは、AD サーバーでのみサポートされています。

- **デジタル証明書の検証** - デジタル証明書の検証を使用する LDAP 認証サーバーの構成は、レガシー環境のお客様向けの方法です。新しいユーザーは、PKI 認証サーバーの構成に記載されている標準の方法を使用してください。構成ページでは、**LDAP の Digital Certificate (デジタル証明書)** オプションと **Public key infrastructure (PKI) [パブリック キー インフラストラクチャ (PKI)]** オプションのどちらでも、[**Trust intermediate CAs without verifying the entire chain (チェーン全体を検証せずに中間 CA を信頼する)**] オプションを使用できます。

トピック:

- ユーザー名とパスワードを使用する LDAP の構成
- PKI 認証サーバーの構成
- CA 証明書のインポート
- 中間証明書について

ユーザー名とパスワードを使用する LDAP の構成

LDAP を構成する場合は、以下の点に注意してください。

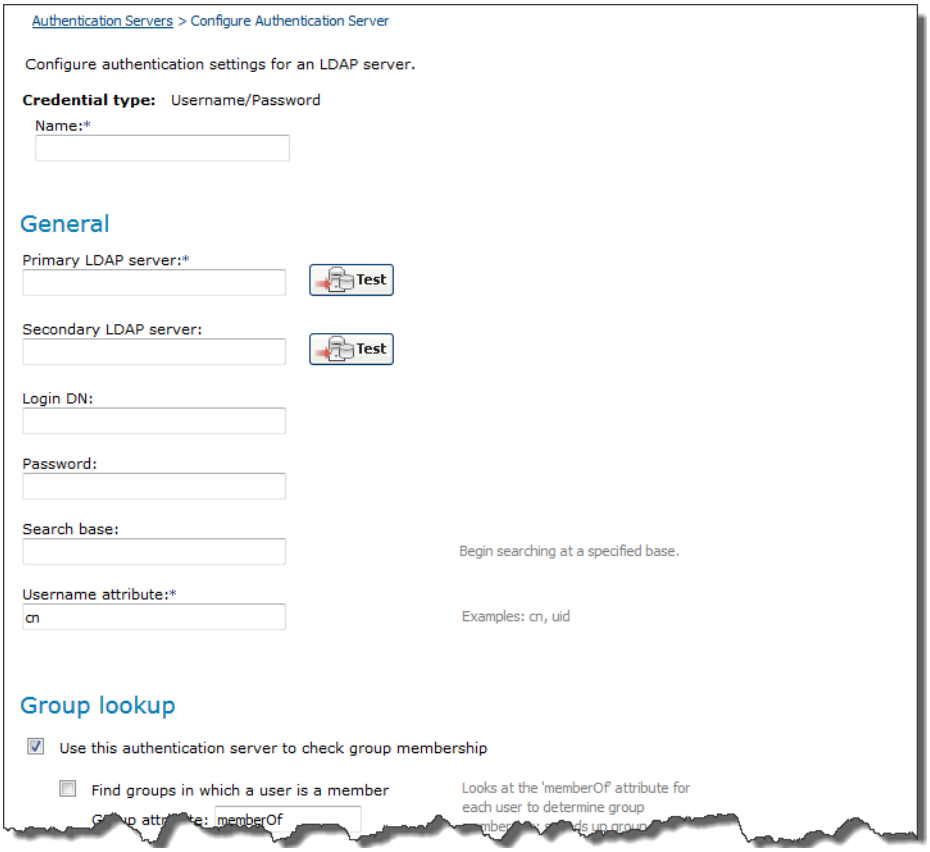
- [**Password management (パスワード管理)**] エリアの [**Notify user before password expires (パスワードが期限切れになる前にユーザーに通知)**] と [**Allow user to change password when notified (通知時にユーザーによるパスワード変更を許可)**] の設定には、いくつかの制限があります。
  - これらの設定は IBM Directory Server でのみサポートされています。
  - Web アクセス (Web プロキシ エージェント、または変換されマッピングされたカスタム ポート、または Web アクセスにマッピングされているカスタム FQDN) または Connect Tunnel を使用してアプライアンスに接続するユーザーだけが利用できます。
  - パスワードを変更するユーザーには、LDAP サーバーに対する権限が必要です。
- [**Login DN (ログイン DN)**]および[**Password (パスワード)**]フィールドは、LDAP サーバーへの接続の必須のフィールドではありませんが、入力しないと (または、パスワードを指定しないと)、アプライアンスが LDAP に匿名でバインドすることになり、一般的には、ユーザやグループの情報の検索を実行する正しい権限が設定されません。
- 複数の LDAPS サーバーを定義する場合は、[**Match certificate CN against LDAP server name (証明書 CN を LDAP サーバー名に対して一致させる)**]設定も各レルムで同じになるように構成してください。（実稼働環境ではこのオプションを有効にすることが推奨されます。）AMC では、この設定をレルム単位で構成できますが、アプライアンスは実際には、最後にロードされた LDAPS レルムで構成された設定を使用します。つまり、3 つの LDAPS サーバーでこのチェックボックスを選択し、4 つ目の LDAPS レルムで選択解除すると、4 つのサーバーすべてでこの機能が無効になります。
- デジタル証明書の検証を使用する LDAP 認証サーバーの構成は、レガシー環境のお客様向けの方法です。新しいユーザーは、PKI 認証サーバーの構成に記載されている標準の方法を使用してください。

ユーザー名/パスワード検証を使用する LDAP 認証サーバーを構成するには:

1 AMC のメイン ナビゲーション ページから [**Authentication Servers (認証サーバ)**] をクリックし、[**New...(新規...)**] をクリックします。

2 [**Authentication directory (認証ディレクトリ)**] で [**LDAP**] をクリックします。

3 [**Credential type (認証タイプ)**]で[**Username/Password (ユーザー名/パスワード)**]をクリックし、[**Continue... (続行...)**]をクリックします。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



4 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

5 [**General (一般)**] の下に表示される情報を入力します。

- [**Primary LDAP server (プライマリ LDAP サーバー)**]フィールドに、LDAP サーバーのホスト名または IP アドレスを入力します。フェイルオーバー サーバーを使用している場合 (オプション)、[**Secondary LDAP server (セカンダリ LDAP サーバー)**]フィールドでそのアドレスを指定します。

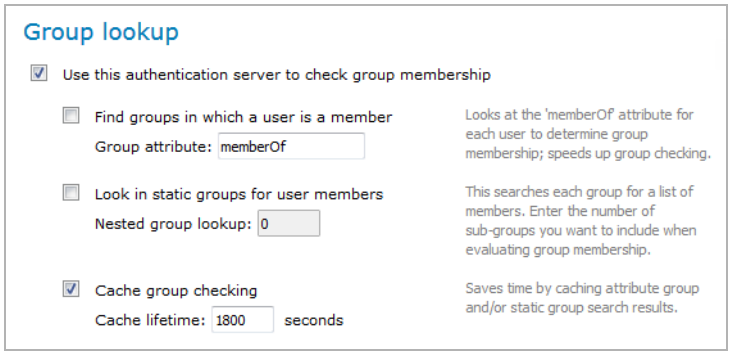
  LDAP サーバーが一般的なポート (非暗号化 LDAP 接続の場合は 389、SSL接続の場合は 636) 以外でリッスンする場合、コロンの後に接尾辞としてポート番号を指定できます (例えば、`myldap.example.com:1300`)。

- [**Login DN (ログイン DN)**]フィールドに、LDAP サーバーとの接続を確立するときに使用する識別名 (DN) を入力します。

- [**Password (パスワード)**]フィールドに、LDAP サーバーとの接続を確立するときに使用するパスワードを入力します。

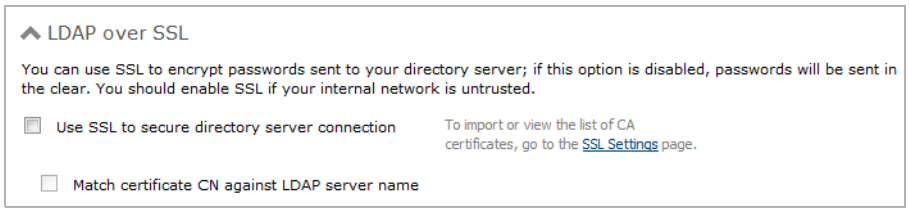
- [**Search base (検索ベース)**]フィールドに、ユーザー情報の検索を始める LDAP ディレクトリ内のポイントを入力します。通常これは、ユーザー情報が含まれるディレクトリ ツリーの最下層になります。例えば、「`ou=Users,o=xyz.com`」と入力します。LDAP ディレクトリにバインドするユーザーには、このレベルでディレクトリを表示する権限が必要です。
- [**Username attribute (ユーザー名属性)**]フィールドに、ユーザー名の一致に使用する属性を入力します。通常これは、「`cn`」または「`uid`」です。
- 指定したそれぞれのサーバーで [**Test (テスト)**] ボタンをクリックして、接続をテストします。

6 [**Group lookup (グループ ルックアップ)**] の下に表示される情報を入力します。



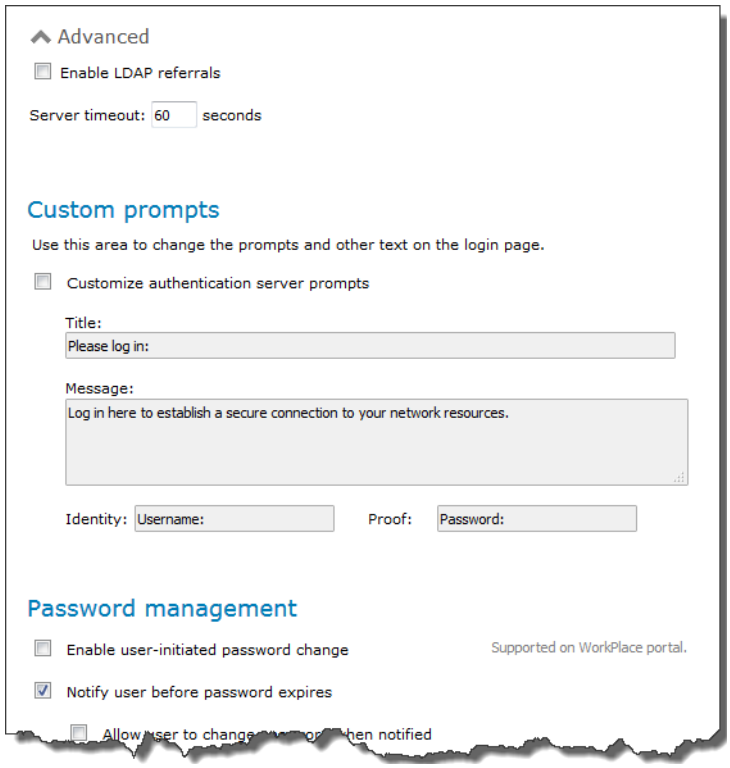
- このサーバーのグループ チェックを有効にするには、[**Use this authentication server to check group membership (この認証サーバーを使用してグループのメンバーシップを確認する)**] チェックボックスを選択します。このチェックボックスを選択解除すると、グループ チェックの動作だけに適用されるため、ネストされたコントロールは無効になります。このチェックボックスを選択解除すると、LDAP、AD、または AD のツリーの認証サーバーを、許可チェックを有効にせずに構成できます。これにより、スタックド/アフィニティ認証のサポートが向上し、効率が向上します。
- LDAP 検索のときに、ユーザー コンテナのグループ属性を検索することでユーザーのグループ メンバーシップを判断するようにしたい場合、[**Find groups in which a user is a member (ユーザーがメンバーであるグループを検索)**] チェックボックスを選択し、[**Group attribute (グループ属性)**]にグループ属性を入力します。この属性は通常、「**memberOf**」です。LDAP サーバーが属性ベースのグループをサポートしていて、有効になっている場合を除き、このチェックボックスを選択しないでください。
- LDAP サーバーが属性ベースのグループをサポートしていないか、この機能を有効にしていない場合、[**Look in static groups for user members (静的グループでユーザー メンバーを検索する)**]チェックボックスを選択します。検索の深度 (検索対象とするサブグループの数) を指定するには、[**Nested group lookup (ネストされたグループの参照)**]チェックボックスに数値を入力します。このタイプの検索では LDAP ツリー全体の検索が必要になるため、時間がかかる可能性があります。[**Cache group checking (グループ チェックをキャッシュ)**] をオンにすることを強く推奨します。
- ディレクトリの負荷を軽減し、パフォーマンスを向上させるには、属性グループや静的グループの検索結果をキャッシュします。[**Cache group checking (グループ チェックをキャッシュ)**]チェックボックスを選択して、[**Cache lifetime (キャッシュの持続時間)**]ボックスにキャッシュの持続時間を秒単位で入力します。デフォルト値は **1800** 秒 (30 分) です。

7 LDAP 接続を SSL で保護するには、[**LDAP over SSL**] の下に表示される情報を入力します。



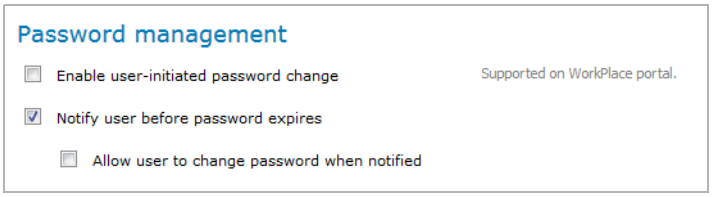
- LDAP 接続を SSL で保護するには、[**Use SSL to secure LDAP connection (SSL を使用して LDAP 接続を保護)**]チェックボックスを選択します。
- 証明書の詳細を表示し、アプライアンスがルート証明書を使用できることを確認します。詳細については、CA 証明書のインポートを参照してください。
- LDAP ホスト名が LDAP サーバーで提示された証明書の名前と同じであることを確認するようにアプライアンスを構成するには、[**Match certificate CN against LDAP server name (証明書 CN を LDAP サーバー名に対して一致させる)**]チェックボックスを選択します。通常、サーバー名はデジタル証明書で指定されている名前と一致します。これが当てはまる場合は、SonicWall は実稼働環境でこのオプションを有効にすることを推奨します。こうしておくと、デジタル証明書または DNS サーバーが危険にさらされた場合でも、許可されていないサーバーが LDAP サーバーをマスカレードすることは困難になります。

8 オプションで、[**Advanced (詳細設定)**] の下に表示される情報を入力します。

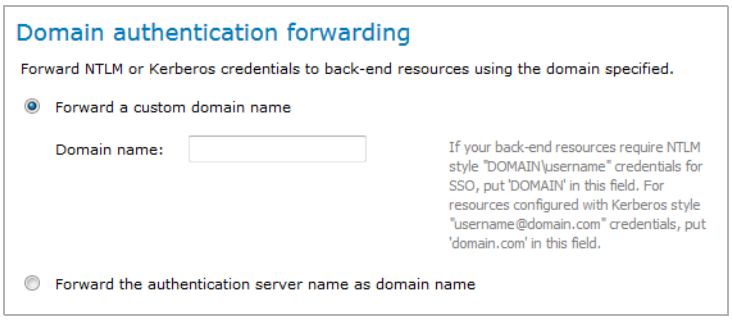


- [**Enable LDAP referrals (LDAP 照会を有効にする)**]チェックボックスを選択すると、LDAP サーバーがクライアントの照会に回答できない場合、他の LDAP サーバーを照会できます。この機能を使用する場合は、認証プロセスの速度が低下することがあるため、注意してください。Microsoft Active Directory に照会して認証するよう LDAP を構成している場合は、この機能を無効にすると良いでしょう。
- [**Server timeout (サーバーのタイムアウト)**]フィールドに、LDAP サーバーからの応答を待つ時間を秒単位で入力します。デフォルト値は **60** (1 分) です。

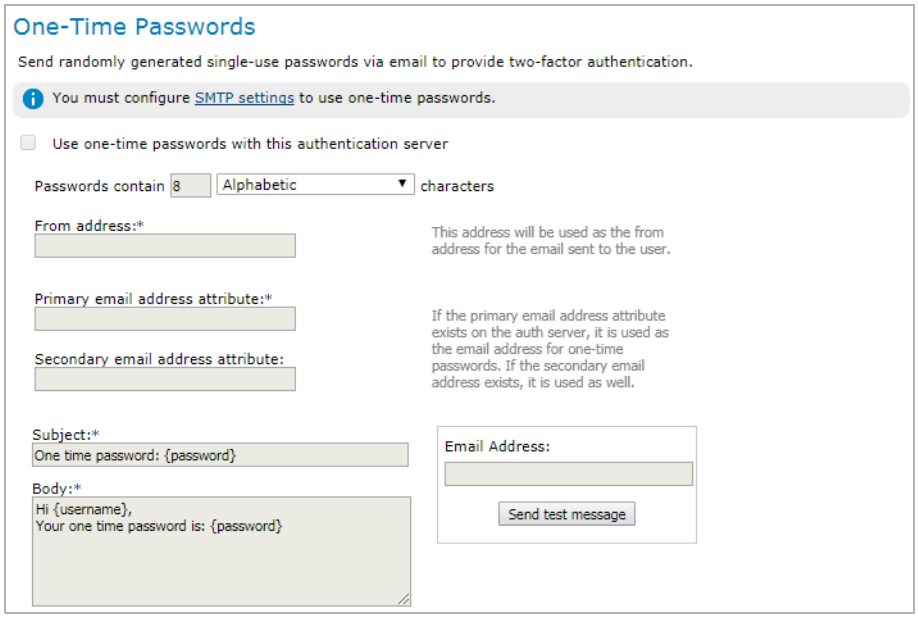
- 認証サーバーへのログイン時に Windows ユーザーに表示されるプロンプトやその他のテキストを変更するには、[**Customize authentication server prompts (認証サーバーのプロンプトをカスタマイズする)**]チェックボックスを選択します。ページ タイトル、メッセージ、ログイン プロンプトなどをすべてカスタマイズできます。例えば、ユーザーが PIN をパスワードとして使用している場合は、[**Proof (実証)**] プロンプトのテキストを「**Password: (パスワード)**:」から「**PIN**:」に変更します (カスタマイズした [**Message (メッセージ)**] に PIN を忘れた場合の取得方法を表示することもできます)。
- ユーザーが (WorkPlace のみで) 自分のパスワードを変更できるようにする場合は、[**Enable user-initiated password change (ユーザーが開始したパスワードの変更を有効にする)**] を選択します。レルムがスタックド認証で構成されており、2 セットのユーザー名/パスワード クレデンシャルが必要な場合、ユーザーが自分のパスワードを変更するときに、2 つの認証サーバーのうちの最初のサーバーに対するクレデンシャルだけを変更することになります。



- LDAP サーバーがユーザーにパスワードの有効期限が切れることを通知できるようにするには、[**Notify user before password expires (パスワードが期限切れになる前にユーザーに通知)**]チェックボックスを選択します。LDAP サーバーのプロンプトが表示されたときにもユーザーがパスワードを変更できるようにするには、[**Allow user to change password when notified (通知時にユーザーによるパスワード変更を許可)**]チェックボックスを選択します。これにより、ユーザーに表示されるパスワード プロンプトが LDAP サーバーによって制御されるようになります。
- NTLM 認証転送を有効にするには、[**Domain authentication forwarding (ドメイン認証の転送)**] オプションのいずれかをクリックします。詳細については、NTLM 認証転送を参照してください。



9 OTP を含む認証を構成するには、[**Use one-time passwords with this authentication server (この認証サーバーでワンタイム パスワードを使用)**] を有効にします。メール サーバーも構成する必要があり、OTP が外部ドメインに配信される場合 (例えば、SMS アドレスや外部 Web メール アドレス)、SMTP サーバーを構成してアプライアンスから外部ドメインにパスワードを送信できるようにする必要があります。



- OTP の文字数を [**Password contains (パスワードが次を含む)**] フィールドに入力します。デフォルトの長さは **8**、最小は 4、最大は 20 です。
- OTP の文字のタイプをドロップダウン リストから選択します。[**Alphabetic (アルファベット)**]、[**Alphabetic and numeric (アルファベットと数字)**]、または [**Numeric (数字)**] を選択します。
- [**From address (送信元アドレス)**] フィールドに、OTP の送信元の電子メール アドレスを入力します。
- [**Primary email address attribute (プライマリ電子メール アドレス属性)**] ボックスに、ワンタイム パスワードを送信する電子メール アドレスのディレクトリ属性を入力します。プライマリ属性が認証サーバーに存在する場合は、その属性が使用されます。
- [**Secondary email address attribute (セカンダリ電子メール アドレス属性)**] を指定すると、プライマリ電子メール アドレスに加えて使用されます。OTP が両方のアドレスに送信されます。

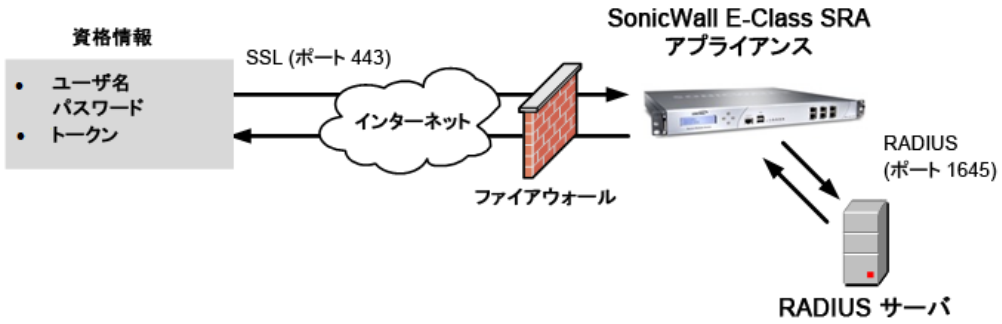
  OTP が (電子メール メッセージではなく) テキスト メッセージとして送信されるようにするには、対応する属性名を入力します (例えば、[`Mail`] または [`primaryEmail`] の代わりに [`SMSphone`])。詳細については、AD または LDAP ディレクトリ サーバーの構成を参照してください。
- [**Subject (件名)**] フィールドで、OTP 電子メールの件名をカスタマイズします。置換変数 *{password}* を使用すると、件名で実際のパスワードを表示する場所を指定できます。
- [**Body (本文)**] フィールドで、OTP メッセージの本文をカスタマイズします。置換変数 *{username}* を使用すると、メッセージでユーザーのアカウント名を表示する場所を指定できます。置換変数 *{password}* を使用すると、メッセージで実際のパスワードを表示する場所を指定できます。
- ユーザーへの OTP の配信をテストするには、OTP を受け取るユーザーの電子メール アドレスを [**Email address (電子メール アドレス)**] フィールドに入力し、[**Send test message (テスト メッセージを送信)**] ボタンをクリックします。アプライアンスがメッセージを送信できる場合は、ボタンの下に「メッセージが正常に送信されました」というステータスが表示されます。SMTP サーバーへの接続エラー、AD/LDAP サーバーとの通信エラー、指定したユーザーの AD/LDAP サーバーでの検索エラーなどのメッセージも、このボタンの下に表示されます。

10 [**Save (保存)**] を選択します。

RADIUS 認証の構成

アプライアンスは、ユーザ名/パスワードまたはトークン ベースのクレデンシャルを RADIUS データベースと対照させて検証できます。RADIUS 認証設定オプションで、一般的な RADIUS の設定オプションを紹介しています。

RADIUS 認証設定オプション



アプライアンスが RADIUS サーバーと通信できるようにするために、ファイアウォールまたはルータを変更する必要があります。RADIUS 認証プロトコルでは通常、ポート 1645/udp を使用します。また、RADIUS クライアント (一般的に*Network Access Server (ネットワーク アクセス サーバー)*と呼ばれます) としてアプライアンスの IP アドレスを含めるよう、RADIUS サーバーを構成する必要があります。

メモ：アフィニティ サーバーは、RADIUS、RSA、PKI サーバーなど、フル グループ検索機能を持たない認証サーバーにのみ使用する必要があります。

トピック:

- ユーザーまたはトークン ベースのクレデンシャルを使用する RADIUS の構成
- 高度な RADIUS 設定の構成

ユーザーまたはトークン ベースのクレデンシャルを使用する RADIUS の構成

このアプライアンスでは、RADIUS で、ユーザー名/パスワード クレデンシャルの他に、SecurID や SoftID などの、RADIUS サーバーのデータベースと照会して検証するトークン ベースのクレデンシャルもサポートしています。いずれかのタイプのクレデンシャルを使用する RADIUS 認証方式を構成するには、次の手順を実行します。

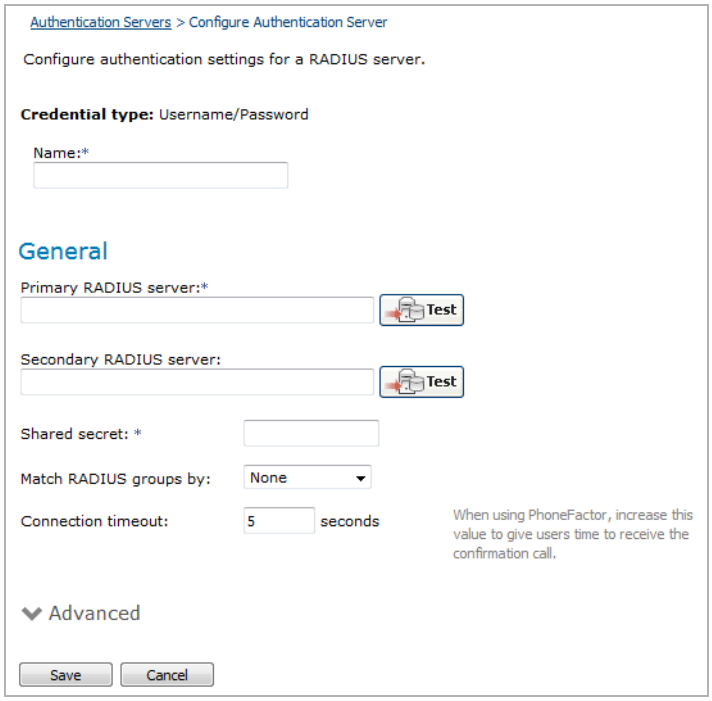
RADIUS を使用する PhoneFactor 認証も展開できます。ユーザーが会社の VPN にログインすると、RADIUS プロキシ サーバーとして動作する PhoneFactor エージェントに対して RADIUS 要求が発生します。PhoneFactor 認証の開始前に、ターゲット RADIUS サーバーでユーザー名とパスワードを最初に検証します。PhoneFactor を使用する 2 要素認証には、2 つの方法があります。

- ユーザーがユーザー名とパスワードを入力し、PhoneFactor がユーザーに発信します。ユーザーが電話に出て # を押し、PIN を入力します。
- ユーザーがユーザー名とパスワードを入力すると、PhoneFactor からワンタイム パスコードを含むテキスト メッセージが送信されます。ユーザーが認証のためにパスコードまたはパスコードと PIN でテキスト メッセージに返信します。

ユーザーベースまたはトークンベースのクレデンシャルを使用する RADIUS を構成するには、

1 AMC のメイン ナビゲーション ページから [**Authentication Servers (認証サーバ)**] をクリックし、[**New...(新規...)**] をクリックします。

2 [**Authentication directory (認証ディレクトリ)**]で[**RADIUS**]をクリックし、[**Continue... (続行...)**]をクリックします。[**Configure Authentication Server (認証サーバーの設定)**]が表示されます。



3 [**Credential type (認証タイプ)**]で[**Username/Password (ユーザー名/パスワード)**]または[**Token/SecurID (トークン/SecurID)**]をクリックし、[**Continue... (続行...)**]をクリックします。PhoneFactor の場合は、[**Token/SecurID (トークン/SecurID)**] を選択します。

4 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

5 [**Primary RADIUS server (プライマリ RADIUS サーバー)**]フィールドに、プライマリ RADIUS サーバーのホスト名または IP アドレスを入力します。RADIUS サーバーが 1645 (RADIUS の一般的なポート) 以外のポートでリッスンする場合、コロンの後に接尾辞としてポート番号を指定できます (:<ポート番号>)。

6 [**Secondary RADIUS server (セカンダリ RADIUS サーバー)**]フィールドに、セカンダリ RADIUS サーバーのホスト名または IP アドレスを入力します。必要に応じて、ポート番号も追加できます。

7 [**Shared secret (事前共有鍵)**]フィールドに、RADIUS サーバーとの通信の保護に使用するパスワードを入力します。これは、RADIUS サーバーで指定されたのと同じシークレット パスワードである必要があります。

8 [**Match RADIUS groups by (次の属性で RADIUS グループを照合)**] リストから、ユーザーが所属するグループの属性を選択します。RADIUS から返される値が、アプライアンス アクセス ルールのグループ部分で使用されます。次の 3 種類の値があります。

RADIUS グループの一致

次について RADIUS グループと一致	説明
None	グループ属性を無視します
filterid attribute (11)	**FilterID** 属性と一致します
class attribute (25)	**Class (クラス)** 属性と一致します

9 [**Connection timeout (接続タイムアウト)**]フィールドに、認証の試行がタイムアウトになるまでに RADIUS サーバーからの応答を待つ時間を秒単位で入力します。デフォルトは **5** 秒で、5 ～ 300 秒の範囲で指定します。PhoneFactor を使用する場合は、この値を大きくして、ユーザーが確認の着信を受け取ることができるようにします。

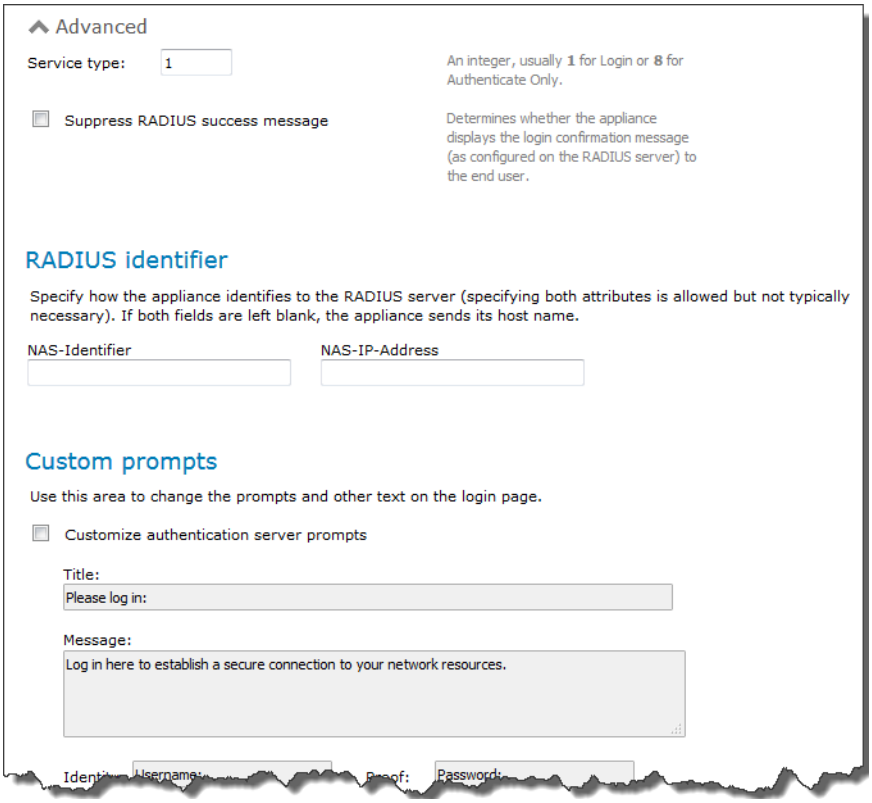
10 [**Advanced (詳細設定)**] ボタンを展開すると、追加のオプションが表示されます。これらのオプションについては、高度な RADIUS 設定の構成を参照してください。

11 [**Save (保存)**] を選択します。

高度な RADIUS 設定の構成

追加 (オプション) RADIUS 設定を構成するには

1 [**Advanced (詳細設定)**] ボタンをクリックして、追加 (オプション) RADIUS 設定を表示します。

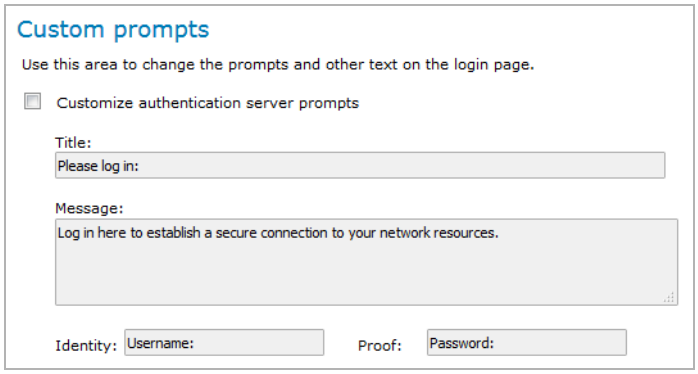


2 [**Service type (サービス タイプ)**]フィールドに、RADIUS Service-Type の整数を入力します。この値は、要求するサービスのタイプを示します。ほとんどの RADIUS サーバーでは、**1**（ログイン、デフォルト）または**8**（認証のみ）を入力します。

3 ユーザーのクレデンシャルが承認されると、RADIUS サーバーは通常、確認メッセージを送信します (例えば、「パスワード認証成功」)。このメッセージが表示されないようにするには、[**Suppress RADIUS success message (RADIUS 成功メッセージを抑制)**]チェックボックスを選択します。

4 アプライアンスは通常、ホスト名を使用して自分自身を識別します。RADIUS サーバーがその名前を承認できない場合は、[**NAS-Identifier (NAS 識別子)**] または [**NAS-IP-Address (NAS IP アドレス)**] を指定します (両方を指定することもできますが、通常はその必要はありません)。

5 認証サーバーへのログイン時に Windows ユーザーに表示されるプロンプトやその他のテキストを変更するには、[**Customize authentication server prompts (認証サーバーのプロンプトをカスタマイズ)**] を選択します。ページ タイトル、メッセージ、ログイン プロンプトなどをすべてカスタマイズできます。例えば、ユーザーが従業員 ID を使用してログインする場合、[**Identity (ID)**] プロンプトを [**Username (ユーザ名):**] から [**Employee ID (従業員 ID):**] に変更できます。



6 RADIUS サーバーが UTF-8 文字エンコーディングをサポートしていない古いバージョンの RADIUS プロトコルを使用する場合は、[**Local encoding (ローカル エンコーディング)**]スキームを [**Selected (選択済み)**]リストから選択するか、[**Other (その他)**]ボックスに入力します。詳細については、RADIUS ポリシー サーバーの文字セットを参照してください。

7 (**Credential type (クレデンシャル タイプ)**が**ユーザー名/パスワード**の RADIUS のみ) NTLM 認証転送を有効にするには、[**NTLM authentication forwarding (NTLM 認証転送)**] オプションのいずれかをクリックします。詳細については、NTLM 認証転送を参照してください。

ユーザーがマップしたトンネルのアドレッシング

ユーザーがマップしたトンネルのアドレッシングにより、ネットワーク管理者はトラフィックの送信元 IPv4 アドレスによって特定のユーザからのネットワークトラフィックを識別できます。

内部ネットワーク上では、特定のエンドユーザーを、管理者によってユーザーに割り当てられる特定の IPv4 アドレスに関連付けることがあります。

特定のユーザに IP アドレスを割り当てることは、現在、外部 RADIUS サーバーを使用してサポートされていますが、管理者は、ユーザがマップしたトンネルのアドレッシングを使用して、アプライアンスのローカル認証サーバーの属性から割り当てを指定できます。

RADIUS サーバーを認証サーバーとして展開する管理者は、特定のユーザーの RADIUS の構築された IP アドレス パラメーターに IPv4 アドレスを含め、そのユーザーのコミュニティを RADIUS アドレスプー

ルに関連付けることができます。このタイプの割り当ては、アドレスが使用可能でアドレス競合が禁止されていない場合にのみ実行できます。

メモ：アドレス競合によってこのタイプの割り当てが行えない場合、通常のトンネル アドレッシングのプロセスは、コミュニティによって許可されたリスト内の次のトンネルで継続されます。使用可能なプールがこれ以上ない場合、トンネル構成は失敗します。

ネットワーク トンネル サービスの構成内の RADIUS プールは、現在はユーザーがマップしたプールと呼ばれています。RADIUS サーバーの IP アドレスが認証サーバーから利用可能な場合、そのアドレスはユーザーがマップしたプールで使用できます。ユーザーのローカル認証サーバーによって提供される IPv4 アドレスは、ユーザーがマップしたプールでも使用でき、RADIUS プールからのものとまったく同じように使用されます。ユーザーがマップしたトンネル アドレッシング機能によって、ユーザーがマップしたアドレスが、ローカル ユーザーの認証サーバーに拡張されます。他のアドレス プールがアドレスを供給することはできません。

認証サーバから複数のアドレスを取得し、1 人のユーザが複数のトンネルを別々のデバイスに同時に確立できるようにすることができます。単一のユーザーが確立できる同時トンネル接続の数は、認証サーバー内のユーザーのアドレス数を指定することによって構成できます。この値は、[**Configure Community (コミュニティの設定)**]ページで特定のコミュニティのすべてのユーザーに対して[**Maximum Active Sessions (最大アクティブ セッション)**]の制限を設定することによっても設定できます。

RADIUS と同様に、ユーザーがマップしたトンネルのアドレス プールを使用して、仮想 IPv4 アドレスとトンネル クライアント間の厳密な対応（またはマッピング）を提供できます。特定のクライアントが[**Network Tunnel Client Settings (ネットワーク トンネル クライアント設定)**]ページの特定のプールから仮想アドレスを取得するように指定できます。クライアントは特定のコミュニティに割り当てられ、コミュニティは特定のアドレスプールから IPv4 アドレスのみを取得します。

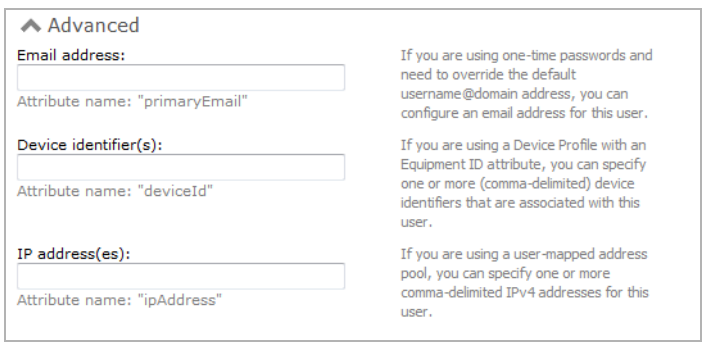
ユーザーがマップしたトンネルのアドレス プールは、トンネル接続時にトンネル仮想アドレスとして IPv4 アドレスを確立しようとします。アドレスが使用可能で、クライアント側の競合が発生しない場合は、仮想アドレスが割り当てられます。アドレスが失敗すると、システムはコミュニティが許可しているリスト内の次のアドレス プールに進みます。他のアドレス プールが利用できない場合、トンネル接続の試行は失敗します。

IPv4 アドレスを取得するために使用される認証サーバーは、独自の認証サーバーに限定されません。ユーザーがマップしたトンネルのアドレス プールは、独自の認証サーバまたはクライアントのローカル認証サーバからアドレスを取得することがあります

認証サーバは、単一のアドレスだけでなく、IPv4 アドレスのオーダ リストを供給することができるので、別々のデバイス上の単一のクライアントに複数のトンネル接続を同時に割り当てることができます。

[**Users & Groups (ユーザーおよびグループ)**]ページの[**Add/Edit Local User (ローカル ユーザーの追加/編集)**]ダイアログの[**Advanced (詳細)**]セクションで、次のフィールドを設定できます。

- 電子メール アドレス
- デバイス識別子
- IP アドレス



ローカルユーザー情報を編集するには:

1 AMC のメイン ナビゲーション メニューから、「**Users & Groups (ユーザとグループ)**」をクリックします。

2 [**Local Accounts (ローカル アカウント)**]をクリックし、編集するローカル アカウントの[**Name (名前)**]をクリックします。

3 [**Advanced (詳細)**]セクションを展開して、追加オプションにアクセスします。

4 [**Email address (電子メール アドレス)**] フィールドで、ユーザーの電子メール アドレスを構成します。このアドレスは、ユーザーにワンタイム パスワードを送信する際に使用され、デフォルトの電子メール アドレス `username@domain` を上書きします。この電子メール アドレスは、ユーザーの「mail (メール)」属性に割り当てられます。

5 [**Device identifier(s) (デバイス識別子)**]フィールドには、このユーザーに関連付けられているコンピュータや他のデバイスのデバイス識別子を 1 つまたは複数 (カンマで区切る) 入力します。

6 [**IP address(es) (IP アドレス)**]フィールドに、単一の IPv4 アドレスまたは IPv4 アドレスのリスト (カンマ区切り) を入力します。次を入力した場合:

- 単一の IPv4 アドレス: 各 IPv4 アドレスはリソースインターフェイスのネットワークアドレスと一致する必要があります。
- IPv4 アドレスのリスト: これらのアドレスは、リストに表示されている順序で、ユーザーがマップしたトンネルのアドレス プールに表示されます。

RSA サーバー認証の構成

このアプライアンスは、RSA Authentication Manager サーバーのデータベースに対して検証される、トークンベースのユーザー クレデンシャルである、SecurID をサポートしています。このタイプの認証の構成では、RSA サーバーと SMA アプライアンスの両方で変更が必要になります。RSA Authentication Manager 7.1 の手順については、ナレッジ ベースの記事「*E クラスのセキュア リモート アクセス アプライアンスで使用する RSA 認証の設定 (SW6571)* 」を参照してください。

メモ：アフィニティ サーバーは、RADIUS、RSA、PKI サーバーなど、フル グループ検索機能を持たない認証サーバーにのみ使用する必要があります。

RSA Authentication Manager にトークンベースのクレデンシャルを構成するには、

1 SMA アプライアンスの内部インターフェースの IP アドレスを使用して、RSA サーバーにエージェント ホストを作成します。

2 構成を変更して、RSA サーバーと SMA アプライアンスの両方の名前が解決されるようにします。

- DNS が RSA サーバーの名前を解決できる必要があります。アプライアンスとその IP アドレスを `/etc/hosts` ファイルに追加するだけでは、正しく動作しません。
- (RSA サーバーに構成されている) アプライアンスの名前がアプライアンスの内部 IP アドレスに解決される必要があります。

3 DNS が RSA サーバーの名前を両方向で解決できる必要があります。

- (RSA サーバーに構成されている) アプライアンスの名前がアプライアンスの内部 IP アドレスに解決される必要があります。アプライアンスとその IP アドレスを `/etc/hosts` ファイルに追加するだけでは、正しく動作しません。

- RSA サーバーには、SMA アプライアンスの内部インターフェースに対するリバース DNS エントリが必要です。

4 エージェント ホストを RSA サーバーに追加した後に、正しいエージェント ホストの構成ファイル (`sdconf.rec`) を生成します。

5 AMC のメイン ナビゲーション ページから [**Authentication Servers (認証サーバ)**] をクリックし、[**New...(新規...)**] をクリックします。

6 [**Authentication directory (認証ディレクトリ)**]で、[**RSA Authentication Manager (RSA 認証マネージャ)**] を選択します。[**Credential type (認証タイプ)**]は自動的に[**Token/ SecurID (トークン/SecurID)**]に設定されます。

7 [**Continue...(続ける...)**] を選択します。

8 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

9 RSA 認証マネージャ サーバーの SecurID 構成ファイル、`sdconf.rec` の場所を指定します。この構成ファイルはバイナリ形式で、RSA 認証サービスに関連するポートとプロセスが含まれます。このファイルがアップロードされると、RSA ライブラリによって RSA サーバーへのネットワーク経由の通信に使用されます。

10 [**Save (保存)**]をクリックしてアプライアンスにアップロードします。

11 エージェント ホストからの最初の認証要求で、ノード シークレットがネゴシエーションされます。[**node secret created (ノード シークレットの作成)**]フラグが RSA サーバーでクリアされていることを確認します。

メモ：

- RSA サーバーを変更した場合 (例えば、IP アドレスやホスト名の変更や再インストールなど)、`sdconf.rec` ファイルをアプライアンスに再アップロードする必要があります。
- 一部の古いバージョンからのアップグレード後に、ノード シークレットが正しく移行されなかったために、ユーザーが RSA サーバーで認証できなくなることがあります。この場合には、RSA サーバーの認証エージェントのノード シークレットをクリアします。

PKI 認証サーバーの構成

ユーザーが自分のデバイス上のクライアント証明書を使用して認証するように認証サーバーを設定することもできます。デジタル証明書認証は、単独で使用することも、RADIUS などの他の認証方法と組み合わせて使用することもできます。(連鎖式認証を設定し、デジタル証明書も 1 つの方法として使用する場合は、デジタル証明書認証が最初の方法である必要があります。詳細については、連鎖式認証の構成を参照してください。)

メモ：アフィニティ サーバーは、RADIUS、RSA、PKI サーバーなど、フル グループ検索機能を持たない認証サーバーにのみ使用する必要があります。

メモ：

- CA 証明書で CRL と OCSP の両方が有効な場合は、OCSP だけが使用されます。
- CRL から OCSP へ、または OCSP から CRL へのフォールバックはサポートしていません。

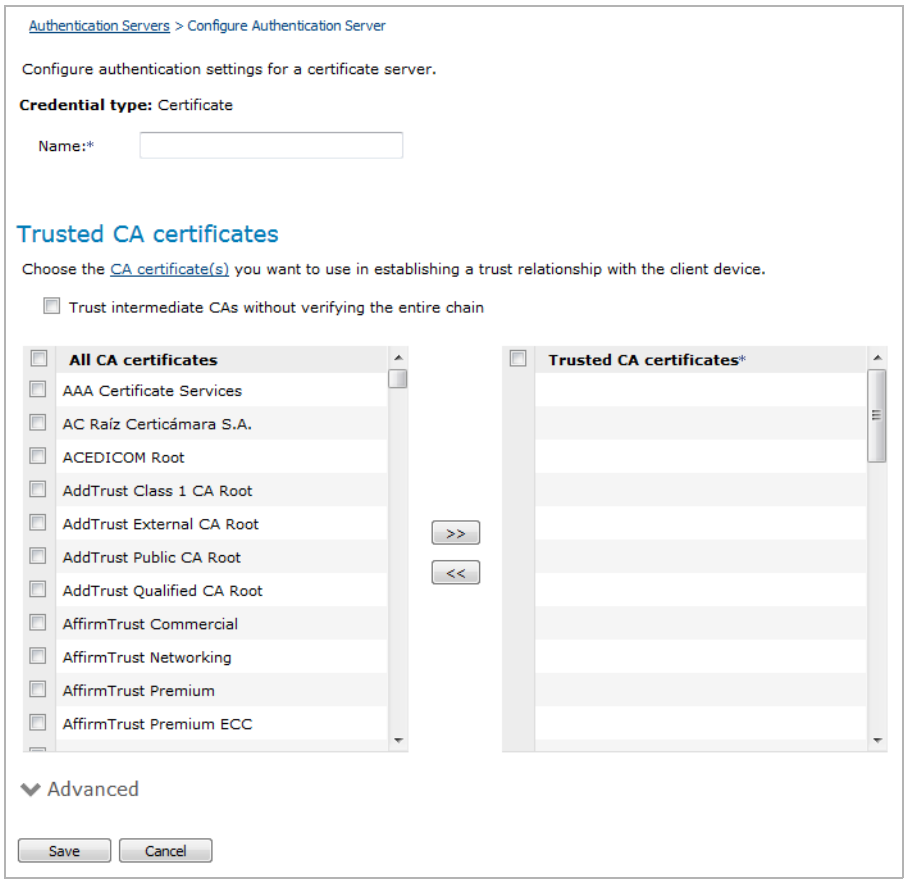
PKI 認証サーバーを構成するには、

1 AMC のメイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

2 [**New...(新規...)**] をクリックします。

3 [**Authentication directory (認証ディレクトリ)**] で **Public key infrastructure (PKI) [パブリック キー インフラストラクチャ (PKI)]** をクリックします。選択できるクレデンシャル タイプ ([**Credential type (種別)**] 列には、オブジェクトが ユーザーか グループかを示す]) は [**Digital certificate (デジタル証明書)**] だけです。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



5 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

6 [**Trusted CA certificates (信頼済み CA 証明書)**]で、オプションで[**Trust intermediate CAs without verifying the entire chain (チェーン全体を検証せずに中間 CA を信頼する)**]チェックボックスを選択します。このチェック ボックスを選択すると、信頼できる中間署名認証局証明書のセットをネットワークの複数のセクター (多くの場合は、組織や部門ごと) に展開できます。詳細については、中間証明書について**を参照してください。**

7 左側の[**All CA certificates (すべての CA 証明書)**]リストに、アプライアンスが使用しているすべての CA 証明書が表示されます。クライアント デバイスとの信頼関係を確立するには、証明書の左にあるチェックボックスを選択して[>>]ボタンをクリックすることで、1 つ以上のルート証明書を指定します (**Subject (タイトル)**と**Issuer (発行者)**が同じであるのがルート証明書です)。クライアントの証明書が [**Trusted CA certificates (信頼された CA 証明書)**] リストのルート証明書と一致すれば、信頼されることになります。

8 [**Advanced (詳細)**]の[**Username attribute (ユーザー名属性)**]ボックスに、シングル サインオンに使用する属性 (例えば `cn` または `uid`) を入力します。

9 OCSP レスポンダを使用してクライアント証明書のステータスを判断するには、[**Use OCSP to verify client certificates (OCSP を使用してクライアントの証明書を検証する)**]チェックボックスを選択

します。このチェック ボックスを選択すると、ユーザーが任意のアクセス方法 (ExtraWeb または Connect Tunnel) を使用して、この PKI 認証方法を使用するレルムに認証できます。

10 [**Use this OCSP responder (この OCSP レスポンダを使用)**] には、次のいずれかのオプションを選択します。

- [**System default (システムの既定値)**] : 手動で構成した OCSP レスポンダが優先されます。OCSP レスポンダが構成されている場合、その OCSP レスポンダの URL がここに表示されます。[**here (ここ)**] というリンクをクリックすると、[**SSL Settings (SSL 設定)**] からアクセスできる [**OCSP**] ページが表示され、OCSP レスポンダを構成できます。
- [**User certificate's AIA extension (ユーザー証明書の AIA 拡張)**] : ユーザー証明書が解析されて、OCSP レスポンダの URL が抽出されます。証明書の AIA (Authority Information Access) 拡張領域には、発行元の CA の証明書を提供する URL が含まれます。AIA 拡張領域に含まれるのは、HTTP、FTP、LDAP、または FILE の URL です。
- CA 証明書の AIA 拡張: CA 証明書が解析されて、OCSP レスポンダの URL が抽出されます。

11 エラーが発生するか、**不明**ステータスが返されるか、OCSP レスポンダにアクセスできない場合に認証を成功させる場合は、[**Allow certificate if responder is unavailable (応答者が利用不可の場合に証明書を許可する)**]を選択します。

12 [**Trust signing certificates in response (応答で署名証明書を信頼する)**]チェックボックスを選択して、OCSP レスポンスの証明書を信頼します。これは既定で有効になっています。

使用する CA 証明書の OCSP 応答署名証明書をインポートし、インポート時に [**OCSP response verification (OCSP 応答の検証)**] を有効にする必要があります。OCSP レスポンスの署名証明書を OCSP レスポンダまたはサーバーからローカル管理マシンにコピーし、AMC にログインした状態で、[**SSL Settings (SSL 設定)**] ページからインポートできます。

13 悪意ある攻撃から保護し、対象とする証明書の失効後に成功したレスポンスが再生されるのを防ぐには、[**Send nonce in request (要求にナンスを送信する)**]チェックボックスと[**Require nonce in response (要求にナンスを必要とする)**]チェックボックスを選択します。

14 [**Save (保存)**] を選択します。

カスタム証明書の追加フィールド

カスタム SSL クライアント証明書には、従業員 ID 番号（10 桁の番号）を含む追加フィールドがあります。この従業員 ID 番号は解析され、アクティブ ディレクトリ認証サーバーに渡されます。このサーバーはこの追加情報を使用してクライアントの承認およびクライアント アクセス特権を判断し、そのクライアントを承認されたグループに追加します。

カスタム証明書を使用して SMA を生成してアクセスするには:

1 カスタム証明書を作成します。カスタム フィールドに従業員 ID 番号を含めます。

2 従業員 ID 番号フィールドに基づいて、アクティブ ディレクトリ認証サーバー上にユーザー グループを作成します。

3 アクティブ ディレクトリ認証サーバー上のそのユーザー グループ用に SMA アクセス ポリシーを作成します。

4 従業員 ID 番号フィールドをアクティブ ディレクトリ認証サーバー上の SSO ユーザー名として構成します。

5 アクティブ ディレクトリ認証サーバーでグループ アフィニティー チェックを構成します。

6 適切なリソースを追加し、設定されたユーザー名に対して SSO を有効にします。

カスタム証明書は、そのユーザー名でクライアントに割り当てられ、クライアントのデバイスにインストールされます。クライアントは、そのデバイスを使用して、SMA およびそのクライアントの SSO で有効になっているすべてのリソースにアクセスできるようになりました。

SAML ベースの認証サーバーの構成

SAML (Security Assertion Markup Language) は、ユーザー認証、権限、および属性の情報を交換するための、XML ベースのフレームワークです。SAML は、ビジネス エンティティが対象者 (人であるユーザーなど) の ID、属性、および権限に関するアサーションをパートナー企業や他のエンタープライズ アプリケーションに対して作成することで、Web ベースのシングル サインオン (Web SSO) の基盤を提供します。

Web SSO では、ユーザーは、サービス プロバイダ (EX-Series アプライアンスなど) 経由でリソースにアクセスするか、サービス プロバイダと必要なリソースが理解されているか暗黙的である ID プロバイダ (IDP) にアクセスします。ユーザーは IDP に対して認証され、IDP が認証アサーションを生成し、サービス プロバイダがアサーションを使用してユーザーのセキュリティ コンテキストを確立します。セキュリティ コンテキストが存在するユーザーは、追加の認証なしに別のサイトのリソースにアクセスできます。SAML は、シングル ログアウト (SLO) サービスも提供します。

本リリースでは、パブリック インターネットに展開されている外部 IDP がサポートされています。ユーザーが標準ブラウザを使用し、SAML のスコープの外部の何らかの方法で IDP に対して認証できることを前提としています。ユーザーは、SAML で認証されたレルム経由でアプライアンスにアクセスします。

CA SiteMinder などの SAML 2.0 ID プロバイダを使用するように EX Series アプライアンスを構成する場合は、以下の構成情報を参照してください。

- アプライアンスは、`https://<appliance>/saml2ssoconsumer` で SAML SSO サービスをホスティングします。
- アプライアンスは、`https://<appliance>/saml2sloconsumer` で SAML SLO サービスをホスティングします。
- IDP で、次のように構成します。
  - HTTP-POST と HTTP-Redirect バインディングを有効にし、構成します。
  - SAML SSO と SLO サービスを有効にし、構成します。
  - nameID とアサーションの暗号化を無効にします。

SAML 2.0 ID プロバイダ認証サーバーの設定

メモ：

- SAML 2.0 ID プロバイダ認証サーバーは、Web ベースのアクセスでサポートされています。Tunnel エージェントはサポートされていません。
- SAML 2.0 ID プロバイダ認証サーバーは、連鎖式認証には使用できません。

メモ：サードパーティの SAML ID プロバイダ (IDP) の設定方法の詳細については、SAML ID プロバイダの設定を参照してください。

SAML 2.0 ID プロバイダ (IDP)は、集中セキュリティ管理の基盤として、お客様、パートナー、および従業員向けの、Web を使用するアプリケーションやクラウド サービスでのセキュリティを確立します。

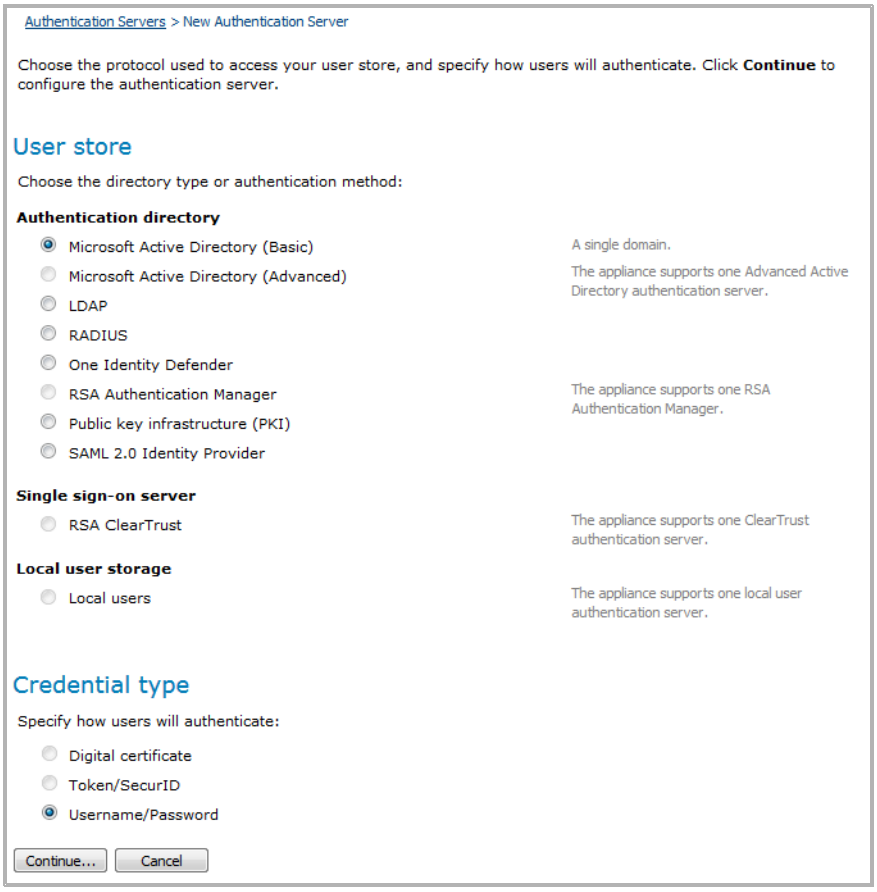
SMA は、CA SiteMinder や他の IDP をサポートする CA SiteMinder を SAML 2.0 ID プロバイダに置き換えました。SAML 2.0 ID プロバイダは、次の IDP をサポートしています。

- Microsoft Azure IDP
- 1 つの ID のクラウド アクセス マネージャ
- Shibboleth IDP
- OneLogin
- CA シングル サインオン (CA SiteMinder)
- PingIdentity PingOne
- CA SiteMinder

SAML 2.0 ID プロバイダの認証サーバーの構成方法:

1 AMC で、[**System Configuration (システム構成) > Authentication Servers (認証サーバー)**]ページに移動します。

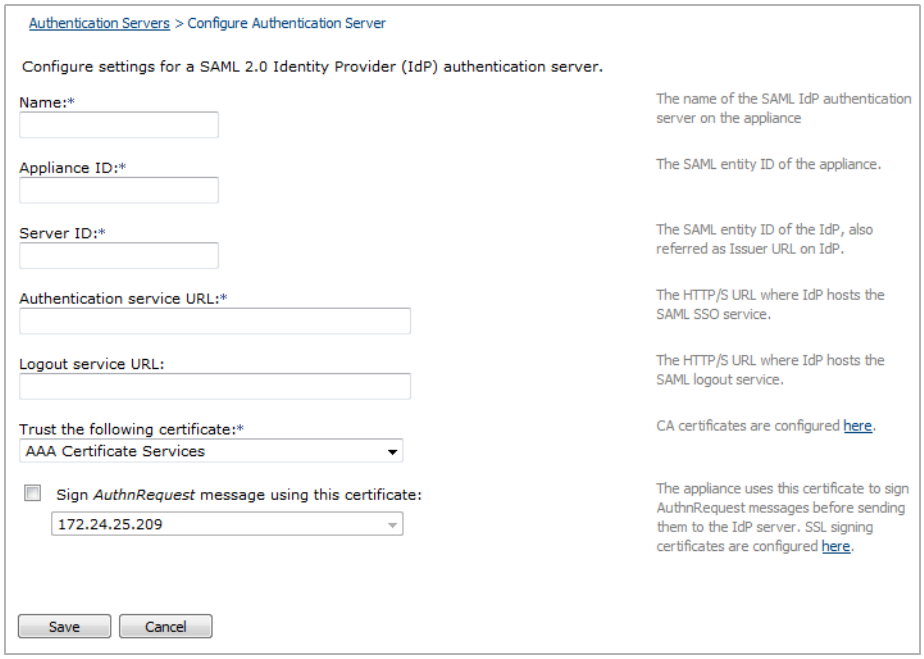
2 [**New...(新規...)**] をクリックします。[**New Authentication Server (新しい認証サーバー)**]ダイアログが表示されます。



3 [**Authentication directory (認証ディレクトリ)**]で、[**SAML 2.0 Identity Provider (SAML 2.0 ID プロバイダ)**]を選択します。

4 [**Credential type (認証情報タイプ)**]で、[**Username/Password (ユーザー名/パスワード)**]を選択します。

5 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



6 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

7 [**Appliance ID (装置 ID)**] フィールドにアプライアンスの SAML エンティティ ID を入力します。長さが 1024 文字以下の URI を入力します。

8 [**Server ID (サーバー ID)**]フィールドに IDP サーバーの SAML エンティティ ID を入力します。アプライアンスは、これを使用して、IDP 認証サーバーの ID を判断します。長さが 1024 文字以下の URI を入力します。

9 [**Authentication Service URL (認証サーバー URL)**]に IDP が SAML SSO サービスをホスティングする URL を入力します。

10 [**Logout service URL (ログアウト サービス URL)**]に IDP が SAML シングル ログアウト (SLO) サービスをホスティングする URL を入力します。

11 IDP サーバーの CA 証明書を[**Trust the following certificate (以下の証明書を信頼する)**]ドロップダウン メニューから選択します。CA 証明書を構成するには、右側の説明文にある [**here (ここ)**] リンクをクリックします。この CA 証明書がアプライアンスにない場合は、インポートする必要があります。

12 [**Sign AuthnRequest message using this certificate (この証明書を使用して AuthnRequest メッセージに署名する)**]チェックボックスを選択し、署名証明書をドロップダウン メニューから選択します。アプライアンスはこの証明書を使用して、IDP サーバーへの送信前に認証要求メッセージに署名します。SSL 署名証明書を構成するには、右側の説明文にある [**here (ここ)**] リンクをクリックします。この署名証明書がアプライアンスにない場合は、インポートする必要があります。

13 [**Save (保存)**] を選択します。

シングル サインオン認証サーバーを設定する

シングル サインオン (SSO) を使用すると、ユーザー認証情報をバックエンド Web リソースに転送するようにアプライアンスを設定できます。つまり、ユーザーが何回もログインする必要がないというこ

とにもなります (アプライアンスにアクセスできるようになれば、アプリケーション リソースにまたアクセスできます)。

アプライアンスは多くの種類の Web SSO (セキュリティ手段として、SSO はデフォルトでは無効) をサポートしています。

メモ：

- トンネル セッションで Web アプリケーションへのアクセスで SSO 機能を有効にするには、[**Web resource filtering (Web リソースのフィルタリング)**] を有効にします。詳細については、Web リソースのフィルタリングの構成を参照してください。
- Web プロキシ エージェントは、SSL で保護されたバックエンド Web サーバーへのシングル サインオンをサポートしていません。Web プロキシ エージェント経由でアクセスされるこれらのリソースへのリンクでは、シングル サインオンを使用できません。HTTPS リソースへの転送で基本認証または NTLM 認証のいずれかを提供するには、Web リソースのエイリアスを作成して、WorkPlace にリンクとして追加します。これにより、アプライアンスが変換、カスタム ポート マッピング、またはカスタム FQDN マッピングの Web アクセスを提供するようになります。
- デフォルトでは、OnDemand Tunnel を実行するユーザーの Web コンテンツは、アプライアンスが直接プロキシとなります。AMCの[**Configure WorkPlace (WorkPlace の設定)**]ページの[**Web shortcut access (Webショートカットアクセス)**]エリアで[**Use Web content translation (Web コンテンツ翻訳を使用)**]を選択します。

トピック:

- フォームベースのシングル サインオン
- 基本認証転送
- NTLM 認証転送
- RSA ClearTrust 認証の使用

フォームベースのシングル サインオン

多くの Web アプリケーションでは、フォームベースの認証が使用されており、その場合、認証のユーザー インターフェースは Web フォームです。AMC を使用してシングル サインオン プロファイルをセットアップすることで、ユーザーのアプライアンスのクレデンシャルがフォームベースの認証を使用する Web アプリケーションに転送されるようにできます。いくつかの組み込みプロファイルがあり、環境に合わせて変更できます。

- OWA (複数のバージョン)
- Citrix Nfuse 1.7
- Citrix XenApp

詳細については、フォームベースのシングル サインオン プロファイルの作成を参照してください。

メモ：フォームベース SSO は、変換のみでサポートされています。変換を必要とするバックエンド Web アプリケーション クッキーへのその他のアクセス エージェント (Web プロキシおよび OD トンネル) のアクセスは、サーバーにプロビジョニングされません。

基本認証転送

この認証転送方式は、広範囲のプラットフォームでサポートされていますが、パスワードをそのままネットワークで送信するため、あまり安全であるとは言えません。アプライアンスを、それぞれの

ユーザーの認証クレデンシャル、または「静的」クレデンシャル (つまり、すべてのユーザーで同じクレデンシャル) を送信するように構成できます。

基本認証転送を構成するには、

1 Web アプリケーション プロファイルを SSO を使用するよう構成し、使用するユーザー クレデンシャルを指定します。

2 この Web アプリケーション プロファイルを、SSO を使用する任意の Web リソースに添付します。

基本認証転送は、Web アプリケーション プロファイル内で構成します。詳細については、Web アプリケーション プロファイルの追加を参照してください。

NTLM 認証転送

NTLM (Windows NT LAN Manager) では、ネットワーク経由でパスワードをそのまま送信せずに、チャレンジ/レスポンスのメカニズムを使用して、ユーザーを安全に認証します。Windows ネットワーク クレデンシャルを Microsoft IIS (Internet Information Services) Web サーバーに安全に送信できます。

NTLM 認証転送では、Windows ドメイン名がユーザーの認証クレデンシャルと一緒に渡されます。これにより、パスワードがそのまま送信されることなく、Windows ネットワークに安全に認証され、Web リソースにアクセスできるようになります。

メモ：

- クレデンシャルが一致しない状況で NTLM 認証転送を使用するには、NTLM をサポートする Web ブラウザが実行中である必要があります。
- シングル サインオンが有効である場合、Web プロキシ サービスとバックエンド サーバーが、使用されている認証方式を判断します。AMC で 1 つの認証方式 (基本認証または NTLM 認証) だけが有効である場合、その認証方式が使用されます。AMC で両方の認証方式が有効である場合、NTLM 認証の方が安全であるため、こちらが使用されます。

NTLM 認証転送を構成するには、

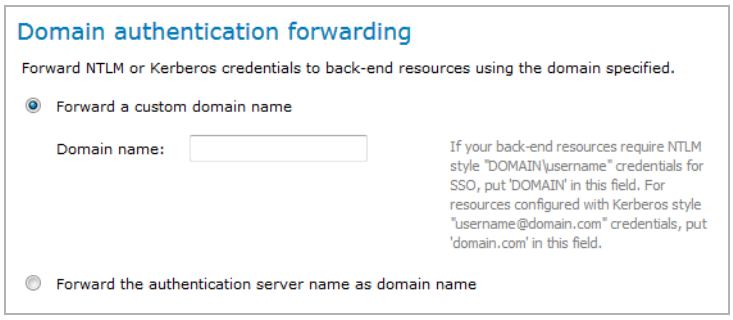
1 Web アプリケーション プロファイルの SSO オプションを有効にし、ユーザー認証情報を転送する任意の Web リソースにそのプロファイルを添付します。

2 AMC のメイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

3 構成するサーバーに対応する [**Edit (編集)**] リンクをクリックします。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。

4 [**Advanced (詳細設定)**] 設定を展開します。

5 [**Domain authentication forwarding (ドメイン認証の転送)**]エリアで、転送するドメイン名を指定します。



- [**Domain name (ドメイン名)**]フィールドにカスタム名を入力できますが、必須ではありません。ドメイン名を指定しないと、空 (ヌル) のドメイン名がユーザー クレデンシャルと一緒に転送されます。
- (ページ上部の[**Name (名前)**]フィールドで指定した) 認証サーバー名をユーザー クレデンシャルと一緒に転送するには、[**Forward the authentication server name as domain name (認証サーバー名をドメイン名として転送する)**]をクリックします。

RSA ClearTrust の使用

シングル サインオンでは、ユーザー認証クレデンシャルが RSA ClearTrust サーバーからアプライアンスに転送され、アプライアンスからさらに、認証でこれを必要とするバックエンド リソースに転送されます。この認証環境でのアプライアンスのセットアップについては、RSA ClearTrust 構成を参照してください。

CAM を使用したレガシーおよびフェデレーション型 ID SSO のサポート

トピック:

- CAM を使用したレガシーおよびフェデレーション型 ID SSO について
- CAM を使用した SSO の設定

CAM を使用したレガシーおよびフェデレーション型 ID SSO について

CAM を使用したレガシーおよびフェデレーション型 ID SSOは、クラウド アクセス マネージャ (CAM) を ID プロバイダ (IDP) として使用して、レガシーおよび SAML フェデレーション型のサービスとしてのソフトウェア (SaaS) アプリケーションに対して、統一されたシングル サインオン (SSO) サポートを提供します。

CAM を使用したレガシーおよびフェデレーション型 ID SSO はフェデレーション型 SSO 機能を使用し、SMA アプライアンスを社内ネットワーク上の CAM IDP と連携させることができます。また、内部およびクラウド ベースの SAML リソースに透過的な SSO を提供します。

フェデレーション型 ID SSO は、Office 365、Google Apps、Salesforce、および Citrix XenApp などの SaaS アプリケーションとオンプレミス アプリケーションの両方をサポートします。

CAMを使用したレガシーおよびフェデレーション型 ID SSO は、従来のアプリケーション SSO を提供します。SMA のユーザーがログインする必要があるのは一度だけです。SSO は、オンプレミス アプリケーションとクラウド SaaS の両方に認証情報を提供します。

CAM への接続は、SMA アプライアンスから CAM IDP へと移動する際に、SAML トラフィックに認証資格情報を注入することで行われます。CAM IDP は SAML トークンを生成し、それをユーザーの Web ブラウザーに添付して、フェデレーション型サービスに SSO を提供します。

SAML SSO と連携した連鎖式認証を含むすべての形式の SMA 認証は、Tunnel エージェントでサポートされています。この機能により、連鎖式認証を必要とするユーザーを含むユーザーは、SAML 認証のレルムに対してのみ認証できるのではなく、任意の認証のレルムで認証できます。

CAM を使用したレガシーおよびフェデレーション型 ID SSO により、SMA はアクティブ ディレクトリ認証サーバーで既存の認証システムを使用できます。これは、個別で、または連鎖式認証で行うことができます。従来の SSO を維持するために、SMA は HTTP または HTTPS トラフィック ストリームにユーザーの資格情報を注入します。

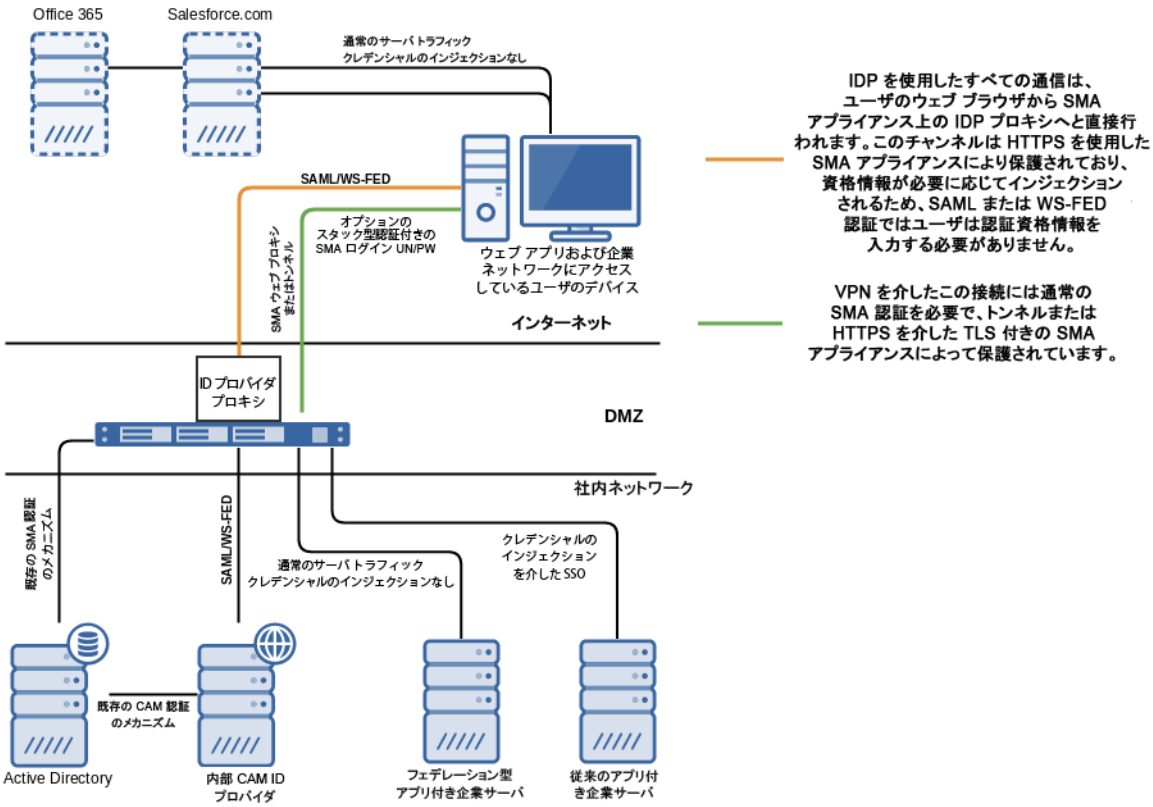
フェデレーション型 ID SSO は、SMA が IDP プロキシを内部ネットワークにある CAM IDP に示すと有効になります。IDP プロキシは、トラフィックが IDP にリダイレクトされて SAML または WS-FED トークンを取得したときに、ユーザーの Web ブラウザからすべてのトラフィックを受信します。IDP プロキシは、IDP へのログイン要求にユーザーの認証情報を注入します。これにより、CAM IDP はユーザの介入なしに SAML および WS-FED トークンを生成できます。

この機能を使用すると、企業ネットワーク内のレガシー アプリケーションや、パブリック クラウドとプライベート クラウドのフェデレーション型アプリケーションを使用した、高度に統合されたハイブリッド環境に対して、SSO 用の SMA 認証情報を使用できます。

これを機能させるには、SMA および CAM IDP がマスターのユーザー認証情報リポジトリと同じ認証ストアを使用している必要があります。

CAM トラフィックフローを持つレガシーおよびフェデレーション型 ID SSO は、一般的な環境におけるトラフィックの流れを示しています。

CAM トラフィックフローを持つレガシーおよびフェデレーション型 ID SSO



SMA アプライアンスは、自らのユーザおよびレガシー SSO 向けに、内部認証サーバーへの独自の接続を使用するサービスです。CAM を使用して SaaS アプリケーションに SAML と WS-FED SSO の両方を提供します。

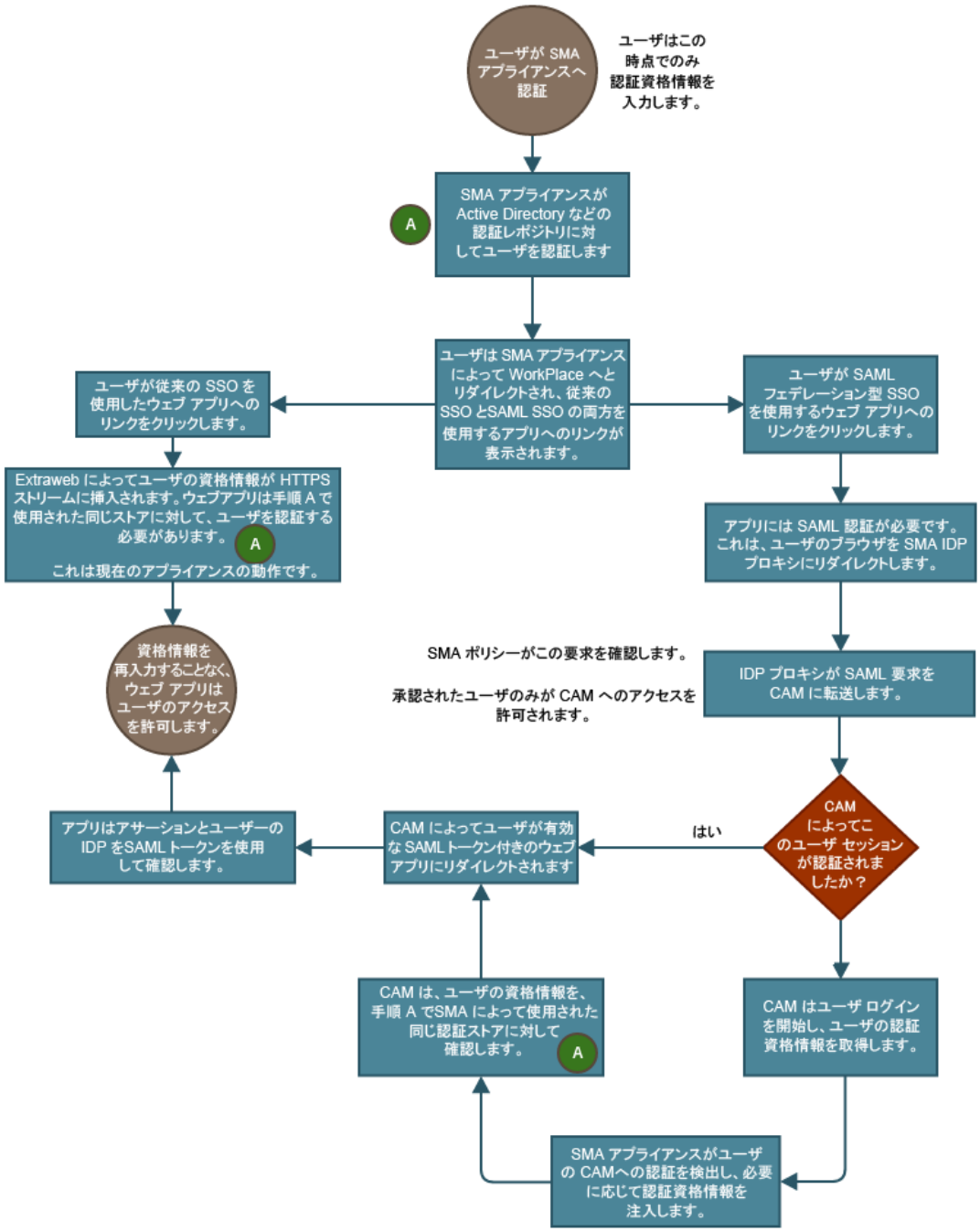
SMA アプライアンスは、インターネット上のどこからでも企業ネットワーク上のサービスに安全にアクセスできるように設計されているため、この目的に適しています。エンド ユーザと同じ VPN セッ

ションを利用して、同じ中央集中ポイント ポリシーを介してクラウドにある SaaS アプリケーションへのリクエストを仲介できます。

ユーザは、既存の非 SAML レルムを通じて最初に SMA アプライアンスに認証されます。次に、内部 CAM IDP にトラフィックを送信するように IDP プロキシが設定されます。これにより、必要に応じてユーザーの認証資格情報が注入されます。したがって、SAML および WS-FED トークンは、ユーザの操作なしに CAM によって生成され、レガシー SSO およびフェデレート型 SSO の両方を内部および外部のアプリケーション サーバにアクセスできるようにします。

CAM ユーザー認証を使用したレガシーおよびフェデレーション型 ID SSO は、ユーザーの認証方法を示しています。

CAM ユーザー認証を使用したレガシーおよびフェデレーション型 ID SSO



CAM を使用した SSO の設定

シングル サインオン (SSO) サービスがフェデレーション型 ID リソースにアクセスするときに、VPN セッションにクラウド アクセス マネージャ (CAM) を注入するように SMA を構成できます。次の制限事項に留意してください。

- SMA と CAM は、両方とも SSO 認証情報向けに同じ認証サーバーを使用する必要があります。
- SAML 2.0 フェデレーション型シングル サインオンは現在グローバル トラフィック オプティマイザ (GTO) では使用できません。スタンドアロンの 1 台の装置でのみ使用できます。

CAM を使用した SSO を設定するには:

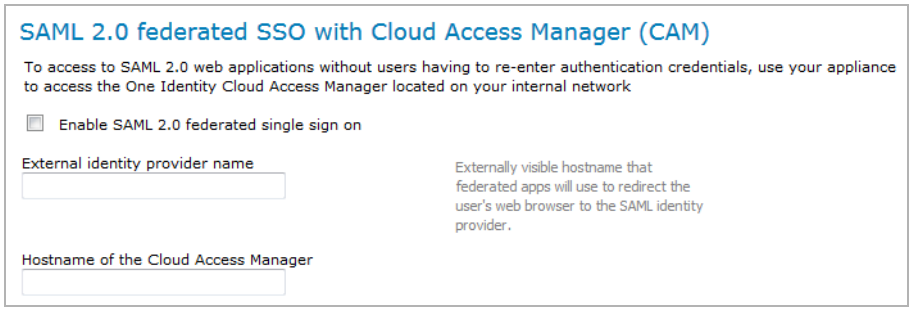
1 [**Managed Appliances (管理対象装置)** > **Configure (設定)** > **Define Policy (ポリシーの定義)**]ページに移動します。

2 [**User Access (ユーザ アクセス)**]セクションで[**Realms (レルム)**]をクリックします。

3 編集するレルムの名前をクリックします。

4 [**General (一般)**]ページで、[**Advanced (詳細)**]パネルを展開します。

5 [**Enable SAML 2.0 federated single sign on (SAML 2.0 フェデレーション型シングル サインオンを有効にする)**]のチェックボックスをオンにします。



6 [**External identity provider name (外部 ID プロバイダ名)**]フィールドで、SMA アプライアンスに CAM IDP プロキシ サービスの FQDN を入力します。次向けの **外部 ID プロバイダ名**:

- 非分割 DNS は、CAM のホスト名とは異なる必要があります。
- 分割 DNS は、CAM のホスト名と同じである必要があります。

7 **Hostname of the Cloud Access Manager (クラウド・アクセス・マネージャーのホスト名)**フィールドに、CAM が内部ネットワーク上で認識されている名前の FQDN を入力します。

[**Enable SAML 2.0 federated single-sign on (SAML 2.0 フェデレーション型シングル サインオンを有効にする)**]のチェックボックスをオンにすると、[**App Configuration (アプリ設定)**]リンクが使用可能になります。この場合、SMA は、CAM に中継される認証サービスにサービスプロバイダが使用する、透過的な IDP プロキシです。

[**App Configuration (アプリ設定)**]をクリックすると、SAML サービス プロバイダが SAML IDP で認証するために必要な次の 3 つの URL を表示できます。

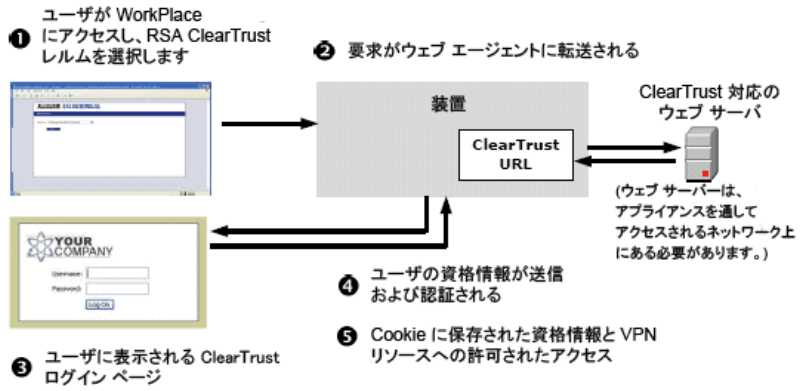
- サーバ ID: `urn:external_idp.example.com/CloudAccessManager/RPSTS`
- ログオン URL: `https://external_idp.example.com/CloudAccessManager/RPSTS/Saml2/Default.aspx`
- ログオフ URL: `https://external_idp.example.com/CloudAccessManager/RPSTS/Saml2/Logout.aspx`

RSA ClearTrust 認証の使用

SMA アプライアンスは、RSA ClearTrust 認証環境の認証情報を受け取ることで、認証をサポートします。ユーザーは、Web ブラウザを使用して接続する場合のみ、RSA ClearTrust サーバー経由で認証を受けることができます。

図 RSA ClearTrust 認証シーケンスは、ユーザーがログインして RSA ClearTrust 環境で認証を受ける場合の一般的なイベントの流れを示しています。

RSA ClearTrust 認証シーケンス



1 ユーザーが WorkPlace の URL を入力し、ドロップダウン メニューから ClearTrust レルムを選択します。ユーザーに対して 1 つのレルムのみを構成している場合、自動的にそれが選択されます。

2 SMA アプライアンスは、要求を適切な Web エージェントに転送します。ClearTrust Web エージェントは、AMC で指定した別の ClearTrust 対応の Web サーバー上にあります。

3 Web エージェントは、ClearTrust ポリシー サーバーとのチェックを実行し、対応する認証ページを表示して、ユーザーにクレデンシャルを入力するよう要求します。

4 ユーザーのクレデンシャルが Web エージェントに転送され、そのポリシー サーバーと比較して評価されます。

5 ユーザーのアクセスが承認または拒否されます。認証が成功すると、クレデンシャルが Cookie に保存され、WorkPlace セッションの間、ユーザーは VPN リソースにアクセスできます。

RSA ClearTrust 構成

RSA ClearTrust を構成してユーザーを認証するようにするには、アプライアンスは ClearTrust エージェントをホスティングしていないため、外部サーバーの URL を指定する必要があります。構成では、AMC を使用してプライベート キーを含む `.zip` ファイルと CGI スクリプトをエクスポートする必要があり、どちらも、ClearTrust 対応の Web サーバーにインストールする必要があります。

メモ：CGI スクリプト ファイルを RSA ClearTrust 対応 Web サーバーにインストールする場合、そのファイルの所有者、グループ、および権限がそのサーバーで正しく設定されている必要があります。

RSA ClearTrust 認証を構成するには、

1 AMC のメイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

2 [**New...(新規...)**] をクリックします。

3 [**Single sign-on (シングル サインオン)**] の下にある [**RSA ClearTrust**] をクリックします (指定できるのは 1 つの ClearTrust サーバーだけで、すでに構成済みである場合、このオプションはグレー表示されます)。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。

5 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

6 [**ClearTrust server URL (ClearTrust サーバー URL)**]フィールドに ClearTrust エージェントをホスティングする Web サーバーの URL を入力します。ClearTrust 対応の Web サーバーがデフォルトである 636 以外のポートでリッスンする場合、コロンの後に接尾辞として続けることでポート番号を指定できます。セキュア SSL 接続を使用する場合、このボックスに `https://` プロトコル識別子を含めます。

7 プライベート キーと CGI スクリプトを、RSA ClearTrust サーバー、またはRSA ClearTrust Web エージェントがインストールされているコンピュータにインストールする必要があります。[**Export (エクスポート)**]をクリックして `.zip` ファイル (デフォルトの名前は `ctAgent.zip`) にこれらを保存し、次のようにインストールします。

- プライベート キー ファイル (「***webagent.key***」という名前) を RSA ClearTrust サーバーの `/usr/local/webagent` ディレクトリに置きます。RSA ClearTrust Web エージェントがインストールされるコンピュータには、`/usr/lib` ディレクトリに `openssl` ライブラリが含まれている必要があります。または、少なくとも、`libssl.so.0.9.7` ライブラリと `libcrypto.so.0.9.7` ライブラリが同じディレクトリに含まれている必要があります。
- CGI スクリプトが RSA ClearTrust サーバーの `/cgi-bin` ディレクトリに置かれている必要があります。

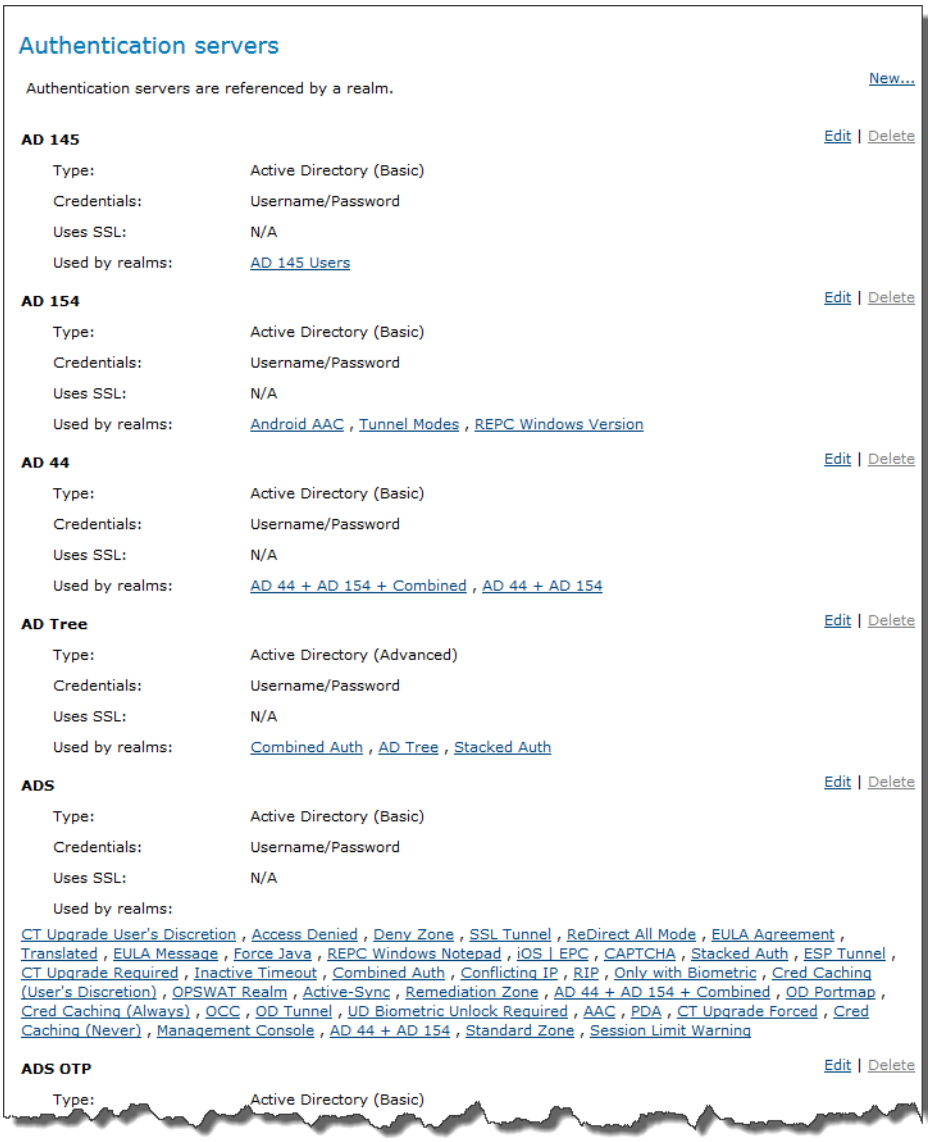
8 [**Save (保存)**] を選択します。

One Identity Defender

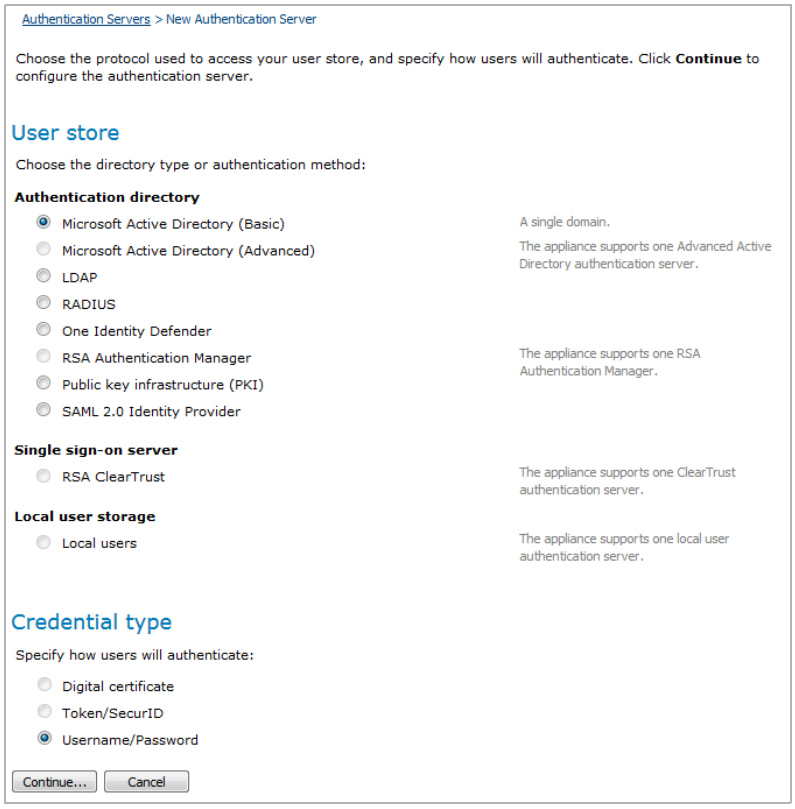
Defender は、2 要素認証用の製品です。SMA は、汎用 RADIUSサーバとして Identity Defender の設定をサポートします。

One Identity Defender を使用して新しい認証サーバーを設定するには:

1 AMC で、[**System Configuration (システム構成) > Authentication Servers (認証サーバー)**]ページに移動します。



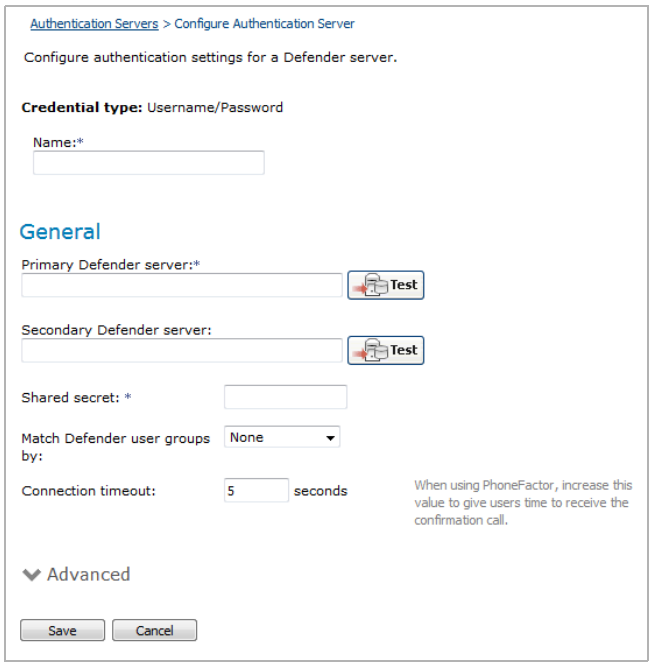
2 [**New... (更新...)**]をクリックします。[**New Authentication Server (新しい認証サーバー)**]ダイアログが表示されます。



3 [**One Identity Defender**]オプションを選択します。

4 [**Credential Type (認証情報タイプ)**]で、[**Token/SecurID (トークン/SecurID)**]または[**Username/Password (ユーザー名/パスワード)**]のいずれかを選択します。

5 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (認証サーバーの設定)**]ダイアログが表示されます。



6 [**Name (名前)**]フィールドに、認証サーバーの名前を入力します。

7 [**Primary Defender server (プライマリ Defender サーバー)**]フィールドに、プライマリ Defender サーバの IP アドレスを入力します。

8 [**Secondary Defender server (セカンダリ Defender サーバー)**]フィールドに、セカンダリ Defender サーバの IP アドレスを入力します。

9 [**Shared Secret (事前共有鍵)**]フィールドに事前共有鍵を入力します。

10 [**Match Defender user groups by (次で Defender のユーザー グループを一致させる)**]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。

- **なし** (既定)
- **filterid attribute (11)**
- **class attribute (25)**

11 [**Connection timeout (接続タイムアウト)**]フィールドに、接続タイムアウト値を秒単位で入力します。

12 [**Save (保存)**] を選択します。

ローカル ユーザー ストレージの構成

AMC でローカル ユーザー アカウントを作成し、ローカル認証レポジトリに対応させることができます。ローカル ユーザー アカウントの作成に関する詳細については、ローカル ユーザー アカウントの管理を参照してください。

アプライアンスには、ローカル ユーザー ストアを 1 つだけ作成できます。

ローカル ユーザー認証を設定するには、

1 AMC のメイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

2 [**New...(新規...)**] をクリックします。

3 [**Local user storage (ローカル ユーザー ストレージ)**] の下にある [**Local users (ローカル ユーザ)**] をクリックします (ローカル ストアがすでに存在する場合、このオプションはグレー表示されます)。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。

5 [**Name (名前)**] フィールドに認証サーバーの名前を入力します。

6 [**Password policy (パスワード ポリシー)**] エリアで、パスワードに許可する最小文字数と最大文字数を指定します。最小値は 4 に、最大値は 256 に設定できます。

7 ユーザーのパスワードに 1 文字以上の小文字が含まれている必要があることを指定するには、[**Lowercase letters (小文字)**]チェックボックスを選択します。

8 ユーザーのパスワードに 1 文字以上の大文字が含まれている必要があることを指定するには、[**Uppercase letters (大文字)**]チェックボックスを選択します。

9 ユーザーのパスワードに 1 文字以上の数字 (0 ～ 9) が含まれている必要があることを指定するには、[**Uppercase letters (数字)**]チェックボックスを選択します。

10 ユーザーのパスワードに 1 文字以上の記号 (~`!@#$%^&*()_-+={}[]|\:;"'<,>.?/) が含

メモ：パスワードでは、UTF-8 文字がサポートされています。

まれている必要があることを指定するには、[**Symbols (記号)**]チェックボックスを選択します。

11 [**Password expiration (パスワードの有効期限)**]エリアで[**Passwords expire after (次の後にパスワードを有効期限切れにする)**]チェックボックスをオンにします。チェックボックスの選択を解除すると、ユーザー パスワードは期限切れになりません。

- ユーザー パスワードの有効期限が切れるまでの日数を入力します。デフォルトは 60 日、最小値は 1 日、最大値は 365 日です。

12 [**Begin prompting user (ユーザーへの要求を開始)**]チェックボックスを選択し、ユーザーにパスワードの変更を要求するまでの日数を入力します。既定値は **14** 日間 です。

13 ログイン時に Windows ユーザーに表示されるプロンプトやその他のテキストを変更するには、[**Advanced (詳細)**]セクションを展開します。

14 [**Customize authentication server prompts (認証サーバーのプロンプトをカスタマイズ)**]チェックボックスをオンにします。

ページ タイトル、メッセージ、ログイン プロンプトなどをすべてカスタマイズできます。例えば、従業員 ID を使用してユーザーを識別する場合、[**Identity (ID)**] プロンプトを [**Username (ユーザ名):**] から [**Employee ID (従業員 ID):***] に変更できます。*この構成をテストに使用する場合、[**Message (メッセージ)**] をカスタマイズして、テストの手順やその他の指示が表示されるようにできます。

15 パスワードまたはその他の身元を証明するものを [**Proof (実証)**] フィールドに入力します。

16 ワンタイム パスワードによる二要素認証を構成するには、[**One-Time Passwords (ワンタイム パスワード)**]エリアで[**Use one-time passwords with this authentication server (この認証サーバーでワンタイム パスワードを使用)**]を選択します。

17 [**Passwords contain (パスワードが次を含む)**] フィールドにパスワードの文字数と文字タイプを入力して、パスワードの形式を定義します。

18 [**From address (送信元アドレス)**] フィールドに、ワンタイム パスワードの送信元の電子メール アドレスを入力します。

19 オプションで、[**Default domain (既定ドメイン)**] フィールドに、ワンタイム パスワードを送信するローカル ユーザーの電子メール アドレスを作成するために、それぞれのユーザー名に付加するドメインを入力します。

20 [**Email address (電子メール アドレス)**] フィールドでそれぞれのローカル ユーザー名の電子メール アドレスを構成することで、デフォルト ドメインを上書きできます。この電子メール アドレスは、`primaryEmail` という名前の User 属性タイプ ポリシー変数として使用できるようになります。ユーザーごとに 1 つの電子メール アドレスがサポートされています。

21 [**Send test message (テスト メッセージを送信)**] ボタンをクリックしてテスト用の電子メール メッセージを送信し、そのメッセージ、パスワード、および SMTP の設定が正しいことを確認します。

22 [**Subject (件名)**] フィールドに、ワンタイム パスワードを電子メールで送信するときの件名のテキストを入力します。

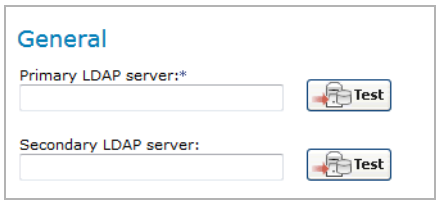
23 [**Body (本文)**] フィールドに、ワンタイム パスワードを含む電子メールの内容を入力します。

ワンタイム パスワードの詳細については、ワンタイム パスワードの使用によるセキュリティの強化を参照してください。

24 [**Save (保存)**] を選択します。

LDAP および AD 認証構成のテスト

認証構成の設定を検証するため、Microsoft Active Directory サーバーと LDAP サーバーの構成に使用する AMC ページには、[**Test (テスト)**] ボタンがあります。このボタンをクリックすると、外部ユーザーレポジトリとの通信が確立され、ステータス情報が提供されます。



アプライアンスが正しく構成されていれば、「`Valid connection!`」というメッセージが表示されます。構成の設定に問題があると、問題を説明するメッセージが表示されます。

メモ：テスト接続機能は、あくまでもアプライアンスが外部ディレクトリにバインドできるかどうかをテストするためのものです。ログイン クレデンシャルを入力すると、アプライアンスはそれを使用しますが、入力しないと、ディレクトリにアノニマスにバインドしようとします。実際にはディレクトリを検索しないため、接続をテストしても、このログイン クレデンシャルで構成されているドメインにアクセスできるかどうかは検証されません。

連鎖式認証の構成

セキュリティを強化するために、ユーザーが 2 つの異なる認証方法を使用して 1 つのレルムで認証されるようにすることもできます。例えば、RADIUS またはデジタル証明書を最初の認証方法として設定し、LDAP または Active Directory を 2 番目の認証方法として設定できます。ローカル認証ストアを、プライマリまたはセカンダリのいずれかの認証サーバーとして使用できます。ユーザーの名前がプライマリおよびセカンダリの認証サーバーの名前と同じでなければならないように設定することもできます。ユーザーのログオン時の作業を 1 ステップ プロセスにするためには、AMC を構成して 1 セットのプロンプトだけがユーザーに表示されるようにします。

連鎖式認証を設定するには、

1 AMC のメイン ナビゲーション ページから、[**Realms (レルム)**] をクリックします。

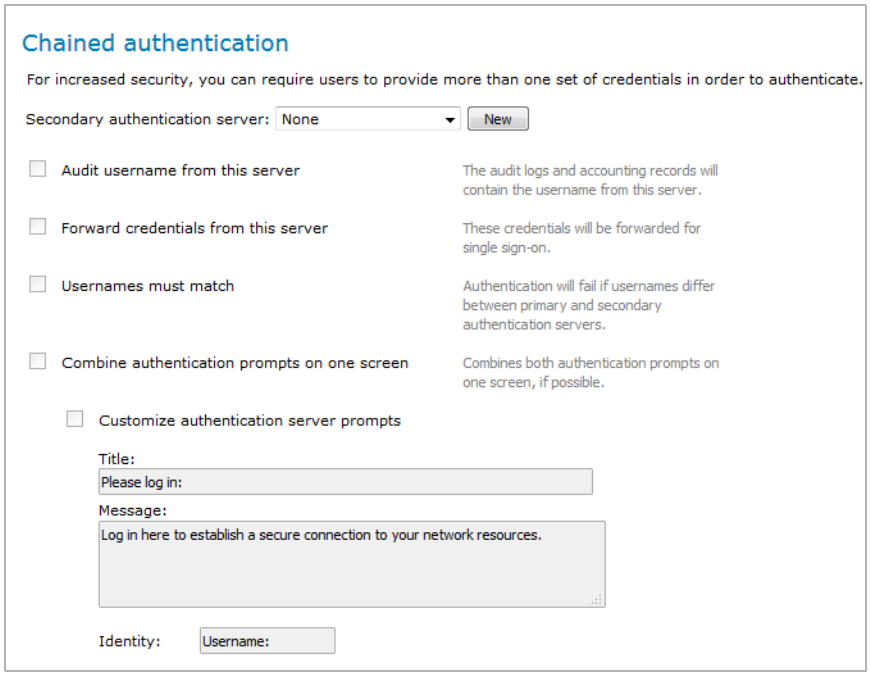
2 次のどちらかを選択します。

- 変更するレルムの名前
- [**New (新規)**]を選択し、[**Authentication server (認証サーバー)**]ドロップダウン メニューでエントリを選択します。

これがプライマリ認証サーバーになります。

連鎖式認証のいずれかのクレデンシャル タイプがデジタル証明書である場合、対応する認証はプライマリ サーバーである必要があり、PKI サーバーをセカンダリ認証サーバーとして構成することはできません。

3 「**Advanced (詳細)**」をクリックし、「**Chained authentication (連鎖式認証)**」セクションまでスクロールします。



4 [**Secondary authentication server (セカンダリ認証サーバー)**]を選択します (何も定義されていない場合は[**New (新規)**]をクリックします。認証サーバーの設定の手順については、認証サーバーの構成を参照してください)。

5 認証の設定にリストされた、これ以外の (オプションの) 設定は、セキュリティを強化したり、トラブルシューティングに利用したり、ログイン プロセスを簡略化したりするために使用します。

認証の設定

設定	説明
このサーバーからのユーザ名を監査	監査ログとアカウンティング ログに (プライマリ認証サーバーのユーザー名ではなく) セカンダリ認証サーバーのユーザー名を表示します。
Forward credentials from this server	シングル サインオンでは、1 セットのクレデンシャルをバックエンド Web リソースに転送する必要があります。このチェックボックスを選択すると、この (セカンダリ) 認証サーバーからクレデンシャルが転送されます。

認証の設定

設定	説明
Usernames must match	このチェックボックスが選択されている場合、最初の認証手順で送信されたユーザー ID が 2 番目の手順で送信されたユーザー ID が異なると、認証が失敗します。このオプションは、認証方法でユーザー名/パスワードまたはトークン、または証明書のいずれかが使用される場合に使用できます。 このオプションの用途として、プライマリ認証サーバーは証明書を使用し、セカンダリ認証サーバーはユーザー名/パスワードを使用する例が考えられます。このオプションが有効になっていないと、エンド ユーザーは、最初のユーザーに有効なクレデンシャルがあった場合に、別のユーザーのクレデンシャルでログインできます。この設定をオンにすると、証明書のユーザー名がユーザー名/パスワード クレデンシャルのユーザー名と一致しないため、その認証は失敗します。
認証情報の要求を 1 つの画面にまとめる	このチェックボックスを選択すると、アプライアンスは、ユーザ名が両方の認証サーバーで同じであるかどうかを確認します。ユーザー名が同じである場合、ユーザーのクレデンシャルを要求するプロンプトが 1 つの画面に組み合わせて表示されます。ユーザー名が異なる場合、ログインが拒否され、(安全上の理由から) 理由を説明するエラー メッセージは表示されません。 ユーザー クレデンシャルにデジタル証明書が含まれている場合は、ユーザー名が両方のサーバーで同じであっても、認証プロンプトを組み合わせることはできません。
認証サーバーのプロンプトをカスタマイズ	([**Combine authentication prompts on one screen (認証情報の要求を 1 つの画面にまとめる)**] が選択されている場合に、Windows クライアントでのみ指定できます。) 認証サーバーの構成時に、ユーザーに表示されるプロンプトをカスタマイズするオプションがあります。2 つのこのようなサーバーが連鎖されている場合、[**Title (タイトル)**]、[**Message (メッセージ)**]、[**Identity (ID)**] フィールドをカスタマイズして組み合わせた認証プロンプトをユーザーに提示できます。パスワード フィールドの名前は、それぞれの認証サーバーの構成から取り込まれます。 このカスタマイズ構成が選択されていない場合、2 つの認証サーバーで構成されているプロンプトが表示されます。

連鎖式認証ログインの例

この例では、システム管理者が「*Employees*」という名前のレルムに対して 2 つの認証方法を設定しています。

プライマリ認証サーバーは RADIUS を使用しています。([**Configure Authentication Server (設定認証サーバ)**] ページの [**Advanced (詳細設定)**] 設定にある) [**Proof (実証)**] プロンプトは「*Passcode*」にカスタマイズされています。

セカンダリ認証サーバーは LDAP を使用しています。[**Proof (実証)**] プロンプトは「*Remote access password*」にカスタマイズされています。

[**Configure Realm - Employees (レルムの設定 - 従業員)**]ページの[**Advanced (詳細)**]には、カスタマイズされた[**Title (役職)**]、[**Message (メッセージ)**]、および[**Identity (ID)**]のプロンプトが表示されます。

AMC の設定に基づき、次のようなログイン画面がユーザーに表示されます。

両方の認証サーバーでユーザー名が同じであるため、ユーザーは自分のユーザー名を 1 度だけ入力します。

メモ：

- ユーザーがユーザー名またはパスワードの入力を間違えると、エラー メッセージ (「設定した認証情報が無効です」) が表示され、セカンダリ認証サーバーのプロンプトのみが表示されます。クレデンシャルを再入力するには、ブラウザの [**Back (戻る)**] ボタンをクリックして最初のログイン ページに戻る必要があります。
- ユーザー名とパスワードが両方の認証方法で使用される場合、ユーザー名が同じである必要はありません (ただし、一般的には同じです)。プライマリ ユーザー名が AMC の AMC 管理者などの役割にマッピングされている場合、セカンダリ ユーザー名を同じ役割に割り当てる必要はありません。両方のサーバーで両方のユーザー名の認証が成功すると、プライマリ ユーザー名の役割に対応するアクセスが付与されます。

レルムでのグループ アフィニティ チェックの有効化

アプライアンスは、「グループ アフィニティ チェック」をサポートしています。これは、あるサーバーでユーザーを認証し、2 番目のディレクトリでユーザーが属するグループ (ある場合) の情報を提供するようなネットワーク環境です。このような状況は、認証には RADIUS SecurID トークンが使用され、ユーザーのグループ情報は LDAP サーバーまたは アクティブ ディレクトリ サーバーから送られてくるような場合に当てはまります。(これに対し、連鎖式認証では、2 つの認証サーバーでユーザーを認証する必要があります。詳細については、連鎖式認証の構成を参照してください)。

グループ メンバーシップは、アクセス制御の重要な要素です。ディレクトリに保管されているユーザー グループを参照し、アクセス制御ルールでそれらのグループを参照するよう、アプライアンスを構成できます。

メモ：アクティブ ディレクトリ (AD) サーバーを LDAP サーバーとして使用すると、ACL 検査を実行できません。短縮名 (SN) または共通名 (CN) は、LDAP サーバーではサポートされていません。これらは、AD サーバーでのみサポートされています。

グループ アフィニティ チェックを有効にするには、

1 AMC のメイン ナビゲーション ページから、[**Realms (レルム)**] をクリックします。

2 変更するレルムの名前をクリックします。

3 「**詳細設定**」を選択します。[**Group authorization (グループ認証)**]エリアで、[**Enable group affinity checking (グループ アフィニティ チェックを有効にする)**]チェックボックスを選択します。

4 [**Server (サーバー)**]ドロップダウン メニューで、グループ情報を保管する LDAP サーバーまたは アクティブ ディレクトリ サーバーの名前を選択します。[**New (新規)**] をクリックして新しいグループアフィニティ グループ サーバーを定義することもできます。

認証サーバーのグループ承認チェックが無効の場合、サーバーは指定可能なアフィニティ サーバーのリストに表示されません。詳細については、認証チェックの無効化を参照してください。

5 [**Save (保存)**] を選択します。

レルムの作成のプロセスでグループ アフィニティ チェックを有効にすると、使用できるボタンが異なります。

- [**Next (次へ)**]をクリックして、[**Configure Realms (設定レルム)**] ページの [**Communities (コミュニティ)**] タブを表示します。
- [**Finish (完了)**] をクリックして、[**Authentication (認証)**] ページに戻ります。

ワンタイム パスワードの使用によるセキュリティの強化

ワンタイム パスワード (OTP) は、ランダムに生成され、1 度だけ使用されるパスワードです。OTP を認証の 2 番目の要素として使用すると、ユーザーのセキュリティが強化されます。標準のユーザー名とパスワードのクレデンシャルの送信後に、システムによって生成されたワンタイム パスワードが、事前に定義された SMS または電子メール アドレスのユーザーに送信されます。ユーザーは次に、その電子メール アカウントにログインして OLT を取得し、プロンプトに入力します。ログインの成功、取り消し、または失敗の後に新しい OTP が毎回生成されるため、パスワードが危険にさらされる可能性が低くなります。

OTP を含む認証を構成するには、以下の手順を実行する必要があります。

- メール サーバーを構成します。ワンタイム パスワードが外部ドメインに配信される場合 (例えば、SMS アドレスや外部 Web メール アドレス)、SMTP サーバーを構成してアプライアンスから外部ドメインにパスワードを送信できるようにする必要があります。
- 認証サーバーの構成の [**Advanced (詳細設定)**]エリアで、OTP を構成します。OTP が送信される電子メール アドレスを保管するディレクトリ属性を指定します。

トピック:

- ワンタイム パスワードの配信のための SMTP の構成
- ワンタイム パスワードのための認証サーバーの構成
- AD または LDAP ディレクトリ サーバーの構成

ワンタイム パスワードの配信のための SMTP の構成

ワンタイム パスワードを配信する電子メール アドレスが外部ドメインにある場合 (SMS アドレスや外部の Web メール アドレスなど)、SMTP サーバーを構成して、アプライアンスから外部ドメインにパスワードを送信できるようにする必要があります。

Microsoft Exchange を構成してワンタイム パスワードをサポートするようにするには、

1 [**Exchange System Manager (Exchange システム マネージャ)**]に移動します。

2 [**Servers (サーバ) > Protocols (プロトコル) > SMTP (SMTP)**]を展開します。

3 [**Default SMTP Virtual Server (既定の SMTP 仮想サーバー)**]または該当する SMTP サーバー インスタンスを右クリックします。

4 [**Property (プロパティ)**] を選択します。

5 [**Access (アクセス)**]タブを選択します。

6 [**Relay Restrictions (中継の制限)**] エリアの [**Relay (中継)**] をクリックします。

7 [**Only the list below (以下のリストのみ)**]を選択します。

8 [**Add (追加)**] を選択します。

9 SMA アプライアンスの IP アドレスを入力します（例: `10.50.165.5`）。

10 [**OK**] を選択します。アプライアンスが [*アクセスが許可されました*] のステータスでリストに表示されます。

11 [**OK**] を選択します。

ワンタイム パスワードのための認証サーバーの構成

ワンタイム パスワードを配信する電子メール アドレスが外部ドメインにある場合 (SMS アドレスや外部の Web メール アドレスなど)、ワンタイム パスワードの配信のための SMTP の構成に記載されている方法で、SMTP サーバーを構成して、アプライアンスから外部ドメインにパスワードを送信できるようにする必要があります。

認証サーバーごとに、OTP が送信される電子メール アドレスを保管するディレクトリ属性も指定する必要があります。プライマリ属性を指定する必要があり、プライマリが見つからなかった場合に問い合わせるセカンダリ属性も指定できます。

認証サーバーを構成してワンタイム パスワードをサポートするようにするには、

1 AMC のメイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

2 構成を変更する AD (**マイクロソフト アクティブ ディレクトリ**または**マイクロソフト アクティブ ディレクトリ ツリー**)、LDAP、またはローカルの認証サーバーの隣にある [**Edit (編集)**] をクリックします。

3 必要があれば[**Credential type (認証タイプ)**]を選択します。

4 [**Continue...(続ける...)**] を選択します。

5 [**Advanced (詳細)**]エリアを展開し、

6 [**Use one-time passwords with this authentication server (この認証サーバでワンタイム パスワードを使用)**]を選択します。

7 ワンタイム パスワードを送信する電子メール アドレスのディレクトリ属性を入力します。プライマリ属性が認証サーバーに存在する場合はそれが使用され、存在しない場合にセカンダリ属性が指定されていればそれが使用されます。

AD または LDAP ディレクトリ サーバーの構成

AD または LDAP ディレクトリ サーバーのスキーマには、ワンタイム パスワードを送信する電子メール アドレスを含む属性が含まれている必要があります。ローカル認証ストアは [**primaryEmail**] 属性を使用しますが、この属性は、ローカル ユーザー アカウントを編集することで、ユーザー単位で構成できます。ローカル ユーザー アカウントの管理を参照してください。

このアドレスは、ユーザーの会社の電子メール アドレスでなくても構いません。認証を完了するには、OTP が含まれる電子メールをユーザーが開くことができる必要があり、会社のアドレスに送信されると、ユーザーがそのアカウントにまだアクセスできない可能性があります。

ワンタイム パスワードを構成して、SMS 対応の携帯電話に電子メールのメッセージが直接送信されるようにできます。SMS 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。

ユーザーの SMS アドレスが含まれる属性 (例えば、**SMSphone**) に合わせて、ディレクトリ サーバー (AD または LDAP) のスキーマを変更する必要があります。使用するアドレスは、ユーザーの電話番号やサービス プロバイダによって異なります。例えば、米国の電話番号の Verizon の電話の属性値であれば、*<10 桁の電話番号>*`@vtext.com` というようになります。

個人用機器認証の設定

個人用機器認証によって、ユーザがアプライアンスに登録されていない個人用機器を使用して企業ネットワークに接続すると、デバイスを登録するよう求められます。企業のリソースにアクセスするには、個人用機器の企業ポリシーとプライバシーポリシーに同意する必要があります。

ユーザーが機器の企業ポリシーに同意すると、機器の一意の機器 ID が決定され、装置によってその機器がユーザーに登録されます。この機器からの以降の接続には、機器の承認は必要ありません。

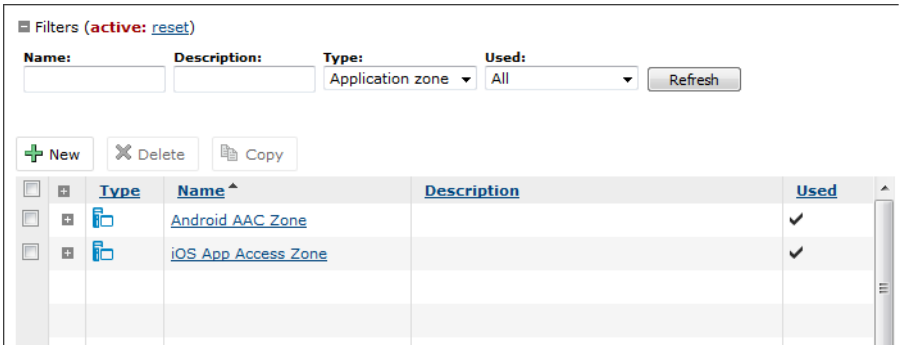
また、ユーザー アクセスとポリシー詳細の表示で説明されているように、装置にアクセスした個人用機器の使用状況を監視することもできます。

個人用機器認証のためのアプリケーション ゾーンを作成するには:

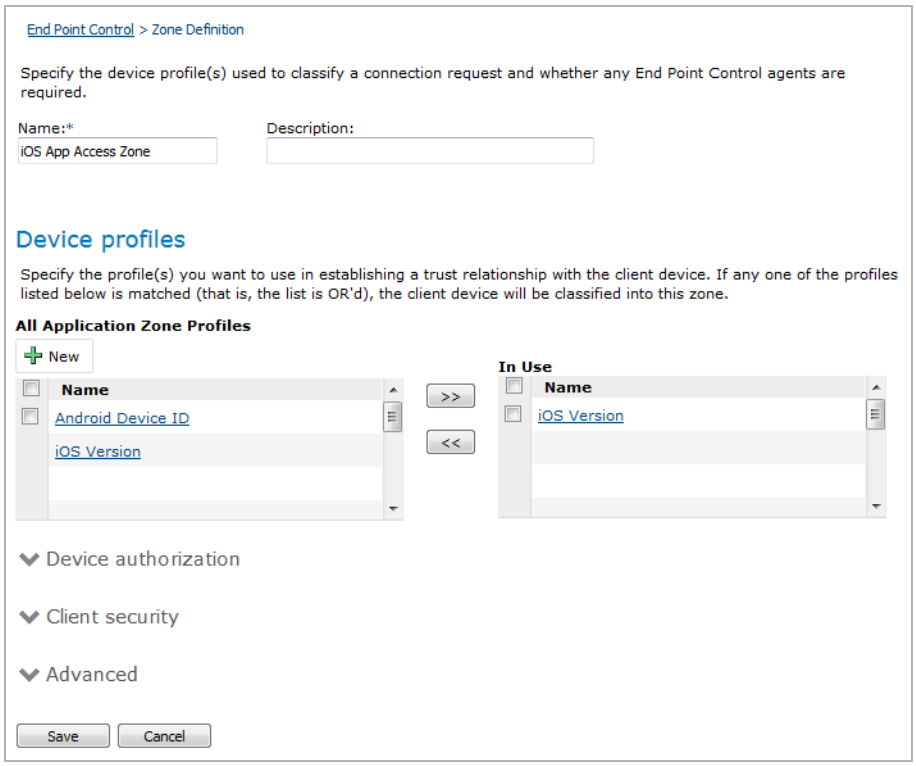
1 [**Managed Appliances (管理対象装置) > Configure (設定) > Define Policy (ポリシーの定義) > End Point Control**]ページに移動します。

2 [**Zones and Profiles (ゾーンとプロファイル)**]セクションで、[**Zones (ゾーン)**]の横にある[**Edit (編集)**]をクリックします。

3 [**Filters Type (フィルタ タイプ)**]ドロップダウン メニューから[**Application zone (アプリケーション ゾーン)**]を選択し、[**Refresh (更新)**]をクリックします。すべてのアプリケーション ゾーンが表示されます。



4 任意のアプリケーション ゾーンをクリックすると、[**Device profiles (機器プロファイル)**]が表示されます。アプリケーション アクセス制御対応のもののみがプロファイルに含まれます。

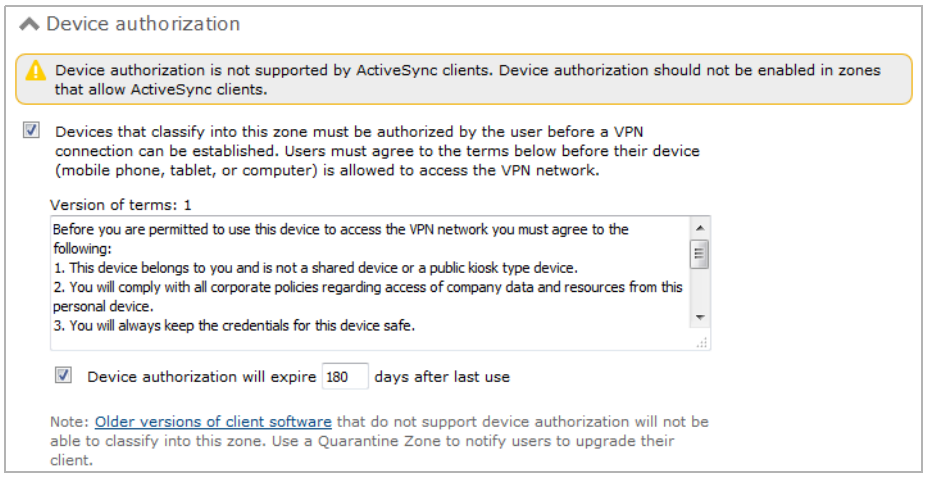


5 [**All Application Zone Profiles (すべてのアプリケーション ゾーンのプロファイル)**]リストで、ゾーンに必要なプロファイルのチェックボックスをオンにします。

6 右矢印 (>>) ボタンをクリックします。アプリケーションが作成中のゾーンに入るために一致する必要があるのは、[**In Use (使用中)**]リストのプロファイルのいずれか 1 つだけです。

このゾーンにデバイス プロファイルが存在しない場合は、[**New (新規)**] をクリックして 1 つ追加します。

7 [**Device authorization (機器の認証)**]を展開します。



8 [**Device Authorization (機器の認証)**]エリアの一番上のチェックボックスをオンにして、VPN 接続が確立される前にユーザーに個人用機器の認証を要求します。デフォルトでは、このチェックボックスは、アプリケーション ゾーンに対してEPC が有効になっている場合にチェックされています。

9 ユーザーが同意する必要がある承認条件を変更するには、[**Device Authorization (機器の認証)**]エリアの[**Terms (条件)**]セクションに必要な承認条件を入力します。条件を編集するには、[**Device Authorization (機器の認証)**]チェックボックスをオンにする必要があります。

10 デフォルトでは、ユーザー認証は、機器が最後に使用された **180** 日後に失効します。機器の認証が有効になっている場合は、有効期限チェックボックスをオフにするか、期限が切れるまでのお好みの日数を入力して変更することで、ゾーン認証の有効期限を無効にすることができます。

11 デフォルトでは、接続がアクティブでない場合、ゾーンへのユーザー接続は破棄されません。ただし、[**Inactivity timer (休止タイマー)**]エリアで休止タイマーを設定して、一定時間休止した後に接続を終了することができます。休止タイマー間隔は 3 分から 10 時間まで設定できます。

12 コミュニティでの End Point Control 制約の使用の説明に従って、ゾーンをコミュニティに追加します。

生体認証

トピック:

- 生体認証について
- 生体認証の設定
- コマンド ライン インターフェイス (CLI) での API の使用

生体認証について

この機能によって、モバイル接続デバイスでキャッシュされた資格情報のロックを、生体認証を使用して解除するオプションを使用できます。

認証情報のキャッシュにより、ユーザは認証資格情報を再入力せずに SMA アプライアンスへの接続を確立できます。認証情報のキャッシュは利便性に優れますが、ユーザーの機器が所有者以外の者に

よって使用されている場合、許可されていないユーザーが企業ネットワークにアクセスする可能性があります。生体認証を使用して、これらのキャッシュされた認証情報にアクセスできるユーザーを制御できます。

生体認証では、ユーザーは顔または指紋を使用してキャッシュされた認証情報をロック解除できます。

管理者は、iOS 端末や Android 搭載端末で生体認証を有効にすることができます。エンド ユーザーは、認証のためにキャッシュされた認証情報に加えて、生体認証を必要とすることもできます。

管理者が行えること:

- 認証情報のキャッシュを有効にするよう選択できます。
- 特定の種類のクライアント (iOS、Android、または両方) が認証情報のキャッシュを使用できるようにできます。
- 生体認証と組み合わせた場合のみ認証情報のキャッシュを許可するようにできます。

構成設定でユーザーの生体認証を無効にすることにより、他のユーザーの生体 ID を使用して企業ネットワークにアクセスすることを防ぐことができます。生体情報を使用してキャッシュされた認証情報をロック解除するデバイスには、認証情報がキャッシュされている個人の認証署名のみが含まれていることを示す*利用規約*を記載することを推奨します。この機能では、キャッシュされた認証情報をロック解除し、キャッシュされた認証情報を認証に使用するためにのみ生体認証を使用できます。

メモ：Connect Tunnel クライアントまたは Web アクセス方式では、生体認証はサポートされていません (モバイル接続のみ)。

生体認証の設定

SMA ユーザ インタフェース (UI) を使用して生体認証を設定できます。

生体認証の許可を有効にするには:

1 SMA アプライアンスで、[**Realms (レルム) > Configure Community (コミュニティの設定) > Access Methods (アクセス方法) > Network Tunnel Client Configure (ネットワーク トンネル クライアントの設定) > Connect Tunnel (トンネルに接続) > User interface (ユーザ インターフェース) > Use cached credentials (キャッシュされた認証情報の使用)**]ページに移動します。

2 以下のいずれかのオプションを選択します。

   a [**Always (常に)**] - 常にキャッシュされた認証情報を使用します

   b [**At user's discretion (ユーザーの裁量で)**] - [**no caching (キャッシュなし)**]、[**biometric unlock required (生体認証でのアンロックを要求)**]、[**auto login from cache (キャッシュからの自動ログイン)**]を選択します。

   c [**Only with biometric verification (生体認証のみで使用)**] - 生体認証がサポートされ、有効になっている場合のみ、生体認証のキャッシュを使用します。キャッシュされた認証情報は、生体認証の検証後にのみ使用されます。

3 [**Only with biometric verification (生体認証のみで使用)**]を選択した場合、次のオプションのうち少なくとも 1 つを選択します。

   a [**Touch ID**] - iOS 機器

   b [**Fingerprint authentication (指紋認証)**] - Android 機器

   c [**Never (使用しない)**] - キャッシュされた認証情報を使用しない

コマンド ライン インターフェイス (CLI) での API の使用

次の API を使用して、コマンドラインインターフェイス (CLI) で、生体 ID の現在の状態を取得したり生体認証を有効にして設定したりできます。

- 属性: `autoCredentialLogon: require_biometrics`
- 属性: `clientSettings`

以下の SMA 12.1 APIガイドを参照してください。

- *Secure Mobile Access 認証 API*
- *Secure Mobile Access アプライアンス管理コンソール セットアップ API*
- *Secure Mobile Access アプライアンス管理コンソール API*

次のステップ

基本的なセットアップが終了し、アプライアンスの SSL 証明書を取得し、認証設定を構成したら、ユーザーとユーザー グループの管理、リソースの定義、アクセス制御ルールの構成に着手できます。

第 5 部

管理

- セキュリティ管理
- システム管理

セキュリティ管理

- リソースの作成と管理
- アクセス制御ルール

リソースの作成と管理

セキュリティの管理は、管理者にとって最も重要な役割でしょう。装置管理コンソール (AMC) を使用すると、セキュリティ管理の基本要素 (リソースやアクセス制御リスト) を簡単に管理できます。

このセクションでは、個別のリソース、リソース グループ、リソースの構成設定の作成と管理の方法を説明します。リソースは、アクセス制御ルールで参照する前に定義することも、アクセス制御ルール インターフェースで直接定義することもできます(後者の方法については、アクセス制御ルールからのユーザーとリソースの追加を参照してください)。

アプライアンスのコマンドラインで使用できるツールで、DNS で解決できないホストを参照しているかどうか、アクセス制御ルールに参照されていないリソースが含まれているかどうかを確認できます。詳細については、ホストの確認を参照してください。

トピック:

- リソース タイプ
- リソースとリソース グループ
- リソースと WorkPlace ショートカットの定義での変数の使用
- リソース グループの作成と管理
- Web アプリケーション プロファイル
- フォームベースのシングル サインオン プロファイルの作成
- Kerberos の制限付き委任
- Microsoft Outlook Anywhere 向け SMA のサポートの設定

リソース タイプ

SMA アプライアンスは、次のカテゴリに分類されるさまざまな企業リソースへのアクセスを提供します。

- 組み込みリソース
- Web リソース
- クライアント/サーバー リソース
- ファイル共有リソース

組み込みリソース

アプライアンスにはいくつかのリソースが組み込まれており、これらのリソースを使用すると、WorkPlace ポータルのセットアップですぐに取得できます。これらのリソースは削除できず、一部のリソースには、WorkPlace のショートカットからアクセスできます。

Secure Mobile Access WorkPlace (リソース タイプ: URL)

WorkPlace ポータルを使用すると、ユーザーが Web ベースのリソースにアクセスできます。このタイプのリソースは、他の組み込み項目によって使用され、あらゆるゾーンのあらゆるユーザーにデフォルト WorkPlace ポータルへのアクセスを許可する、「permit-all」 (すべて許可)のルールを変更できます。

値:`http://127.0.0.1:8085/workplace/`

Connect Tunnel (リソース タイプ: URL)

Connect Tunnel は、ネットワーク リソースへのブロード アクセスを提供するアプリケーションです。Connect Tunnel クライアントへのユーザーのアクセス方法を管理者が決定します。

- ユーザーが WorkPlace のリンク (ショートカット) から Connect Tunnel クライアントをダウンロードして有効にできるようにします。ユーザーにこのリソースへのアクセスを許可すると、クライアントのインストールと使用の両方を許可することになります。このリソースへのアクセスが許可されていないユーザーは、Connect Tunnel を使用してネットワーク リソースにアクセスできません。WorkPlace のこのリソースのショートカット (*Install Connect Tunnel*) は変更または削除できますが、リソースそのものは変更または削除できません。
- Connect Tunnel クライアントのセットアップ パッケージを展開します。ユーザーが Secure Mobile Access WorkPlace にログインする必要はありません。

値:`http://127.0.0.1:8085/ctdownload/`

Network Explorer (リソース タイプ: ネットワーク共有)

Network Explorer は、WorkPlace からアクセスできる Web ベースの拡張機能で、ユーザーに使用が許可されている任意の Windows ファイル システム リソースにアクセスできます (Windows 以外のプラットフォームのデスクトップ ブラウザからであっても)。該当するリソースとしては、サーバー、コンピュータ、ワークグループ、フォルダ、ファイルがあります。WorkPlace のこのリソースのショートカット (*Network Explorer*) は変更または削除できますが、リソースそのものは変更または削除できません。

値:`smb://127.0.0.1/networkexplorer/`

Web リソース

Web リソースには、HTTP または HTTPS を使用してアクセスする、Web ベースのアプリケーションやサービスが含まれます。例えば、Microsoft Outlook Web Access などの Web ベースの電子メール プログラム、Web ポータル、企業のイントラネット、標準 Web サーバーなどがこれに該当します。

Web トラフィックは、Web プロキシ サービスによってプロキシされます。ユーザーは、このセキュアなゲートウェイ経由で、インターネットからプライベートの Web リソースにアクセスできます。Web リソースをアクセス制御ルールの接続先として定義する場合、その **Web browser (Web ブラウザ)** が、ルールで使用できるクライアント ソフトウェア エージェントに入っていることを確認してください。詳細については、無効な接続先リソースの解決を参照してください。

Web リソースの定義例 に記載されている通り、Web リソースは、いくつかの方法で定義できます。

Web リソースの定義例

URL のタイプ	例
標準 URL	`http://host.example.com/index.html`
ポート番号付きの標準 URL	`http://host.example.com:8445/index.html`
セキュア サイトの URL	`https://host.example.com/index.html`
IP アドレスを含む URL	`http://192.0.34.0/index.html`
マッチング URL	ワイルドカードを使用して、Web リソースのグループを参照します。 `http://mailserver*.company.com/` **メモ：** クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。
パスとクエリ文字列のマッチング URL	パス エレメントやクエリ文字列値を特定の URL と一致させることで、電子メールの添付ファイルをブロックしたり、Web ベースのアプリケーションが制限されているデータを表示しないようにします。 `http://www.patient-records.com/reports.aspx?last_name=`

メモ： Web ベースのアプリケーションの中には、HTTP 以外のプロトコルを使用する Java アプレットやその他のブラウザ エクステンションを使用するものもあります。これらのアプリケーションにも Web ブラウザを使用してアクセスしますが、これらは、Web リソースとしてではなく、クライアント/サーバーとして定義し、ネットワーク トンネル クライアントまたはクライアント/サーバー プロキシ エージェントを使用してアクセスする必要があります。このようなアプリケーションとしては、Citrix NFuse、Oracle J-Initiator、および一部のバージョンの SAP および PeopleSoft などがあります。

クライアント/サーバー リソース

クライアント/サーバー リソースは、TCP/IP 経由で動作する企業アプリケーションです (UDP を使用するアプリケーションを含む)。このようなアプリケーションとしては、Citrix のようなシンクライアント アプリケーション、Microsoft Outlook のようなフル クライアント/サーバー アプリケーション、Lotus Notes、SAP、ターミナル サーバーなどがあります。

これらのタイプのクライアント/サーバー アプリケーションは、ホスト名、IP アドレスまたは IP 範囲、サブネット IP アドレス、または DNS ドメインを指定することで定義します。これらのリソースは、複数の Web リソースを含むネットワーク オブジェクト (ドメインなど) の定義や、接続要求の送信元によってアクセスを制御できるネットワーク オブジェクトの定義にも使用できます。

リソース タイプの構文に、これらのリソース タイプのそれぞれの定義で使用する構文を記載します。ホスト名は、完全修飾または修飾なしで記述できます。

リソース タイプの構文

リソースのタイプ	例
ドメイン	`private.example.com`
ホスト名	`bart.private.example.com`
ホストの IP アドレス	`192.0.34.72`
IP 範囲	`192.0.34.72 - 192.0.34.74`
サブネット	`192.0.34.0 / 255.255.255.0`

例

この例では、Web 開発チームが 1 台の Web サーバー、3 つの仮想 Web サーバーを使用していて、開発プロセスのステージごとに 1 つの仮想 Web サーバーを使用しています。それぞれの仮想 Web サーバーは異なるポートでリッスンします。

Web 開発チームは、3 つの異なる URL リソースを作成するのではなく、Web サーバーを定義することで、すべてのポートのトラフィックを**Host name or IP (ホスト名または IP)** (例えば、`webdev.yourcompany.com`) のリソース タイプとしてプロキシするようにできます。さらに、シングル サインオン Web アプリケーション プロファイルを追加し、3 つの仮想 Web サーバーすべてを 1 度に定義し、同じ SSO プロファイルを共有します。

```
webdev.yourcompany.com
webdev.yourcompany.com:8080
webdev.yourcompany.com:8443
```

メモ：Microsoft Outlook は、非修飾ホスト名を使用して Microsoft Exchange に接続します。Microsoft Exchange サーバーをリソースとして定義する場合は、非修飾名 (例えば、CorpMail) として定義します。

Exchange を Symbian、Android、iPad、iPhone で使用するには、タイプ ActiveSync の URL リソースをExchange 用に作成します。

ファイル共有リソース

ユーザーが WorkPlace にログインすると、設定したファイル システム リソースにアクセスできるようになります。これらのファイル システム リソースとしては、共有フォルダや共有ファイル、Windows ネットワーク サーバーなどがあります。

UNC パスを入力して特定のファイル システム共有を定義することも、Windows ドメイン全体を定義することもできます。

- 特定のファイル システム リソースとして定義できるのは、サーバー全体 (例えば、`\\ginkgo`)、共有フォルダ (`\\john\public`)、またはネットワーク フォルダ (`\\ginkgo\news`) です。
- Windows ドメイン全体を定義すると、ドメイン内のすべてのネットワーク ファイル リソースに対してユーザー アクセスを許可できます。これらのリソースは、Windows Explorer でネットワークを閲覧すると表示されるものと同じものです [**My Network Places (マイ ネットワーク) > Entire Network (ネットワーク全体) > Microsoft Windows Network (Microsoft Windows ネットワーク)**]。

リソース変数を使用すると、ネットワーク上の複数のフォルダを動的に参照できます。例えば、各ユーザーが個人フォルダにアクセスできるようにするには、ユーザー名の変数を使用してリソースを作成し、WorkPlace にショートカットを作成するときにその変数を使用します。詳細については、セッション プロパティ変数の使用の例を参照してください。

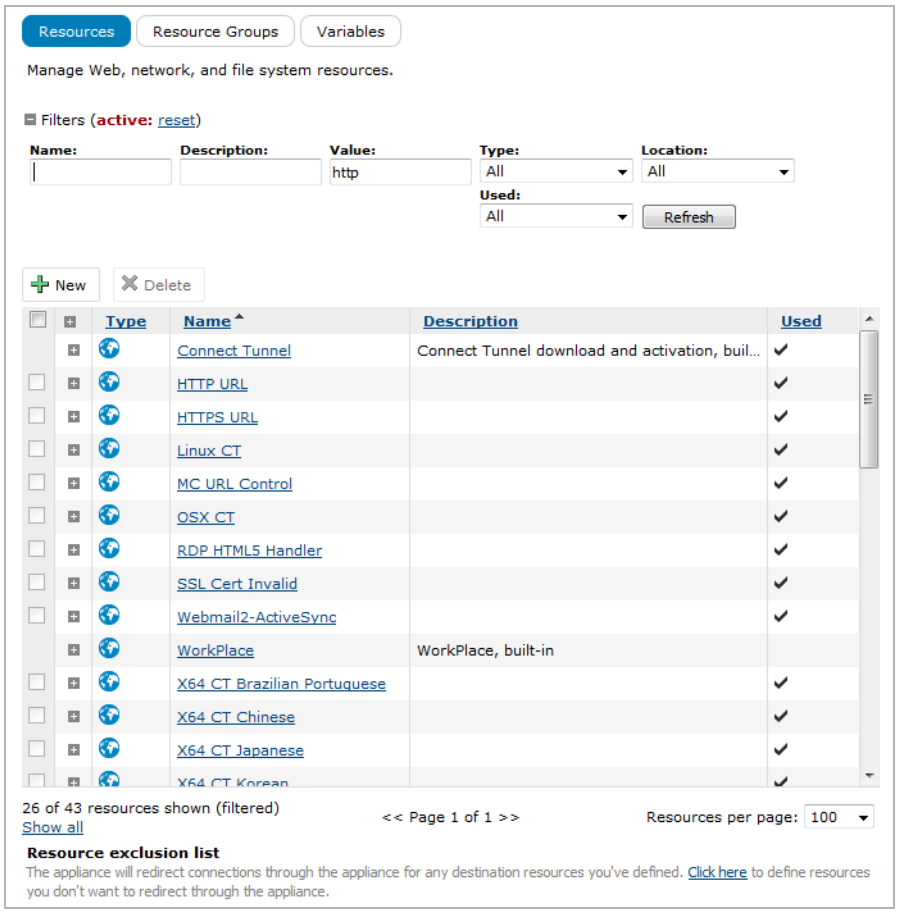
リソースとリソース グループ

トピック:

- 例: 電子メール添付ファイルのブロック
- 例: iPhone での Exchange のサポート
- 例: 機密データへのアクセスの制限
- リソースの編集
- リソースの削除
- リソース排除リストの使用

リソースとリソース グループの表示

[Security Administration (セキュリティ管理)] > [Resources (リソース)] を選択することで、個々のリソースまたはリソースのグループを AMC で表示および定義できます。



利用可能なリソースとリソース グループのリストを表示するには、

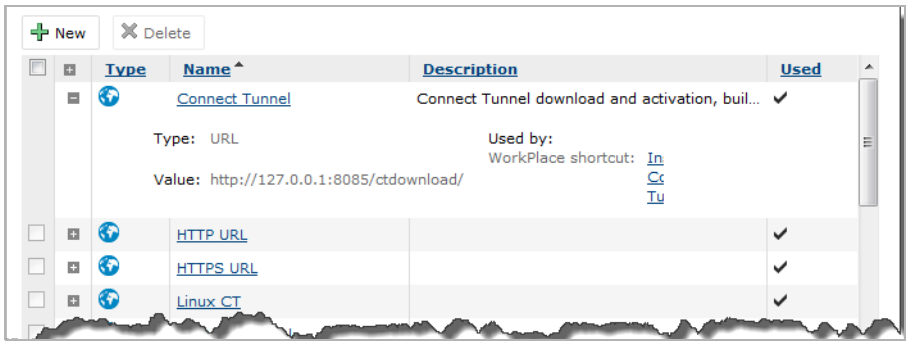
1 AMC のメイン ナビゲーション メニューの **[Security Administration (セキュリティ管理)]** で、**[Resources (リソース)]** をクリックします。

2 **Resources (リソース)** タブで、利用可能な個々のリソースのリストを参照できます。(**Resources Groups (リソース グループ)** タブには、リソースの集まりが表示されます)。

3 ページの上部にある **Filters (フィルタ)** 設定を使用すると、ここに表示されるリソースをフィルタリングできます。フィルターの使用方法については、フィルタを参照してください。

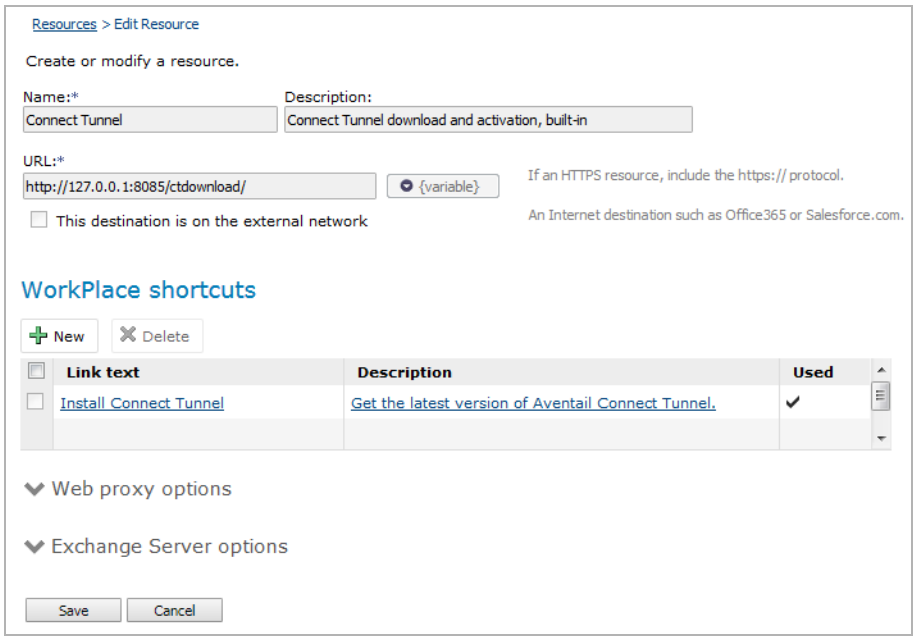
- **Type (種別)** 列には、それぞれのリソースのタイプが表示されます (**Domain name (ドメイン名)** や **Host name (ホスト名)** など)。クライアント/サーバー リソースには、Web アプリケーションとクライアント/サーバー アプリケーションの両方が含まれます。
- [**Used (使用中)**] 列は、リソースが WorkPlace のショートカットで指定されているかどうかを表します。

4 特定のリソースの概要を表示するには、リソースの隣にあるプラス記号 (+) をクリックします。そのリソースのタイプ、値、およびWorkPlace のショートカットやアクセス ルールで使用されているかどうかが表示されます。



メモ：デフォルトでは、アプライアンスには、Secure Mobile Access WorkPlace や Connect Tunnel Download などのいくつかの読み取り専用リソース定義が付属しています。これらの定義は、アプライアンス サービスに必要であり、削除できません (読み取り専用リソースの横にはチェック ボックスが表示されません)。

5 リソースを編集するには、リソース リストでそのリソースのリンクをクリックします。



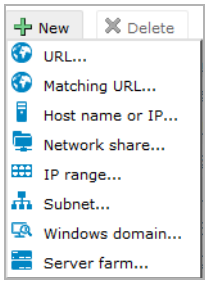
リソースの追加

アプリケーション リソース (Web、クライアント/サーバー、ファイル共有リソース) を作成することが、アクセス ポリシーを構築する最初の手順です。

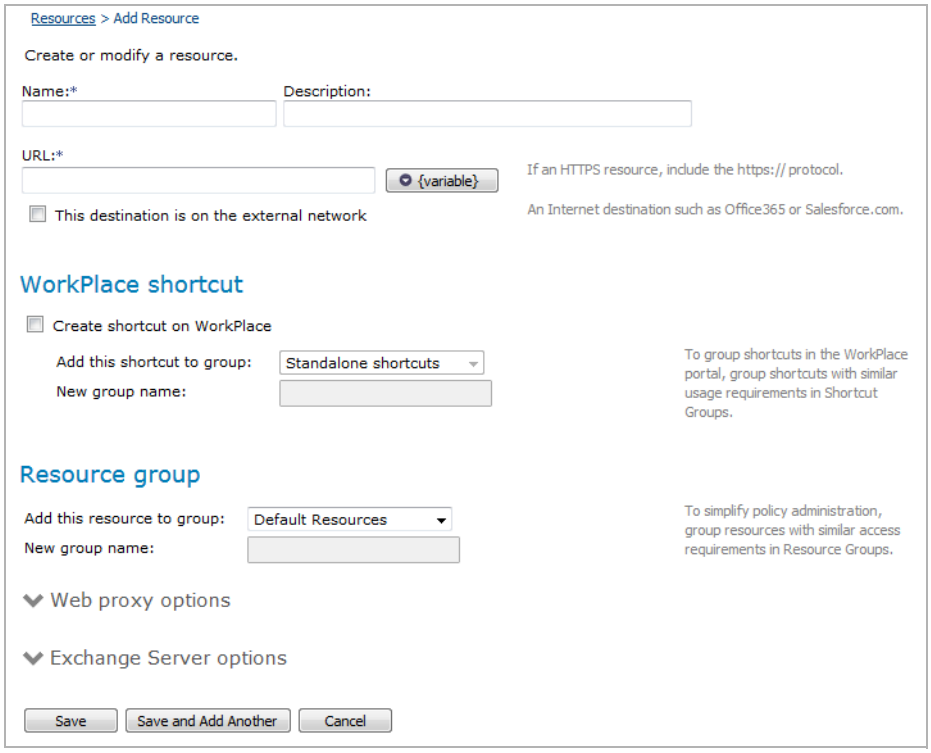
リソースを追加するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 **New (新規)** をクリックし、ドロップダウン リストからリソース タイプを選択します。



3 [**Add Resource (リソースの追加)**] ページが表示されます。**Add Resource (リソースの追加)** ページに表示されるオプションは、選択したリソース タイプによって異なります。

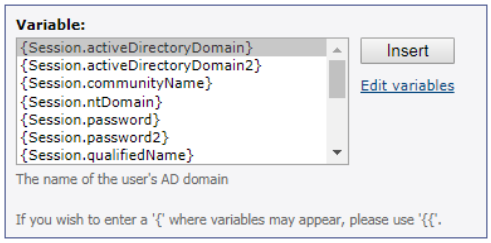


共通オプション に示されているオプションは、指定するリソース タイプで共通です。

共通オプション

オプション	説明	リソースのタイプ
名前	リソースの名前	すべて
説明	リソースの説明	すべて
URL	リソースの URL	
この宛先は外部ネットワーク上にあります。	このリソースが外部ネットワーク上にある場合は、このオプションを選択します。	

共通オプション

オプション	説明	リソースのタイプ
変数	動的リソースを定義するには、メニューから変数を選択します。リソースと WorkPlace ショートカットの定義での変数の使用 を参照してください。 	• Citrix サーバーファーム • ドメイン • ホスト名または IP • マッチング URL • ネットワーク共有 • URL
WorkPlace でショートカットを作成する	WorkPlace に Web リソースへのショートカットを追加します。リソースに割り当てた名前は、**Secure Mobile Access WorkPlace** ページの **Shortcuts (リソース)** のリストに表示されます。新規または既存のショートカット グループにショートカットを追加すると、用途が似ているショートカットを WorkPlace ポータル ページでまとめることができます。	• ドメイン • ネットワーク共有 • URL
(Web プロキシ オプション、または [Advanced (詳細設定)] エリア)	このリストには、いくつかの主要 Web アプリケーションで推奨される構成済みの Web プロファイル、カスタム Web プロファイル、およびデフォルト Web プロファイルが含まれます。選択すべきプロファイルがわからない場合は、[*Default*] を選択します。プロファイルを参照するには、[**View selected profile (選択したプロファイルを表示)**] をクリックします。Web アプリケーション プロファイルの追加も参照してください。	• ドメイン • ホスト名または IP • IP 範囲 • マッチング URL • サブネット • URL

URL リソース タイプ固有のオプションに表示されるオプションは、**URL** リソース タイプに固有です。

URL リソース タイプ固有のオプション

オプション	説明
URL	プロトコル識別子を入力しないと、AMC が URL の前に`http://`を自動的に挿入します。安全なサイトの URL の場合は、`https://` プロトコル識別子を含める必要があります。例えば、「`https://example.domain.com`」と入力します。
カスタム アクセス エリア (Web プロキシ オプション)	**[Translate this resource (このリソースを変換)]**、**[Access this resource on a custom port (カスタム ポート上でこのリソースにアクセスする)]**、**[Access this resource using a custom IPv4 or IPv6 FQDN (カスタムの IPv4 または IPv6 の FQDN を使用してこのリソースにアクセスする)]** のいずれかを選択します。 変換では URL 書き換えが使用されますが、他の代替方法ではクライアントレス Web アプリケーション アクセスが提供されるため、URL 書き換えの制限は発生しません。URL 書き換えでは、AJAX などの Web プログラミング テクノロジで問題が発生する可能性があります。 以下のオプションは、選択した方法によって異なります。
エイリアス名 (Web プロキシ)	プライベート URL を表すパブリック エイリアスを指定します。このエイリアス名はユーザーに提示されるため、短くて具体的な覚えやすい名前にします。次のような場合に、**[Alias name (エイリアス名)]** を使用してください。 • リソースの内部ホスト名を隠したい場合。 • URL リソースが **Network Settings (ネットワーク設定)** ページの **Name resolution (名前解決)** で構成されている検索ドメインに含まれていない場合。 • 通常はネットワーク エージェント経由でトラフィックをリダイレクトするが、変換 Web アクセスを使用してリソースをプロキシするようにする場合。詳細については、Web ショートカットの追加を参照してください。 **メモ：** • エイリアスで示すプライベート URL は、特定のファイルではなく、バックエンド サーバーのディレクトリをポイントする必要があります。 • エイリアスの指定では、ASCII 文字を使用します。ユーザーが変換 Web アクセスを使用して WorkPlace に接続すると、ASCII 以外の文字が使用されている場合にエラー メッセージが表示されます。 • URL (接頭辞 `http` または `https` が付くアドレス) にのみ対応するエイリアスを作成します。例えば、UNC パスや FTP リソース (`ftp://`) に対するエイリアスは指定できません。 エイリアスの使用方法の詳細については、例: URL エイリアスの指定を参照してください。
ポート (Web プロキシ)	**[Custom access (カスタム アクセス)]** の下にある **[Access this resource on a custom port (カスタム ポートでこのリソースにアクセスする)]** を選択すると、**[Port (ポート)]** オプションを指定できます。カスタム ポート番号を入力します。それぞれの WorkPlace サイトのそのポートでリソースを使用できるようになります。そのポートは、すべてのファイアウォールで開いている必要があり、アプライアンスの外側ですでに使用されていないものである必要があります。Web コンテンツの実際の配信は、ポリシー チェックによって異なり、通常のアプライアンスの処理に従って実行されます。

URL リソース タイプ固有のオプション

オプション	説明
カスタム FQDN (ウェブ プロキシ)	[**Custom access (カスタム アクセス)**] の下にある [**Access this resource using a custom FQDN (カスタムの FQDN を使用してこのリソースにアクセスする)**] を選択すると、[**Custom FQDN (カスタム FQDN)**] オプションを指定できます。アプライアンスの外部アクセス可能な Web サーバーがホスティングする**Custom FQDN name (カスタム FQDN の名前)**を入力します (`custom.mydomain.com` など)。 デフォルトでは、AMC はすべてのサービスについてすべてのインターフェースを監視し、要求される FQDN に基づいて、要求を正しいサービスに接続します。WorkPlace site サイトに対する相対的なホスト名は指定できません。外部で定義されたホスト名に対して最大 32 の IPv4 または IPv6 アドレスをホスティングされる Web アプリケーション名と WorkPlace サイトの間で独立して指定できるため、合計で最大 64 のホスト名をサポートします。 Web アクセスにマッピングされたカスタム FQDN により、シングル サインオンのサポートが提供されます。証明書のホスト名または IP アドレスがこのサイトに指定したカスタム FQDN または IP アドレスと一致しないと、ユーザーがサイトにアクセスしたときにセキュリティ警告が表示されます。カスタム FQDN は、WorkPlace サイトの構成 (WorkPlace サイトを追加するには、を参照) と同様に処理されます。
Listen on an additional IP address (Web proxy)	**(移行/インポートされた構成のみ)** `https://10.4.124.222/workplace/assets/help/index.html`。前バージョンから AMC をアップグレードし、WorkPlace サイトの IP アドレスが構成されているか、CEM が使用されている場合は、追加のリッスン アドレスを指定できます。監視アドレスを追加するには、[**Listen on an additional IP address (追加の IP アドレスをリッスンする)**] チェック ボックスを選択して IP アドレスを入力します。 新規インストールの場合、[Listen on an additional IP address (追加の IP アドレスをリッスンする)] フィールドは表示されません。部分的インポートを行うと仮想 IP アドレスの情報は失われ、未解決の変更を適用すると、管理者は、別の IP アドレスを使用するよう構成した WorkPlace サイトや URL リソースを修正することが必要になります。その場合、[**Listen on an additional IP address (追加の IP アドレスをリッスンする)**] フィールドが、追加のアドレスの監視を有効化するチェック ボックスが選択された状態で表示されます。IP アドレスを入力するか、チェック ボックスの選択を解除します。 既存の仮想ホストを使用して移行/インポートされた構成の場合、UI セクションは表示されますが、管理者は、新しい仮想アドレスを作成できません。必要であれば、CEM を使用して、新規または移行/インポートされた構成に仮想ホスト アドレスを作成します。 証明書のホスト名または IP アドレスがこのサイトに指定した [**IP address (IP アドレス)**] と一致しないと、ユーザーがサイトにアクセスしたときにセキュリティ警告が表示されます。
IP アドレス (Web プロキシ)	(移行/インポートされた構成のみ) 既存の IP アドレスを選択するか、[**(New) (更新)**] を選択して [**New IP address (新しい IP アドレス)**] フィールドに IP アドレスを追加します。
新しい IP アドレス (Web プロキシ)	リソースの IP アドレスをドット区切り形式 (`w.x.y.z`) で入力します。このアドレスは、アプライアンス インターフェースと同じサブネットである必要があります。

URL リソース タイプ固有のオプション

オプション	説明
SSL 証明書 (Web プロキシ)	既存の SSL 証明書を選択するか、[**(New) (更新)**] を選択してこのリソースの新しい SSL 証明書を追加します。名前が一致する証明書がアプライアンスにすでにある場合、その証明書が選択されます。ない場合は、[**SSL certificate (SSL 証明書)**] リストから選択するか、証明書をインポートします。
組織 (Web プロキシ)	会社または組織の名前を入力します。
国 (Web プロキシ)	国の 2 文字の省略形 (US や AU など) を入力します。
シノニム (Web プロキシ)	URL リソース名の別名を定義します。これは、ユーザーが異なる名前 (一般的には非修飾名や圧縮名) を使用してサーバーにアクセスする場合や、Web ページに DNS エイリアスを指すリンクが含まれていて Web プロキシ サービスがその名前を正しく変換できない場合に便利です。複数のシノニムを指定する場合はセミコロンで区切ります。 アプライアンスでは、リソースの短縮名を自動的にシノニムとして定義します。例えば、URL が「`http://mail.example.com`」の場合、アプライアンスは「`mail`」というシノニムを追加します。ただし、このシノニムは [**Synonyms (シノニム)**] フィールドには表示されません。 [**Translate this resource (このリソースを変換)**] が選択されている状態で [**Synonyms (シノニム)**] を指定する場合、[**Alias name (エイリアス名)**] フィールドが指定されている必要があります。それ以外のカスタム アクセス オプションの場合は、[**Synonyms (シノニム)**] フィールドは他のフィールドと関係なく指定できます。
[Provide Exchange ActiveSync and Outlook Anywhere access to this resource (Exchange Server) (このリソースへの Exchange ActiveSync および Outlook Anywhere のアクセスを提供する (Exchange Server))]	Exchange ActiveSync と Outlook Anywhere がこのリソースにアクセスできるようにするには、このチェックボックスを選択します。詳細については、Exchange ActiveSync Web アクセスを参照してください。使用例については、例: iPhone での Exchange のサポートを参照してください。Outlook Anywhere については、Microsoft Outlook Anywhere 向け SMA のサポートの設定 を参照してください。
[Exchange server FQDN (Exchange Server) (Exchange server の FQDN (Exchange Server))]	アプライアンスの外部アクセス可能な Web サーバーがホスティングする **Exchange server の FQDN** (IPv4 または IPv6) の名前を入力します (`custom.mydomain.com` など)。デフォルトでは、AMC はすべてのサービスについてすべてのインターフェースを監視し、要求される FQDN に基づいて、要求を正しいサービスに接続します。

URL リソース タイプ固有のオプション

オプション	説明
Listen on an additional IP address (Web proxy)	(移行/インポートされた構成のみ) 前バージョンから AMC をアップグレードし、WorkPlace サイトの IP アドレスが構成されているか、CEM が使用されている場合は、追加のリッスン アドレスを指定できます。監視アドレスを追加するには、[**Listen on an additional IP address (追加の IP アドレスをリッスンする)**] チェック ボックスを選択して IP アドレスを入力します。 新規インストールの場合、[Listen on an additional IP address (追加の IP アドレスをリッスンする)] フィールドは表示されません。部分的インポートを行うと仮想 IP アドレスの情報は失われ、未解決の変更を適用すると、管理者は、別の IP アドレスを使用するよう構成した WorkPlace サイトや URL リソースを修正することが必要になります。その場合、[**Listen on an additional IP address (追加の IP アドレスをリッスンする)**] フィールドが、追加のアドレスの監視を有効化するチェック ボックスが選択された状態で表示されます。IP アドレスを入力するか、チェック ボックスの選択を解除します。 既存の仮想ホストを使用して移行/インポートされた構成の場合、UI セクションは表示されますが、管理者は、新しい仮想アドレスを作成できません。必要であれば、CEM を使用して、新規または移行/インポートされた構成に仮想ホスト アドレスを作成します。 証明書のホスト名または IP アドレスがこのサイトに指定した [**IP address (IP アドレス)**] と一致しないと、ユーザーがサイトにアクセスしたときにセキュリティ警告が表示されます。
IP アドレス (Exchange Server)	(移行/インポートされた構成のみ) 既存の IP アドレスを選択するか、[**(New) (更新)**] を選択して新しい IP アドレスを追加します。
レルム (Exchange Server)	ドロップダウン リストからレルムを選択します。ActiveSync アクセスでは、単一の Active Directory 認証サーバーを使用するレルムを使用する必要があります。そのレルムはすでに構成済みである必要があります。
代替 Exchange Server の URL (Exchange Server)	フォールバック サーバーとして使用する Exchange Server の URL を入力します。フォールバック サーバーの構成の詳細については、代替サーバーの構成を参照してください。

マッチング URL リソース タイプ固有のオプションに表示されるオプションは、**マッチング URL リソース タイプ**に固有です。

マッチング URL リソース タイプ固有のオプション

オプション	説明
URL	プロトコル識別子を入力しないと、AMC が URL の前に「http://」を自動的に挿入します。安全なサイトの URL の場合は、https:// プロトコル識別子を含める必要があります。例えば、「https://example.domain.com」と入力します。 Matching URL (マッチング URL) リソースのアドレス セグメント (ピリオドの間) に、ワイルドカード文字「*」と「?」を使用できます。ドメイン名の後に「?」文字 (URL クエリ文字列を表します) を使用しないでください。 ワイルドカード文字は、次のような場合に使用します。 • www.yourcompany*.com と入力すると、yourcompany で開始して .com で終了する複数のドメインを参照します。www.yourcompany.* と入力すると、http://www.yourcompany.com と http://www.yourcompany.deの両方を参照します。 • mail*.yourcompany.com などのエントリを作成すると、yourcompany ドメイン内の mail *で開始するものに対するユーザー アクセスを許可します。*この例では、mail.yourcompany.com とmail2.yourcompany.com へのアクセスは許可されますが、mail3.wemmet.yourcompany.com へのアクセスは許可されません。 URL では大文字と小文字が区別されません。 **メモ：** クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。
パスとクエリ文字列のマッチング	このオプションは、パス エレメントやクエリ文字列値を特定の URL と一致させることで、電子メールの添付ファイルをブロックしたり、Web ベースのアプリケーションが制限されているデータを表示しないようにします。詳細については、例: 電子メール添付ファイルのブロックと例: 機密データへのアクセスの制限を参照してください。 [**Query string (クエリ文字列)**] 値では大文字と小文字が区別されますが、[**Path element (パス エレメント)**] では区別されません。

ホスト名または IP リソース・タイプ固有のオプション に表示されるオプションは、[**Host name or IP (ホスト名または IP)**] リソース タイプに固有のものです。

ホスト名または IP リソース・タイプ固有のオプション

オプション	説明
ホスト名または IP	ホストには、ネットワーク上の任意のコンピュータ、例えば、「bart.private.example.com」や「192.0.34.72」を指定できます。 ホスト名を指定する場合は、アドレス セグメント (ピリオドとピリオドの間) で、ワイルドカード文字「*」と「?」を使用できます。例えば、エントリ mail*.yourcompany.com を指定すると、ユーザーは、yourcompany ドメイン内の mail で始まるすべてのアドレス (例えば、mail.yourcompany.com や mail2.yourcompany.com) にはアクセスできますが、mail3.wemmet.yourcompany.com にはアクセスできません。ホスト名では大文字と小文字が区別されません。 **メモ：** クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

ネットワーク共有リソース タイプ固有のオプション に表示されるオプションは、[**Network share (ネットワーク共有)**] リソース タイプに固有です。

ネットワーク共有リソース タイプ固有のオプション

オプション	説明
ネットワーク共有	UNC パスを入力します。ここでは、サーバー全体 (例えば、\\ginkgo)、共有フォルダ (\\john\public)、またはネットワーク フォルダ (\\ginkgo\news) を指定できます。

IP 範囲リソース タイプ固有のオプションに表示されるオプションは、[**IP range (IP 範囲)**] リソース タイプに固有です。

IP 範囲リソース タイプ固有のオプション

オプション	説明
IP 範囲	IP 範囲は通常、サブネット内のコンピュータの部分範囲を識別します。例えば、「192.0.34.72-192.0.34.74」というように指定します。

サブネットリソースタイプの一意のオプションに表示されるオプションは、[**Subnet (サブネット)**] リソース タイプに固有です。

サブネットリソースタイプの一意のオプション

オプション	説明
[Subnet IP]	サブネットは、共通のアドレス コンポーネントを共有するネットワークの一部です。例えば、「192.26.34.0」というように指定します。
サブネット マスク	例えば、255.255.255.0 と入力します。

ドメイン リソース タイプ固有のオプションに表示されるオプションは、[**Domain (ドメイン)**] リソース タイプに固有です。

ドメイン リソース タイプ固有のオプション

オプション	説明
ドメイン	ドメインは、1 つ以上のホストを包含する領域です。 [**Windows domain (Windows ドメイン)**] チェック ボックスがクリアされている場合、ドメイン名は DNS 構文である必要があります。例えば、`sampledomain.com` のように入力します。
Windows ドメイン	Windows ドメイン全体を定義するには、[**Windows domain (Windows ドメイン)**] チェック ボックスを選択し、[**Domain (ドメイン)**] に NetBIOS または DNS の構文でドメイン名を入力します (例えば、「`example`」や「`example.com`」)。ドメインを定義すると、そのドメイン内のすべてのネットワーク ファイル リソースに対してユーザー アクセスを許可できます。

サーバー ファームのリソース タイプ固有のオプション に表示されるオプションは、[**Server farm (サーバーファーム)**] リソース タイプに固有です。

サーバー ファームのリソース タイプ固有のオプション

オプション	説明
サーバー ファーム リスト	[**Host name or IP (ホスト名または IP)**]を指定し、XML サービスが動作している 最大 6 台の Citrix サーバー、または XML サービスが動作している VMware サーバー、またはブローカー サービスが動作している WMware サーバーのサービス ポートを [**Port (ポート)**] で指定します。詳細については、Citrix サーバー ファーム リソースの追加または VMware View リソースの追加を参照してください。

4 リソースの定義が終了したら、[**Save (保存)**] をクリックします。

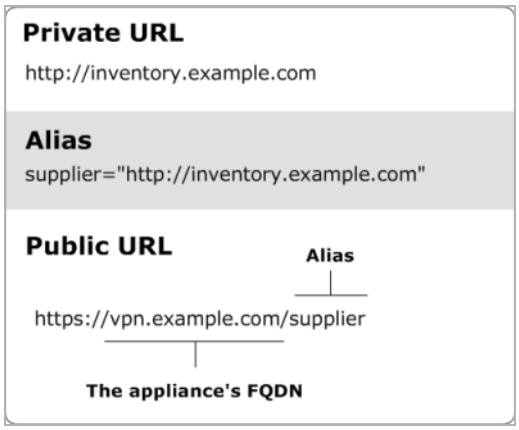
例: URL エイリアスの指定

Web アプリケーション、Web ポータル、Web サーバーなどの任意の Web リソースを、「URL リソース」として定義できます。Web リソースを URL として定義すると、次のような利点があります。

- WorkPlace の Web ショートカットを作成すると、ユーザーが URL リソースにすばやくアクセスできます。
- 非常に詳細なアクセス ルールを定義すると、ユーザーがアクセスできる URL を細かく制御できます。
- 内部ホスト名を隠して (または「エイリアスにして」)、一般に公開されないようにできます。ユーザーがエイリアスにアクセスすると、要求がダウンストリームの Web リソースにプロキシされ、指定されたエイリアスからプライベート URL に変換されます。ユーザーには、パブリック (「エイリアス」) の URL だけが提示されます。

パブリック URL に変換されたプライベート アドレスでは、インベントリ アプリケーションのプライベート アドレスがパブリック URL にどのように変換されるかを示しています。

パブリック URL に変換されたプライベート アドレス



このリソースのプライベート URL は `http://inventory.example.com` で、管理者はこの URL に対して「`supplier`」という名前のエイリアスを作成しています。

サプライヤーは、(重要なホスト名が一般公開されることになる) プライベート URL を使用する代わりに、パブリック URL (`https://vpn.example.com/supplier`) にアクセスします。

パブリック URL は、次の要素で構成されます。

- `http://` ではなく、`https://` 接頭辞:これは、SMA アプライアンスと送受信されるすべてのトラフィックが SSL を使用して保護されるためです。
- アプライアンスの完全修飾ドメイン名 (この例では「`vpn.example.com`」)
- リソースのエイリアス名 (この例では「`supplier`」)

メモ:

- Web ベースのアプリケーションの中には、トラフィックの送信に HTTP 以外のプロトコルを使用する Java アプレットやその他のブラウザ エクステンションを使用するものもあります。そのようなアプリケーションの例としては、Citrix NFuse や一部のバージョンの SAP などがあります。これらのアプリケーションは、Web ブラウザを使用してアクセスされますが、クライアント/サーバー リソースとして定義し、OnDemand 経由でクライアント/サーバー アクセス サービスを使用してプロキシする必要があります。
- 作成するエイリアスに対応するプライベート URL は、バックエンド サーバーのディレクトリである必要があり、ファイルを指定することはできず、`http://` または `https://` のいずれかで開始する必要があります。
- エイリアスの指定では、ASCII 文字を使用します。ユーザーが変換 Web アクセスを使用して WorkPlace に接続すると、ASCII 以外の文字が使用されている場合にエラー メッセージが表示されます。
- URL リソースの定義については、リソースの追加を参照してください。

例: 電子メール添付ファイルのブロック

組織では、管理対象外や信頼されていない公共システムからユーザーがアクセスする際に機密データへのアクセスを制限する必要がある場合があります。例えば、ユーザーに電子メール メッセージの参照を許可しつつ、コンピュータにダウンロードした電子メールの添付ファイルがそのまま残り、許可を受けていないユーザーがそのファイルにアクセスできるという状況は回避したいという場合もあるでしょう。

次の例は、アクセス制御ルールを **Matching URL (マッチング URL)** リソースおよび End Point Control ゾーンと併用して、信頼されていないデバイスに添付ファイルがダウンロードされないようにする方法を示しています。アクセス制御の概要については、アクセス制御ルールを参照してください。

この例では、IT 部門の管理対象外のデバイスが分類される EPC ゾーン (この例では、「*Untrusted (非保護)*」という名前) が構成されていることを前提としています。ゾーンの構成と使用については、を参照ゾーンおよびデバイス プロファイルによる EPC の管理してください。

マッチング URL リソースを使用して電子メール添付ファイルをブロックするには

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 [**New (新規)**] をクリックします。[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] ページが表示されます。

3 [**Position (位置)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。

4 [**Action (動作)**] ボタンを使用して、[**Deny (禁止)**] を指定します。これにより、次の手順で指定するパターンと一致するリソースに対するユーザー アクセスが拒否されるようになります。

5 [**Basic settings (基本設定)**] で、次のように情報を指定します。

   a [**User (ユーザ)**] が選択されていますが、そのままにしておきます (これにより、ルールのユーザーがリソースへのアクセスを試行します)。

   b [**From (送信元)**] フィールドでは、ルールを適用する対象ユーザーを指定します。この例では、値を「**Any user**」のままとしています。

   c [**To (送信先)**] フィールドで、[**Edit (編集)**] をクリックし、このルールに対する対象リソースを指定します。[**Resources (リソース)**] ウィンドウが表示されます。

   d [**New (新規)**] をクリックし、[**Matching URL (マッチング URL)**] を選択します。[**Add Resource - Matching URL (リソースの追加 - マッチング URL)**] ページが表示されます。

   e リソースの名前を入力します。例えば、「`Block email attachments`」と入力します。

   f [**URL**] ボックスに、メール サーバーの URL アドレスを入力します。

   g [**Path and query string matching (パスとクエリ文字列のマッチング)**] エリアで、[**Type of match (マッチの種類)**] リストから [**Exchange/OWA attachments (Exchange/OWA の添付)**] を選択します。

   h [**Save (保存)**] を選択します。[**Add Resource - Matching URL (リソースの追加 - マッチング URL)**] ダイアログが閉じます。

6 [**End Point Control zones (エンド ポイント制御の制限)**] エリアで [**Edit (編集)**] をクリックして、リソースに対するアクセスを拒否するゾーンを選択します ([*Untrusted (非保護)*])。

7 マッチング URL リソース タイプを指定するルールを作成する場合は、ユーザーがブラウザをアクセス方法として使用できる必要があります。[**Advanced (詳細)**] タブの [**Access method restrictions (アクセス方法の制限)**] エリアで、[**Client software agents (クライアント ソフトウェア エージェント)**] が [**Any (すべて)**] に設定されているか、選択したエージェントに [**Web browser (Web ブラウザ)**] が含まれていることを確認します。

8 「**完了**」をクリックします。

メモ：

- Web ベース アプリケーションの中には、他の Web ページにユーザーを自動的にリダイレクトするものもあります。電子メールの添付ファイルをブロックするようアプライアンスを構成する場合は、ターゲット URL アドレス (ユーザーがリダイレクトされる Web ページ) を使用するようにしてください。詳細については、例: URL リダイレクトの操作を参照してください。
- マッチング URL リソースでは、OnDemand Tunnel または Connect Tunnel を使用してアプライアンスに接続するユーザーの添付ファイルをブロックするよう構成することはできません。

例: iPhone での Exchange のサポート

Exchange ActiveSync の電子メールと関連機能は、Android、Windows Mobile、および Apple iPad と iPhone でサポートされています。

次の例で、URL リソースを構成して Microsoft Exchange にアクセスする iPhone ユーザーをサポートする方法を説明します。

メモ：この例では、単一の Active Directory 認証を使用するレルムがあることを前提としています。

iPhone ユーザーが会社の Exchange サーバーにアクセスできるようにするには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**New (新規)**] をクリックします。[**URL**] を選択します。[**Add Resource URL (リソース URL の追加)**] ページが表示されます。

3 名前、説明、および外部からのアクセスに使用する URL を入力します。先頭ページまたは索引ページを指定せずに、サーバー名だけを入力します。この例では、「`internalexchangeserver.SMA.com`」を使用します。

4 このリソースを追加するグループを選択します。この例では、デフォルト グループのままにします。

5 [**Exchange Server options (Exchange Server オプション)**] をクリックします。[**Exchange Server options (Exchange Server オプション)**] セクションが表示されます。

6 [**Enable Exchange ActiveSync and Outlook Anywhere access to this resource (このリソースへの Exchange ActiveSync および Outlook Anywhere アクセスを有効化)**] チェックボックスをオンにします。

7 [**Host and domain name (ホスト名とドメイン名)**] フィールドに、外部ホスト名と iPhone ユーザーがアクセスするドメインを入力します。

8 [**Realm (レルム)**] ドロップダウン メニューからレルムを選択します。Active Directory を認証に使用するレルムのみを選択できます。

9 [**Save (保存)**] を選択します。

10 iPhone の ActiveSync デバイス プロファイルを構成するには、AMC のメイン ナビゲーション メニューで [**End Point Control in (End Point Control を)**] クリックします。

11 [**Device Profiles (デバイス プロファイル)**] タブで [**New (新規)**] をクリックし、[**Exchange ActiveSync**] を選択します。

12 デバイス プロファイルの名前と説明を [**Name (名前)**] と [**Description (説明)**] フィールドに入力します。

13 **Add attribute(s) (属性の追加)** セクションで、**Type (種別)** に **Equipment ID (周辺機器 ID)** を選択します。

14 [**Device identifier (デバイス識別子)**] フィールドに、デバイス識別子を含むユーザー属性変数を入力します。iPhone の場合、識別子はデバイスのシリアル番号です。詳細については、デバイスプロファイルの属性の「周辺機器 ID 表」を参照してください。

15 [**Save (保存)**] を選択します。

16 iPhone ユーザーに外部からのアクセスに使用する URL を通知し、自分の Active Directory クレデンシャルを使用してログインするよう指示します。ユーザーは、デバイスで Exchange の ActiveSync を構成する必要があります。

   a iPhone で、**Settings (設定) > Mail (メール) > Contacts and Calendars (連絡先とカレンダー) > Add Account (アカウントを追加) > User's account info (ユーザーのアカウント情報)**に移動します。

   b サーバー名を管理者から指示された URL (外部ホスト名とドメイン) に設定します。

メモ： Exchange サーバーを正しく構成して iPhone が動作するようにするには、Exchange サーバーでの iPhone アクセスをテストすることを推奨します。電子メールへの iPhone アクセスを確認してから、iPhone と Exchange サーバーの間に SMA アプライアンスを追加します。Exchange サーバーにインターネットからアクセスできない場合は、WiFi アクセス ポイントをセットアップして、iPhone アクセスをテストします。

iPhone アクセス向けの Exchange サーバーの設定の詳細については、『*iPhone エンタープライズ配備ガイド*』を参照してください。以下でご覧いただけます。
http://images.apple.com/ie/iphone/business/docs/Enterprise_Deployment_Guide.pdf

例: 機密データへのアクセスの制限

次の例は、アクセス制御ルールをマッチング URL リソースおよび End Point Control ゾーンと併用して、Web ベースのアプリケーションで信頼されていないデバイスに制限されたデータが表示されないようにする方法を示しています。

- アクセス制御の概要については、アクセス制御ルールを参照してください。
- この例では、IT 部門の管理対象外のデバイスが分類される EPC ゾーン (この例では、「*Untrusted (非保護)*」という名前) が構成されていることを前提としています。ゾーンの構成と使用については、を参照ゾーンおよびデバイス プロファイルによる EPC の管理してください。

Web ベースのアプリケーションで [Matching URL (マッチング URL)] リソースを使用してデータを取得できないようにする、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 [**New (新規)**] をクリックします。[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] ページが表示されます。

3 [**Position (位置)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。

4 [**Action (動作)**] ボタンを使用して、[**Deny (禁止)**] を指定します。これにより、次の手順で指定するパターンと一致するリソースに対するユーザー アクセスが拒否されるようになります。

5 [**Basic settings (基本設定)**] で、次のように情報を指定します。

   a [**User (ユーザ)**] が選択されていますが、そのままにしておきます (これにより、リソースへのアクセスを試行するユーザーにルールが適用されます)。

b [**From (送信元)**] フィールドでは、ルールを適用する対象ユーザーを指定します。この例では、値を「*Any user*」のままとしています。

c [**To (送信先)**] フィールドで、[**Edit (編集)**] をクリックし、このルールに対する対象リソースを指定します。[**Resources (リソース)**] ダイアログが表示されます。

d [**New (新規)**] をクリックし、[**Matching URL (マッチング URL)**] を選択します。[**Add Resource - Matching URL (リソースの追加 - マッチング URL)**] ページが表示されます。

e リソースの名前を入力します。例えば、「`Patient Records`」と入力します。

f [**URL**] ボックスに、Web ベースのアプリケーションの URL アドレスを入力します。例えば、「`www.patient-records.com`」と入力します。

g [**Path and query string matching (パスとクエリ文字列のマッチング)**] エリアで、[*Type of match (一致種別)*] リストから [**Custom (ユーザ定義)**] を選択します。

h [**New (新規)**] をクリックし、[**Path element (パス エレメント)**] を選択します。「`reports.aspx`」と入力し、[**OK**] をクリックします (パスでは大文字と小文字が区別されません)。

i [**New (新規)**] をもう 1 度クリックし、[**Query string (クエリ文字列)**] を選択します。「`last_name=`」と入力し、[**OK**] をクリックします (クエリ文字列では大文字と小文字が区別されます)。

j [**Save (保存)**] を選択します。[**Add Resource - Matching URL (リソースの追加 - マッチング URL)**] ダイアログが閉じます。

6 [**End Point Control zones (エンド ポイント制御の制限)**] エリアで [**Edit (編集)**] をクリックして、リソースに対するアクセスを拒否するゾーンを選択します ([**Untrusted (非保護)**])。

7 マッチング URL リソース タイプを指定するルールを作成する場合は、ユーザーがブラウザをアクセス方法として使用できる必要があります。[**Advanced (詳細)**] タブの [**Access method restrictions (アクセス方法の制限)**] エリアで、[**Client software agents (クライアント ソフトウェア エージェント)**] が [**Any (すべて)**] に設定されているか、選択したエージェントに [**Web browser (Web ブラウザ)**] が含まれていることを確認します。

8 「**完了**」をクリックします。

変更を保存して適用すると、[*Patient Records (患者レコード)*] リソースを (`http://www.patient-records.com/reports.aspx?last_name=` と一致する URL を使用して) 開こうとするユーザーや [**Untrasted (非保護)**] ゾーンに分類されているユーザーはアクセスが拒否されます。

メモ：

- Web ベース アプリケーションの中には、他の Web ページにユーザーを自動的にリダイレクトするものもあります。電子メールの添付ファイルをブロックするようアプライアンスを構成する場合は、ターゲット URL アドレス (ユーザーがリダイレクトされる Web ページ) を使用するようにしてください。詳細については、例: URL リダイレクトの操作を参照してください。
- マッチング URL リソースでは、OnDemand Tunnel または Connect Tunnel を使用してアプライアンスに接続するユーザーの機密データへのアクセスを制限するよう構成することはできません。

リソースの編集

リソースを変更する前に、対応する [**Access Control (アクセス制御)**] ルールをよく検討し、変更がセキュリティ ポリシーにどのように影響するかを理解しておきます。

リソースを編集するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 編集するリソースの名前をクリックします。

3 [**Add/Edit Resource (リソースの追加/編集)**] ページで、必要な箇所を変更します。

4 「**Save (保存)**」を選択します。

メモ：既存のクライアント/サーバー リソースの定義設定は、変更できません (例えば、ホスト名から IP 範囲への変更)。変更する場合は、新しいリソースを作成し、該当する定義設定を適用する必要があります。

リソースの削除

アクセス制御ルール、リソース グループ、または WorkPlace ショートカットで参照されているリソースは、削除できません。リソースを削除する前に、そのリソースを参照しているルールから削除する必要があります。詳細については、参照されているオブジェクトの削除を参照してください。

リソースを削除するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**Resources (リソース)**] ページで、削除するリソースの左にあるチェック ボックスを選択します。

3 [**Delete (削除)**] ボタンを選択します。このリソースがアクセス制御ルール、リソース グループ、または WorkPlace ショートカットからまだ参照されていると、AMC からエラー メッセージが表示されます。エラー メッセージをクリックすると、このリソースのすべての参照のリストを確認できます。

リソース排除リストの使用

デフォルトでは、アクセス エージェントと Web ブラウザが、AMC に定義されている対象リソースに対して、アプライアンス経由で接続をリダイレクトします。このリダイレクトは、ユーザーのアクセス方法によって少し異なります。

- トンネル アクセス エージェントは、ユーザーにアクセスが許可されているすべての対象リソースに対して、アプライアンス経由で接続をリダイレクトします。
- Web ブラウザは、AMC で拒否されているすべての対象リソースをアプライアンスにリダイレクトします。つまり、ユーザーにアクセスが許可されていない場合、「permission denied」という Web ページが表示されます。

しかしながら、場合によっては、アプライアンス経由でリダイレクトしないようにしたいリソースもあるでしょう。例えば、ユーザーがアプライアンス経由で Outlook Web Access を起動し、アプライアンスに構成されているドメイン リソース内のパブリック サイトへのリンクが含まれた電子メール メッセージを読むとします。そのリンクを使用することで生成されるトラフィックは、アプライアンス経由で送信されることになりますが、パブリック リソースを排除リストで指定することで、これを回避できます。

リソース排除リストを使用すると、アプライアンス経由でリダイレクトされるリソース (ホスト名、IP アドレス、ドメインなど) を指定できます。Wドメインの指定では、ワイルドカード文字のアスタ

リスク (*) と疑問符 (?) も使用できます。このリストは、すべてのアクセス サービスにグローバルで適用されます。

メモ：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

リソース排除リストは、アクセス制御やセキュリティには影響しません。特定のリソースにアクセスされないようにするには、拒否ルールをアクセス制御リストに追加します。

アプライアンス経由でリダイレクトするよう構成されているリソースを確認するには、[**Show network redirection list (ネットワーク リダイレクト リストを表示)**] リンクをクリックします。[**Redirection List (リダイレクト リスト)**] ページが表示されます。

リソースを排除リストから削除するには、そのリソースのチェック ボックスを選択して、[**Delete (削除)**] をクリックします。

完全修飾ドメイン名 (FQDN) を指定してリソースを除外した場合、変換 Web モードを使用してアクセスを提供するレルムから WorkPlace に接続するユーザーは、WorkPlace [**Intranet Address (イントラネット アドレス)**] フィールドに非修飾ドメイン名を入力すれば、リソースにアクセスできます。

リソース排除リストにリソースを追加するには、

注意：AMC でドメイン リソース (例えば、「`win.yourcompany.com`」) を作成し、IP アドレス (`10.20.30.40`) を使用してそのドメインからリソースを排除する場合、FQDN (`server.win.yourcompany.com`) を使用すると、そのリソースにアクセスできます。これは、Web プロキシ サービスを使用するエージェントのみに該当し、トンネル クライアントを使用するエージェントには該当しません。

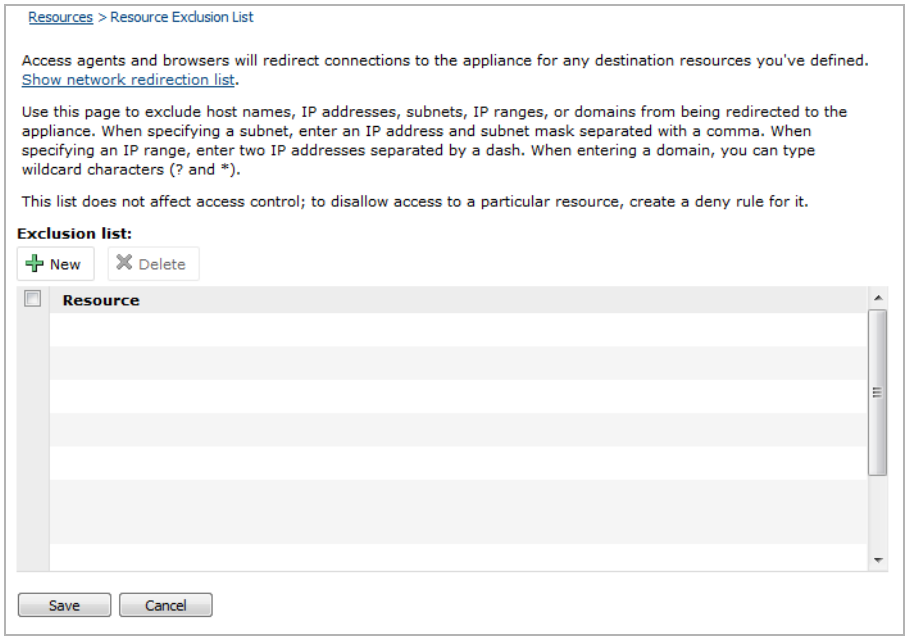
1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 ページの下部にある [**Resource exclusion list (リソース除外リスト)**] の [**Click here (ここをクリック)**] リンクをクリックします。

3 [**Exclusion list (排除リスト)**] フィールドで、[**New (新規)**] をクリックして、アプライアンス経由のリダイレクトから除外するホスト名、IP アドレス、またはドメインを入力します。ワイルドカード文字 (* と ?) を使用できます。

メモ：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

例えば、3 つのパブリック Web サーバー (`www.YourCompany.com`、`www2.YourCompany.com`、`www3.YourCompany.com`) がある場合は、対応するネットワーク トラフィックがアプライアンスを回避するように設定でき、それによって、パフォーマンスが向上します。ワイルドカード文字「`www*.YourCompany.com`」を使用して、3 つのパブリック サイトすべてを [**Exclusion list (排除リスト)**] に追加します。このリストのリソースには、変数も使用できます。詳細については、リソースと WorkPlace ショートカットの定義での変数の使用を参照してください。



4 [**Exclusion list (排除リスト)**] に追加したら、そのたびに [**OK**] をクリックします。

5 [**Save (保存)**] を選択します。

リソースと WorkPlace ショートカットの定義での変数の使用

変数を使用すると、1 つのリソースや WorkPlace のショートカットを定義し、ユーザーごとに固有のプロパティにその値を設定できます。変数は、ユーザーが開始したセッションに対応するプロパティによって (ユーザー名や、例えば、ユーザーに割り当てられたゾーンの名前)、または、外部 LDAP ストアに対するグループやコンピュータ名などの特定の属性セットのクエリによって、定義できます。

変数は、**IP range (IP 範囲)**と**Subnet (サブネット)**を除くすべてのリソース タイプに使用できます。変数が何にも解決されないと、その変数を使用するすべての構成項目が未定義になります。例えば、LDAP ストアに対して IMEI 番号 (モバイル デバイスに組み込まれている ID 番号) のクエリを実行する場合、IMEI 番号がないユーザーでは、そのユーザーのセッション中に変数が何にも解決されません。変数を使用する WorkPlace ショートカットは表示されず、例えば、その変数を使用するポリシー ルールも失敗します。

トピック:

- セッション プロパティ変数の使用
- クエリ ベース変数の使用
- クエリ結果の変更
- 1 つの定義を使用した複数のショートカットの表示

セッション プロパティ変数の使用

ユーザーがログインして WorkPlace セッションを開始すると、ユーザーに割り当てられているコミュニティの名前などのいくつかのセッション プロパティが既知の状態になります。これらのプロパティを使用して、動的リソースを作成できます。

例えば、モバイル ユーザーがデスクトップ コンピュータのユーザーとは異なるネットワーク共有にアクセスできるようにしたい場合もあるでしょう。そのような場合には、次のような手順を実行します。

- 2 つのコミュニティ (*Mobile* と *Desktop*) を定義します。
- 2 つのファイル共有をネットワークにセットアップします。例えば、*company**Mobile* と *company**Desktop* をセットアップします。
- WorkPlace のリソース : *company**{Session.communityName}* を定義します。

この方法では、1 つのリソースがどちらのユーザーにも提示され、それぞれのデバイスに正しくリンクが設定されます。組み込み変数 の変数を使用します。

組み込み変数

組み込み変数	説明
{Session.activeDirectoryDomain}	検索ベースとして使用する AD ドメインの FQDN または IP アドレス。
{Session.activeDirectoryDomain2}	検索ベースとして使用する 2 つ目の AD ドメインの FQDN または IP アドレス (連鎖式認証を使用する場合)。
{Session.communityName}	ログイン時にユーザーに割り当てられたコミュニティの名前。コミュニティによって、使用できるアクセス エージェントとエンド ポイントが制御されます。
{Session.ntDomain}	ログイン ドメイン。例えば、この FQDN: `server3.uk.company.com` では `server3` です。
{Session.password}	1 つ目の認証方法のパスワード。
{Session.password2}	2 つ目の認証方法 (使用する場合) のパスワード。
{Session.qualifiedName}	1 つ目 (または唯一) の認証方法の場合、これは、完全修飾ユーザー名 (`username@userdomain.company.com`) です。
{Session.qualifiedName2}	2 つ目の認証方法の場合、これは、完全修飾ユーザー名です。
{Session.realmName}	ユーザーがログインするレルムの名前。
{Session.remoteAddress}	アプライアンスから認識されるユーザーのホストの IPv4 または IPv6 のアドレス。
{Session.userName}	1 つ目の認証方法でのユーザーの短い名前。短い名前は通常、ユーザーの電子メール アドレスとホーム フォルダの両方に使用されます。
{Session.userName2}	2 つ目の認証方法 (使用する場合) でのユーザーの短い名前。
{Session.zoneName}	ユーザーのデバイスのプロファイルに基づいてユーザーに割り当てられたゾーンの名前。

ユーザー名に基づくネットワーク共有への WorkPlace ショートカットを作成するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**New (新規)**] をクリックし、[**Network share (ネットワーク共有)**] を選択します。

3 このリソースに名前を付け (例えば、「Personal Folder（個人フォルダ）」)、ネットワーク上のユーザー フォルダの UNC パスを [**Network share (ネットワーク共有)**] フィールドに入力します。例えば、「\\marine_lab\users\」と入力します。

4 **{variable}** をクリックし、[**Session.userName**] を選択して、ユーザーの短いログイン名を表す変数を追加します。[**Insert (挿入)**] をクリックすると、[**Network share (ネットワーク共有)**] のエントリは次のようになります: \\marine_lab\users\{Session.userName}

5 [**Create shortcut on WorkPlace (WorkPlace 上にショートカットを作成)**] チェックボックスを選択し、[**Save (保存)**] をクリックします。作成したリソースは、デフォルトでは、WorkPlace に **Personal Folder (個人フォルダ)** というタイトルのリンクとして表示されます。このリンク テキストを変更する場合は、AMC の [**WorkPlace**] ページに移動し、新しいショートカットのリンクをクリックします。

ユーザー jdoe が WorkPlace に接続すると、変数は自動的にログイン時に入力された名前に置き換えられ、\\marine_lab\users\jdoe という名前のフォルダにアクセスできるようになります。ユーザー rsmith のリンクも同様になりますが、\\marine_lab\users\rsmith フォルダにアクセスできるようになります。

メモ：

- LDAP クエリに基づく新しい変数の定義の手順については、クエリ ベース変数の使用を参照してください。
- {URL_REF_VALUE} という名前の追加の組み込み変数があり、ショートカットの URL の最初の変数の値が設定されます。この変数の使用方法については、1 つの定義を使用した複数のショートカットの表示を参照してください。

クエリ ベース変数の使用

Active Directory または LDAP の認証サーバーを使用するようにレルムを構成した場合、LDAP ストアに対する特定の属性または属性セットのクエリによって、リソースを定義できます。例えば、LDAP クエリを使用してユーザーごとに 1 つのリソースを用意し、ユーザーが自宅またはその他の場所から Windows に組み込まれたリモート デスクトップ プロトコル (RDP) を使用して、WorkPlace リンクから個人のデスクトップにアクセスできるようにします。

トピック:

- ユーザーのリモートデスクトップを指すリソースの作成
- ユーザーがリモート デスクトップにアクセスするための WorkPlace リンクの作成
- 変数を含む変数の作成

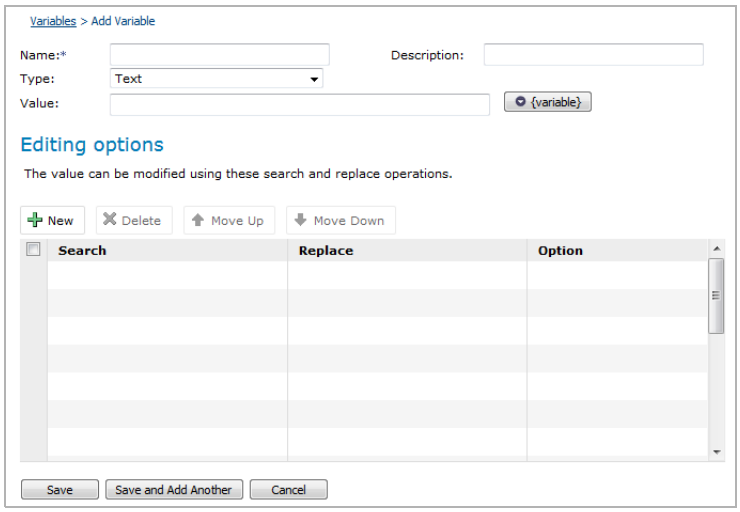
ユーザーのリモートデスクトップを指すリソースの作成

ユーザーのリモートデスクトップを指すリソースを作成するには、LDAP ストアを変更し、rdp という名前の属性を追加する必要があります。

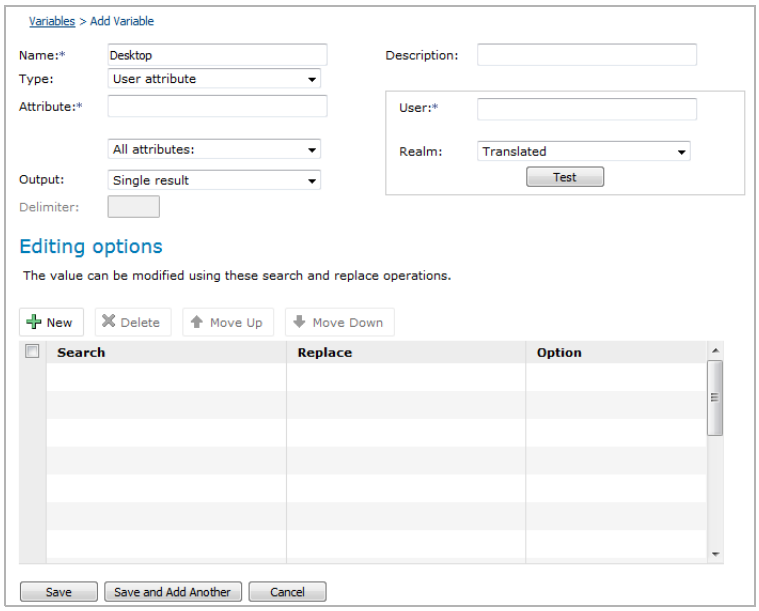
ユーザーのリモート デスクトップを指すリソース変数を作成するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**Variables (変数)**] タブをクリックし、[**New (新規)**] をクリックします。



3 変数の名前 (例えば、`Desktop`) を入力し、[**User attribute (ユーザ属性)**] を [**Type (種別)**] として選択します。オプションが次のように変化します。

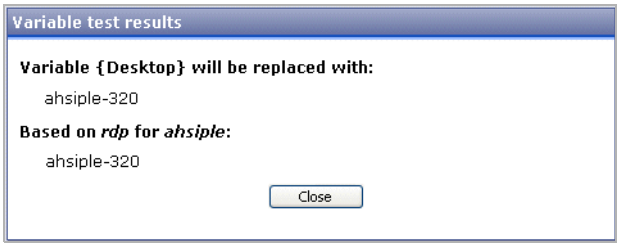


4 [**Attribute (属性)**] テキスト ボックスに「`rdp`」と入力します。

5 [**Output (出力)**] ドロップダウン メニューで、各ユーザーが LDAP ストアで 1 台のコンピュータだけに関連付けられている場合は、[**Single result (単一の結果)**] (既定) が選択されたままにします。

6 この新しい変数を適用するレルムを選択し、そのレルムにアクセスできる任意のユーザーのユーザー名を [**User (ユーザー)**] フィールドに入力します。

7 [**Test (テスト)**] をクリックして、指定したユーザー属性からこのユーザーの値が返されることを確認します。



8 [**Save (保存)**] を選択します。

9 [**Resources (リソース)**] タブで [**New (新規)**] をクリックし、[**Host name or IP (ホスト名または IP)**] を選択します。

10 このリソースに名前を付けます (例えば、`Personal computer`)。

11 [**Host name or IP address (ホスト名または IP アドレス)**] フィールドで、[**{variable (変数)}**] をクリックし、前に作成した変数 *{Desktop (デスクトップ)}* を選択します。[**Insert (挿入)**] をクリックします。

12 [**Host name or IP address (ホスト名または IP アドレス)**] のエントリを編集して、ネットワーク共有のパーソナル コンピュータのアドレスの部分を追加します。編集後のエントリは、次のようになります。

`{Desktop}.dept.company.com`

ユーザーがログインするたびに、*{Desktop}* が、**rdp** 属性を使用して LDAP ストアでそのユーザーに関連付けられているマシン名に置き換えられます。

13 [**Save (保存)**] を選択します。

ユーザーがリモート デスクトップにアクセスするための WorkPlace リンクの作成

ユーザーがリモート デスクトップにアクセスするための WorkPlace リンクを作成するには、

1 AMC のメイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**New (新規)**] をクリックし、[**Graphical terminal shortcut (グラフィカル ターミナル ショートカット)**] を選択します。

3 [**Resource (リソース)**] リストで [**Personal computer (PC)**] を選択し、WorkPlace でのリンク テキストを指定します。例えば、「`My remote desktop`」と指定します。

4 [**Save (保存)**] を選択します。作成したリソースは、デフォルトでは、WorkPlace に *My remote desktop* というタイトルのリンクとして表示されます。

ユーザー John Doe が自宅または外出先から WorkPlace に接続すると、**{Desktop}** は LDAP ストアでそのユーザーに関連付けられた **rdp** 属性の内容に置き換えられ、会社のコンピュータ (`john_doe-340.dept.company.com`) にアクセスするための WorkPlace リンク (*My remote desktop*) が表示されます。ユーザー Paula Smith のリンクも同様ですが、アクセス先は `paula_smith-452.dept.company.com` になります。ユーザーの **rdp** 属性に何も設定されていない場合、そのユーザーがログインしても、WorkPlace ショートカットは表示されません。

変数を含む変数の作成

変数を含む変数を作成するには、

1 つ以上の変数を使用して別の変数を定義することで、ユーザーごとのリンクやショートカットを簡単に作成できます。例えば、上記の手順では、**Host name or IP address (ホスト名または IP アドレス)** リソースが **{Desktop}** という名前の変数とそれに続く文字列を使用して定義されたため、パスは次のようになります。

```
{Desktop}.dept.company.com
```

上記のパス全体を解決する、**{Desktop_path}** という名前の変数を代わりに作成する方法もあります。

複数の変数を使用して 1 つの変数を作成する別の例として、上記のパスの *dept* を LDAP ストアのユーザーの *ou* (organizational unit) 属性に置き換える方法も考えられます。AMC 変数に、これらの例で変数がどのように解決されるかを記載します。

AMC 変数

AMC 変数名	解決後の値	前提
{Desktop}	*john_doe-340*	*rdp* (LDAP 属性)
{dept}	*Sales*	*ou* (LDAP 属性)
{Desktop_path}	*john_doe-340.dept.company.com*	AMC 変数の定義 `{Desktop}.dept.company.com`
{Desktop_by_dept}	*john_doe-340.Sales.company.com*	AMC 変数の定義 `{Desktop}.{ou}.company.com`

変数を 2 つを超えてネストすることはできません。変数が別の変数を参照し、その変数がさらに別の変数を参照することはできません。

クエリ結果の変更

外部I AD/LDAP ストアに対する特定の属性または属性セットのクエリを実行することで、変数を作成できます。クエリ結果をさらに便利に利用するには、クエリ結果から自動的にデータを抽出し、クエリが送信されてすべての変数文字列が確定した後に、値の検索と置換の操作を実行できます。

例えば、複数の支社がある会社で、支社ごとに異なる Exchange サーバーを電子メールに使用しているとします。いくつかの編集オプションを使用して、場所に関係なく、両方の Exchange サーバーを表す 1 つの変数を定義します。

クエリ結果を自動編集によって変数を定義するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**Variables (変数)**] タブをクリックし、[**New (新規)**] をクリックします。

3 変数の名前を入力します。例えば、「`Exchange_server`」と入力します。

4 [**Type (種別)**] リストで、[**User attribute (ユーザ属性)**] を選択します。

5 リストから、クエリを実行する、AD/LDAP ストアを指しているレルムを選択します。

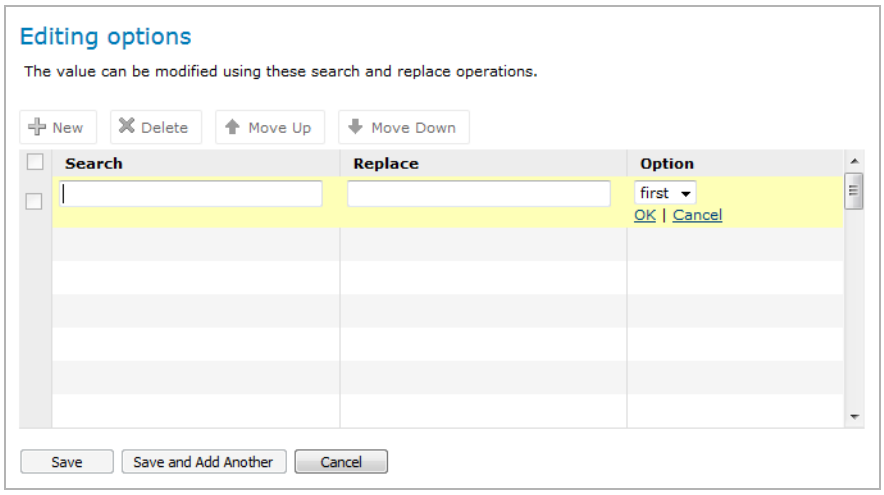
6 [**Attribute (属性)**] リストで、[**msExchHomeServerName**] を選択します。

7 2 つの異なる従業員 (例えば、1 人は London の本社で 1 人は California) のユーザー名を入力し、それぞれで [**Test (テスト)**] をクリックして、ディレクトリ サーバーに対してクエリを実行します。この例での唯一の相違点は、結果の文字列の末尾のサーバー名です。

```
/o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=LN0EXL09
```

```
/o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=CA0EXV08
```

8 [**Editing options (編集オプション)**] エリアの [**New (新規)**] をクリックして、クエリ結果を変更します。



a 「**Search (検索)**」フィールドに、次のように入力します。

```
/o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=
```

b [**Replace (変換前)**] ボックスには何も入力せずに、[**OK**] をクリックします。

London と California の従業員の場合、**Exchange_server** という名前の変数には、そのユーザーに対応する `LN0EXL09` または `CA0EXV08` のいずれかの名前が設定されます。

同じクエリを使用して、従業員がいる場所を表す追加の変数を作成できます。例えば、*Location (場所)* という名前の新しい変数を作成し、それぞれのディレクトリ サーバーの名前を場所に置き換えます。

Location 変数は、ユーザーによって、*London* または *California* のいずれかに解決されます。

例えば、[**User (ユーザー)**] フィールドにロンドンの従業員の名前を入力し、[**Test (テスト)**] をクリックすると、次の結果が表示されます。

1 つの定義を使用した複数のショートカットの表示

ユーザーのセッションのプロパティまたはクエリ結果に基づいて変数を作成する場合、変数は、ユーザー属性ごとに 1 つの値 (例えば、**sAMAccountName** と **lastLogon**)、または複数の値 (ユーザーが所属するグループのリストや、ユーザーがログインを許可されているいくつかのワークステーション) に解決されます。変数に複数の値が存在する可能性がある場合、1 つのショートカットを作成して WorkPlace に一連のショートカットとして自動的に表示されるようにするオプションがあります。

この例では、1 つのショートカットを作成し、結果として、WorkPlace の一連のショートカットが作成されます。そして、それらのショートカットのそれぞれが、ユーザーにアクセスが許可されているそれぞれのワークステーションに対応します。このプロセスの概要を以下に示します。

ショートカット作成プロセス

ステップ	説明
A	*User_workstations* という名前の変数を作成します。この変数は、*userWorkstations* という名前の AD または LDAP サーバーの複数値属性を指します。ディレクトリ ストアでは、この属性は、ユーザーにアクセスが許可されているワークステーションをリストします。例えば、あるユーザーは、パーソナル ワークステーションを仕事に使用し、別のワークステーションを注文の在庫管理に使用しています。
B	*User_workstations* 変数を指す、*Workstation_list* という名前のホスト リソースを作成します。この例のユーザーの場合、リソースには 2 つの値の候補があります。
C	*Workstation_list* リソースを指す、WorkPlace グラフィカル端末ショートカットを作成します。このショートカットのリンクは、*{URL_REF_VALUE}* という名前の特別な組み込み変数を参照し、ユーザーに使用が許可されているワークステーションのそれぞれに対して、WorkPlace で別々のリンクが設定されます。
D	WorkPlace をテストします。ショートカットが表示されない場合、ディレクトリ ストアのクエリで何も結果が返されていないためである可能性があります。テストを実行することで、WorkPlace のレイアウトのショートカットの位置を調整する必要があるかどうかも確認できます。

A: AD サーバーのユーザー属性を指す変数を作成する、

1 [**Security Administration (セキュリティ管理)**] の AMC のメイン ナビゲーション メニューで [**Resources (リソース)**] をクリックし、[**Variables (変数)**] ページに移動します。

2 [**New (新規)**] をクリックし、変数の名前「`User_workstations`」を入力します。

3 [**Type (種別)**] リストで [**User attribute (ユーザ属性)**] を選択し、クエリでディレクトリ ストアを使用するレルムを指定します。

4 AD ストアから返された属性のドロップダウン メニューで、[*userWorkstations*] を選択します。

5 [**Output (出力)**] リストで、[*Multiple results (複数の結果)*] を選択します。

6 [**User (ユーザー)**] テキスト ボックスに代表ユーザー (このショートカットを使用する可能性が高いユーザー) の名前を入力し、[**Test (テスト)**] をクリックして、AD/LDAP ストアに対して [*userWorkstations*] の値のクエリを実行します。

7 テスト結果から、[**Delimiter (境界)**] フィールドに入力すべき文字 (カンマやセミコロンなど) が分かります。

8 [**Save (保存)**] を選択します。新しい変数 (*{User_workstations}*) がリストに表示され、他の変数、リソース、または WorkPlace ショートカットの定義や記述に使用できるようになりました。

B: {User_workstations} 変数を指すホスト リソースを作成する

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**New (新規)**] をクリックし、[**Host Name or IP Address (ホスト名または IP アドレス)**] を選択します。

3 「Workstation_list」をリソース名として入力します。

4 [**Host name or IP address (ホスト名または IP アドレス)**] フィールドで、**{variable}** をクリックし、ステップ A で作成した変数 **{User_workstations}** を選択します。

5 [**Insert (挿入)**] をクリックし、**{variable}** をもう 1 度クリックしてリストを閉じます。

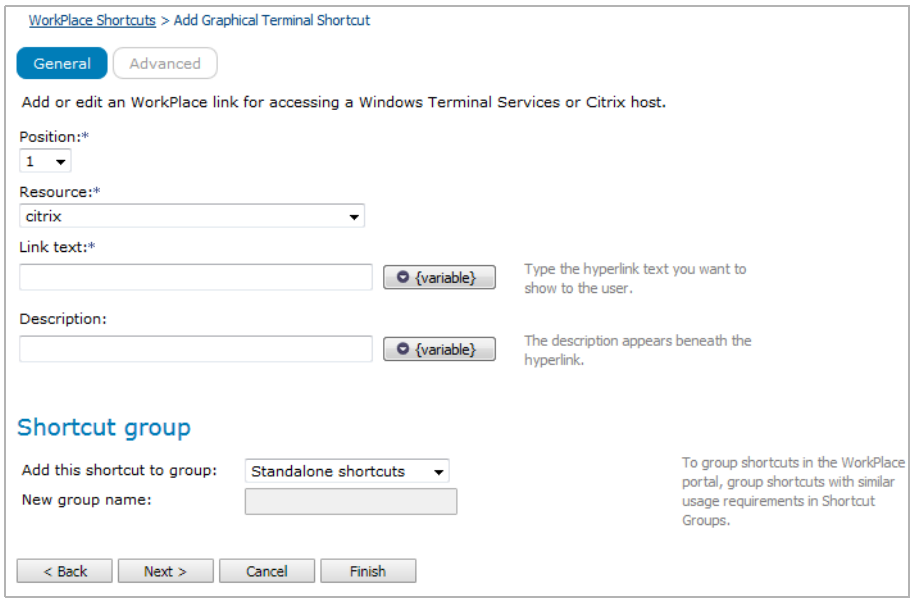
6 [**Host name or IP address (ホスト名または IP アドレス)**] のエントリを編集して、ネットワーク共有のコンピュータのアドレスの部分を追加します。編集後のエントリは、次のようになります。

```
{User_Workstations}.dept.company.com
```

C: Workstation_list リソースを指す WorkPlace ショートカットを作成する

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**Shortcuts (ショートカット)**] ページで [**New (新規)**] をクリックし、リストから [**Graphical terminal shortcut (グラフィカル ターミナル ショートカット)**] を選択します。[**Add Graphical Terminal Shortcut (グラフィカル ターミナル ショートカットを追加)**] ページの [**General (一般)**] タブが表示されます。



3 [**Position (位置)**] フィールドに、リスト内でのショートカットの位置を指定します。既定値は **1** です。(ショートカットの位置は、後で WorkPlace レイアウトで変更できます)。

4 [**Resource (リソース)**] ドロップダウン メニューで、このショートカットにリンクするリソースを選択します。**Workstation_list**。

5 [**Link text (リンク テキスト)**] フィールドに、ユーザーに提示されるハイパーリンクの最初の部分を入力します。例えば、「My workstation(s):」とその後にスペースを入力します。

6 変数を使用すると、複数の値が存在する場合に、[**Workstation_list**] の後に続く値にリンクの終了を設定し、複数のショートカットが WorkPlace に表示されるようにできます。**{variable}** をク

リックし、リストから **{URL_REF_VALUE}** を選択します。[**Insert (挿入)**] をクリックすると変数がリンク テキストに追加されます。再度 [**{variable}**] をクリックするとリストが閉じます。**Link (リンク)** のエントリは次のようになりました。

```
My workstation(s): {URL_REF_VALUE}
```

7 [**Finish (完了)**] をクリックしてショートカットを保存します([**Advanced (詳細)**] ページの設定の説明については、を参照個別のホストに対するグラフィカル ターミナル ショートカットの追加してください)。

このショートカットによって、ユーザーに使用が許可されているそれぞれのワークステーションに対する別々の WorkPlace リンクが自動的に設定されます。この例では、2 つの WorkPlace リンク (1 つはパーソナル ワークステーション、1 つは注文入力用のワークステーション) が存在し、ユーザー「*ageorge*」の場合は次のようになります。

D: WorkPlace のトラブルシューティング

1 ユーザーが WorkPlace にログインしても作成したショートカットが表示されない場合は、次の点を確認します。

- ユーザーが正しいコミュニティにいるかどうか。AMC のメイン ナビゲーション メニューで [**User Sessions (ユーザー セッション)**] をクリックし、ユーザーの名前をクリックしてセッションの詳細を取得します。ユーザーが正しいコミュニティに割り当てられていない、または、ユーザーがリソースにアクセスできなくしているルールが存在する可能性があります。
- 変数からこのユーザーの結果が返されるかどうか。AMC のメイン ナビゲーション メニューで [**Resources (リソース)**] をクリックし、[**Variables (変数)**] ページに移動します。**User_workstations** という名前の変数をクリックし、ショートカットが表示されないユーザーの名前を入力して、[**Test (テスト)**] をクリックします。結果が返されなければ、ショートカットは表示されません。

2 WorkPlace レイアウトをチェックします。ショートカットを作成する場合、ショートカットのグループまたはデフォルトのグループ **(Standalone shortcuts) (スタンドアロンのショートカット)** に追加することもできます。ショートカットの位置を変更するには、[**Realms (レルム)**] をクリックし、このユーザーが所属するコミュニティの名前をクリックします。[WorkPlace Appearance (WorkPlace の外観)] ページで、使用されるレイアウトを確認できます。ページ内容を変更するには、[**Manage layouts (レイアウトの管理)**] をクリックします。

リソース グループの作成と管理

個々のリソースを定義する方法だけでなく、個々のリソースの集まりであるリソース グループとしてリソースを管理することもできます。リソースをグループにまとめると、特長が似ているリソースのセットを簡単に管理できます。例えば、リモートの従業員にとって重要なアプリケーションを含むリソース グループを定義すると、それらのリソースへのアクセスの管理が容易になります。

リソース グループに所属するリソースの数に制限はありません。新しいリソース グループを作成すると、利用可能なリソースとグループのリストに追加され、アクセス制御ルールでそのリソース グループを使用できます。

トピック:

- 追加リソース グループ
- 例: URL リダイレクトの操作
- リソース グループの編集と削除

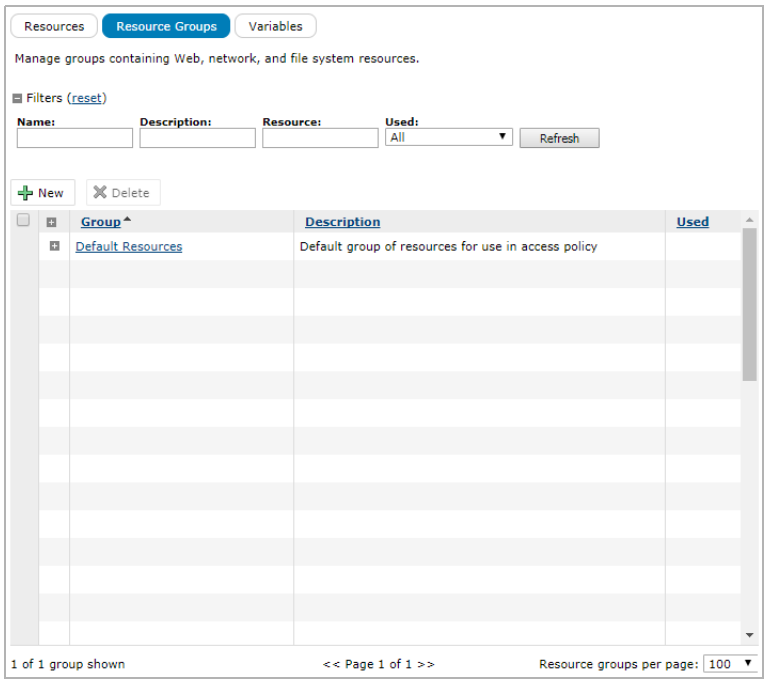
追加リソース グループ

新しいリソース グループを作成すると、[**Resources (リソース)**] ページの [**Resource Groups (リソース グループ)**] タブの利用可能なグループのリストに追加されます。

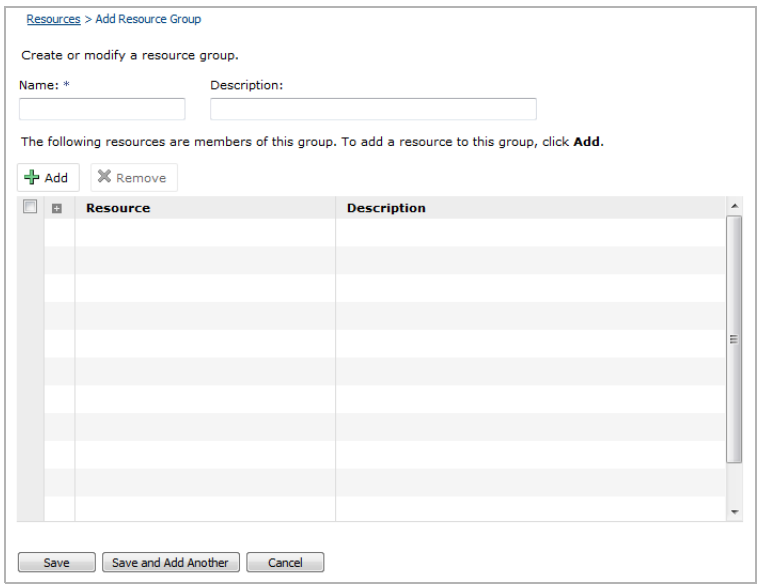
リソース グループを追加するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**Resource Groups (リソース グループ)**] タブをクリックします。



3 [**New (新規)**] をクリックしてリソース グループを追加します。



4 リソース グループの名前を [**Name (名前)**] に入力します。

5 [**Description (説明)**] フィールドに、グループの説明を入力します。

6 グループに入れるリソースのチェックボックスを選択するか、グループを空のままにして後でリソースを追加します。グループに所属するリソースの数に制限はありません。

7 終了したら、[**Save (保存)**] をクリックします。

例: URL リダイレクトの操作

Web ベース アプリケーションの中には、他の Web ページにユーザーを自動的にリダイレクトするものもあります。アプリケーションへのユーザー アクセスでは、特定の Web アドレスを参照しますが、異なるアドレスにリダイレクトされることもあります。

例えば、ある組織が次の URL のメール サーバーを使用しているとします。

```
http://domino.example.com/dwa.nsf
```

このサイトにアクセスするユーザーは、自動的に異なる URL にリダイレクトされます。

```
http://domino.example.com/mail/dwa1.nsf
```

ユーザーが SMA アプライアンスを使用してアプリケーションにアクセスできるようにするには、元の URL とリダイレクトされた URL の両方をリソースとして追加する必要があります。

次の例では、Web ベース アプリケーションを URL リソースのペアとして追加する方法、リソースをグループにまとめる方法、および、アクセス制御ルールを定義してユーザーがアプリケーションにアクセスできるようにする方法を説明します。

Web ベース アプリケーションの URL リソースを構成する、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**New (新規)**] をクリックし、ドロップダウン メニューから [*URL*] を選択します。[**Add/Edit Resource - URL (リソースの追加/編集 - URL)**] ページが表示されます。

3 [**Name (名前)**] フィールドにリソースの名前を入力します。例えば、「`Mail Web App`」と入力します。

4 [**URL**] フィールドに、メール サーバーのアドレスを入力します。以下に例を示します。

```
http://domino.example.com/dwa.nsf.
```

5 [**Save (保存)**] を選択します。

6 ステップ 2 から ステップ 5 を繰り返して 2 つ目の Web リソースを作成し、リダイレクトされた URL アドレスを指定します。アプリケーションが複数のリダイレクトされた URL を使用する場合は、アドレスごとに追加の URL リソースを作成します。この例では、2 つの URL のみを使用します。

両方の URL リソースのリソース グループを作成する、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**Resource Group (リソース グループ)**] タブをクリックし、[**New (新規)**] をクリックします。[**Add/Edit Resource Group (リソース グループの追加/編集)**] ページが表示されます。

3 [**Name (名前)**] フィールドにグループ プールの名前を入力します。例えば、「`Mail Web App Group`」と入力します。

4 以前に作成した Web リソースのそれぞれのチェックボックスを選択します。

5 [**Save (保存)**] を選択します。

リソース グループのアクセス制御ルールを定義する、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 [**New (新規)**] をクリックします。[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] ページが表示されます。

3 [**Position (位置)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。

4 [**Action (動作)**] ボタンを使用して [**Permit (許可)**] を指定します。これにより、次の手順で指定するグループ リソースに対するユーザー アクセスが許可されます。

5 [**Basic settings (基本設定)**] で、次のように情報を指定します。

   a [**User (ユーザ)**] が選択されていますが、そのままにしておきます (これにより、リソースへのアクセスを試行するユーザーにルールが適用されます)。

   b [**From (送信元)**] フィールドでは、ルールを適用する対象ユーザーを指定します。この例では、値を「**Any user**」のままとしています。

   c [**To (送信先)**] フィールドで、[**Edit (編集)**] をクリックし、このルールに対する対象リソースを指定します。[**Resources (リソース)**] ダイアログが表示されます。

   d 以前に作成したリソース グループを選択します。この例では、[*Mail Web App Group*] です。

6 [**Save (保存)**] を選択します。

アクセス制御の概要については、アクセス制御ルールを参照してください。

リソース グループの編集と削除

リソース グループを変更する前に、関連するルールをよく検証し、変更がセキュリティ ポリシーにどのように影響するかを把握します。アクセス制御ルールで参照されているリソース グループは、削除できません。リソース グループを削除する前に、そのリソース グループを参照しているルールから削除する必要があります。詳細については、参照されているオブジェクトの削除を参照してください。

Web アプリケーション プロファイル

Web アプリケーション プロファイルは、Windows NTLM 認証 (v1 と v2 のどちらもサポート) または基本認証を使用する Web アプリケーションのシングル サインオンと変換制御を可能にします。

- Windows NTLM 認証を使用する Web アプリケーションでは、Windows クレデンシャルが確認されたユーザーに対してのみ、アクセスが許可されます。NTLM のサポートは Microsoft IIS (Windows マシン用のインターネットベース サービス) に組み込まれており、Internet Explorer でサポートされています。
- 基本認証は、多様なプラットフォームでサポートされています (ただし、ネットワーク上でパスワードが平文で送信されるので注意してください)。

Web プロキシ サービスを AMC で構成することで、フォームベース認証をサポートするようにもできます。この場合、任意の組み合わせのブラウザと Web サーバーを使用する標準 HTML 形式の Web にユーザー認証を組み込みます。詳細については、フォームベースのシングル サインオン プロファイルの作成を参照してください。

トピック:

- Web アプリケーション プロファイルの表示
- Web アプリケーション プロファイルの追加
- 構成済みの Web アプリケーション プロファイル
- Web アプリケーション プロファイルの例
- Web アプリケーション プロファイルの編集と削除

Web アプリケーション プロファイルの表示

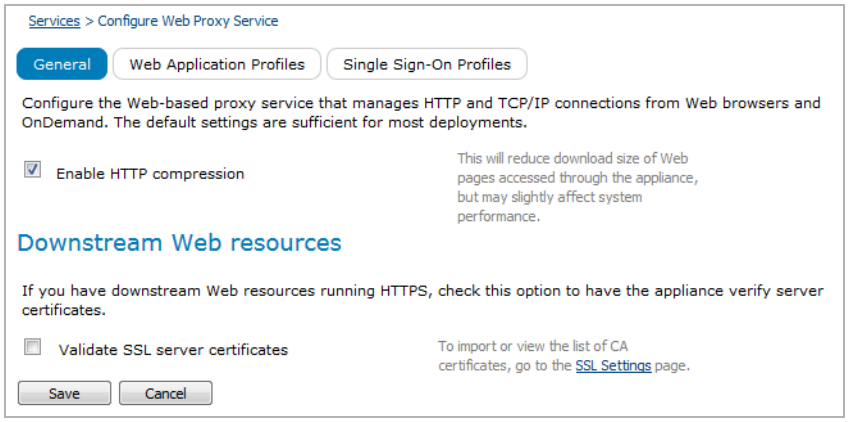
Web アプリケーション プロファイルは、[**Configure Web Proxy Service (ウェブ プロキシ サービスの設定)**] ページに表示されます。

利用可能な Web アプリケーション プロファイルのリストを表示するには、

1 AMC のメイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access Services (アクセス サービス)**] エリアで、[**Web proxy service (ウェブ プロキシ サービス)**] の [**Configure (設定)**] リンクをクリックします。

3 利用可能な Web プロファイルを表示するには、[**Web Application Profiles (Web アプリケーション プロファイル)**] タブをクリックします。[**Configure Web Proxy Service (ウェブ プロキシ サービスの設定)**] ページが表示されます。



4 このリストには、いくつかの主要 Web アプリケーションで推奨される構成済みの Web アプリケーション プロファイル、作成したカスタム Web プロファイル、およびデフォルト Web プロファイルが含まれます。Web アプリケーション プロファイルの設定を表示するには、プロファイルの名前をクリックします。

Web アプリケーション プロファイルの追加

重要：新しいバージョンのアプライアンス ソフトウェアでは、AMC が実行する Web 変換の完全性と堅牢性が強化されました。バージョン 10.x 以降で、バージョン 8.6.x での Web アプリケーション プロファイルでの古い変換に戻すことはできません。

Web アプリケーション プロファイルは、シングル サインオンの特性や特定の Web リソースのコンテンツ変換オプションを制御します。Web リソースごとに Web アプリケーション プロファイルを作成し、関連付けます。

- **Single sign-on (シングル サインオン)** オプションは、ユーザーのログイン クレデンシャルの下位の Web アプリケーションへの転送方法を制御します。これらのオプションは既定では無効になっています。また、シングル サインオンを構成するためには、次のいずれかが必要です。
  - AMC の [**Configure WorkPlace (WorkPlace の設定)**] ページにある [**Use Web content translation (ウェブ コンテンツの変換を使用)**] をクリックします。
  - WorkPlace リンクをエイリアスの URL として定義します。これは、通常はネットワーク エージェントによってトラフィックをリダイレクトする場合に実行すべき方法ですが、この場合、リソースが変換され、マッピングされたカスタム ポートまたはシングル サインオンのために Web アクセスにマッピングされた Exchange サーバ FQDN を使用して強制的にプロキシされるようにすることになるでしょう。

  詳細については、Web ショートカット アクセスおよび WorkPlace の一般設定の構成 を参照してください。

  メモ：Windows ターミナル サービスまたは Citrix のホストにアクセスするための WorkPlace ショートカットを作成した場合は、シングル サインオンを構成できます。個別のホストに対するグラフィカル ターミナル ショートカットの追加を参照してください。

- **Content translation (コンテンツ変換)** オプションは、JavaScript コード、Cookie 本体、および Cookie パスを Web プロキシ サービスで変換するかどうかを制御します。これらのオプションは、変換 Web アクセス エージェントだけで使用され、標準の Web アクセスでは無視されます。

Web アプリケーション プロファイルは、AMC の [**Configure WorkPlace (WorkPlace の設定)**] ページ内の [**Web shortcut access (ウェブ ショートカット アクセス)**] が [**Redirect through network agent (ネットワーク エージェントを通してリダイレクトする)**] に設定されていると、使用されません。WorkPlace の一般設定の構成を参照してください。

Web アプリケーション プロファイルを追加するには、

1 AMC のメイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

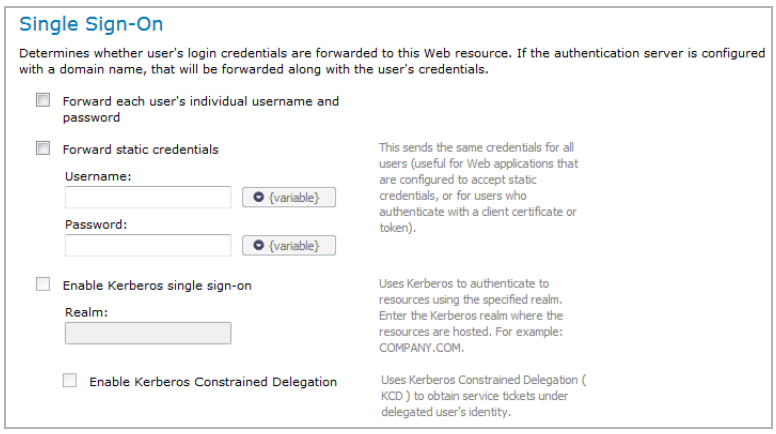
2 [**Access Services (アクセス サービス)**] エリアで、[**Web proxy service (ウェブ プロキシ サービス)**] の [**Configure (設定)**] リンクをクリックします。[**Configure Web Proxy Service (ウェブ プロキシ サービスの設定)**] ページが表示されます。

3 [**Web Application Profiles (Web アプリケーション プロファイル)**] タブをクリックし、[**New (新規)**] をクリックします。[**Add Web Application Profile (Web アプリケーション プロファイルの追加)**] ページが表示されます。

4 [**Name (名前)** ()] フィールドにプロファイルの名前を入力します。プロファイルを作成して特定のアプリケーションに関連付ける場合は、そのアプリケーションに似た名前を付けるとよいでしょう。

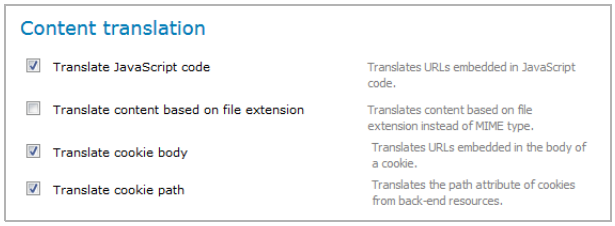
5 [**Description (説明)**] フィールドに、プロファイルについての分かりやすいコメントを入力します。

6 [**Single Sign-On (シングル サインオン)**] エリアで、ユーザー クレデンシャルを Web リソースに渡すかどうか、また、どのように渡すのかを指定します。ユーザー クレデンシャルを転送すると、ユーザーが何回もログインする必要がなくなります (アプライアンスにアクセスできるようになれば、アプリケーション リソースにまたアクセスできます)。



- [**Forward each user's individual username and password (各ユーザーの個別のユーザー名とパスワードを転送)**] チェックボックスを選択すると、WorkPlace への認証に使用されたユーザー名とパスワードがバックエンド Web サーバーに転送されます。
- [**Forward static credentials (静的資格情報を転送)**] チェックボックスを選択すると、アプライアンスは、すべてのユーザーに同じユーザー名とパスワードを転送します。これは、HTTP 基本認証を必要とするものの、ログイン名に基づいてユーザーごとにコンテンツをカスタマイズする必要がない Web サイトに有効です。また、クライアント証明書やトークンで認証するユーザーにも有効です。
- いずれのオプションも選択しないと、シングル サインオン機能が無効になります。両方のオプションを選択すると、個々のユーザー名とパスワードのオプションが優先されます。例えば、ユーザーがユーザー名/パスワードのペアを指定すると、それが転送されますが、指定しないと、Web プロキシ サービスが固定のクレデンシャルを転送します。
- [**Enable Kerberos single sign-on (Kerberos のシングル サインオンを有効化)**] チェックボックスを選択し、リソースがホスティングされる Kerberos レルムを指定すると、WorkPlace と Connect Tunnel のユーザーが http リソースにアクセスできます。このレルムは、Kerberos が推奨される認証メカニズムとして構成されている、Active Directory、Active Directory ツリー、Active Directory フォレストのような環境の認証に使用されます。

7 [**Content translation (コンテンツ変換)**] エリアで、Web プロキシ サービスで変換する項目を選択します。



- Web プロキシ サービスで Web リソースが使用する JavaScript コードに埋め込まれたリンクを変換する場合は、[**Translate JavaScript code (JavaScript コードを変換)**] チェック ボックスを選択します。これは、絶対 URL または絶対参照 (`/to/path/xyz`)、または動的に生成される URL (`location="http://" + host name + "/index.html"` など) が含まれる JavaScript に有効です。これにより、JavaScript を使用する Microsoft Outlook Web Access やその他のアプリケーションとの互換性が向上します。このオプションは既定で有効です。

  ただし、Subject (件名)、From (差出人)、または Sent To (宛先) フィールドに基づく検索に問題があったり、WorkPlace ショートカットを使用する OWA へのアクセスでログイン後にエラーが表示されたりした場合は、OWA プロファイルの [**Translate JavaScript code (JavaScript コードを変換)**] チェック ボックスをクリアします。

- Web プロキシ サービスがファイルの拡張子で MIME タイプでないことを確認することでコンテンツ タイプを判断するようにする場合は、[**Translate content based on file extension (ファイル拡張子に基づいてコンテンツを変換)**] チェックボックスを選択します。通常、Web プロキシ サービスは、一定のコンテンツ タイプ (テキストと HTML を含む) を変換します。HTTP ヘッダーの MIME タイプでコンテンツ タイプを判断します。Web リソースから正しくない MIME タイプが送信される場合は、このオプションを選択して、Web プロキシ サービスがファイル拡張子に基づいてファイルを変換するかどうかを判断するようにします。このオプションは、既定では無効になっています。
- Web プロキシ サービスが Cookie の本体に埋め込まれた URL を変換するようにする場合は、[**Translate cookie body (Cokkie の本体を変換)**] チェックボックスを選択します。Web リソースが Cookie の本体に埋め込まれた URL を使用する場合 (一般的な方法ではありません) に、このオプションが有効になっていないと、ユーザーに問題が報告される可能性があります。一般的な現象としては、予期せず別の URL にリダイレクトされます。このオプションは既定で有効です。
- Web プロキシ サービスがバックエンド リソースから送信される Cookie の path 属性を変換するようにする場合は、[**Translate cookie path (Cookie の path を変換)**] チェックボックスを選択します。ブラウザは、Cookie のパスを使用して、Cookie をサーバーに送信するタイミングを判断します。アプライアンスは、ブラウザが認識するパスを変更するため、Cookie のパスが変換されていないと、ブラウザから Cookie が送信されません。この状況の一般的な現象としては、有効なログイン クレデンシャルを入力した後に何回も入力が要求されます。このような現象が発生する場合は、このオプションを有効にします。このオプションは既定で有効です。

8 [**Save (保存)**] を選択します。

構成済みの Web アプリケーション プロファイル

いくつかの構成済みの Web アプリケーション プロファイルがアプライアンスに付属しています。一般的に使用される一部の Web アプリケーションには、これらのプロファイルを使用することを推奨します。 (さらに追加することもできます。Web アプリケーション プロファイルの追加を参照してください)事前設定されたプロファイルは 構成済みの Web アプリケーション プロファイルに示されています。

構成済みの Web アプリケーション プロファイル

Web アプリケーション プロファイル	説明
既定	NTLM または基本認証のシングル サインオンを使用しない大部分の Web アプリケーションやサイトに使用できる、デフォルト プロファイル
Domino Web Access 8.x	Lotus Domino Web Access のプロファイル (バージョン 8.x のみ)
iNotes 5.x	Lotus iNotes のプロファイル (バージョン 5.x のみ)
Onyx CRM	Onyx CRM Employee Portal のプロファイル (バージョン 4 以降)
Outlook Web Access	NTLM または基本認証のシングル サインオンを使用する Microsoft Outlook Web Access やその他のサイトのプロファイル
WorkPlace	WorkPlace の読み取り専用プロファイル

Web アプリケーション プロファイルの例

ここでは、アプライアンスが到着する要求に適用する Web アプリケーション プロファイルをどのように決定するかを説明し、リソースの指定でプロファイルをどのように柔軟に使用できるかを解説します。

Web リソースの要求の評価方法

Web リソースは定義が極めて広範であるため、アプライアンスは、ルールに従って、到着する要求に適用する Web アプリケーション プロファイルを決定し、最も明確なリソースに関連付けられているプロファイルを選択します。

例えば、次の 2 つのリソースが定義されているとします。

- DNS ドメイン (*xyz.com*) - *Web アプリケーションプロファイル A* が添付されている
- 特定の Web サーバー (*web1.xyz.com*) - *Web アプリケーションプロファイル B* が添付されている

https://web1.xyz.com/timesheet.html に対するユーザー要求が到着した場合、アプライアンスは、*Web アプリケーション プロファイル B* を使用します。これは、*Web アプリケーション プロファイル A* (ドメイン) よりも限定的なリソース (Web サーバー) がこのプロファイルに関連付けられているためです。アプライアンスが実際に使用する順番は、次のようになります。

URL -> Host name -> IP address -> Subnet/IP range -> DNS domain

1 つのプロファイルとドメイン全体の関連付け

1 つのドメイン内のすべてのリソースに同じ Web アプリケーション プロファイルを関連付ける場合は、そのドメインにプロファイルを関連付けてから、そのドメイン内に定義するすべての個々のリソースで、[*None*] をプロファイルとして選択します。個々のリソースは、ドメインのプロファイルを継承します。特定のリソースにプロファイルが関連付けられておらず、継承するプロファイルも存在しない場合、アプライアンスは、システム デフォルトをプロファイルに使用します。

Web アプリケーション プロファイルの編集と削除

プロファイルの変更前に、関連付けられているアプリケーションとその変更に互換性があることを確認します。

プロファイルに 1 つ以上のリソースが関連付けられていると、AMC でプロファイルを削除できません。プロファイルを削除する前に、すべての関連付けを削除する必要があります。詳細については、参照されているオブジェクトの削除を参照してください。

フォームベースのシングル サインオン プロファイルの作成

多くの Web アプリケーションで使用されている、フォームベース認証では、ユーザーが HTML フォームのフィールドに一連のクレデンシャルを入力し、セッション トークンがブラウザの Cookie に保存されます。このタイプの認証は、ブラウザと Web サーバーの任意の組み合わせでもサポートされているため、よく使用されます。それ以外に、ログイン ページをカスタマイズできるというメリットもあります。

AMC を使用してシングル サインオン プロファイルをセットアップすることで、ユーザーのアプライアンスのクレデンシャルがフォームベースの認証を使用する Web アプリケーションに転送されるようにできます。このプロセスは自動化されていないため、SonicWall テクニカル サポートの支援が必要になる可能性があります。HTML コードに精通していて、フォームの要素名やユーザー クレデンシャルが保存される Cookie の名前などの情報を知っている必要があります。

いくつかの組み込みプロファイルもあり、環境に合わせて変更できます。

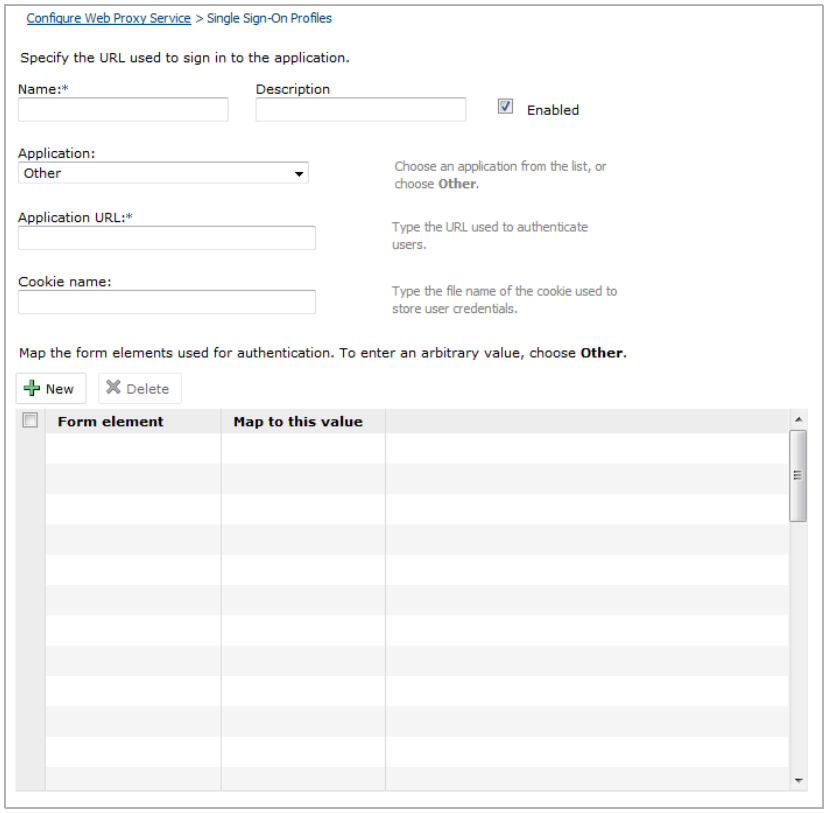
- OWA 2003
- OWA 2007/2010
- OWA 2013
- Citrix Nfuse 1.7
- Citrix XenApp
- Citrix XenDesktop

Outlook Web Access の組み込みシングル サインオン プロファイルを変更するには、

1 AMC のメイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] エリアで、[**Web proxy service (ウェブ プロキシ サービ)**] の下にある [**Configure (設定)**] をクリックします。

3 [**Single Sign-On Profiles (シングル サインオン プロファイル)**] タブをクリックし、[**New (新規)**] をクリックします。[**Configure Single Sign-On Profile (シングル サインオン プロファイルの設定)**] ページが表示されます。



4 [**Name (名前)**] と [**Description (説明)**] に入力し、[**Application (アプリケーション)**] リストから該当する OWA (Outlook Web Access) アプリケーションを選択します。(新規作成してカスタム フォームの要素を指定する場合は、[**Other (その他)**] を選択します)。

5 [**Application URL (アプリケーション URL)**] フィールドに、アプリケーション タイプの URL (例えば、Citrix XenApp/XenDesktop サイトや Microsoft Exchange OWA のフォームベース認証 DLL) を入力します。OWA DLL の場合、一般的には、Exchange サーバーの FQDN の後ろに `/exchweb/bin/auth/owaauth.dll` が続きます。例えば、

```
https://owaserver.domain.com/exchweb/bin/auth/owaauth.dll
```

6 [**Cookie name (Cookie 名)**] フィールドに、ユーザー クレデンシャルの保存に使用する Cookie のファイル名を入力します。OWA 2013 の Cookie の名前は **cadata** です。

7 リンクをクリックしてフォーム要素を変更します。(少なくとも、宛先の要素を変更して [**Application URL (アプリケーション URL)**] と一致させる必要があります)。

8 [**Save (保存)**] を選択します。

プロファイルをセットアップすると、WorkPlace リンクがクリックされるかどうかにかかわらず、ユーザーがログインするたびに、ユーザーのクレデンシャルがバックエンド サーバーに自動的に送信されるようになります。許容ライセンス数に制限があると、この動作が問題になる可能性があります。

ユーザーがログインすると、そのユーザーのクレデンシャルが、シングル サインオン プロファイルが構成されているすべての Web アプリケーションに送信されます。Web アプリケーション プロファイルとは異なり、シングル サインオン プロファイルは AMC ではリソースに関連付けられず、アプリケーション リソースはプロファイル内に定義されます。

Windows NTLM または基本認証を使用する Web アプリケーションでの SSO の構成については、Web アプリケーション プロファイルを参照してください。

Kerberos の制限付き委任

SMA は Kerberos の制限付き委任 (KCD) をサポートしています。Kerberos の制限付き委任 (KCD) は、サービスを委任するためにフロントエンドサービスを信頼する必要のない、既存の Kerberos インフラストラクチャを使用した認証サポートを提供します。

Kerberos の制約付き委任 (KCD) では、証明書、スマートカード、または RADIUS などの Kerberos 以外の方法を使用して認証されたユーザーは、追加の資格情報を入力することなく Kerberos 保護リソースにアクセスできます。例えば、Kerberos ではなく シングル サインオン (SSO) を使用して認証するユーザーには、Kerberos 保護ウェブ リソースへのアクセスが許可されます。

ほとんどのシングル サインオン (SSO) の方法は、従来のユーザー名 / パスワードの資格情報に依存しています。ただし、これらの資格情報は、証明書、スマートカード、または RADIUS 認証では機能しません。Kerberos 制約付き委任 (KCD) では、管理者が Kerberos の制約付き委任 (KCD) のユーザー名とパスワードを構成します。

Microsoft の Kerberos v5 拡張機能は、ユーザーのためのサービス (S4U) と呼ばれ、次の 2 つの部分から構成されています。

- S4U2Self
- S4U2Proxy

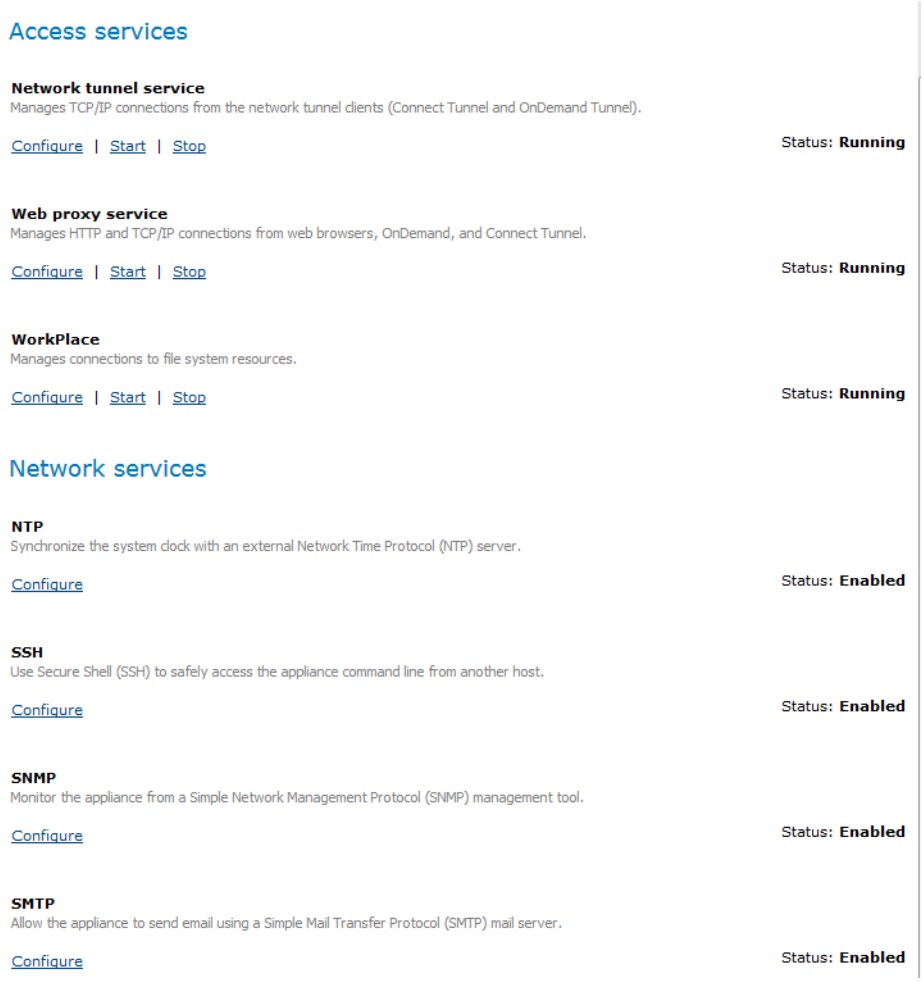
S4U2Self は、サービスがクライアントに代わってサービスチケットを取得することを可能にし、通常はクライアント証明書とともに使用されます。S4U2Self は Kerberos プロトコル移行拡張です。

S4U2Proxy は、ユーザーのサービスチケットのみを持つユーザーに代わって、サービスが任意のサービスへのサービスチケットを取得できるようにします。サービスは管理者によって制約されます。S4U2Proxy は Kerberos の制限付き委任 (KCD) 拡張です。

Kerberos の制約付き委任の設定

Kerberos の制約付き委任 (KCD) を有効にするには:

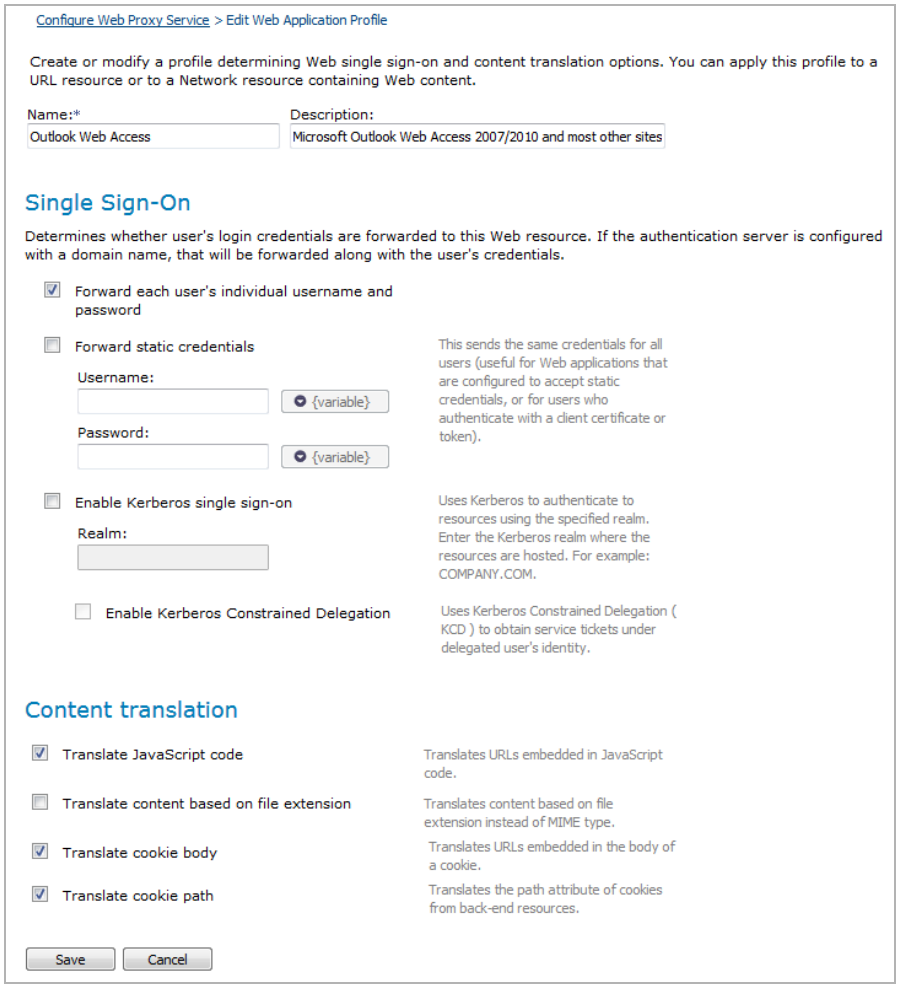
1 [**Services (サービス)**] > [**Access services (アクセス サービス)**] ページに移動します。



2 [**Web proxy service (ウェブ プロキシ サービス)**] で、[**Configure (設定)**] をクリックします。

3 [**Configure Web Proxy Service (ウェブ プロキシ サービスの設定)**] ダイアログで、[**Web Application Profiles (ウェブ アプリケーション プロファイル)**] を選択します。

4 [**Web Proxy Services (ウェブ プロキシ サービス)**] の一覧から、[**Web Proxy Service (ウェブ プロキシ サービス)**] を選択します。[**Edit Web Application Profile (ウェブ アプリケーション プロファイルの編集)**] ダイアログが表示されます。



5 必要なオプションのチェックボックスをオンにします。

- [**Enable Kerberos Constrained Delegation (Kerberos の制約付き委任を有効にする)**] - [**Enable Kerberos Constrained Delegation (Kerberos の制約付き委任を有効にする)**] オプションは、[**Kerberos Single Sign-On (Kerberos シングル サインオン)**] オプションが選択されている場合にのみチェックする必要があります。
- [**Enable fallback (フォールバックを有効にする)**] - [**Enable fallback (フォールバックを有効にする)**] オプションは、[**Enable Kerberos Constrained Delegation (Kerberos の制約付き委任を有効にする)**] オプションがチェックされている場合のみチェックする必要があります。

  [**Enable fallback (フォールバックを有効にする)**] オプションによって、何らかの理由で KCD に障害が発生した場合、ユーザーは再度資格情報を入力するよう求められます。[**Enable fallback (フォールバックを有効にする)**] がオフになっていて、KCD が失敗した場合、エラー ページが表示されます。

  メモ：Firefox では、[**Enable fallback (フォールバックを有効にする)**] は、ネゴシエートと NTLM の両方がバックエンド リソースでそれぞれの順序で有効になっている場合にのみ機能します。この場合、[**Enable fallback (フォールバックを有効にする)**] は Safari では機能しません。Safari は資格情報を再入力するよう求めるプロンプトを表示しますが、成功しません。[**Enable fallback (フォールバックを有効にする)**] は、**NTLM** がバックエンド上の唯一の認証プロバイダである場合にのみ機能します。これは KCD でサポートされていない構成です。

6 [**Save (保存)**] を選択します。

Microsoft Outlook Anywhere 向け SMA のサポートの設定

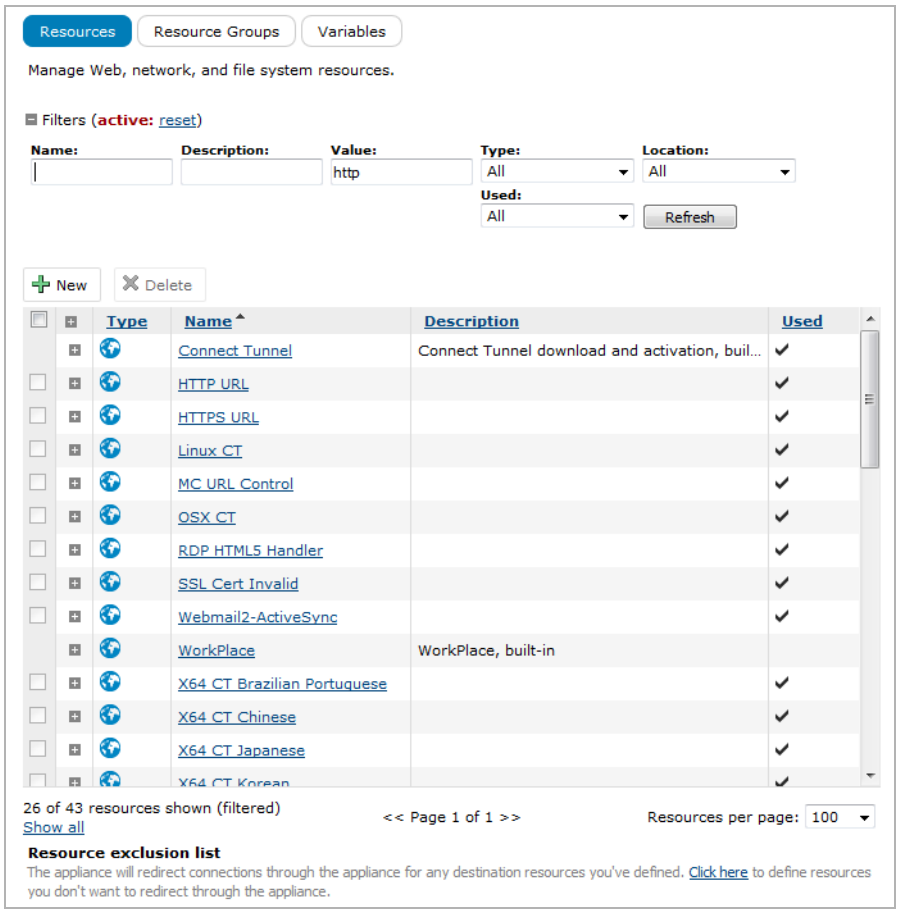
SMA は、Windows Outlook クライアント用の Microsoft Outlook Anywhere をサポートします。Outlook Anywhere は基本的に、次のいずれかのプロトコルを使用して Microsoft Exchange サーバーに接続する Outlook クライアントです。

- HTTP 経由のリモート プロシージャ コール (RPC)
- HTTP 経由の MAPI

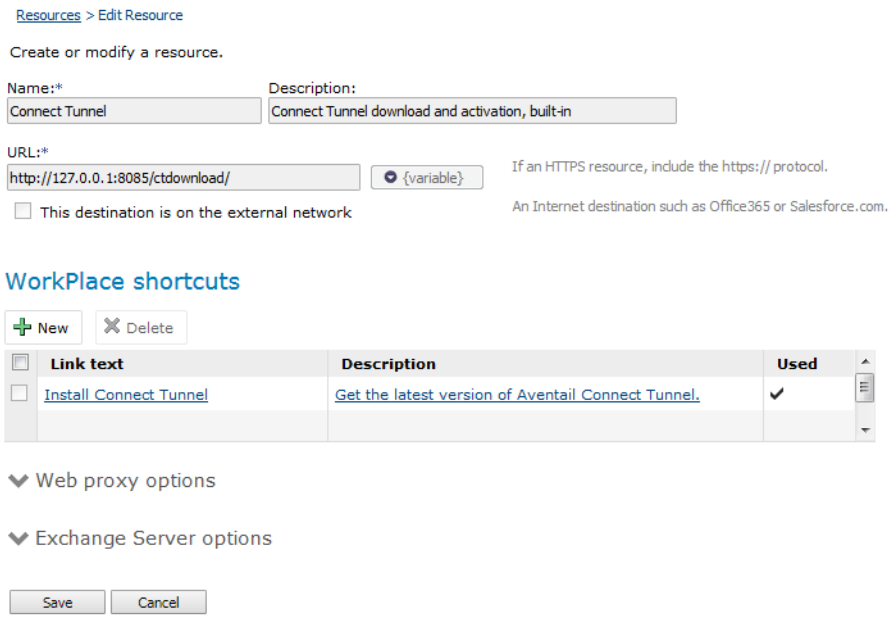
Microsoft Outlook Anywhere を使用すると、Microsoft Office Outlook を使用するエンドユーザーは、社内ネットワークの外部からインターネット経由で Exchange サーバーに接続できます。

Outlook Anywhere 向け SMA のサポートを構成するには:

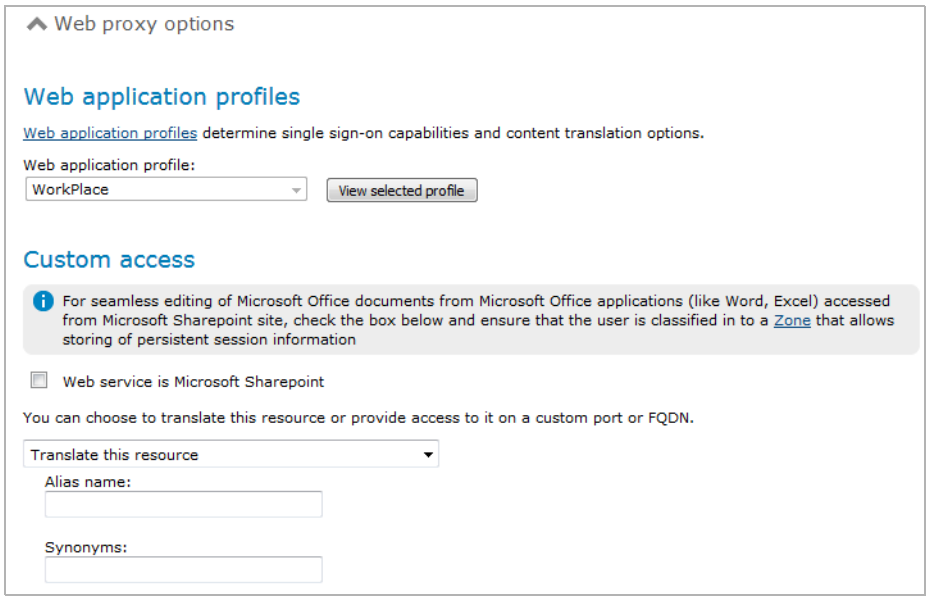
1 SMA デバイスで、**[Security Administration (セキュリティ管理)] > [Resources (リソース)]** ページに移動します。



2 編集するリソースをクリックします。[**Edit Resource (リソースの編集)**] ダイアログが表示されます。



3 [**Web proxy options (Web プロキシ オプション)**] パネルをクリックして開きます。



4 [**Web application profile (Web アプリケーション プロファイル)**] ドロップダウン メニューから [**OWA/Single Sign-on (OWA/シングル サインオン)**] を選択します。

5 [**Exchange Server options (Exchange Server オプション)**] パネルをクリックして開きます。

6 [**Enable Exchange ActiveSync and Outlook Anywhere access to this resource (このリソースへの Exchange ActiveSync および Outlook Anywhere アクセスを有効化)**] チェックボックスをオンにします。

7 [**Exchange server FQDN (Exchange Server の FQDN)**] フィールドに、ユーザーの Exchange サーバーの外部 FQDN URL を入力します。

これは、Exchange サーバーでの Outlook Anywhere サービス (RPC / HTTP および MAPI / HTTP プロトコルと EWS サービス) の外部 FQDN URL として構成されているものと同じ値にする必要があります。

8 [**Realm (レルム)**] ドロップダウン メニューで、目的の**レルム**を選択します。

9 [**Exchange Autodiscover FQDN**] に、Exchange Autodiscover サービスの FQDN を入力します (例: **autodiscover.example.com**)。

Autodiscover FQDN は Autodiscover サービスを決定するために Outlook クライアントによって使用され、Outlook クライアントがユーザーの電子メールアドレスを承認するだけで Outlook オプションを構成できるようにします。例えば、電子メール アドレス `user@yourcompany.com` の Autodiscover FQDN は `autodiscover.yourcompany.com` になります。

autodiscover.yourcompany.com という名前は、アプライアンスのパブリック IP アドレスを持つパブリック DNS サーバーで設定する必要があります。

10 Outlook Anywhere の [**Fallback Exchange server URL (フォールバック Exchange Server の URL)**] フィールドを空白のままにします。

> **メモ：**RPC over HTTP を使用する Outlook Anywhere の場合、基本認証のみがサポートされます。したがって、バックエンド交換サーバーは、Outlook Anywhere - ExternalClientAuthenticationMethod の基本認証をサポートするように構成する必要があります。HTTP 経由の MAPI の場合、任意の認証方法を構成できます。

> **メモ：**Outlook クライアントからの要求の場合、ゾーンの分類は属性なしで行われ、ユーザーは一致するゾーンに分類されます。

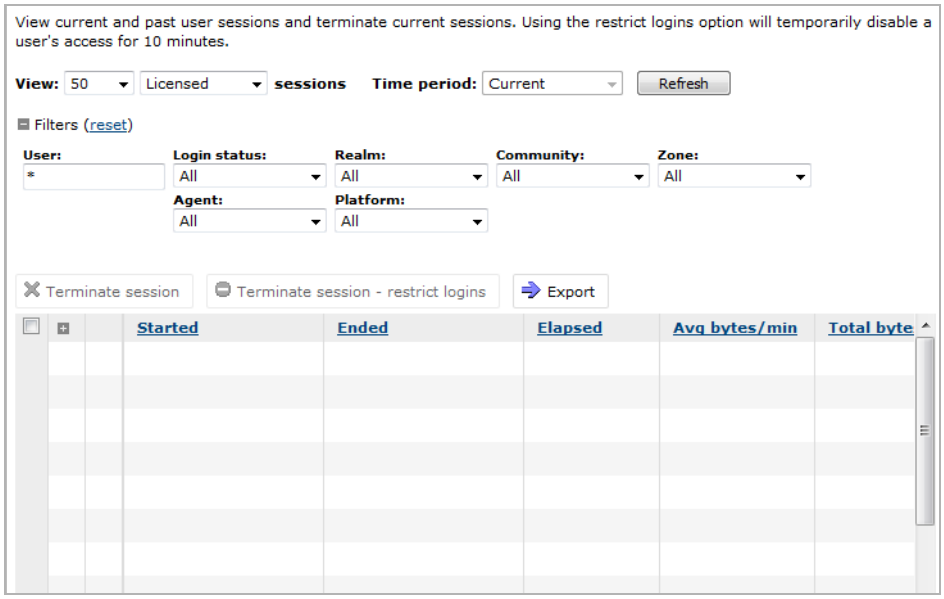
Autodiscover FDQN は、[**System Configuration (システム設定)**] > [**Network Settings (ネットワーク設定)**] ページにも表示されます。

ユーザー セッションの表示

[**Agents (エージェント)**] ドロップダウン メニューのフィルタとして [**Exchange**] を選択すると、[**Monitoring (監視)**] > [**User (ユーザ)**] > [**Sessions (セッション)**] ページに Exchange ActiveSync および Outlook Anywhere を使用する SMA ユーザを表示できます。**Exchange** フィルタは、Exchange ActiveSync および Outlook Anywhere ユーザーをフィルタ処理します。詳細ビューには、そのユーザーのアクセス エージェントの内容が表示されます。

Outlook Anywhere ユーザーセッションを表示するには:

1 **Monitoring (監視) > User Sessions (ユーザー セッション)** ページに移動します。



2 [**Agents (エージェント)**] ドロップダウン メニューで、[**Exchange**] を選択します。

[**Exchange Server**] オプションにカーソルを置くと、Exchange ActiveSync および Outlook Anywhere ユーザーがこのオプションで表示されます。

3 [**Refresh (更新)**] をクリックして新しいユーザー リストを表示します。

4 一覧に表示されているユーザーの詳細を表示するには、そのユーザーをクリックします。

詳細表示の [**Access Agent (アクセス エージェント)**] フィールドには、ユーザーが使用しているエージェントが表示されます。Outlook Anywhere は [**Access-Agent (アクセス エージェント)**] フィールドに表示されます。

アクセス制御ルール

アクセス制御ルールは、ユーザーまたはグループが使用できるリソースを決定します。ルールの定義を広げて、どのような方法でのアクセスも可能することもできますが、ルールの定義を狭くして、Web ブラウザ、Connect と OnDemand、またはネットワーク エクスプローラといった特定のアクセス方法だけを許可することもできます。

ユーザーごとにリソースへのアクセスを許可するかどうかを評価することに加えて、アクセス制御ルールでは、End Point Control ゾーンやデバイスのプロファイルを使用するユーザーのアクセス ポイントの信用度も判断要素として使用できます。詳細については、ゾーンおよびデバイス プロファイルによる EPC の管理を参照してください。

トピック:

- 構成アクセス制御ルール
- 拒否ルールの非互換性の解決
- 無効な接続先リソースの解決

構成アクセス制御ルール

時間の経過に伴ってネットワークが変化すると、アクセス制御ルールを構成して、ユーザーやグループが使用できるアプリケーション リソースを決定することが必要になります。

アクセス制御ルールを追加する前に、既存のルールをよく検証し、新しいルールを作成するのではなく、ルールを変更できないかを確認します。既存のルールをコピーし、パラメータを変更することもできます。

新しいルールを追加する場合は、現在の構成を見直して、新しいルールをルール順のどこに置くかを決定します。新しいルールは、デフォルトではリストの 1 番上に追加されますが、正しい位置に移動できます。

トピック:

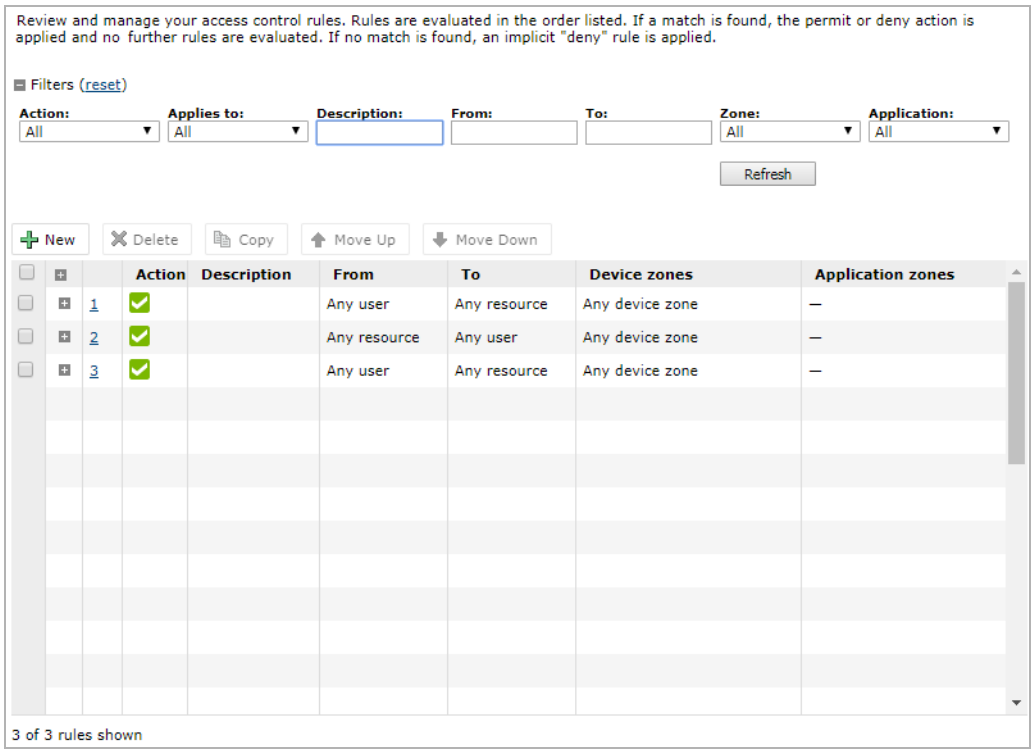
- アクセス制御ルールの表示
- 双方向接続のアクセス制御ルール
- 逆方向接続と相互接続の要件
- 逆方向接続のアプリケーション ポートの保護
- 順方向接続のアクセス制御ルールの追加
- アクセス制御ルールの詳細属性の指定
- 逆方向接続のアクセス制御ルールの追加
- 相互接続のアクセス制御ルールのペアの追加
- アプリケーションのアクセス制御用にアクセス制御ルールを追加する
- アクセス制御ルールの詳細属性の構成
- アクセス方法と詳細オプション
- アクセス制御ルールからのユーザーとリソースの追加
- アクセス制御ルールの編集、コピー、削除

アクセス制御ルールの表示

アクセス制御ルールは、[**Access Control (アクセス制御)**] ページに番号順に表示されます。アプライアンスは各ルールを番号順に評価します。デフォルトでは、すべてのアクセス制御ルールが表示されますが、[**Filters (フィルタ)**] 設定を使用すると、リソース タイプやその他の基準でフィルタできます。

アクセス制御ルールを表示するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。



2 デフォルトでは、リソース タイプにかかわらず、作成したすべてのルールが表示されます。[**Filters (フィルタ)**] セクションを使用すると、ルールのサブセットを表示できます。フィルターの使用方法については、フィルタを参照してください。特定のルール セットを表示するには、[**Filters (フィルタ)**] の [**Method (方式)**] ドロップダウン メニューから次のいずれかを選択します。ルールセットの説明

ルールセットの説明

方法	説明
ウェブ ブラウザ	Web ベース (HTTP と HTTPS) リソースへのアクセスを制御するルールを表示します。
トンネル / OnDemand マップ モードを接続する	クライアント/サーバー (TCP/IP) リソースへのアクセスを制御するルールを表示します。
ネットワーク エクスプローラ	WorkPlace を使用する Windows ファイル システム リソースへのアクセスを制御するルールを表示します。

3 アクセス制御ルールリストに表示されるデータを確認します。

- チェック ボックスの列を使用して、削除、コピー、または並べ替える 1 つ以上のルールを選択します ([**Move Up (上に移動)**] ボタンと [**Move Down (下に移動)**] ボタンを使用します)。
- 番号の列は、ルールが評価される順番を表します。ルールを編集するには、対応する番号をクリックします。
- 構成の詳細やルールが参照するオブジェクトを表示するには、ルールの隣にあるプラス記号 (+) をクリックします。

- [**Action (動作)**] 列は、ルールによってアクセスが許可または拒否されるのか、または無視されるのかを表します。ルール アクション インジケータ をご覧ください。

ルール アクション インジケータ

インジケータ	説明
緑	アクセスは許可されます。
赤	アクセスは拒否されます。
グレー	ルールは評価されません(ルールを無効にすると、ルールを削除せずに一時的に使用を中止できます)。

- [**Description (説明)**] 列には、ルール作成時に入力して説明テキストが表示されます。
- [**From (送信元)**] 列は、ルールが適用されるユーザーを表します ([**Any (すべて)**] はすべてのユーザーに適用されます)。逆方向接続の場合、この列は、ユーザーまたはグループに接続されるリソースを表します。双方向接続のアクセス制御ルールを参照してください。
- [**To (送信先)**] 列には、ルールを適用する対象リソースが表示されます ([**Any (すべて)**] はすべてのユーザーに適用されます)。逆方向接続の場合、この列は、リソースに逆方向接続するユーザーまたはグループに接続されるリソースが表示されることもあります。双方向接続のアクセス制御ルールを参照してください。
- [**Method (方式)**] 列は、特定のアクセス方法がルールに関連付けられているかどうかを表します。地球のアイコンは、Web ブラウザベースの HTTP アクセスを表します。フォルダ付きの地球のアイコンは、ネットワーク エクスプローラを表し、ファイル システム リソースへの Web アクセスが提供されます。Secure Mobile Access のロゴは、Connect Tunnel クライアントまたはプロキシ クライアント、または OnDemand Tunnel エージェントまたはプロキシ エージェントを使用するアクセスを表します。[**Any**] は、ルールがすべてのアクセス方法に適用されることを表します。
- [**Zone (ゾーン)**] 列は、アクセス ルールが特定の End Point Control ゾーンに関連付けられているかどうかを表します。EPC ゾーンは、クライアント デバイスの属性に基づいて接続要求を分類するために使用されます。[*Any (すべて)*] は、ルールがすべての EPC ゾーンに適用されることを表し、赤の「**制限付き**」アイコンは、1 つ以上の特定のゾーンに対するアクセスがルールによって制御されることを表します。

双方向接続のアクセス制御ルール

VPN 接続では一般的に、ユーザーが開始する、クライアント/サーバー リソースに対する「順方向接続」が実行されます。これに対し、SonicWall のユーザーに対するネットワーク トンネル クライアント (Connect Tunnel または OnDemand Tunnel) では、双方向接続が有効です。

SonicWall VPN の場合、双方向接続には以下のものが含まれます。

- VPN ユーザーからクライアント/サーバー リソースへの順方向接続。順方向接続のアクセス制御ルールの追加を参照してください。
- クライアント/サーバー リソースから VPN ユーザーへの逆方向接続。逆方向接続の一例として、ユーザーのマシンにソフトウェアの更新を「送出する」SMS サーバーがあります。逆方向接続のアクセス制御ルールの追加を参照してください。
- 相互接続は VoIP (Voice over Internet Protocol) アプリケーションだけに使用され、VPN ユーザー同士の通話を可能にします。相互接続には、1 つは順方向接続用、もう 1 つは逆方向接続用のペアのアクセス制御ルールが必要です。相互接続のアクセス制御ルールのペアの追加を参照してください。

双方向接続のこれ以外の例としては、VPN ユーザーがファイルをダウンロードやアップロードに使用する FTP サーバーや、リモートのヘルプデスク アプリケーションなどがあります。

逆方向接続と相互接続の要件

逆方向接続と相互接続のアクセス制御ルールを構成する前に、次の要件を満足している必要があります。

- ネットワーク トンネル サービスがアプライアンスで実行中である必要があります。AMC の [**Services (サービス)**] ページで、[**Network tunnel service (ネットワーク トンネル サービス)**] のステータスが [**Running (実行中)**] であることを確認します。
- ネットワーク トンネル クライアントの IP アドレス プールが構成されている必要があります。セットアップ方法については、IP アドレス プールの構成を参照してください。
- VoIP アプリケーションにアクセスするユーザーは、ネットワーク トンネル クライアント (Connect Tunnel または OnDemand Tunnel) を自分のコンピュータに展開するよう構成されているコミュニティに所属している必要があります。コミュニティの作成と構成を参照してください。

逆方向接続のアプリケーション ポートの保護

デフォルトでは、リソースからユーザーへの逆方向接続では、ユーザーのコンピュータのすべてのポートに対してアクセスできます。セキュリティを強化するには、逆方向接続にアクセス制御ルールを作成し、アプリケーションが使用するポートだけにアクセスを限定します。アプリケーションのドキュメントで、アプリケーションを使用するために開いている必要があるファイアウォール ポートを確認します。

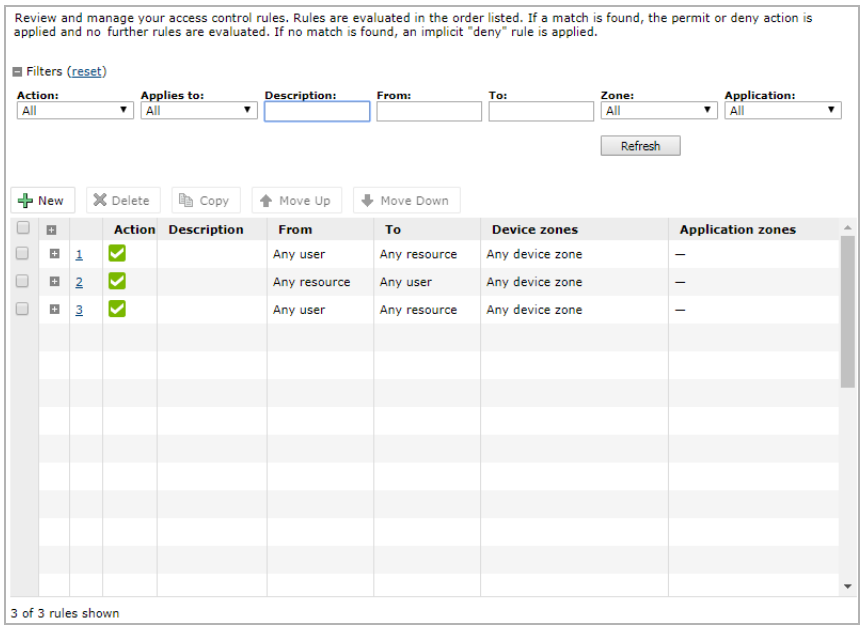
逆方向接続のアクセス ルールを構成する場合、[**Destination restrictions (送信先の制限)**] オプションを使用して、逆方向接続するアプリケーションが必要とするポートへのアクセスを限定します。このオプションについては、アクセス制御ルールの詳細属性の構成を参照してください。

順方向接続のアクセス制御ルールの追加

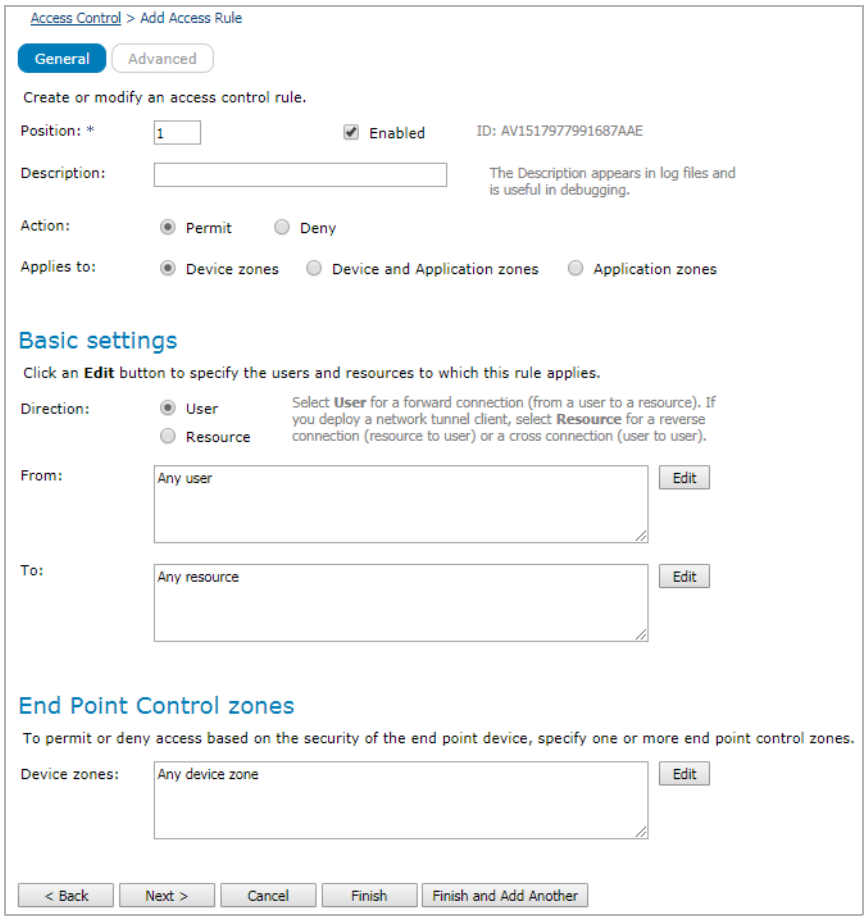
以下の手順で、ユーザーから対象リソースへの順方向接続のアクセス制御ルールを追加します。相互接続 (VoIP アプリケーション用など) のアクセス制御ルールの作成については、相互接続のアクセス制御ルールのペアの追加を参照してください。

順方向接続のアクセス制御ルールを追加するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。



2 [**New (新規)**] をクリックします。[**Edit Access Rule (アクセス ルールの追加)**] ページが表示されます。



3 [**Number (番号)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。デフォルトでは、新しいルールはリストの 1 番上に追加されますが、このボックスを使用すると、ルールをどの位置にでも移動できます。例えば、番号「3」を新しいルールに割り当てると、新しいルールは、現在のルール「**3**」 (ルール「**4**」になります) の前に挿入されます。このフィールドは必須です。

[**Number (番号)**] フィールドの右側には、トラブルシューティングに使用できる、ルールの一意の識別子が表示されます。ルールを追加または変更すると、例えば、管理コンソールの監査ログには、この ID を使用して変更のレコードが表示されます。ログの詳細については、システム ロギングおよびモニタリングを参照してください。

4 [**Description (説明)**] フィールドに、ルールについての分かりやすいコメントを入力します。この手順はオプションですが、わかりやすい説明を入力すると、ルールのリストを後で表示する場合に役立ち、ログ ファイルにも表示されるため、デバッグに役立ちます。[**ID**] は、AMC によって自動的に割り当てられる一意の識別子で、削除できません。

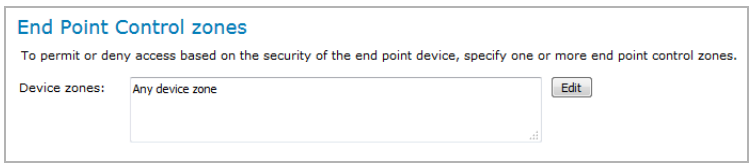
5 [**Action (動作)**] ボタンを使用して、ルールを許可 ([**Permit (許可)**]) または拒否 ([**Deny (禁止)**]) のどちらのアクセスに使用するか、またはルールを無効にするのか [**Disabled (無効)**] を指定します。

6 [**Basic settings (基本設定)**] に、次の情報を入力します。

- [**User (ユーザ)**] をクリックして、(ユーザーからリソースへの) 順方向接続を構成します。
- ネットワーク トンネル クライアントを展開する場合は、[**Resource (リソース)**] (リソースからユーザーへの) 逆方向接続または (ユーザーからユーザーへの) 相互接続を制御するルールを作成します。逆方向接続を使用する前に、ネットワーク トンネル サービスを IP アドレス プールで構成する必要があります (IP アドレス プールの構成を参照)。
    - [**From (送信元)**] フィールドでは、ルールを適用するユーザーまたはユーザー グループを指定します。ユーザーやグループをリストから選択する場合は、[**Edit (編集)**] をクリックします。ユーザーまたはグループが指定されないと、このフィールドの値は [**Any** *user*] になります。
    - [**To (送信先)**] は、ルールの対象となるリソースまたはリソース グループを指定します。[**Edit (編集)**] をクリックして、リソースのリストから選択します。対象となるリソースが選択されないと、このフィールドの値は [**Any** *resource*] になります。宛先リソースにモバイルコネクトの非互換性を示すワイルドカードが含まれていると、警告が表示されます。

> **メモ**：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

7 [**End Point Control zones (エンド ポイント制御の制限)**] エリアで、リソースへのアクセスを許可または拒否するゾーンを選択します。[**Edit (編集)**] をクリックして、リストから選択します。このフィールドのデフォルトは [**Any (すべて)**] ゾーンです。ゾーンの構成と使用については、ゾーンおよびデバイス プロファイルによる EPC の管理を参照してください。



8 [**Next (次へ)**] をクリックして他の設定も構成するか (アクセス制御ルールの詳細属性の指定を参照)、[**Finish (完了)**] をクリックして現在の設定を保存します。

アクセス制御ルールの詳細属性の指定

多くのルールでは、ユーザーまたはグループ、対象リソース、およびアクセス方法を含む基本構成だけで十分ですが、アクセスを厳格に制限するための追加オプションも使用できます。例えば、ユーザーの場所に基づいて (IP アドレスで) 接続を制御できます。ソース ネットワークがアクセス ルールで参照されると、要求元の場所に基づき、対象リソースへの接続が許可または拒否されるため、セキュリティがさらに強化されます。

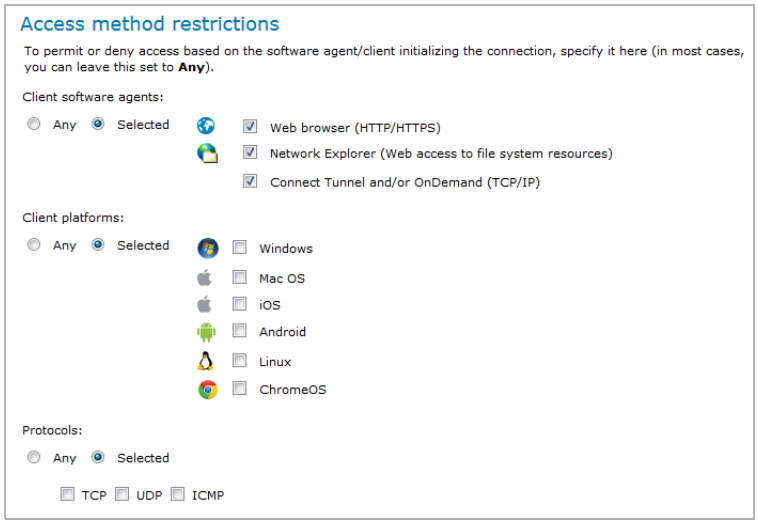
アクセス制御ルールの詳細設定を構成するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 [**New (新規)**] をクリックします。[**Edit Access Rule (アクセス ルールの追加)**] ページが表示されます。

3 [**Next (次へ)**] をクリックすると、[**Advanced (詳細)**] ページが表示されます。

4 [**Access method restrictions (アクセス方法の制限)**] エリアで、リソースへの 1 つ以上のアクセス方法を選択します。リソースに対して特定のアクセス方法を使用する必要がある環境でない限り、[**Any**] が推奨される設定です。



a アクセス方法を選択すると、指定した方法によって、該当する詳細オプションが有効になります。[**Selected (選択)**] をクリックして、このルールで必要となるアクセス方法を選択します。クライアント ソフトウェア エージェント

クライアント ソフトウェア エージェント

アクセス方法	説明
ウェブ ブラウザ (HTTP/HTTPS)	Web ブラウザを使用して接続するユーザーの HTTP または HTTPS のリソースからのアクセスを管理します。 以下の [**Advanced (詳細)**] 設定を使用できます。 • ユーザのネットワーク アドレス • 日時の制限

クライアント ソフトウェア エージェント

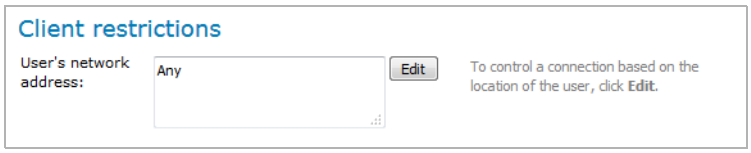
アクセス方法	説明
ネットワーク エクスプローラ 	ネットワーク エクスプローラを使用して接続する WorkPlace ユーザーの Windows ファイル システム リソースからのアクセスを管理します。 以下の [**Advanced (詳細)**] 設定を使用できます。 • ユーザのネットワーク アドレス • [Read/write permissions] • 日時の制限
トンネルおよび / または OnDemand の接続 (TCP/IP)	次のいずれかを使用して接続するユーザーの、クライアント/サーバー アプリケーション、ファイル サーバー、データベースなどの TCP/IP リソースからのアクセスを管理します。 • Connect Tunnel またはプロキシ クライアント • OnDemand Tunnel またはプロキシ エージェント 例えば、Connect または OnDemand を使用するユーザーがネットワーク ドメインにアクセスできるようにし、ただし、そのドメイン内の Web リソースへのブラウザのアクセスを許可しないようにしたいとします。そのためには、[**Connect Tunnel and/or OnDemand Mapped Mode (トンネルおよび / または OnDemand マップモードを接続)**] を唯一のアクセス方法として指定するルールを作成し、[**Client restrictions (クライアントの制限)**] エリアでネットワーク ドメインを指定します。 以下の [**Advanced (詳細)**] 設定を使用できます。 • プロトコル • ユーザのネットワーク アドレス • 送信先の制限 (ポート) • 日時の制限

b [**Selected (選択済み)**] をクリックして、ネットワーク トンネルまたはプロキシ サービスがクライアントから受け付けるプロトコルを [**Protocols (プロトコル)**] (プロトコルの選択 を参照) で指定します。それぞれのコマンドをここでも簡単に説明しますが、詳細については、http://www.ietf.org/rfc/rfc1928.txt を参照してください。

プロトコルの選択

プロトコル	説明
TCP	通常の TCP 接続 (SSH、telnet、SCP など) を有効にします。
UDP	ネットワーク トンネルまたはプロキシ サービスに UDP データ転送を許可します。これは、ストリーミング オーディオや Microsoft Outlook の新着メール通知などの処理に必要です。
ICMP	(Internet Control Message Protocol) ネットワーク トラブルシューティング コマンドの ping と traceroute を有効にします。このオプションを選択すると、ネットワーク トンネルまたはプロキシ サービスにこれらの処理を許可するように構成されます。このオプションは、ネットワーク トンネルまたはプロキシ サービス経由の ICMP パケットのフローも有効にします。

5 [**Client restrictions (クライアントの制限)**] の下の [**User's network address (ユーザーのネットワークアドレス)**] フィールドで、ルールで評価するソースネットワークの名前を指定します。



これは、接続要求元に基づいてアクセスを制御する場合に役立ちます。[**Edit (編集)**] をクリックして、リソースのリストから選択します。ソース ネットワークが指定されないと、このフィールドのデフォルト値は [**Any**] です。逆方向接続の場合、このオプションを使用して、特定のポートまたはアプリケーションのリソースが要求元であるユーザーのコンピュータへのアクセス要求をブロックできます。

6 [**Destination restrictions (送信先の制限)**] を使用して、個々のポート [**Ports (ポート)**] またはポートの範囲によるアクセスを制限します。任意のポートでのアクセスを有効にするには、[**Any (すべて)**] をクリックします。複数のポートを指定するには、[**Selected (選択)**] をクリックし、ポート番号をセミコロンで区切って入力します。ポート範囲を指定するには、開始と終了の番号をハイフンで区切って入力します。例えば、SMTP メール サーバーへのアクセスを制御するポリシーを作成する場合に、ポート 25 (SMTP トラフィックの一般的なポート) によるアクセスのみを許可できます。最新のポート番号割り当てのリストは、http://www.iana.org/assignments/port-numbers に記載されています。

[**Permissions (権限)**] を使用して、ルールでファイル システム リソースへの [**Read (読み取り)**] または [**Read/Write (読み取り/書き込み)**] アクセスのどちらを許可するかを指定します。これらのアクセス権限は、Windows のアクセス制御ルールと併用されます。ユーザーに特定のファイル権限を与えるには、両方のエンティティ (すなわち、Windows とアプライアンス) で許可する必要があります。ファイルのアップロードを無効にすると、書き込みアクセスの権限があってファイルの移動や削除を実行できるユーザーであっても、ファイルへの書き込みを実行できません。これらの設定は、逆方向接続では無視されます。

7 [**Time and date restrictions (日時の制限)**] で、ルールを有効にする日時を指定します(これらの日時制限のフィールドのタイム ゾーンは、ローカル時間です)。[**Shift (シフト)**] または [**Range (範囲)**] を指定するか、ルールを常に有効にするように指定します。

8 [**Save (保存)**] をクリックするか、別のルールを定義する場合は、[**Finish and Add Another (完了して他を追加)**] をクリックします。

AMC では複数のアクセス方法を柔軟にリソースに割り当てられるため、アクセス方法とリソースの間に不一致が発生する可能性があります。そのような状況は、指定されたリソースと互換性のないアクセス方法を割り当てるルールを作成した場合に発生します。例えば、[**Web browser (ウェブ ブラウザ)**] を Windows ドメイン リソースのアクセス方法として指定すると、AMC で「Invalid destination resources (無効な宛先リソース)」というエラー メッセージが発生します。詳細については、無効な接続先リソースの解決を参照してください。

いくつかのリソースとアクセス方法が含まれる [Deny] ルールを作成し、そのルールによって後続のルールが評価できなくなる可能性もあります。この場合、アクセス ポリシーで参照される他のリソースへのユーザー アクセスがブロックされてしまいます。アクセス方法とリソースの互換性の判断に使用するロジックについては、拒否ルールの非互換性の解決を参照してください。

逆方向接続は、IP アドレス プールがネットワーク トンネル クライアントに構成されている場合のみ使用できます。順方向接続から逆方向接続にルールを変更しようとした場合に IP アドレス プールが構成されていないと、AMC からエラー メッセージが表示されます。

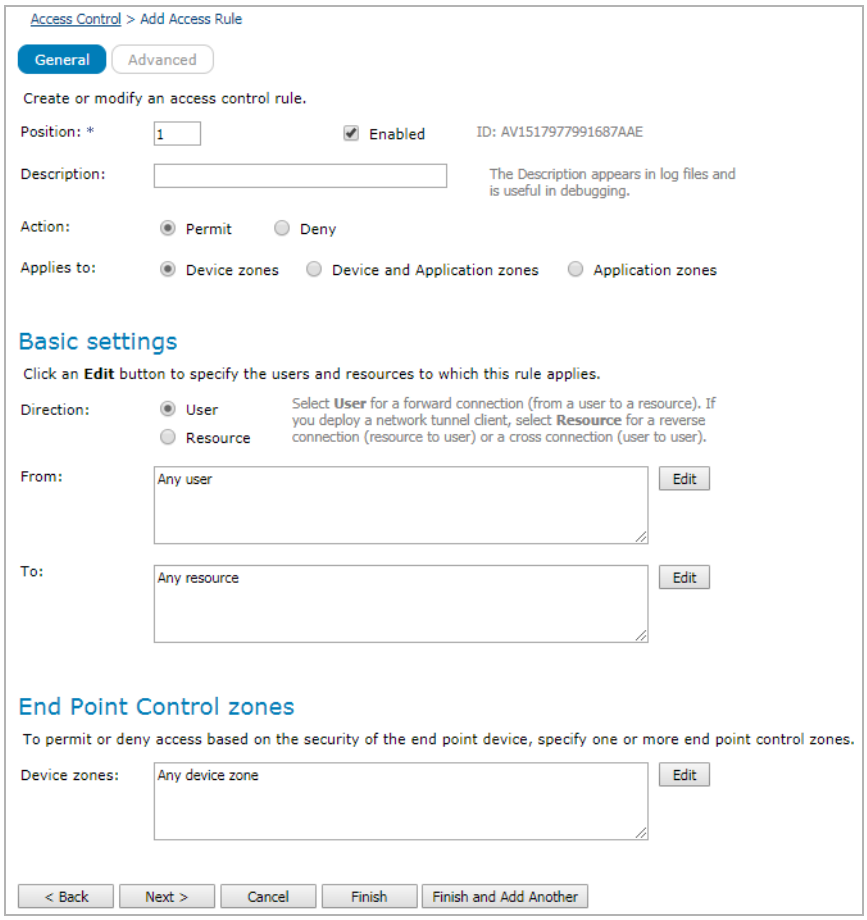
逆方向接続のアクセス制御ルールの追加

以下の手順で、対象リソースからユーザーへの逆方向接続のアクセス制御ルールを追加します。逆方向接続の例としては、IBM の Tivoli プロビジョニング製品や Microsoft の Systems Management Server (SMS) があります。詳細については、逆方向接続と相互接続の要件を参照してください。

逆方向接続のアクセス制御ルールを追加するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 [**New (新規)**] をクリックします。[**Edit Access Rule (アクセス ルールの追加)**] ページが表示されます。



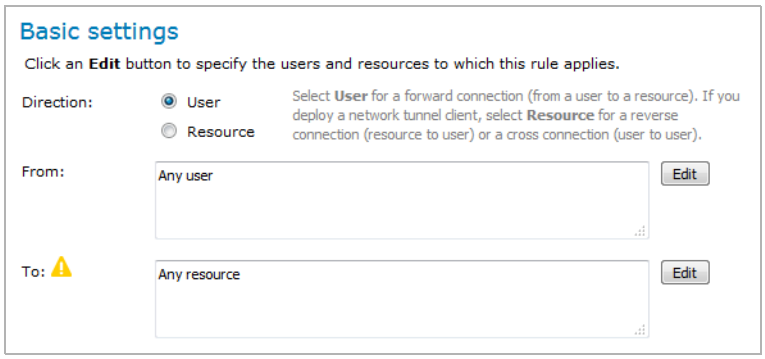
3 [**Number (番号)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。デフォルトでは、新しいルールはリストの 1 番上に追加されますが、このボックスを使用すると、ルールをどの位置にでも移動できます。例えば、4 つのルールがあって番号「3」を新しいルールに割り当てると、現在のルール 3 (挿入後はルール 4 になります) の前に挿入されます。このフィールドは必須です。

4 [**Description (説明)**] フィールドに、ルールについての分かりやすいコメントを入力します。この手順はオプションですが、わかりやすい説明を入力すると、ルールのリストを後で表示する場

合に役立ち、ログ ファイルにも表示されるため、デバッグに役立ちます。[**ID**] は、AMC によって自動的に割り当てられる一意の識別子で、削除できません。

5 [**Action (動作)**] ボタンを使用して、ルールを許可 ([**Permit (許可)**]) または拒否 ([**Deny (禁止)**]) のどちらのアクセスに使用するか、またはルールを無効にするのか [**Disabled (無効)**] を指定します。

6 [**Basic settings (基本設定)**] に、次の情報を入力します。



- [**Resource (リソース)**] ボタンを選択して、リソースからユーザーへの逆方向接続を制御するルールを作成します。[**User (ユーザ)**] と [**Resource (リソース)**] ボタンで、順方向接続ルールと逆方向接続ルールを切り替えます。

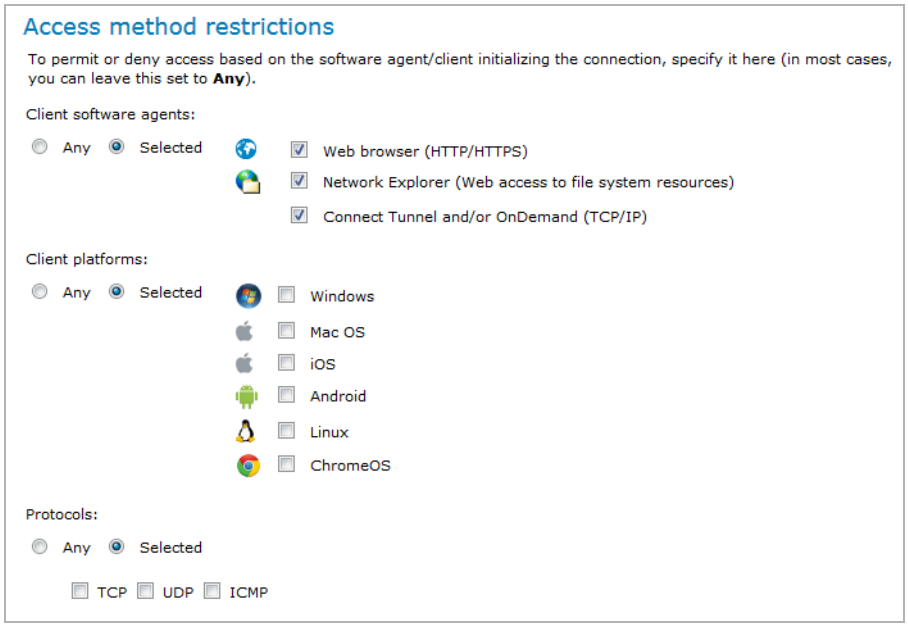
  逆方向接続は、IP アドレス プールがネットワーク トンネル クライアントに構成されている場合のみ使用できます。逆方向接続を作成しようとした場合に IP アドレス プールが構成されていないと、AMC からエラー メッセージが表示されます。詳細については、双方向接続のアクセス制御ルールを参照してください。

- [**From (送信元)**] フィールドでは、ユーザーに接続するリソースを指定します。[**Edit (編集)**] をクリックして、リソースのリストから選択します。リソースが選択されない場合、このフィールドのデフォルト値は [**Any resource**] です。

- [**To (送信先)**] フィールドでは、リソースが接続するユーザーを指定します。[**Edit (編集)**] をクリックして、リストから選択します。ユーザーが選択されない場合、このフィールドのデフォルト値は [**Any user**] です。

7 [**Next (次へ)**] をクリックすると、[**Advanced (詳細)**] ページが表示されます。

8 [**Access methods (アクセス方法)**] エリアで [**Any (すべて)**] を選択し、要求するアクセス方法に関係なく、すべてのリソースへのアクセスをルールで自動的に管理するようにします。こうすると、逆方向接続に必要である Connect Tunnel クライアントまたは OnDemand Tunnel エージェントがルールによって確実に管理されます。これ以外のアクセス方法は逆方向接続をサポートしておらず、迂回されます。



9 ルールの作成が終了したら、[**Save (保存)**] をクリックします。

相互接続のアクセス制御ルールのペアの追加

相互接続のアクセス制御ルールを作成する手順の多くは、順方向接続または逆方向接続のルールを作成する手順と同じです。ただし、重要な違いと要件がいくつかあります。

例えば、VPN ユーザー同士が VoIP アプリケーションを使用して通話できるようにするには、アプライアンスにユーザーが IP アドレス プールに接続するためのルールを 1 つ作成し、IP アドレス プールがユーザーに接続するための 2 つ目のルールを作成します。

また、この手順に従って、FTP サーバーとユーザーの間の双方向接続を許可するルールのペアを作成する必要もあります。

相互接続のアクセス制御ルールを追加するには、

1 逆方向接続を構成するための要件を満足していることを確認します。詳細については、逆方向接続と相互接続の要件を参照してください。

2 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

3 [**New (新規)**] をクリックします。[**Edit Access Rule (アクセス ルールの追加)**] ページが表示されます。

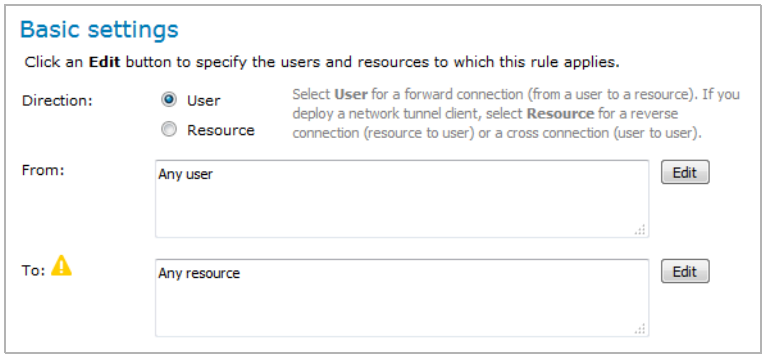
4 [**Position (位置)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。デフォルトでは、新しいルールはリストの 1 番上に追加されますが、このボックスを使用すると、ルールをどの位置にでも移動できます。例えば、4 つのルールがあって番号「3」を新しいルールに割り当てると、現在のルール **3** (挿入後はルール **4** になります) の前に挿入されます。このフィールドは必須です。

5 [**Description (説明)**] フィールドに、ルールについての分かりやすいコメントを入力します。この手順はオプションですが、ルールのリストを後で表示する場合に、説明が役立ちます。ログ ファイルにも表示されるため、ログを検証して接続が特定のルールに一致しない理由を調べる場合にも役立ちます。[**ID**] は、AMC によって自動的に割り当てられる一意の識別子で、削除できません。

相互接続には順方向接続と逆方向接続のルールのペアが必要であるため、2 つのルールに似た名前を割り当てて、アクセス制御ルールのリストで簡単に特定できるようにします。

6 [**Action (動作)**] ボタンを使用して、ルールを許可 ([**Permit (許可)**]) または拒否 ([**Deny (禁止)**]) のどちらのアクセスに使用するか、またはルールを無効にするのか [**Disabled (無効)**] を指定します。

7 [**Basic settings (基本設定)**] で、[**User (ユーザ)**] と [**Resource (リソース)**] ボタンを使用して、順方向接続と逆方向接続のルールを選択します。



- ユーザーから IP アドレス プールへの順方向接続ルールを作成するには、[**User (ユーザ)**] をクリックします。
- IP アドレス プールからユーザーへの逆方向接続ルールを作成するには、[**Resource (リソース)**] をクリックします。

8 [**Basic settings (基本設定)**] の [**From (送信元)**] フィールドで、このルールを適用するユーザーまたはリソースを指定します。

- 順方向接続ルールの場合、ルールを適用するユーザーまたはユーザー グループを指定します。[**Edit (編集)**] をクリックして、ユーザーまたはグループのリストから選択します。デフォルト値は [*Any user*] です。
- 逆方向接続ルールについて、VoIP アプリケーションに使用するアドレス プールを指定します。[**Edit (編集)**] をクリックして、リソースのリストからアドレス プールを選択します。デフォルト値は [**Any resource**] です。

9 [**Basic settings (基本設定)**] の [**To (送信先)**] ボックスで、このルールを適用するユーザーまたはリソースを指定します。

- 順方向接続ルールについて、VoIP アプリケーションに使用するアドレス プールを指定します。[**Edit (編集)**] をクリックして、リソースのリストからアドレス プールを選択します。デフォルト値は [**Any resource**] です。
- 逆方向接続ルールについて、ルールを適用するユーザーを指定します。[**Edit (編集)**] をクリックして、ユーザーまたはグループのリストから選択します。デフォルト値は [**Any user**] です。

10 [**Access method restrictions (アクセス方法の制限)**] エリアで、[**Any (すべて)**] を選択します。これにより、逆方向接続が Connect Tunnel クライアントまたは OnDemand Tunnel エージェントのいずれかであるユーザーのエンド ポイント デバイスの正しいアクセス方法を、アプライアンスの Smart Access 機能が判断できるようになります。これ以外のアクセス方法は相互接続または双方向接続をサポートしておらず、迂回されます。

11 [**Access method restrictions (アクセス方法の制限)**] エリアで [**Any (すべて)**] を選択し、要求するアクセス方法に関係なく、すべてのリソースへのアクセスをルールで自動的に管理するようにします。こうすると、逆方向接続に必要である Connect Tunnel クライアントまたは OnDemand Tunnel エージェントがルールによって確実に管理されます。これ以外のアクセス方法は逆方向接続をサポートしておらず、迂回されます。

12 相互接続ルールのペアの 1 つ目のルールを作成し、2 つ目のルールを作成して保存したら、[**Finish (完了)**] をクリックします (または、最初のルールをペアに保存し、そのコピーを作成して、ユーザーとリソースの設定を元に戻すこともできます)。

相互接続ルールのペアを構成する順方向接続ルールと逆方向接続ルールを構成した後に、2 つのルールをアクセス制御リストで並べて配置します。そうすることで、関連するルールとして識別しやすくなります。

相互接続を作成しようとした場合に IP アドレス プールが構成されていないと、AMC からエラー メッセージが表示されます。詳細については、双方向接続のアクセス制御ルールを参照してください。

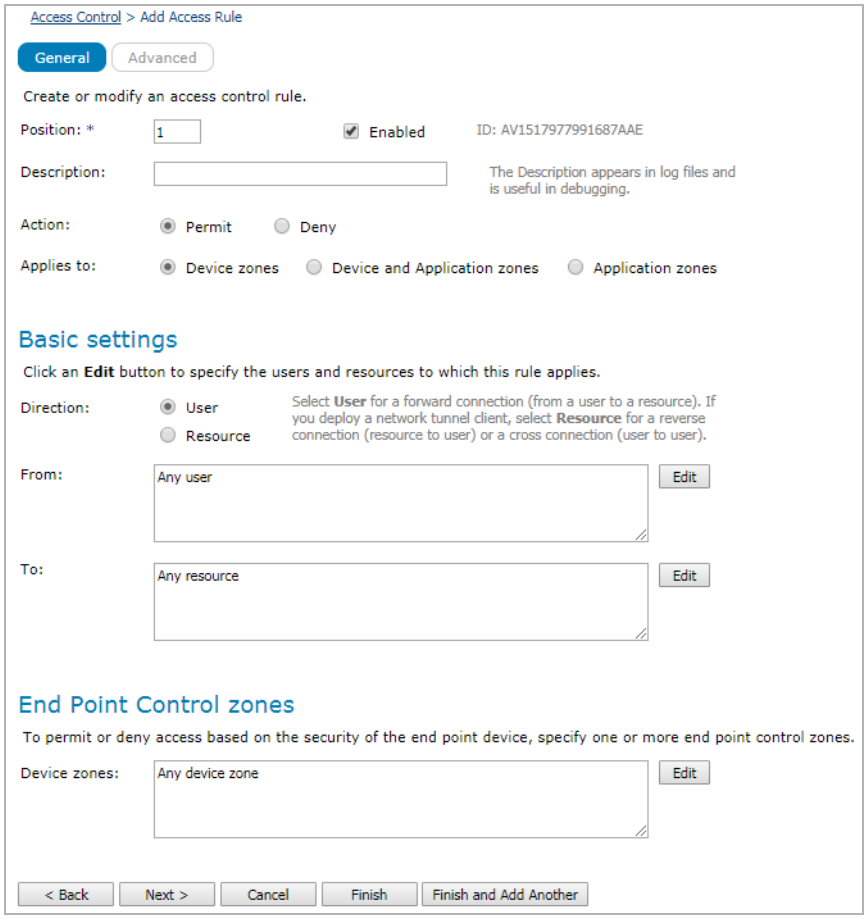
アプリケーションのアクセス制御用にアクセス制御ルールを追加する

次の手順を実行して、特定のアプリケーション ゾーンのコンテキスト内で、特定のアプリケーションを使用して個人デバイスから特定のアプリケーションを使用してアクセスするユーザーまたはグループを制御するアクセス制御ルールを追加します。詳細については、アプリケーション アクセス制御を参照してください。

アプリケーションのアクセス制御用にアクセス制御ルールを追加するには:

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 [**New (新規)**] をクリックします。[**Edit Access Rule (アクセス ルールの追加)**] ページが表示されます。



3 [**Position (位置)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。デフォルトでは、新しいルールはリストの 1 番上に追加されますが、このボックスを使用すると、ルールをどの位置にでも移動できます。例えば、4 つのルールがあって番号「3」を新しいルールに割り当てると、現在のルール 3 (挿入後はルール 4 になります) の前に挿入されます。このフィールドは必須です。

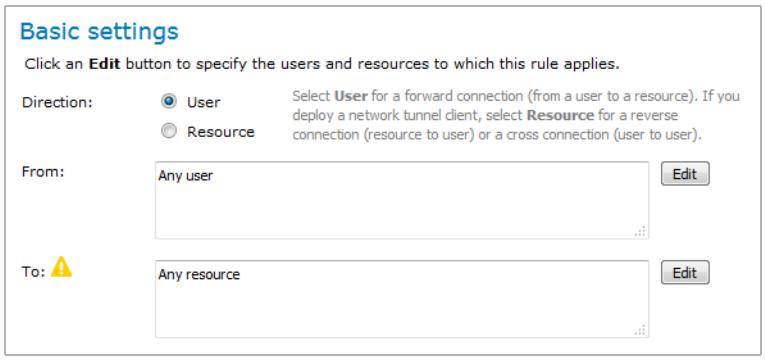
4 [**Description (説明)**] フィールドに、ルールについての分かりやすいコメントを入力します。この手順はオプションですが、わかりやすい説明を入力すると、ルールのリストを後で表示する場合に役立ち、ログ ファイルにも表示されるため、デバッグに役立ちます。[**ID**] は、AMC によって自動的に割り当てられる一意の識別子で、削除できません。

5 [**Action (動作)**] フィールドを使用して、ルールを許可 ([**Permit (許可)**]) または拒否 ([**Deny (禁止)**]) のどちらのアクセスに使用するかを指定します。既定は「**Permit (許可)**」です。

6 [**Applies to (適用先)**] フィールドで、ルールに関連付けられるゾーンのタイプとして [**Device zones (デバイス ゾーン)**]、[**Device and Application zones (デバイスおよびアプリケーション ゾーン)**]、または [**Application zones (アプリケーション ゾーン)**] を選択します。既定値はデバイス ゾーンです。

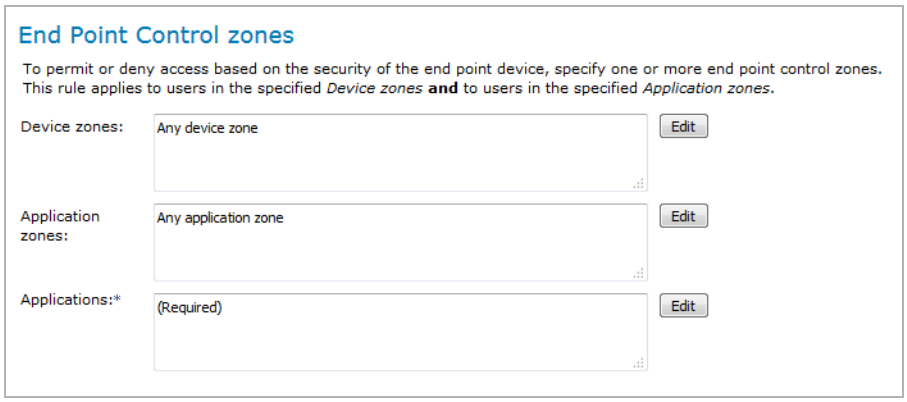
> **メモ**：アクセス制御ルールは、デバイス ゾーン、アプリケーション ゾーン、またはデバイス ゾーンとアプリケーション ゾーン (適用オプションのいずれか) に適用できます。個々のユーザー接続は、任意の時点で単一のデバイス ゾーンまたはアプリケーション ゾーンに適用されます。したがって、ユーザー接続は一度に 1 つのゾーンに適用されますが、デバイス ゾーン、アプリケーション ゾーン、またはデバイス ゾーンとアプリケーション ゾーンに適用するようにアクセス制御リストを書き込むことができます。

7 [**Basic settings (基本設定)**] に、次の情報を入力します。



- [**Direction (方向)**] を選択して、リソースまたはユーザーからの接続を制御するルールを作成します。[**User (ユーザ)**] と [**Resource (リソース)**] ボタンが切り替わります。既定は「**User (ユーザ)**」です。
- [**From (送信元)**] フィールドでは、選択したアプリケーションリスト上のアプリケーションを使用して、関連リソースリストへのアクセスを許可または拒否したユーザーまたはグループを指定します。[**Edit (編集)**] をクリックして、リストから選択します。リソースが選択されない場合、このフィールドのデフォルト値は [**Any user**] です。
- [**To (送信先)**] フィールドは、ユーザーまたはグループが選択したアプリケーション リストのアプリケーションを使用してアクセスできる必要なリソースを指定します。[**Edit (編集)**] をクリックして、リストから選択します。ユーザーが選択されない場合、このフィールドのデフォルト値は [**Any resource**] です。

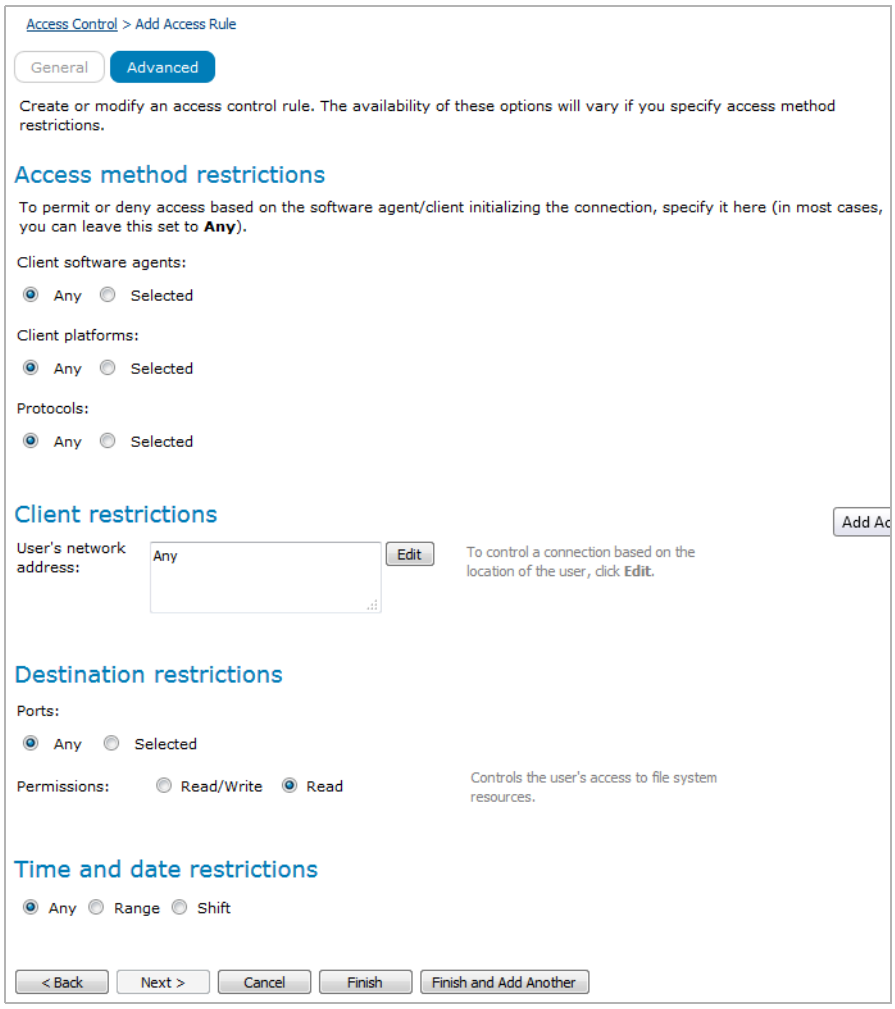
8 [**End Point Control zones (エンド ポイント制御の制限)**] の下に表示される情報を入力します。



- [**Applications zones (アプリケーション ゾーン)**] は、既定値の [**Any application zone (すべてのアプリケーションゾーン)**] を使用するか、アプリケーション ゾーンの [**Edit (編集)**] ボタンをクリックし、このルールを使用するアプリケーション ゾーンを選択します。
- [**Applications (アプリケーション)**] については、アプリケーションの [**Edit (編集)**] ボタンをクリックし、企業ネットワークにこのルールを適用する際にユーザーが使用を許可するアプリケーションを少なくとも 1 つ選択します。ルールを保存するには、表示されたリストから少なくとも 1 つのアプリケーションを選択する必要があります。

メモ：アプリケーション アクセス 制御で説明されているように、アプリケーションはリストされる前に学習する必要があります。

9 下部にある [**Next> (次へ>)**] ボタンをクリックすると、[**Advanced (詳細)**] タブが表示されます。



10 [**Access method restrictions (アクセス方法の制限)**] セクションで、[**Any (任意)**] または [**Selected (選択済み)**] を選択して、接続を初期化するソフトウェア エージェントまたはクライアントに基づいて、アクセスを許可または拒否します。[**Selected (選択済み)**] を選択した場合は、表示されているオプションから目的のすべてのタイプをチェックしてください。オプションの種類 を参照してください。

オプションの種類

クライアント ソフトウェア エージェント	クライアント プラットフォーム	プロトコル
ウェブ ブラウザ (HTTP/HTTPS)	Windows	TCP
ネットワーク エクスプローラ (ファイル システム リソースへの Web アクセス)	Mac OS	UDP
トンネルおよび / または SonicWall OnDemand VPN 接続 (TCP/IP) の接続	iOS Android Linux ChromeOS	ICMP

11 クライアントの制限セクションで、任意のユーザーのネットワークアドレスの既定値を使用するか、[**Edit (編集)**] ボタンをクリックし、このルールを使用するリソースを選択します。

12 送信先制限セクションでは、デフォルトの [**Any (任意)**] のポートを使用して任意のポートでのアクセスを有効にするか、[**Selected (選択済み)**] を選択して個々の [**Ports (ポート)**] またはポートの範囲によるアクセスを制限し、許可するポートのタイプを入力します。例えば、SMTP メールサーバーへのアクセスを制御するポリシーを作成する場合に、ポート 25 (SMTP トラフィックの一般的なポート) によるアクセスのみを許可できます。最新のポート番号割り当てのリストは、http://www.iana.org/assignments/port-numbers に記載されています。

複数のポートを指定するには、ポート番号をセミコロンで区切ります。ポート範囲を指定するには、開始と終了の番号をハイフンで区切って入力します。

13 [**Permissions (権限)**] フィールドで、ルールでファイル システム リソースへの [**Read (読み取り)**] または [**Read/Write (読み取り/書き込み)**] アクセスのどちらを許可するかを指定します。これらのアクセス権限は、Windows のアクセス制御ルールと併用されます。ユーザーに特定のファイル権限を与えるには、Windows とアプライアンスの両方で許可する必要があります。ファイルのアップロードを無効にすると、書き込みアクセスの権限があってファイルの移動や削除を実行できるユーザーであっても、ファイルへの書き込みを実行できません。

14 [**Time and date restrictions (日時の制限)**] セクションで、ルールを有効にする日時を指定します(これらの日時制限のフィールドのタイム ゾーンは、ローカル時間です)。[**Shift (シフト)**] または [**Range (範囲)**] を指定するか、規定値の [**Any (すべて)**] を使用してルールを常に有効にするように指定します。

15 [**Finish (完了)**] をクリックして入力内容を保存します。

アクセス制御ルールの詳細属性の構成

多くのルールでは、ユーザーまたはグループ、対象リソース、およびアクセス方法を含む基本構成だけで十分ですが、[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] の [**Advanced (詳細)**] ページでは、アクセスをさらに限定するための設定を使用できます。

例えば、個別の IP アドレスからの接続のみに制限する場合は、[**User's network address (ユーザのネットワーク アドレス)**] オプションを選択します。ソース ネットワークがアクセス ルールで参照されると、要求元の場所に基づき、対象リソースへの接続が許可または拒否されるため、セキュリティがさらに強化されます。

アクセス制御ルールの詳細設定を構成するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 既存のルールのリンクをクリックします。

3 [**Edit Access Rule (アクセス ルールの編集)**] ページで、[**Advanced (詳細)**] タブをクリックします。

4 [**Access method restrictions (アクセス方法の制限)**] で、接続を初期化するソフトウェア エージェントまたはクライアントに基づいて、アクセスを許可または拒否します。ほとんどの場合、[**Any (すべて)**] の設定のままで構いません。

5 ネットワーク トンネルまたはプロキシ サービスがクライアントから受け付けるプロトコル ([**Protocols (プロトコル)**]) を制限するには、[**Selected (選択)**] をクリックします。それぞれのコマンドをアクセス制御ルールの詳細属性でも簡単に説明しますが、詳細については、http://www.ietf.org/rfc/rfc1928.txt を参照してください。

アクセス制御ルールの詳細属性

プロトコル	説明
TCP	通常の TCP 接続 (SSH、telnet、SCP など) を有効にします。
UDP	ネットワーク トンネルまたはプロキシ サービスに UDP データ転送を許可します。これは、ストリーミング オーディオや Microsoft Outlook の新着メール通知などの処理に必要です。
ICMP	(Internet Control Message Protocol) ネットワーク トラブルシューティング コマンドの ping と traceroute を有効にします。このオプションを選択すると、ネットワーク トンネルまたはプロキシ サービスにこれらの処理を許可するように構成されます。このオプションは、ネットワーク トンネルまたはプロキシ サービス経由の ICMP パケットのフローも有効にします。
サーバーからのバインド要求を許可	クライアントがサーバーからの接続の許可する必要があるプロトコルで使用されます。FTP が顕著な例です。バインドは、Connect/Bind の1 つのペアの接続で行われます。

6 [**User's network address (ユーザのネットワーク アドレス)**] オプションで、ルールで評価する接続元ネットワークの名前を指定します。これは、接続要求元に基づいてアクセスを制御する場合に役立ちます。[**Edit (編集)**] をクリックして、リソースのリストから選択します。ソース ネットワークが指定されないと、このフィールドのデフォルト値は [*Any*] です。逆方向接続の場合、このオプションを使用して、特定のポートまたはアプリケーションのリソースが要求元であるユーザーのコンピュータへのアクセス要求をブロックできます。

7 [**Destination restrictions (送信先の制限)**] を使用して、個々のポート [**Ports (ポート)**] またはポートの範囲によるアクセスを制限します。例えば、SMTP メール サーバーへのアクセスを制御するポリシーを作成する場合に、ポート 25 (SMTP トラフィックの一般的なポート) によるアクセスのみを許可できます。最新のポート番号割り当てのリストは、http://www.iana.org/assignments/port-numbers に記載されています。

任意のポートでのアクセスを有効にするには、[**Any (すべて)**] をクリックします。複数のポートを指定するには、[**Selected (選択)**] をクリックし、ポート番号をセミコロンで区切って入力します。ポート範囲を指定するには、開始と終了の番号をハイフンで区切って入力します。

8 [**Permissions (権限)**] を使用して、ルールでファイル システム リソースへの [**Read (読み取り)**] または [**Read/Write (読み取り/書き込み)**] アクセスのどちらを許可するかを指定します。これらのアクセス権限は、Windows のアクセス制御ルールと併用されます。ユーザーに特定のファイル権限を与えるには、両方のエンティティ (すなわち、Windows とアプライアンス) で許可する必要があります。ファイルのアップロードを無効にすると、書き込みアクセスの権限があってファイルの移動や削除を実行できるユーザーであっても、ファイルへの書き込みを実行できません。これらの設定は、逆方向接続では無視されます。

9 [**Time and date restrictions (日時の制限)**] で、ルールを有効にする日時を指定します(これらの日時制限のフィールドのタイム ゾーンは、ローカル時間です)。[**Shift (シフト)**] または [**Range (範囲)**] を指定するか、ルールを常に有効にするように指定します。

10 ルールの作成が終了したら、[**Save (保存)**] をクリックします。

アクセス方法と詳細オプション

アクセス方法を制限する場合は、選択されているアクセス方法によって詳細オプションが有効または無効になります ([**Any (すべて)**] をアクセス方法として選択すると、すべての詳細オプションを使用できます)。AMC がルールを評価する段階で、そのアクセス方法に関係しないルール属性は選択できなくなります。アクセス方法と詳細オプション の表で、それぞれのアクセス方法に該当する詳細オプションを示しています。

アクセス方法と詳細オプション

アクセス方法	該当する詳細オプション
ウェブ ブラウザ (HTTP/HTTPS)	• ユーザのネットワーク アドレス • 日時の制限
ネットワーク エクスプローラ (ファイル システム リソースへの Web アクセス)	• ユーザのネットワーク アドレス • [Read/write permissions] • 日時の制限
トンネルおよび / または OnDemand の接続 (TCP/IP)	• プロトコル • ユーザのネットワーク アドレス • 送信先の制限 (ポート) • 日時の制限

アクセス制御ルールからのユーザーとリソースの追加

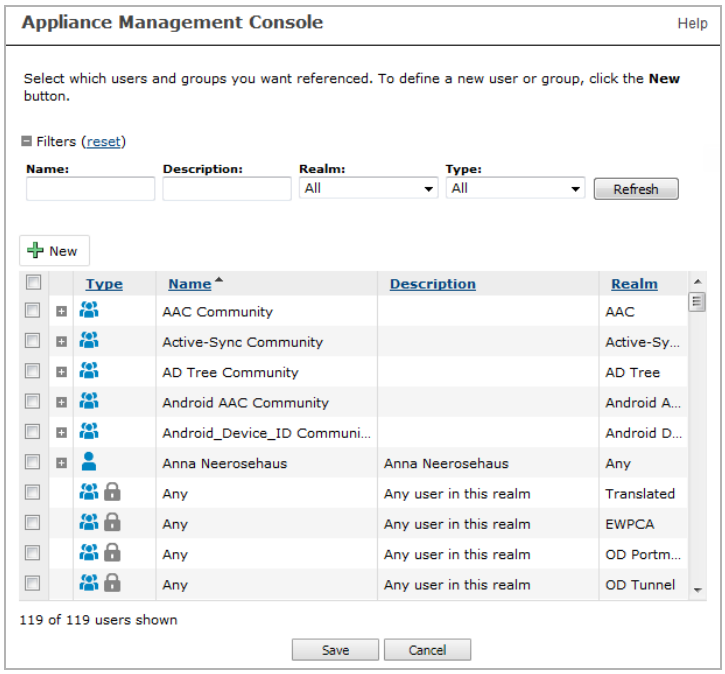
管理者によっては、すべてのポリシー オブジェクト (ユーザー、グループ、リソース) を定義してからアクセス制御ルールを作成したいと考えることもあります。この構造型のアプローチは、初期構成には特に有効ですが、継続的な管理においては不便であることもあります。そのような場合は、アクセス制御ルールの作成に使用するインターフェースから新しいリソースを直接定義できます。

ユーザーまたはリソースを既存のアクセス制御ルールに追加するには、

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 既存のルールのリンクをクリックします。[**Edit Access Rule (アクセス ルールの編集)**] ページが表示されます。

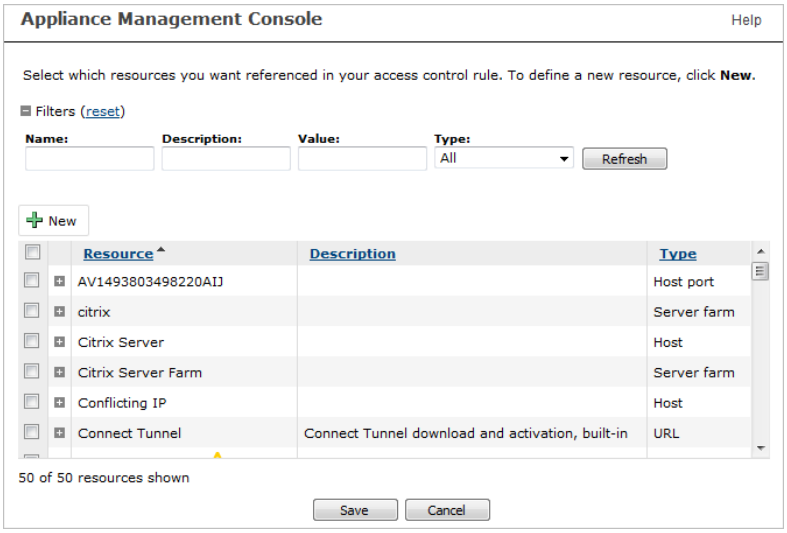
3 [**Basic settings (基本設定)**] エリアの [**From (送信元)**] フィールドの隣にある [**Edit (編集)**] をクリックします。現在のユーザーとグループが別ページに表示されます。アイコンの意味については、アイコンの説明 を参照してください。



アイコンの説明

アイコン	説明
	コミュニティ
	特定のレルムに属してる任意のユーザー
	ユーザーまたはローカル ユーザー

4 [**Basic settings (基本設定)**] エリアの [**To (送信先)**] フィールドの隣にある [**Edit (編集)**] をクリックします。リソースとリソース グループを表示する別のページが表示されます。



5 [**New (新規)**] をクリックします。次に表示されるページは、作成しているオブジェクトのタイプによって異なります。

6 新しいユーザー、グループ、またはリソースの設定を定義します。

7 オブジェクトの作成が終了したら、[**Save (保存)**] をクリックします。

8 アクセス ルールに追加するオブジェクトの隣にあるチェック ボックスを選択し、[**Save (保存)**] をクリックします。

アクセス制御ルールの編集、コピー、削除

アクセス制御ルールを変更または削除する前に、既存のルールをよく検証し、変更がセキュリティ ポリシーにどのように影響するかを理解します。

△ **注意：ルールの削除では確認が求められることがないため、注意してください。**

- アクセス制御リスト内でのルールの並び順を変更できます。並び順を変更する前に、並び替えることでセキュリティ ポリシーにどのように影響するかをよく確認してください。
- 新しいアクセス制御ルールをゼロから作成するのではなく、既存のルールのコピーを作成して一部のパラメータを新しいルールに合わせて変更すると、時間を短縮できます。その際には、作成しようとするルールと特長が似ているルールを選択します。

  ルールのコピーは、新しいアクセス ルールをテストする際にも役立ちます。コピーしたルールを編集し、テスト中は元のルールを無効にします。こうすることで、必要があれば元のルールに戻すことができます。

アクセス制御ルールの編集、削除、コピーについては、参照されているオブジェクトの削除を参照してください。

[**Filters (フィルタ)**] 設定を使用して、表示されるアクセス ルールを特定のアクセス方法やその他の基準でフィルタリングしている場合、[**Move Up (上に移動)**] ボタンや [**Move Down (下に移動)**] ボタンでリストを並べ替えることはできません。[**Method (方式)**] が [**All (すべて)**] に設定されている場合のみ、アクセス制御ルールを移動できます。

複数のルールをリスト内で移動する場合は、[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] ページの [**Number (番号)**] ボックスを変更する方が一般的に速く移動できます。

拒否ルールの非互換性の解決

許可ルールの場合は、リソースとアクセス方法の任意の組み合わせで問題なく使用できますが、拒否ルールに特定の組み合わせのリソースとアクセス方法が含まれていると、後続のルールを評価できなくなることがあります。この場合、アクセス ポリシーで参照される他のリソースへのユーザー アクセスがブロックされてしまう可能性があります。

ポリシーの評価で、拒否ルールが到着する接続要求と一致しているかどうかをアプライアンスが判断できなくなることがあります。このような場合、アプライアンスは、セキュリティ上の予防措置として、ルール セットの処理を停止し、ユーザー アクセスをブロックします。

次の表に示す 3 つの組み合わせのいずれかを参照する拒否ルールを定義しようとすると、AMC から次の警告メッセージが表示されます。

> 「Some of the resources in this rule are not supported by the selected access method(s), which could inadvertently deny access to some resources.」 (このルールの一部のリソースは、選択されたアクセス方法ではサポートされていないため、一部のリソースへのアクセスが誤って拒否される可能性があります。)

ルールの非互換性 に、この警告が表示されるルールの組み合わせを示します。

ルールの非互換性

ルールの動作	リソースのタイプ	アクセス方法
拒否	Windows ドメイン	• すべて • Connect and OnDemand • WorkPlace
拒否	URL	• すべて • Connect and OnDemand
拒否	ファイル共有	• すべて • Connect and OnDemand

例

Windows ドメインへのアクセスをブロックし、**Access methods (アクセス方法)** を [*Any*] に設定する拒否ルールを作成すると仮定します。Windows ドメインには WorkPlace からアクセスできるため、アプライアンスが WorkPlace から接続要求を受け取ると、ルールと一致するため、アクセスが拒否されます。

これに対し、ユーザーが Connect または OnDemand から接続を要求すると、アプライアンスは、(どのリソースが要求されていても) Windows ドメイン ルールがその要求と一致しているかどうかを判断できません。そのため、アプライアンスはポリシー内の後続のルールの評価を停止し、アクセスを直ちに拒否します。Windows ドメイン ルールがアクセス制御ルール リストの先頭にあると、ユーザーが VPN リソースにアクセスできなくなります。また、リストの次のルールが VPN リソースへのアクセスをユーザーに許可する許可のルールであっても、そのルールは評価されません。

問題の解決

ルールの非互換性を解決するには、ルールを変更して、確定できないアクセス方法を参照しないようにします。Windows ドメインやネットワーク共有の場合は、[**Network Explorer (ネットワーク エクスプローラ)**] を唯一のアクセス方法として選択します。URL の場合は、[**Web browser (ウェブ ブラウザ)**] または [**Connect Tunnel and/or OnDemand (トンネルおよび / または OnDemand マップモードを接続) Mapped Mode (トンネルおよび/または OnDemand マップ モードを接続)**] のみを選択します。

無効な接続先リソースの解決

アクセス方法を互換性のない接続先リソースに割り当てるルールを作成しようとすると、AMC は不適合を回避し、「`Invalid resources (無効な リソース)`」という警告を表示します。

無効なアクセス方法と宛先リソースの組み合わせ の表で、この警告が表示されるアクセス方法/接続先リソースの組み合わせを示します。

無効なアクセス方法と宛先リソースの組み合わせ

アクセス方法	無効な接続先リソース
ウェブ ブラウザ	• Windows ドメイン • ネットワーク共有
ネットワーク エクスプローラ	• [URL] (およびマッチング URL)
Connect または OnDemand	• [URL] (およびマッチング URL) • Windows ドメイン

「無効なリソース」の例

AMC では、アクセス方法/リソースの不適合が含まれるルールを保存できません。[**Save (保存)**] をクリックすると、AMC が無効なリソースをルールから削除します。ルールに含まれる不適合リソースが 1 つだけである場合、[**Any**] に置き換えられます。アクセス方法/リソースの不適合の例を以下に示します。

- ルールで [**Web browser (ウェブ ブラウザ)**] が*唯一の*使用できるアクセス方法として指定されている場合、Windows ドメイン リソースを参照できません。(Windows ドメイン リソースは [**Domai (ドメイン)**] がタイプとして設定されており、[**Windows domain (Windows ドメイン)**] チェック ボックスが選択されています)。
- [**Matching URL (マッチング URL)**] リソースを指定するルールでは、[**Web browser (ウェブ ブラウザ)**] がアクセス方法である必要があり、ルールで許可されるアクセス方法に [**Web browser (ウェブ ブラウザ)**] が含まれていないと、「`Invalid resource (無効なリソース)`」という警告が表示されます。

接続先リソースのエラーを解決するには、ルールを変更して、接続先リソースと互換性のあるアクセス方法のタイプにします。アクセス方法/接続先リソースの不整合を回避する最も簡単な方法は、[**Client software agents (クライアント ソフトウェア エージェント)**] と [**Protocols (詳細)**] の両方を [**Any (すべて)**] のままにすることで、[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] ページの [**Advanced (詳細)**] タブですべての [**Access method restrictions (アクセス方法の制限)**] を削除することです。

7

システム管理

- オプションのネットワーク設定
- システム ロギングおよびモニタリング
- 構成データの管理
- システムのアップグレード、リセット、またはロールバック
- SSL 暗号化
- FIPS 認定
- ソフトウェア ライセンス

オプションのネットワーク設定

このセクションでは、システム ロギングとモニタリングの構成方法と使用方法、および Secure Sockets Layer (SSL) 暗号化オプションの構成方法について説明します。また、ソフトウェア バージョンのアップグレード、ロール バック、リセットの他、構成ファイルをバックアップ、リセットするためのさまざまなツールの使用方法についても説明します。

ホストからの SSH アクセスを有効にする方法や、アプライアンスを ping できるよう Internet Control Message Protocol (ICMP) を有効にする方法について説明します。また、アプライアンスで時刻設定を構成する方法についても説明します。

SNMP の構成方法および使用方法については、SNMP の構成を参照してください。

トピック:

- リモート ホストからの SSH アクセスの有効化
- ICMP の有効化
- 時刻設定の構成

リモート ホストからの SSH アクセスの有効化

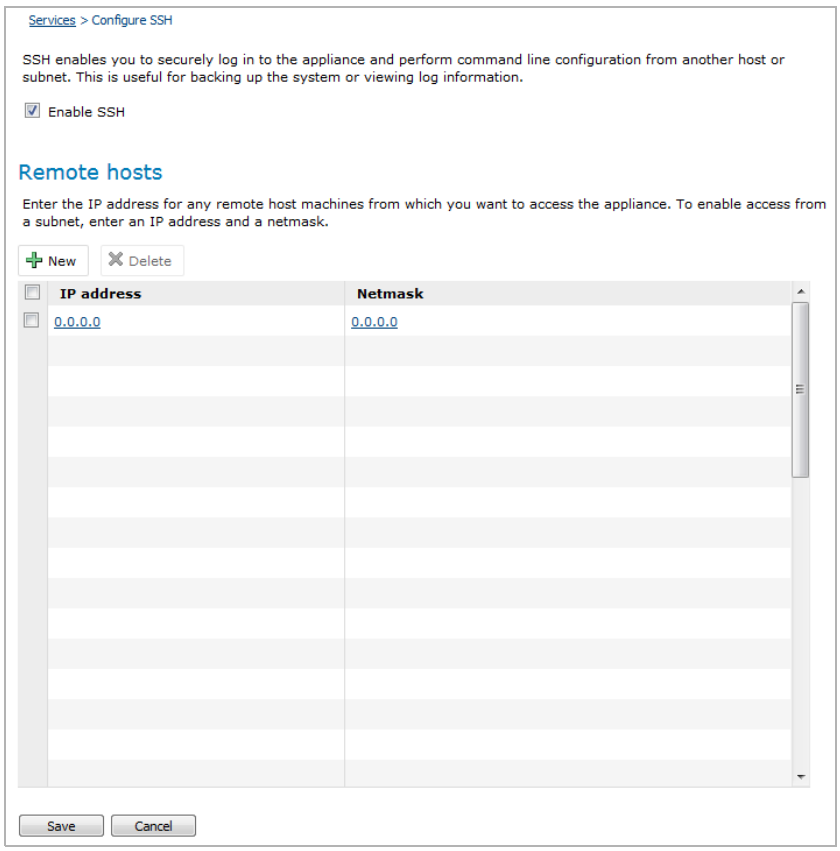
SSH を有効にすると、他のシステムからアプライアンスのコンソールに簡単にアクセスできます。内部ネットワークまたは外部ネットワークからの SSH アクセスを有効にできます。ローカル SSH サーバード メイン (sshd) はポート 22 (SSH で一般的なポート番号) でリッスンします。

SSH アクセスを有効にするには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Network Services (ネットワーク サービス)**] エリアの [**SSH**] に対応する [**Configure (設定)**] リンクをクリックします。

3 SSH を有効にするには、[**Enable SSH (SSH を有効にする)**] チェック ボックスを選択します。



4 SSH アクセスを許可するホストを追加するには、[**New (新規)**] をクリックし、追加するホストの IP アドレスとサブネット マスクを入力して、[**OK**] をクリックします。

5 [**Save (保存)**] を選択します。

ホストを削除するには、

1 削除するホストの左側にあるチェック ボックスを選択します。

2 [**Delete (削除)**] をクリックして、[**Save (保存)**] をクリックします。

メモ：IP アドレスとサブネット マスクの両方に「0.0.0.0」と入力することで、任意のホストからの SSH アクセスを有効にできます。ただしその場合、アプライアンスのセキュリティが低下するという欠点もあります。

ICMP の有効化

ICMP を有効にすると、同じサブネット上の他のコンピュータからアプライアンスへのネットワーク接続をテストするために ping コマンドを使用できるようになります。ただしこれは、ブロードキャスト ping を有効にするものではありません。

注意：ICMP を有効にすると、両方のネットワーク インターフェース (外部および内部) からアプライアンスを ping できるようになります。そのため、ファイアウォールやその他のネットワーク デバイスを使用して ICMP Echo Request トラフィックを禁止しない限り、アプライアンスをインターネットから検出できる状態になります。

ICMP を有効にするには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Network Settings (ネットワーク設定)**] をクリックします。

2 [**Basic (基本)**] エリアの [**Edit (編集)**] リンクをクリックします。[**Configure Basic Network Settings (基本ネットワーク設定の設定)**] ページが表示されます。

3 [**ICMP**] エリアで、[**Enable ICMP pings (ICMP ping を有効にする)**] チェック ボックスを選択します。

4 [**Save (保存)**] を選択します。

時刻設定の構成

重要：時刻またはタイム ゾーンを変更すると、直ちにアプライアンスが再起動します。現在のすべてのユーザー セッションが閉じられます。

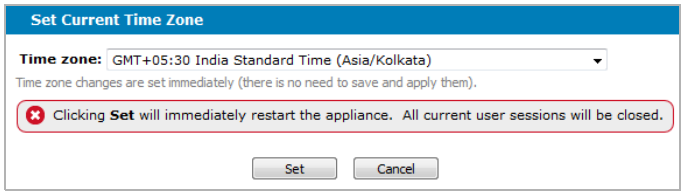
アプライアンスやシステム ログで参照される日付や時刻を設定する場合、タイムゾーンを選択し、必要に応じて現地時間を設定します。現在時刻を設定する方法には、手動で行う方法と、1 つまたは複数の Network Time Protocol (NTP) サーバーと同期する方法の 2 種類があります。

タイムゾーンを変更するには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**General Settings (一般設定)**] をクリックします。

2 [**Appliance options (装置オプション)**] エリアの [**Edit (編集)**] をクリックします。

3 [**Date/time (日付/時刻)**] エリアで、[**Time zone (タイムゾーン)**] の [**Change (変更)**] をクリックします。[**Set Current Time Zone (現在のタイムゾーンを設定)**] ダイアログが表示されます。



4 [**Time zone (タイムゾーン)**] ドロップダウン メニューから現在の現地時間帯を選択します。時間帯はグリニッジ標準時 (GMT) で表示されます。

5 保留中の変更を適用。

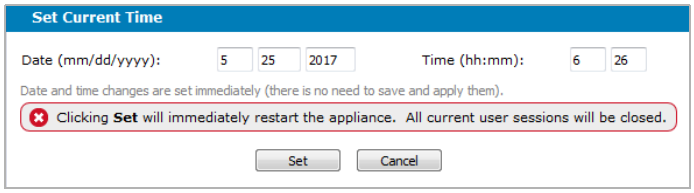
システム時刻を手動で構成するには、

メモ：SonicWall が提供した評価版ライセンスを使用している場合は、システム時刻を現在時刻から前に戻さないでください。時刻を前に戻すと、ライセンス上の理由から、アプライアンスのすべてのサービスが無効になります。

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**General Settings (一般設定)**] をクリックします。

2 [**Appliance options (装置オプション)**] エリアの [**Edit (編集)**] をクリックします。

3 [**Date/time (日付/時刻)**] エリアで、[**Current Time (現在時刻)**] の [**Change (変更)**] をクリックします。[**Set Current Time (現在時刻を設定)**] ダイアログが表示されます。

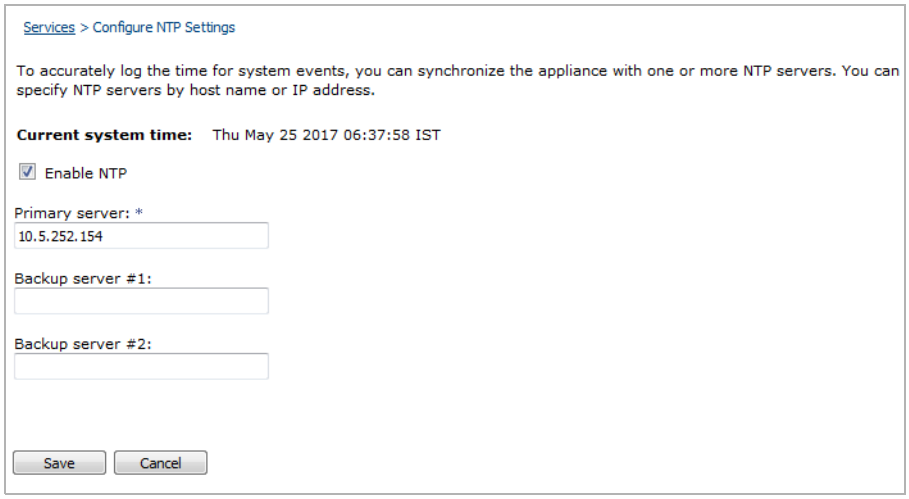


4 現在の日付と時刻を入力します。変更をすぐに適用するには、[**Set (設定)**]をクリックします。

NTP を使用してシステム時刻を構成するには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Network Services (ネットワーク サービス)**] エリアの [**NTP**] に対応する [**Configure (設定)**] リンクをクリックします。[**Configure NTP Settings (NTP 設定の構成)**] ページが表示されます。



3 NTP を有効にするには、[**Enable NTP (NTP を有効化)**] チェック ボックスを選択します。

4 NTP を構成するため、[**Primary server (プライマリ サーバ)**] および [**Backup server (バックアップ サーバ)**] フィールドに 1 つまたは複数の NTP サーバーの IP アドレスを入力します。アプライアンスは、プライマリ サーバーと同期しようとしますが、プライマリ サーバーが使用できないときは、必要に応じてセカンダリ サーバーが使用されます。

5 「**Save (保存)**」を選択します。

メモ：アプライアンスでは NTP 認証鍵を使用していないため、何者かが NTP サーバーになりすまして、アプライアンスに偽の時刻設定を提供することもできます。そのため、NTP サーバーを同期するときは、内部ネットワークのものだけを使用すると良いでしょう。

システム ロギングおよびモニタリング

SMA アプライアンスは、ユーザー アクセスやシステム イベント、AMC の変更など、さまざまな有用な情報をロギングします。このセクションでは、AMC でのログの構成方法と表示方法の他、外部 syslog サーバーへのメッセージの送信方法などについて説明します。また、AMC で表示されるシステム ステータス情報についても説明します。

中央管理 syslog サーバーが使用できない場合は、アプライアンス自体のコマンドライン インターフェースから標準 UNIX コマンドを使用して、ログ ファイルを参照できます。生ログ データの手動での参照方法や解釈の方法については、ログ ファイルの出力フォーマットを参照してください。

トピック:

- 概要: システム ロギングおよびモニタリング
- ログ ファイル
- アプライアンスの監視
- SNMP の構成

概要: システム ロギングおよびモニタリング

アプライアンスでは、AMC の動作およびアプライアンス上のサービスのデータをロギングします。また、管理者がシステムをどのように使用し変更したかというデータも収集します。システム ログは、収集されたら、すべて syslog 形式で保管されます。ログ メッセージは、更新バージョンの標準 syslog 形式を使用して処理されます。

アプライアンスは最初は、ログ ファイルをローカルに保管するよう構成されています。ログ ファイルを中央管理 syslog サーバーに送信するようアプライアンスを構成すると、システムレベルのイベントをほぼリアルタイムに監視できるようになり、重要なイベントについて通知を受けることができます。また、ログ メッセージ データをカンマ区切り形式 (`.csv`) のファイルにエクスポートすることにより、他のアプリケーションで表示と分析を行うこともできます。

ログ ファイル

アプライアンスは、さまざまなタイプのログ ファイルを生成します。このファイルは AMC の [**Logging (ログ)**] ページで表示およびエクスポートできます。また、WorkPlace に関連するログ ファイルで、AMC で表示できないものが 2 つあります。これらについては WorkPlace ログ で説明しています。

トピック:

- ログの表示
- ログ メッセージのソート、検索、フィルタリング
- ログ ファイルのエクスポート
- ログの設定
- システム メッセージ ログ
- 管理メッセージ ログ
- 管理監査ログ

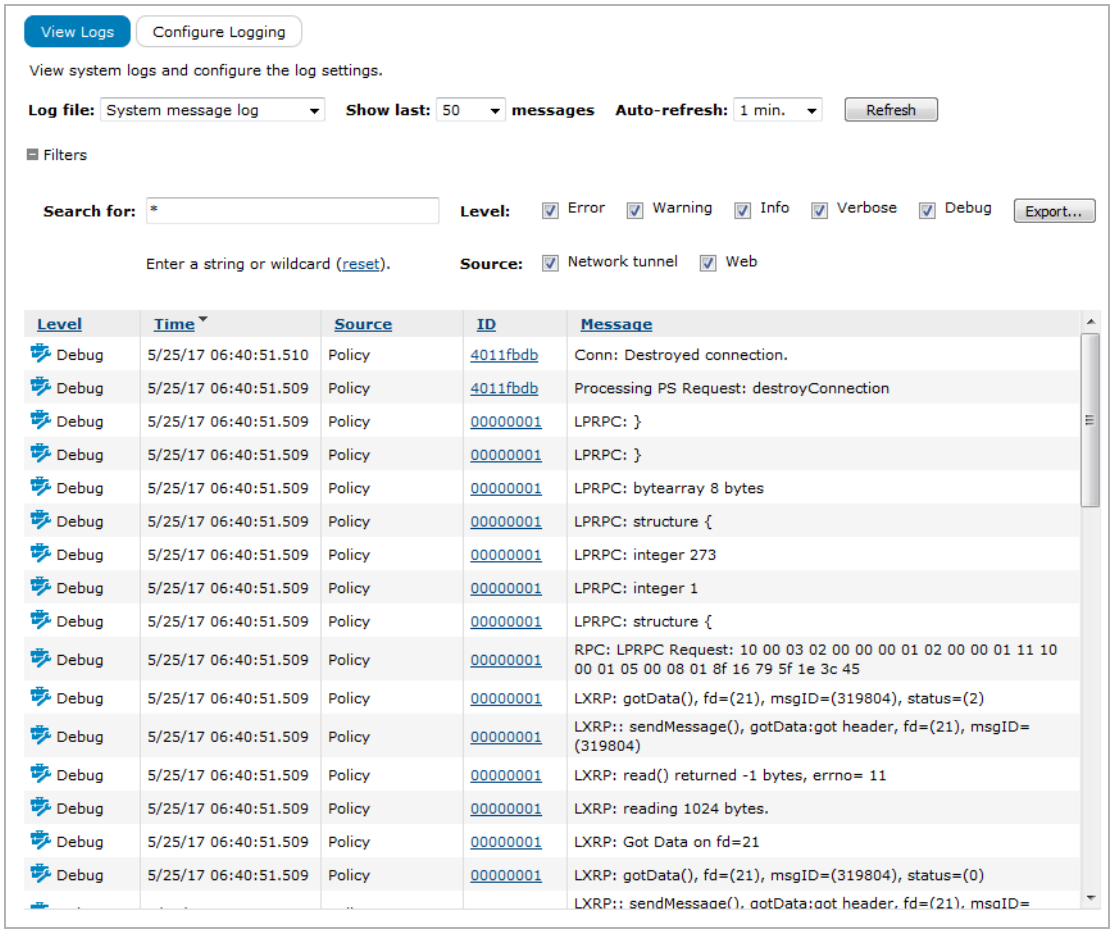
- ネットワーク トンネル監査ログ
- Web プロキシ監査ログ
- クライアント インストール ログ (Windows)

ログの表示

SMA アプライアンスでは、さまざまなログ ファイルが生成されます。AMC では、これらのログ ファイルについて、ソート、検索、フィルタリングできます。

ログを表示するには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。



2 [**Log file (ログ ファイル)**] ドロップダウン メニューから、表示するシステムまたはサービス ログ ファイルを選択します。表示される情報の列は、ログ ファイルの説明 で説明されている通りにそれぞれのログ ファイルの種類ごとに異なります。

ログ ファイルの説明

ログ ファイル	説明
システム メッセージ ログ	ネットワーク トンネル サービス、および Web プロキシ サービスについてのサーバー処理情報および診断情報が表示されます。また、すべてのアクセス制御決定に関する詳細なメッセージも記述されます。つまり、ユーザーの要求がポリシー ルールと合致すると、そのときに実行された動作を示すログ ファイル エントリが記録されます。 詳細については、システム メッセージ ログを参照してください。
管理メッセージ ログ	AMC の動作に関連するエントリが表示されます。コンソールが開始および停止された時間、アプライアンスの管理中にどのようなエラーが発生したかなどが記録されます。 詳細については、管理メッセージ ログを参照してください。
管理監査ログ	AMC で管理者が実施した構成変更の監査履歴が表示されます。いつどの管理者が変更したかが記述されます。 詳細については、管理監査ログを参照してください。
ネットワーク プロキシ/トンネル監査ログ Web プロキシ監査ログ	2 種類のアクセス サービス監査ログがあります。1 つは Web プロキシ サービスを記録したもの (ログ ファイルでは「**ExtraWeb**」と表記される) で、もう 1 つは、ネットワーク プロキシ サービスとネットワーク トンネル サービスの両方のメッセージを組み合わせたもの (ログ ファイルでは「**Anywhere VPN**」と表記される) です。これらの 2 つのログには、ユーザーのリストや転送されたデータの量など、接続動作に関する詳細な情報が記録されます。 詳細については、ネットワーク トンネル監査ログおよび Web プロキシ監査ログを参照してください。
クライアント インストール ログ	Windows が動作するコンピュータへクライアントまたはエージェントをインストールしているときに問題が起こった場合、クライアント インストール ログにエラーが記録されます。これらのログは、アプライアンスに自動的にアップロードされ、ユーザーに Secure Endpoint Manager がインストールされている場合は、AMC に表示されます。 詳細については、クライアント インストール ログ (Windows) を参照してください。
登録されていないデバイスログ	登録されていないデバイスのユーザーからのログイン試行のリストを表示します。これらのデバイスを登録するために使用できる XML 形式にリストをエクスポートすることができます。

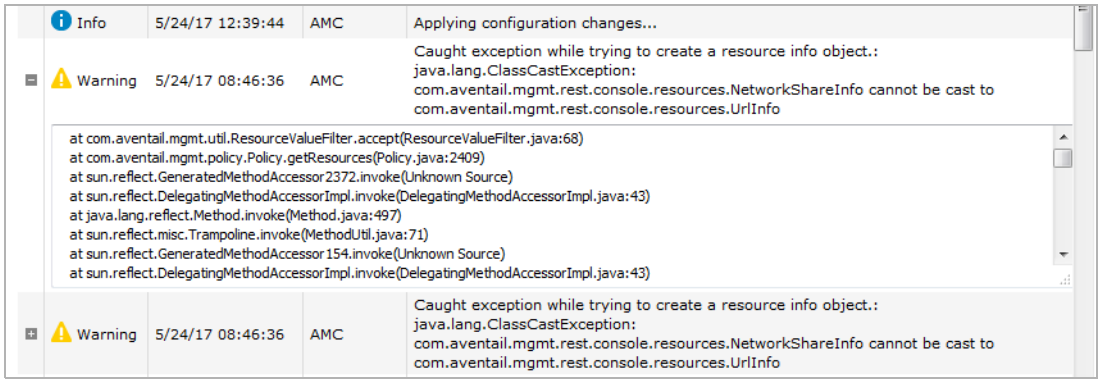
3 [**Show last (最近の次の件数を表示)**] ドロップダウン メニューを使用して、表示するログ メッセージの数を選択します。[**50**] (既定値)、[**100**]、[**250**]、[**500**]、または [**1000**] のいずれかを選択できます。

4 最新のログ メッセージが含まれるようページを更新するときや、実行したばかりのフィルタリングの結果を表示するときは、[**Refresh (再表示)**] をクリックします。

デフォルトの場合、ログ ビューアの [**Auto-refresh (自動更新)**] オプションは [**1 min.**] に設定されています。更新時間は、オプションで [**30 sec.**]、[**5 min.**]、[**10 min.**]、[**15 min.**] のいずれかを選択できます。また、AMC セッションの際に [**Off (オフ)**] を選択することもできます。

5 オプションで [**Search for (検索対象)**]、[**Level (レベル)**]、[**Source (送信元)**]、[**Status (状況)**] などのソート オプションを使用できます。ログ メッセージのソート、検索、フィルタリングを参照してください。

6 ログ エントリが数行以上になる場合は、最初の列にプラス記号 (+) が表示されます。この記号をクリックすると、エントリが展開されます。



メモ：[**Auto-refresh (自動更新)**] が [**Off (オフ)**] 以外に設定されており [**View Logs (ログの表示)**] ページが表示されている場合、更新動作が持続的に行われるため、デフォルトの非アクティブ期間 (**15** 分) が経過しても、AMC セッションが自動的にタイムアウトしなくなります。これは、AMC を実行し、オートリフレッシュ モードを有効にした状態で [**View Logs (ログの表示)**] ページを表示したまま席を外すと、AMC がタイムアウトしなくなることを示しています。セキュリティを向上させるための習慣として、ログ メッセージを表示し終わったら、AMC の他のページに必ず移るようにしておきます。詳細については、アプライアンス セッションを参照してください。

ログ メッセージのソート、検索、フィルタリング

AMC ログ ビューアでは、ソート、検索、フィルタリングなどのオプションを使用して、ログ メッセージ データの表示をカスタマイズできます。これらのオプションは、単独で使用できる他、組み合わせて使用することもできます。

並べ替え

表示されているデータは、ログ テーブルの列の見出しをクリックし、列ごとに昇順または降順にソートできます。デフォルトの場合、ログ メッセージは、[**Time (時間)**] 列でソートされており、最新のメッセージが先頭に表示されるようになっています。

検索

IP アドレスやユーザー ID など、ログ ファイル内のテキスト文字列を検索する場合は、[**Search for (検索対象)**] フィールドに (大文字と小文字を区別して) 検索基準を入力して [**Refresh (再表示)**] をクリックすると、検索結果が表示されます。検索基準では、「*」や「?」などのワイルドカード文字を使用することもできます。検索基準を消去するときは、[**reset (リセット)**] リンクをクリックします。

システム メッセージ ログの場合、[**ID**] 列のセッション ID 番号をクリックすると、同じセッション ID 番号を共有するすべてのログ メッセージが自動的に検索されます。セッション ID の詳細については、システム メッセージ ログに記載されたフィールドについて説明した表を参照してください。

Web プロキシ監査ログおよびネットワーク プロキシ/トンネル監査ログの場合は、[**Username (ユーザ名)**] 列のユーザー ID をクリックすると、特定のユーザーについてのすべてのログ メッセージが自動的に検索されます。

フィルタリング

フィルタリング オプションを使用することで、それぞれのログ ファイルに特定タイプのロギング データを包含または除外できます。例えば、AMC 関連でない管理メッセージ ログ エントリ (システム管理権限メッセージなど) を参照したい場合、すべての [**Level (レベル)**] チェック ボックスを選択して、[**Source (送信元)**] の下にある [**AMC**] チェック ボックスを選択解除します。選択可能なオプションは、参照しているログ ファイルのタイプによって変動します。

ログ ファイルのエクスポート

ログ メッセージ データをさらに分析する必要がある場合、またはデータを異なる方法で表示する必要がある場合は、選択したデータをファイルにエクスポートして、Microsoft Excel などの別のアプリケーション (カンマ区切り形式の値のログの場合) や XML エディタ (未登録のデバイスのログの場合) で使用できます。

最初にフィルタや検索条件を適用することで、エクスポート ファイルのサイズを小さくすることができます。[**Show last <n> messages (最近の <n> 件のメッセージを表示)**] 設定で、エクスポートするログ ファイルに含まれる最大メッセージ数が決定されます。

ログ ファイルをエクスポートするには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Log file (ログ ファイル)**] リストを使用して、表示するシステムまたはサービス ログ ファイルを選択します。

3 ログ データにフィルタリングや検索基準を適用します。ログ メッセージのソート、検索、フィルタリングを参照してください。

4 [**Export (エクスポート)**] を選択します。

5 ファイルを保存またはオープンするよう求められます。[**Save (保存)**] を選択します。

6 [**Save As (名前を付けて保存)**] ダイアログ ボックスで、ファイルを保存するロケーションをブラウズし、オプションで名前を変更して、[**Save (保存)**] をクリックします。既定では、エクスポート ファイルには AMC によって エクスポートされたログのファイル名 で示されたファイル名が割り当てられます。

エクスポートされたログのファイル名

ファイル名	説明
sysmessage.csv	システム メッセージ ログ
management.csv	管理メッセージ ログ
consoleaudit.csv	管理監査ログ
netaudit.csv	ネットワーク プロキシ/トンネル監査ログ
webaudit.csv	Web プロキシ監査ログ
UnregisteredDevices.xml	認識されない機器 ID のデバイスのログ。このログでデバイス ID を収集するために必要な手順については、未登録デバイスからの機器 ID の収集を参照してください。

ログの設定

システムをデバッグしている場合、AMC で、サービスごとにメッセージ ログ レベルを設定できます。また、ログ ファイルを外部 syslog サーバーに送信するよう、アプライアンスを構成することもできます。

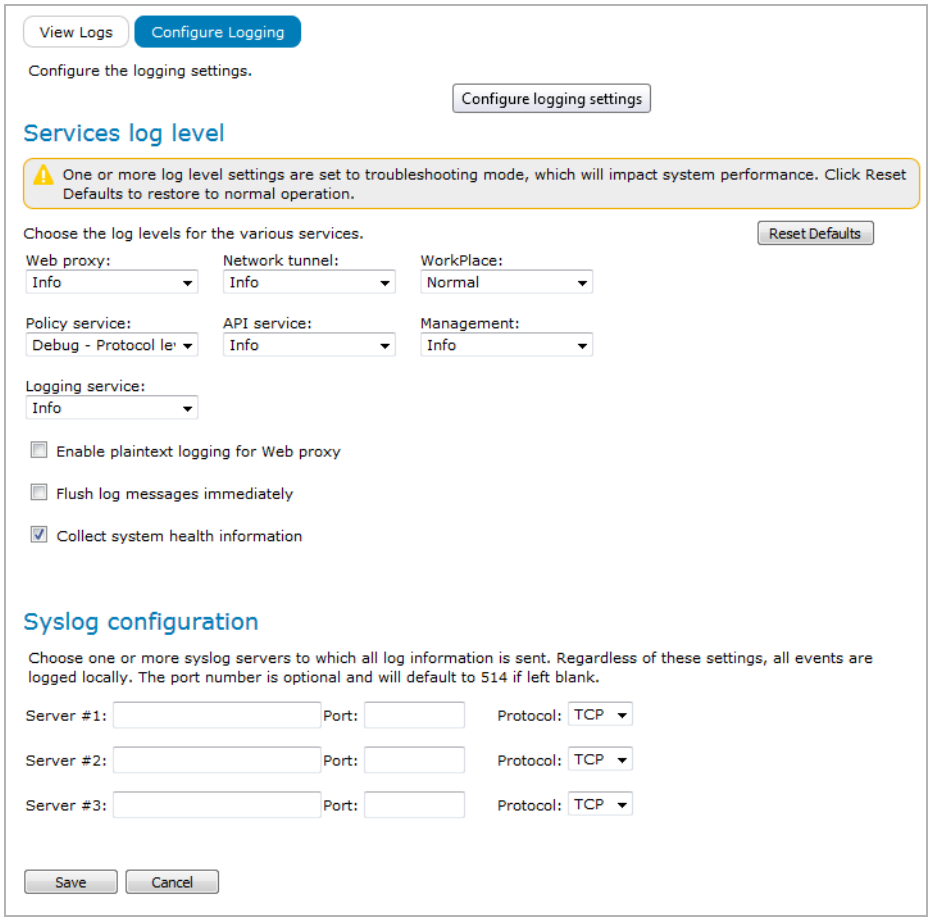
ログ レベルの設定

各サービスでメッセージ ログの詳細レベルを指定できます。メッセージ ログの詳細レベルを上げると、必要なディスク容量が増加し、システムのパフォーマンスにも大きく影響します。

ログ レベルを設定するには、次の操作を行います。

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Configure Logging (ログの設定)**] タブをクリックします。



3 アプライアンスでサービスの適切なメッセージ詳細レベルを選択します。詳細レベルが高い順に表示されます。最も詳細なログ レベル ([**Verbose (詳細)**] および [**Debug (デバッグ)**]) は、トラブルシューティングの目的に利用できますが、必要なディスク容量が増加し、システムのパフォーマンスにも大きく影響する場合があります。通常は使用しないでください。

4 アプライアンスを構成して、システム ログを 1 台または複数の syslog サーバーに送信できます。[**Syslog configuration (Syslog 設定)**] エリアで syslog サーバーの IP アドレスとポート番号を入力します。ポート **514** が標準の syslog-ng ポートですが、必要に応じて、サーバー構成に一致する別

のポートを使用できます。syslog を構成するかどうかに関わらず、すべてのシステム イベントはローカルでロギングされます。

5 変更をすべて破棄するには、[**Cancel (キャンセル)**] をクリックします。変更を保存するには [**Save (保存)**] をクリックします。

syslog サーバーへのログ ファイルの送信

SMA アプライアンスでは、システム ログを syslog サーバーに送信できます。syslog を構成するかどうかに関わらず、すべてのシステム イベントはローカルでロギングされます。ネットワークにログ情報が氾濫する状況を避けるため、上位 3 段階の重大度レベル ([Fatal]、[Error]、[Warning]) のログ メッセージのみが転送されます。

syslog プロトコルの詳細については、RFC 3164 (http://www.ietf.org/rfc/rfc3164.txt) を参照してください。

syslog サーバーへログ ファイルを送信するには、

1 メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Configure Logging (ログの設定)**] タブをクリックします。

3 [**Syslog configuration (Syslog 設定)**] で、1 つまたは複数の syslog サーバーに対する IP アドレスとポート 番号を入力します。デフォルトの syslog-ng ポートは、**514** ですが、サーバー構成に合わせて他のポートを使用することもできます。アプライアンスが syslog と通信するとき、TCP プロトコルと UDP プロトコルのどちらを使用するか指定するときは、[**Protocol (プロトコル)**] リストを使用し ます。

4 変更をすべて破棄するには、[**Cancel (キャンセル)**] をクリックします。変更を保存するには [**Save (保存)**] をクリックします。

メモ：syslog データは暗号化されないため、ログ メッセージを外部サーバーに送信する場合、セキュリティ上の問題が存在することになります。

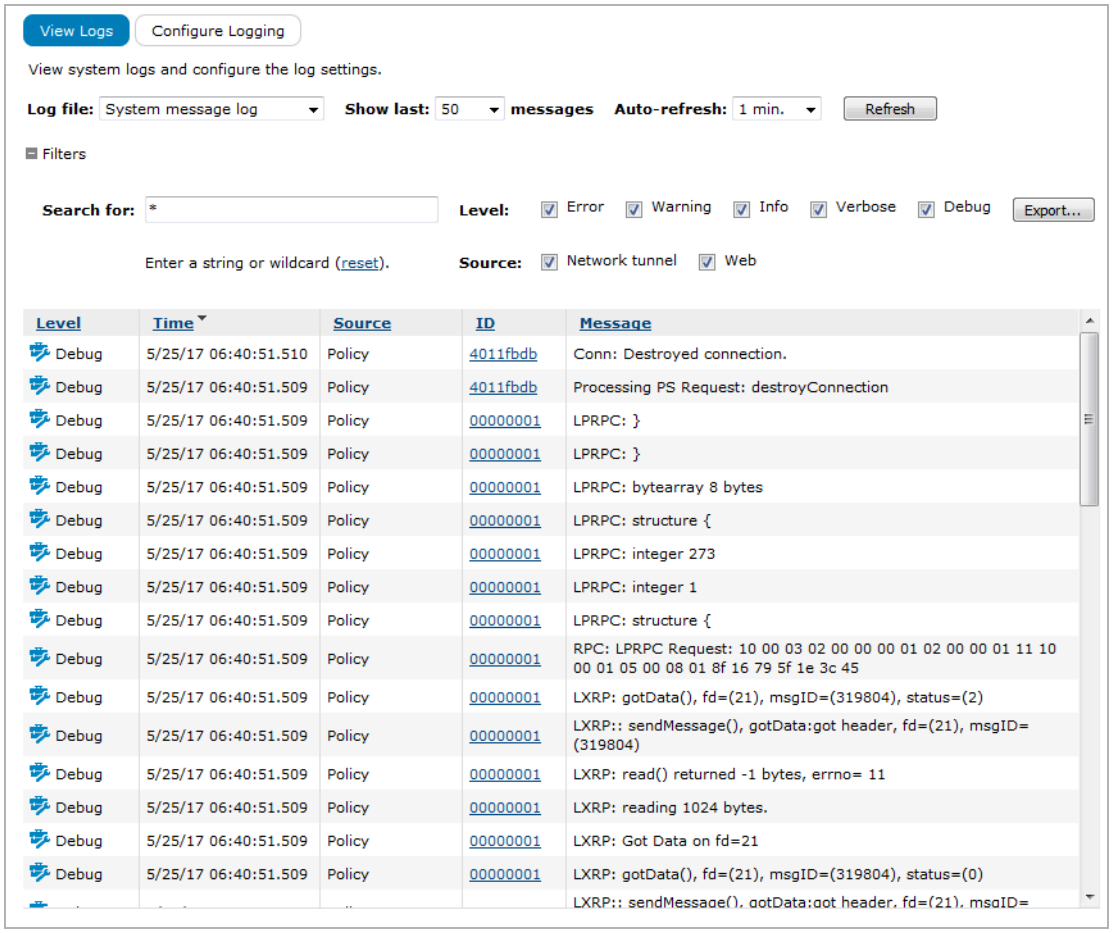
システム メッセージ ログ

システム メッセージ ログには、Web プロキシ サービス、ネットワーク プロキシ サービス、ネットワーク トンネル サービスについてのサーバー処理情報および診断情報が記録されます。また、すべてのアクセス制御決定に関する詳細なメッセージも記述されます。つまり、ユーザーの要求がポリシー ルールと合致すると、そのときに実行された動作を示すログ ファイル エントリが記録されます。

システム メッセージ ログを表示するには:

1 メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Log File (ログファイル)**] ドロップダウン メニューから [**System message log (システム メッセージ ログ)**] を選択します。



[**View Logs (ログを表示)**] ページには、システム メッセージ ログ ファイルに含まれる、システム メッセージ ログ ファイル情報に示された情報が表示されます。

システム メッセージ ログ ファイル情報

列	説明
レベル	ログ メッセージの詳細レベル: [**Fatal (致命的)**]、[**Error (エラー)**]、[**Warning (警告)**]、[**Info (情報)**]、[**Debug (デバッグ)**]、または [**Verbose (詳細)**]。
時間	サービスによってメッセージが生成された日付と時刻が表示されます。
送信元	メッセージを生成したサービスを示します。[**Network proxy (ネットワーク プロキシ)**]、[**Network tunnel (ネットワーク トンネル)**]、[**Web proxy** (ウェブ プロキシ)]、または [**Policy** (ポリシー)] の各サーバー。
ID	各ユーザー セッションに割り当てられた固有の ID 番号が表示されます。セッション ID 番号をクリックすると、それに対応するすべてのログ メッセージが自動的に検索されます。セッション ID 番号の詳細については、システム メッセージ ログを参照してください。
メッセージ	メッセージ テキストが表示されます。

メモ：アプライアンスのコマンドライン インターフェースから手動でログ ファイルを表示する方法については、システム メッセージ ログを参照してください。

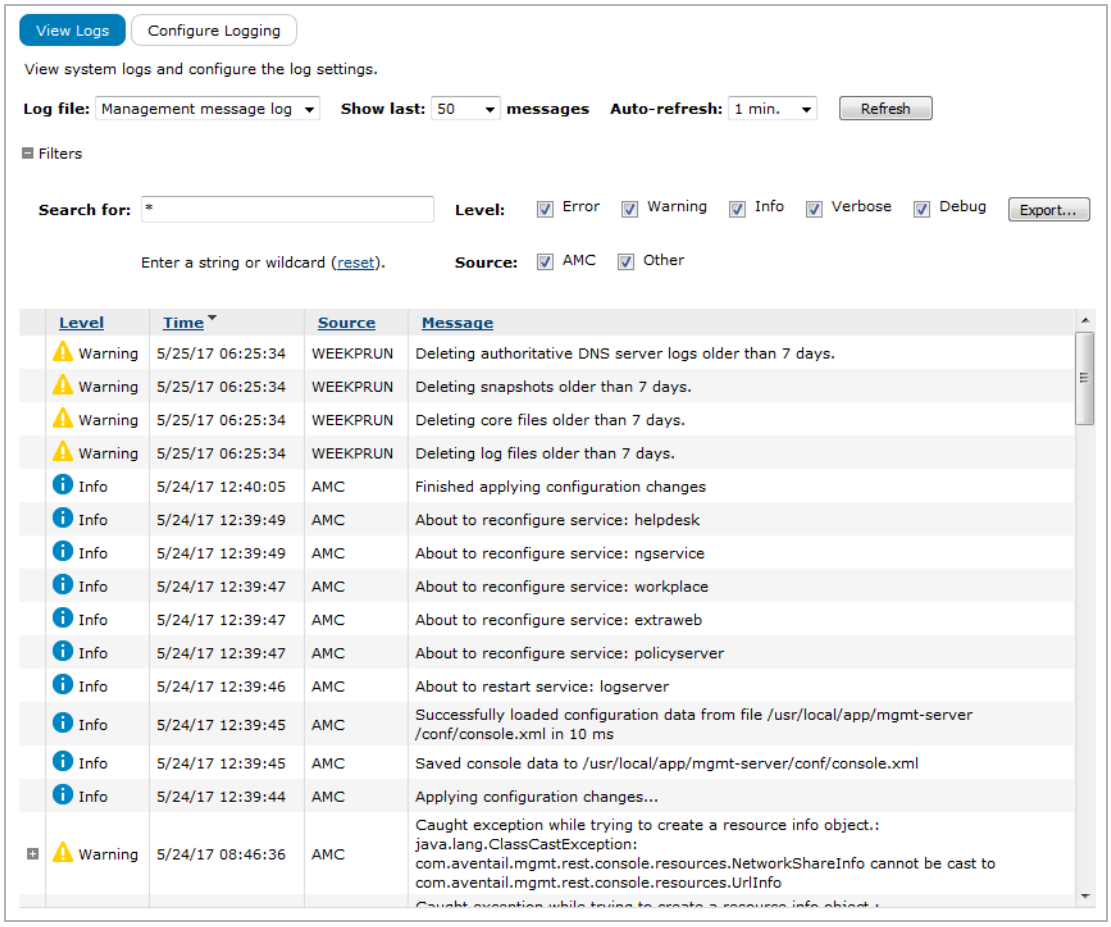
管理メッセージ ログ

管理メッセージ ログには、AMC の動作に関連するエントリが記録されます。コンソールが開始および停止された時間、アプライアンスの管理中にどのようなエラーが発生したかなどが記録されます。

管理メッセージ ログを表示するには:

1 メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Log File (ログファイル)**] ドロップダウン メニューから [**Management message log (管理メッセージ ログ)**] を選択します。



[**View Logs (ログを表示)**] ページには、管理メッセージ ログに関する管理メッセージ ログ情報に示された情報が表示されます。

管理メッセージ ログ情報

列	説明
レベル	ログ メッセージの詳細レベル: [**Error (エラー)**]、[**Warning (警告)**]、[**Info (情報)**]、[**Verbose (詳細)**]、または [**Debug (デバッグ)**]。
時間	ログされた日付と時刻が表示されます。
送信元	変更のソースを示します: [**AMC**] または [**Other (その他)**] が表示されます。*WEEKPRUN* および *sysctrl* が含まれます。
メッセージ	ログ エントリが詳細に記述されます。

管理監査ログ

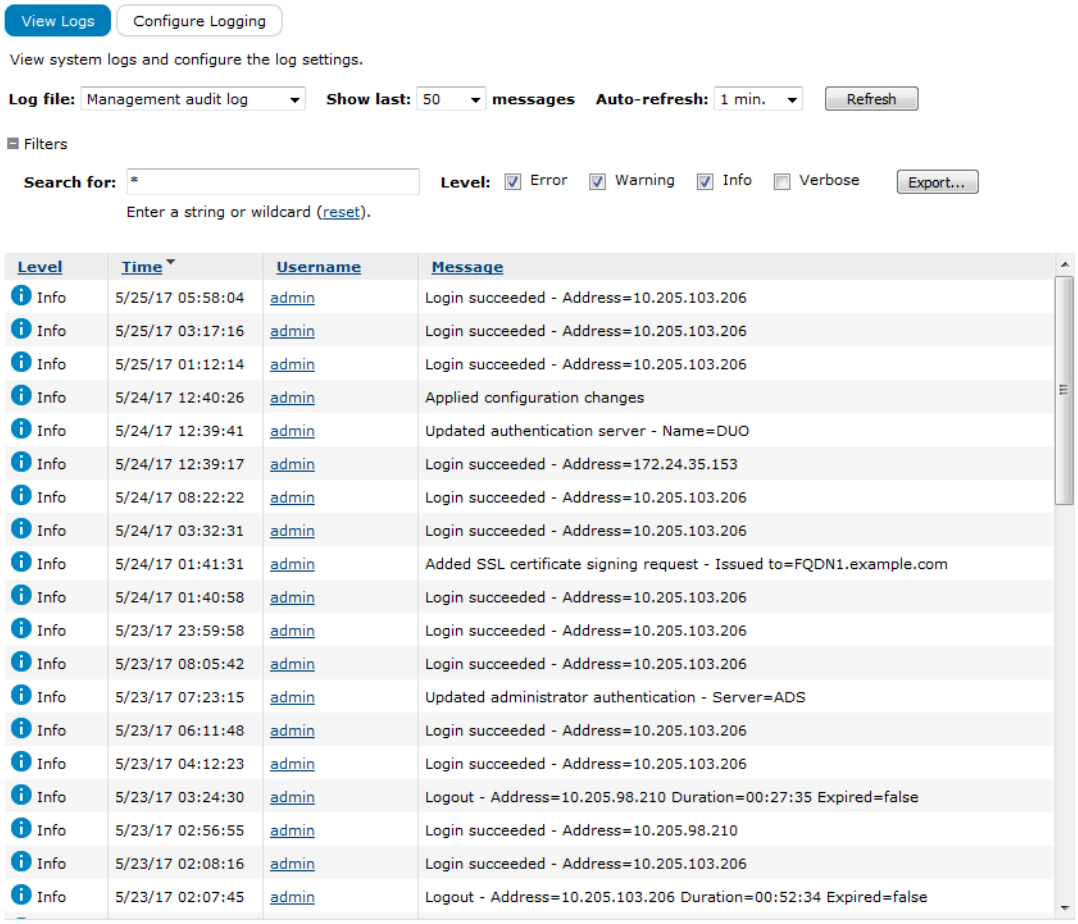
管理監査ログには、AMC で管理者が実施した構成変更の監査履歴が記録されます。いつどの管理者が変更したかが記述されます。構成変更は、アクティブと保留中のいずれかになります。

- **アクティブな構成:** `Applied configuration changes`（構成変更が適用されました）というログ メッセージの前にある構成項目は、適用済みで現在アクティブになっているものです。
- **保留中の変更:** 変更が行われると、ディスクに保存されますが、すぐには適用されません。管理監査ログでは、`Applied configuration changes`（構成変更が適用されました）メッセージの後にあるこのような保留中の変更は、破棄できます。破棄する方法については、保留中の構成変更の破棄を参照してください。

管理監査ログを表示するには:

1 メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Log File (ログファイル)**] ドロップダウン メニューから [**Management audit log (管理監査ログ)**] を選択します。



Level	Time	Username	Message
Info	5/25/17 05:58:04	admin	Login succeeded - Address=10.205.103.206
Info	5/25/17 03:17:16	admin	Login succeeded - Address=10.205.103.206
Info	5/25/17 01:12:14	admin	Login succeeded - Address=10.205.103.206
Info	5/24/17 12:40:26	admin	Applied configuration changes
Info	5/24/17 12:39:41	admin	Updated authentication server - Name=DUO
Info	5/24/17 12:39:17	admin	Login succeeded - Address=172.24.35.153
Info	5/24/17 08:22:22	admin	Login succeeded - Address=10.205.103.206
Info	5/24/17 03:32:31	admin	Login succeeded - Address=10.205.103.206
Info	5/24/17 01:41:31	admin	Added SSL certificate signing request - Issued to=FQDN1.example.com
Info	5/24/17 01:40:58	admin	Login succeeded - Address=10.205.103.206
Info	5/23/17 23:59:58	admin	Login succeeded - Address=10.205.103.206
Info	5/23/17 08:05:42	admin	Login succeeded - Address=10.205.103.206
Info	5/23/17 07:23:15	admin	Updated administrator authentication - Server=ADS
Info	5/23/17 06:11:48	admin	Login succeeded - Address=10.205.103.206
Info	5/23/17 04:12:23	admin	Login succeeded - Address=10.205.103.206
Info	5/23/17 03:24:30	admin	Logout - Address=10.205.98.210 Duration=00:27:35 Expired=false
Info	5/23/17 02:56:55	admin	Login succeeded - Address=10.205.98.210
Info	5/23/17 02:08:16	admin	Login succeeded - Address=10.205.103.206
Info	5/23/17 02:07:45	admin	Logout - Address=10.205.103.206 Duration=00:52:34 Expired=false

[**View Logs (ログを表示)**] ページには、管理監査ログに関する管理監査ログ情報に示された情報が表示されます。

管理監査ログ情報

列	説明
レベル	ログ メッセージの詳細レベル: [**Fatal, Error (致命的、エラー)**]、[**Warning (警告)**]、または [**Info (情報)**]。
時間	AMC 構成変更の日付と時刻が表示されます。
ユーザ名	[**Manage Administrator Accounts (管理者アカウントを管理)**] ページで構成されている管理者の名前が表示されます。
メッセージ	AMC で行われた構成変更が表示されます。

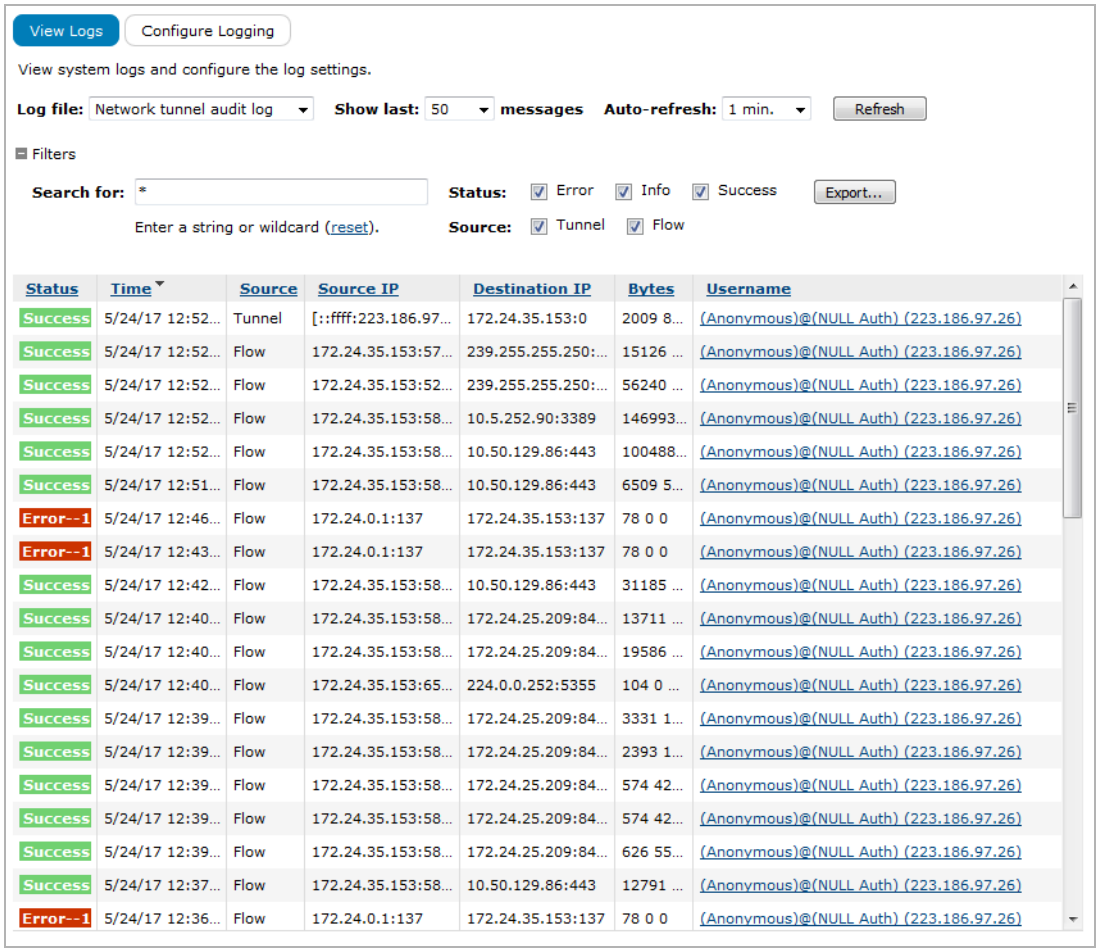
メモ：アプライアンスのコマンドライン インターフェースから手動でログ ファイルを表示する方法については、管理コンソールの監査ログを参照してください。

ネットワーク トンネル監査ログ

ネットワーク プロキシ/トンネル監査ログには、ユーザーのリストや転送されたデータの量など、Connect Tunnel や OnDemand Tunnel を使用してリソースにアクセスしているユーザーの接続活動に関する詳細な情報が記録されます。

ネットワーク トンネル監査ログを表示するには:

1. メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。
2. [**Log File (ログファイル)**] ドロップダウン メニューから [**Network tunnel audit log (ネットワーク トンネル監査ログ)**] を選択します。



[View Logs (ログを表示)] ページには、ネットワーク プロキシ / トンネル監査ログに関する ネットワーク プロキシ/トンネル監査ログ情報 に示された情報が表示されます。

ネットワーク プロキシ/トンネル監査ログ情報

列	説明
状況	それぞれの接続要求に対するステータスが色分けされて表示されます。 • 赤: エラー • オレンジ : 情報 • 緑: 成功 ポインタを特定のログ メッセージの接続ステータス コードの上に置くと、メッセージの下に説明テキストが表示されます。
時間	接続の日付と時刻が表示されます。
送信元	メッセージを生成したサービスを示します。[Network proxy (ネットワーク プロキシ)]、[Network Tunnel (ネットワーク トンネル)]、[Web proxy (ウェブ プロキシ)]、または [Policy (ポリシー)] の各サーバー。
送信元 IP	ネットワーク プロキシまたはトンネル サービスを使用するコンピュータの IP アドレスとポート番号が表示されます。
送信先 IP	アクセスされるリソースの IP アドレスとポート番号が表示されます。

ネットワーク プロキシ/トンネル監査ログ情報

列	説明
バイト	次の 3 つの値のセットが表示されます。 • 送信されたバイト数 • 受信されたバイト数 • 接続期間 (秒単位)
ユーザ名	リソースを要求したユーザーが表示されます。[Username] リンクをクリックすると、特定のユーザーに対するすべてのログ メッセージを検索できます。

メモ：アプライアンスのコマンドライン インターフェースから手動でログ ファイルを表示する方法については、ネットワーク トンネル監査ログを参照してください。

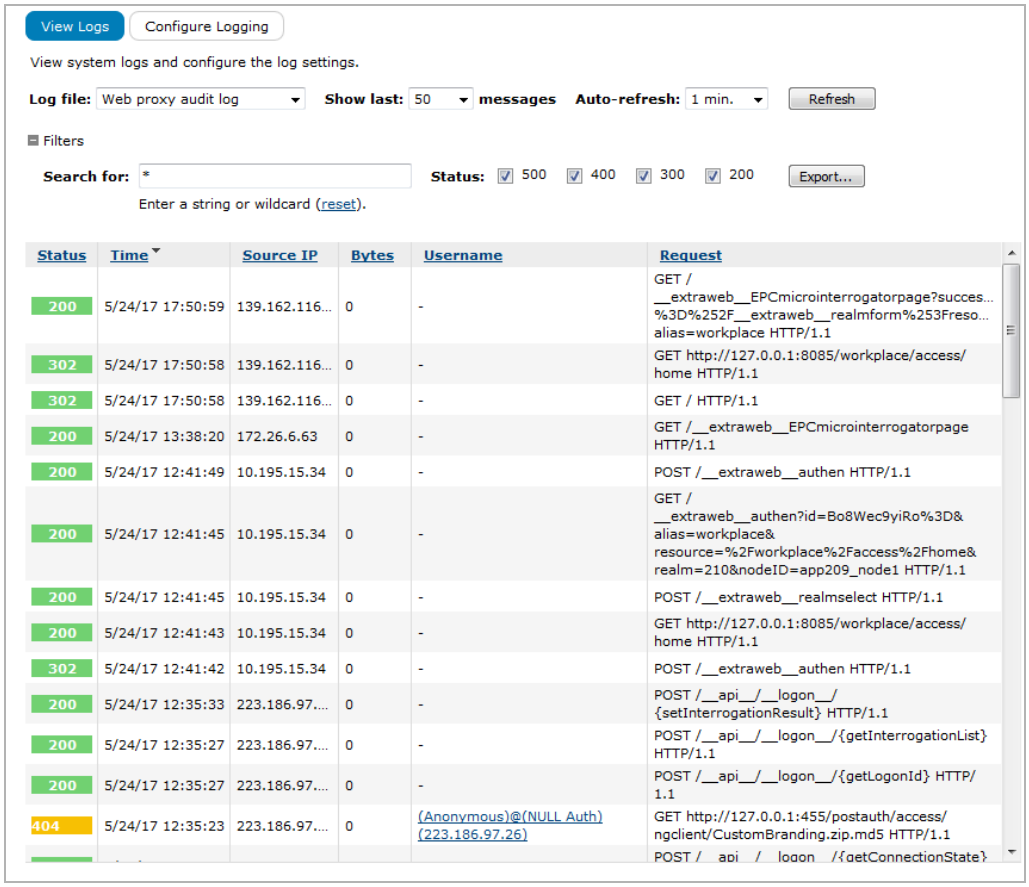
Web プロキシ監査ログ

Web プロキシ/ トンネル監査ログには、ユーザーのリストや転送されたデータの量など、Web Proxy Access や Translated Access を使用してリソースにアクセスしているユーザーの接続活動に関する詳細な情報が記録されます。

ウェブ プロキシ監査ログを表示するには:

1 メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Log File (ログファイル)**] ドロップダウン メニューから [**Web proxy audit log (ウェブ プロキシ監査ログ)**] を選択します。



[**View Logs (ログを表示)**] ページには、Web プロキシ監査ログに関する Web プロキシ監査ログ情報 に示された情報が表示されます。

Web プロキシ監査ログ情報

列	説明
状況	それぞれの HTTP 要求に対する戻りコードが色分けされて表示されます。ポインタを HTTP 戻りコード番号の上に置くと、説明テキストが表示されます。コード番号は、次のような範囲および色になっています。 • 500: サーバー エラー (赤) • 400: クライアント エラー (オレンジ) • 300: リダイレクション (緑) • 200: 成功 (緑)
時間	アプライアンスで要求を受け取った日付および時刻。
送信元 IP	Web プロキシ サービスを使用したコンピュータの IP アドレスとポート番号が表示されます。
バイト	応答の本文で送信されたバイト数が表示されます。ただし HTTP ヘッダは除外されます。
ユーザ名	Web プロキシ サービスで認証されているユーザーの名前が表示されます。[Username] リンクをクリックすると、特定のユーザーに関連するすべてのログ メッセージを検索できます。
要求	HTTP 要求の 1 行目が表示されます。これには HTTP コマンド (GET や POST など)、要求されたリソース、HTTP バージョン番号などが含まれます。

メモ：アプライアンスのコマンドライン インターフェースから手動でログ ファイルを表示する方法については、Web プロキシ監査ログを参照してください。

クライアント インストール ログ (Windows)

ユーザーがレルムにログインするとき、利用できるアクセス方式は、次のような条件によって変動します。

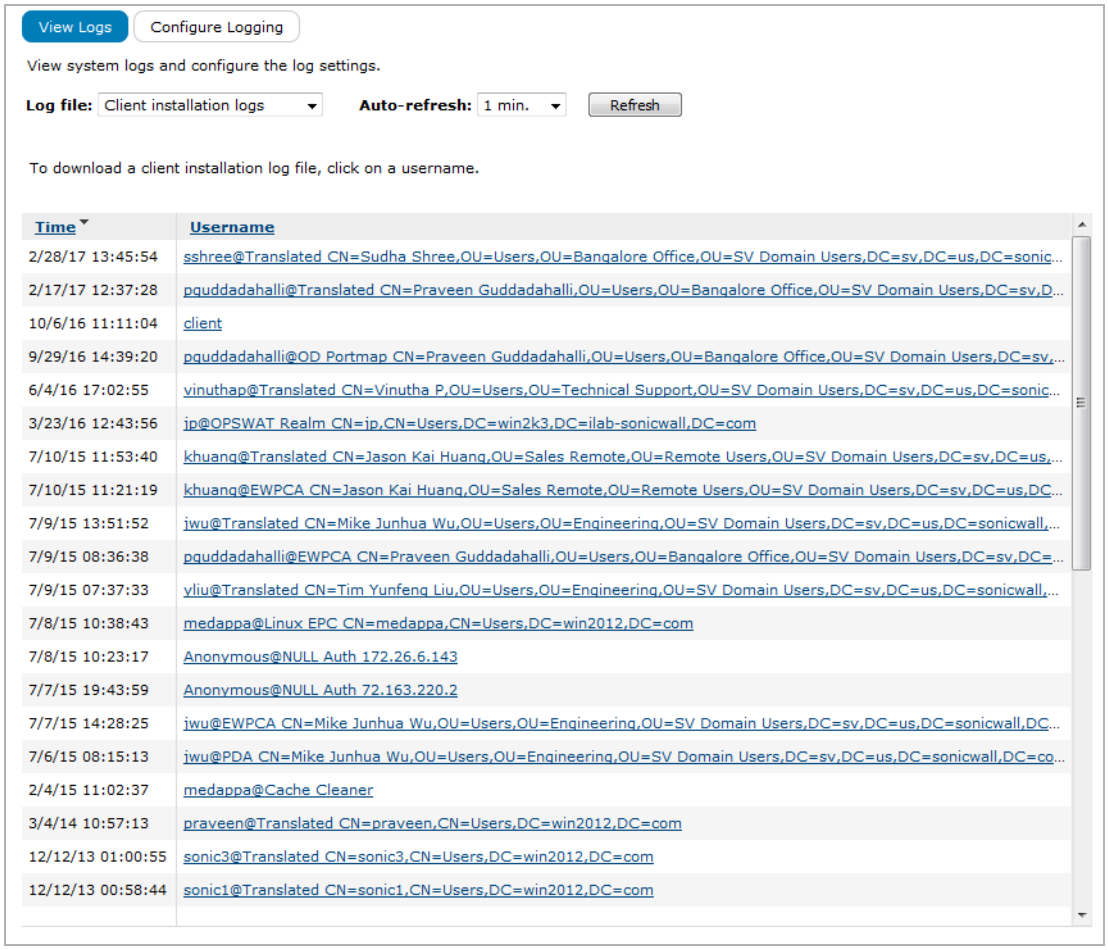
- 特定のコミュニティで許可されているネットワーク アクセス エージェントまたはクライアント (レルムを設定するときに指定するもの)
- ユーザーの環境 : オペレーティング システム、ブラウザ、ActiveX や Java が利用できるかどうか、クライアントやエージェントがすでに存在するかどうか

Windows が動作するコンピュータへクライアントまたはエージェントをインストールしているときに問題が起こった場合、クライアント インストール ログにエラーが記録されます。これらのログは、アプライアンスに自動的にアップロードされ、ユーザーに Secure Endpoint Manager がインストールされている場合は、AMC に表示されます。Secure Endpoint Manager の詳細については、クライアントおよびエージェント プロビジョニング (Windows) を参照してください。

すべてのユーザーのクライアント ログの一覧を表示するには:

1 メイン ナビゲーション メニューから、[**Logging (ログ)**] をクリックします。[**View Log (ログの表示)**] ページが表示されます。

2 [**Log File (ログファイル)**] ドロップダウン メニューから [**Client installation logs (クライアント インストール ログ)**] を選択します。



クライアント インストール ログは、時刻またはユーザー名でソートできます。ログ ファイルをダウンロードするときは、そのファイルをクリックします。ログには、プロビジョニング プロセスにおけるそれぞれの手順に関する情報が追加されます (ブートストラッピング、新しいコンポーネントのプロビジョニング、(デバイス プロファイルの一致を調べるための) デバイスのインタロゲーション)。最後の情報は、多くの場合、インストールで問題が発生した場所を示します。

トラブルシューティングのとき、まず AMC でユーザーのクライアント インストール ログを確認して、(必要であれば) ログ ファイル、`epiBootstrapper.log` をチェックします。このファイルは、ユーザーのローカル マシンの「`\Documents and Settings\<username>\Application Data\SMA1000\LogFiles`」フォルダに保管されています。

アプライアンスの監視

AMC では、基本システム設定、ディスクおよびメモリ使用量、現在の接続、ネットワーク帯域幅利用などを監視する上で役に立つさまざまな情報が表示されます。

このセクションでは、システム ステータスとアクティブ ユーザーを監視する方法や、選択したユーザーの VPN 接続を停止する方法について説明します。

トピック:

- 全体の活動の監視
- 監視システム状況

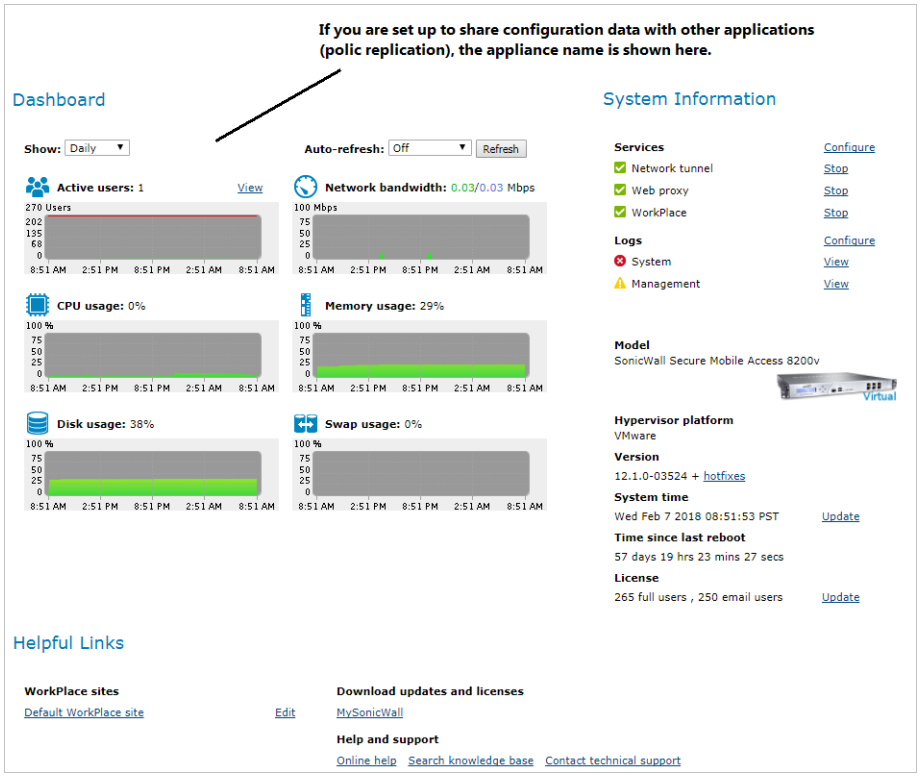
- ユーザー セッションの表示
- オープン セッションとライセンスを消費するセッションの違い
- ユーザー セッションの終了
- ユーザー アクセスとポリシー詳細の表示
- ユーザー セッション データのエクスポート

全体の活動の監視

AMC のホーム ページ (別名、ダッシュボード) では、システム ステータスを監視する上で役に立つさまざまな情報がグラフィカルに表示されます。このグラフは、選択した期間における平均利用度を示し、オプションで、自動リフレッシュで選択した間隔で更新できます。

メモ：警告は、選択された時間間隔を基準に表示されます。時間の間隔を変更して、表示される警告数を増加または減少させます。

AMC のホーム ページ

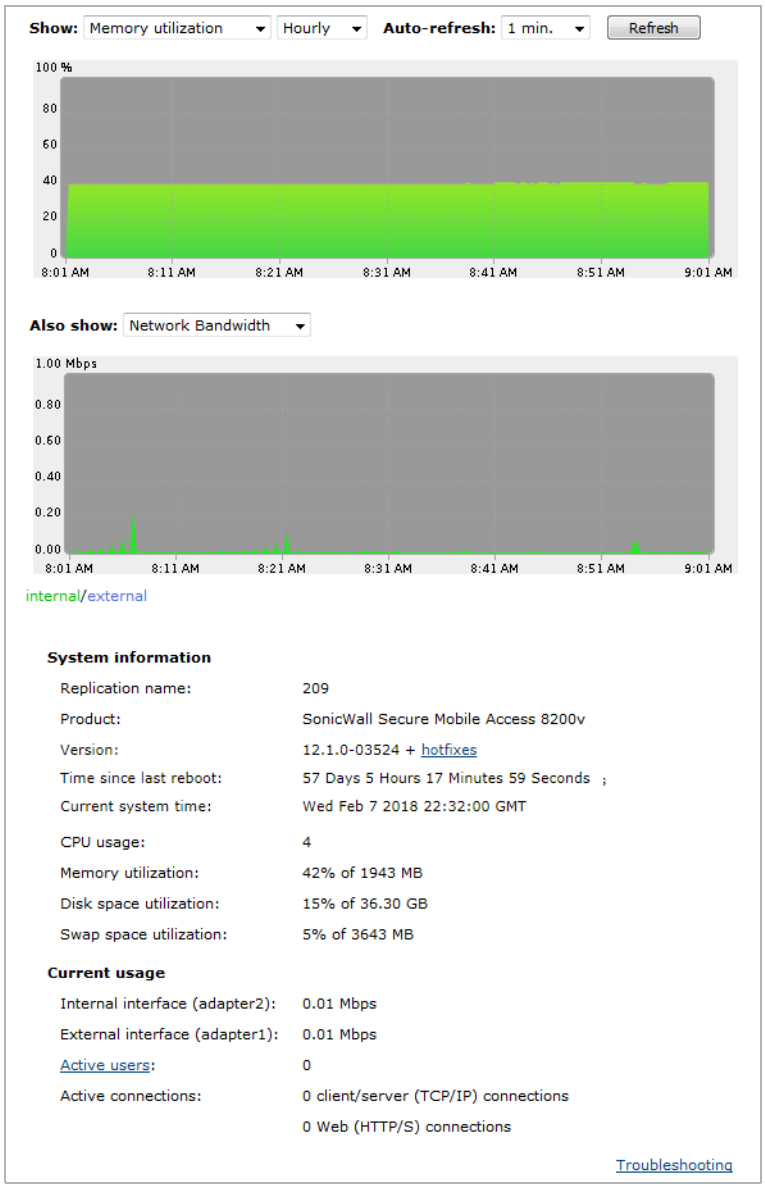


AMC ページの右上にある [**Home (ホーム)**] ページをクリックして、AMC ホーム ページを表示します。システム ステータス グラフの他にも、このページから簡単に次の情報や機能にアクセスできます。

- サービスの開始や停止、ログの表示などの、頻繁に使用される機能。
- ハードウェアおよびライセンス情報。
- デフォルトの WorkPlace、MySonicWall.com、オンライン ヘルプ、サポート オプションへのリンク。

監視システム状況

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**System Status (システム状況)**] をクリックします。メモリの利用率などのアプライアンスの現在のステータスを表示する [**System Status (システム状況)**] ページが表示されます



2 [**Show (表示)**] ドロップダウン メニューで、表示するデータのタイプを指定します。システム状況データ を参照してください。

システム状況データ

データのタイプ	説明
アクティブなユーザー (既定)	指定された時間間隔におけるアクティブ ユーザー セッションの数を表示します。表示されるグラフでは、水平軸が、ライセンスで許可されている同時ユーザーの最大数を示します。 **メモ：**「アクティブ」 ユーザー セッションの数は、ライセンスを消費するユーザー数と同じではありません。詳細は、オープン セッションとライセンスを消費するセッションの違いを参照してください。
CPU 利用	指定された時間間隔における CPU 利用率を表示します。
メモリ使用率	指定された時間間隔におけるメモリ利用率を表示します。この利用率は、アプライアンスの `meminfo` ユーティリティで返された情報から計算されます。 `((MemTotal - Cached - MemFree) / MemTotal) * 100`
ネットワーク帯域幅	指定された時間間隔におけるネットワーク帯域幅を Mbps 単位で表示します。内部インターフェースと外部インターフェースの両方が有効な場合、グラフでは、内部インターフェースのデータが緑の線、外部インターフェースのデータが青の線で表されます。このグラフのスケールは、トラフィックの量に応じて自動的に調整されます (例えば、トラフィック量に応じて 1Mbps または 100Mbps のスケールが使用されます)。
スワップ利用	指定された時間間隔における空きスワップ容量を表示します。
ディスク容量の使用率	指定された時間間隔における使用されたディスク容量の割合を表示します。

3 2 番目の [**Show (表示)**] ドロップダウン メニューで、表示する時間間隔を指定します。時間間隔の選択 を参照してください。

時間間隔の選択

間隔	説明
1 時間ごと	20 秒ごとに収集されたサンプルに基づく最新 1 時間分の平均活動を表示します。
1 日単位	10 分ごとに収集されたサンプルに基づく最新 1 日分の平均活動を表示します。
1 週間ごと	60 分ごとに収集されたサンプルに基づく最新 1 週間分の平均アクティビティを表示します。
1 か月単位	4 時間ごとに収集されたサンプル (1 日に 6 サンプル) に基づく最新 32 日分の平均アクティビティを表示します。

4 [**Auto-refresh (自動更新)**] ドロップダウン メニューでは、AMC が選択しているデータの表示を自動的に更新される頻度を選択します。

5 オプションとして、[**Also show (次も表示)**] ドロップダウン メニューで他のタイプのデータ グラフを選択できます。これは、一定の時間間隔に対する 2 種類のデータを比較する場合に使用すると便利です。既定は「**なし**」です。

6 [**Refresh (再表示)**] をクリックすると、ページをいつでも更新できます。

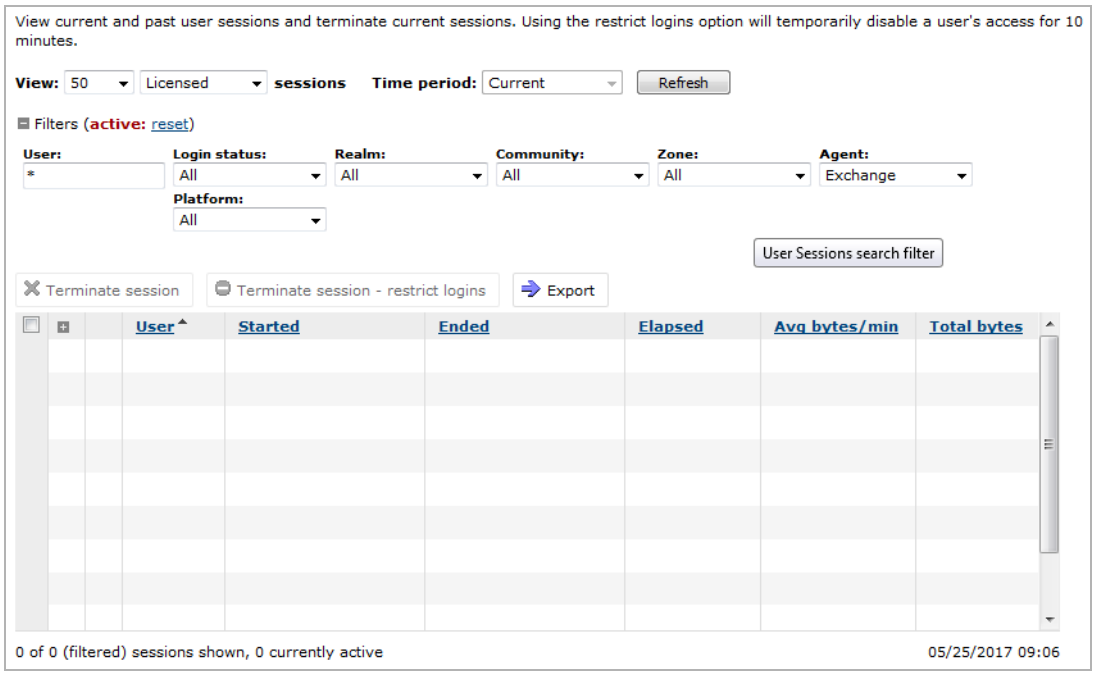
メモ：[**Auto-refresh (自動更新)**] が [**Off (オフ)**] 以外に設定されており [**System Status (システム状況)**] ページが表示されている場合、更新動作が持続的に行われるため、デフォルトの非アクティブ期間 (15 分) が経過しても、AMC セッションが自動的にタイムアウトしなくなります。これは、AMC を実行し、オートリフレッシュ モードを有効にした状態でこのページを表示したまま席を外すと、AMC がタイムアウトしなくなるということを表しています。セキュリティを向上させるための習慣として、ステータスを表示し終わったら、AMC の他のページに必ず移るようにしておきます。詳細については、アプライアンス セッションを参照してください。

ユーザー セッションの表示

AMC で、アプライアンスまたはアプライアンスの HA ペアのユーザー セッションを監視、トラブルシューティング、または終了できます。リストでソートしたり、ユーザー名、レルム (認証サーバー)、コミュニティ、アクセス エージェント、トラフィック ロードなどでセッションをフィルタリングして、絞り検索を行い、特定のセッションを検索して、それらのセッションの詳細を表示できます。2 つのフィルタリングの例をここに示します。

すべてのオープン ユーザー セッションを表示するには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**User Sessions (ユーザ セッション)**] をクリックします。



アイコンからセッションの状態を素早く確認できます。各状態の詳細な説明については、オープン セッションとライセンスを消費するセッションの違いを参照してください。

2 [**View (表示)**] リストで、[**All open (すべてのオープン)**] セッションを選択します。これにより、ライセンスを消費するまたは待機状態にあるセッションが表示されます。待機状態のセッションは、再開できます。接続が 15 分間以上利用されていないと、そのライセンスは解放されます。しかし、15 分が経過するまでは、セッションを再開できます。どのようなセッションが「オープン」と見なされるかの詳細については、オープン セッションとライセンスを消費するセッションの違いを参照してください。

3 セッション リストは、レルムやゾーンなどの他のプロパティを組み合わせて使用してさらにフィルタリングできます。[**Refresh (再表示)**] をクリックして、フィルタを基準としてセッション リストを更新します。

4 セッション リストを確認します。リストを再度ソートするには、列の上にある見出しをクリックします。

5 特定のセッションの概要を素早く確認するには、セッション リストにある項目を展開します。

ユーザーがアクセスしようとしたリソースや、プロセスで適用されていたポリシー ルールなどのセッションの完全な詳細情報については、[ユーザ名] リンクをクリックします。このトラブルシューティング ツールの詳細については、ユーザー アクセスとポリシー詳細の表示を参照してください。

トラフィックの負荷が高いセッションを検索するには、

1 メイン ナビゲーション メニューから、[**User Sessions (ユーザ セッション)**] をクリックします。

2 [**View (表示)**] リストで、[**All (すべて)**] セッションを選択します。

3 帯域幅を非常に多く利用しているセッションを終了することを計画している場合、ライセンスを消費するセッションだけがリストに表示されるように制限します。[**Filters (フィルタ)**] エリアで、[**Status (状況)**] リストから [**Licensed (購読済)**] を選択し、[**Refresh (再表示)**] をクリックします。

4 特定の期間を指定するには、[**Time period (期間)**] ドロップダウン メニューで期間を選択します。選択:

- [**All (すべて)**] では、1 週間までのセッションからのデータが表示されます。
- [**Last 24 hours (最新 24 時間)**] を選択すると、前日のユーザー アクティビティを表示できます。
- [**Custom (個別)**] を選択して、日付と時間の特定の範囲を指定します。

5 [**Refresh (再表示)**] をクリックして、更新された結果を表示します。

6 どのセッションに最も多くのトラフィックがあるか確認するには、列の上部にある [**Avg data (平均データ)**] (この 1 時間におけるトラフィックの総量) をクリックするか、[**Total data (合計データ)**] (セッションにおけるトラフィックの総量) をクリックして、リストをソートします。

オープン セッションとライセンスを消費するセッションの違い

AMC でユーザー セッションを見るときには、セッションの各タイプの違いを把握しておくことが重要です。例えば、あるユーザーにリソースへのアクセスについての疑念がある場合、ライセンスされているセッションだけではなく、そのユーザーに関連するすべてのセッション (失敗したセッションを含め) を表示したい場合があります。セッションタイプは次のように定義されます。

- ライセンスを消費するセッション
- すべてのオープン セッション
- 認証条件が受け入れられない
- すべてのセッション

ライセンスを消費するセッション

ライセンスを消費するセッションは、ユーザーではなく、ユーザー認証が単位となります。例えば、2 台のデバイスにログインしているユーザーは、アプライアンスによって保護されているリソースにアクセスするとすぐに、2 つのライセンスを消費します。

ユーザーがセッションから明示的にログアウトする、あるいは、セッションがタイムアウトするまで (操作がない状態が 15 分経過するまで)、ライセンスは消費されます (例えば、WorkPlace でブラウザ ウィンドウを終了しても、ライセンスは解放されません)。

すべてのオープン セッション

オープン セッションは、ライセンスを消費する、あるいは再開可能なセッションとして定義されます。待機中で再開が可能なこの状態は、ブラウザおよびトンネル セッションで異なります。

- ブラウザ セッションは、15 分以上接続処理が行われないと、ライセンスが解放されます。
- Connect Tunnel セッションは、例えば、モバイル ユーザーが範囲外に移動した場合や、ラップトップを閉じた場合など、ネットワークイベントによってトンネルが切断されてから、15 分後にライセンスが解放されます。(ユーザーがトンネル セッションを使用して停止した場合でも、keep-alive パケットなどのネットワーク トラフィックのためにアクティブのままになります)。

認証トークンが有効である限り、また、セッションが再開されたときにライセンスが利用できる限り、このオープン状態のライセンスを消費しないセッションは再開できます。デフォルトでは、認証トークンはセッションが開始してから数時間有効になります。

認証条件が受け入れられない

このカテゴリは、ユーザーが個人用デバイスを使用しており承認規約を受け入れなかったためにブロックされたセッションに使用されます。

すべてのセッション

このカテゴリには、すべてのオープン セッションと、終了したセッション、または後続の再試行後にログインが失敗したセッションが含まれます。最終的な失敗メッセージを受信する前に、ユーザーがログイン試行を中止した場合、これらの試行に関する情報は、リストには表示されません。7 日以前に終了したセッションに関するデータは破棄されます。

メモ：詳細については、ライセンスの計算方法を参照してください。

ユーザー セッションの終了

ユーザーが異なるサービスやノードで複数の接続を持っている場合でも、ユーザー セッションを即座に終了できます。また、10 分間ユーザーのネットワーク アクセスを一時的に無効にできます (アクセス ポリシーで許可している場合、ユーザーは、この時間が経過すると再度ネットワークにログインできます)。VPN へのログインを永久にユーザーに許可しない場合、次のいずれかの操作を実行する必要があります。

- 適用されるアクセス制御ルールの変更
- 適用されるユーザーおよびグループの定義の修正または削除
- ユーザー ディレクトリからのユーザーの削除

オープン ユーザー セッションを終了するには、

1 メイン ナビゲーション メニューから、[**User Sessions (ユーザ セッション)**] をクリックします。

2 [**View (表示)**] リストから、表示するセッション数を選択して、[**All open (すべてのオープン)**] を選択します (オープンのセッションだけを終了できます)。

3 その他のプロパティを組み合わせて、セッション リストをフィルタリングできます。

- **ユーザ**: ユーザー名のすべてまたは一部を入力します。検索文字列の任意の場所にワイルドカード文字 (* または ?) を使用できます。
- **レルム**: 1 つのレルムまたはすべてのレルムを選択します。
- **コミュニティ**: 1 つのコミュニティまたはすべてのコミュニティを選択します。レルムを選択している場合、リストで表示されるコミュニティは、レルムに関連するコミュニティのみに制限されます。
- **ゾーン**: 1 つのゾーンまたはすべてのゾーンを選択します。
- **エージェント**: エージェントまたはすべてのアクセス エージェントを選択するか、エージェントを有効にしないこと (変換のみ) を指定します。
- **プラットフォーム**: プラットフォームまたはすべてのプラットフォームを選択します。

4 AMC で手動でセッションを終了する方法は 2 つあります。ライセンスされている、または再開が可能なオープン セッションだけを終了できます。終了するセッションの横のチェック ボックスを選択するか、上部にあるチェック ボックスを選択してリストにあるすべてのユーザーを選択し、セッション終了ボタンの 1 つをクリックします。

- **セッションの終了** - [**Terminate session (セッションの終了)**] をクリックすると、選択したセッションに関連するすべての接続が終了します。これは例えば、待機中のセッションからライセンスを解放する場合に便利です。セッションは個別に終了できるため、ユーザーがいくつかのセッションを持っている場合、終了するセッションを選択できます。セッションが終了されたユーザーは、すぐに再認証して、アプライアンスにログインできます。
- **Terminate session - restrict logins (セッションの終了 - ログインの制限)** - この終了のタイプは、上記と同じですが、10 分が経過しないと、ユーザーは新しいセッションを作成できません。既存のセッションがあり使用できる場合でも、10 分が経過しないと、新しいセッションを作成できません。例えば、すべてのユーザー セッションを終了し、認証ストアからユーザーのクレデンシャルを削除する間、新しいセッションを確立できないようにする場合などに、このタイプの終了を使用します。

ユーザー アクセスとポリシー詳細の表示

例えば、ログインしたのに接続を確立できない、あるいはリソースへのアクセスを拒否される場合、[**Session Details (セッションの詳細)**] ページを使用して、問題を診断できます。このページではセッションをトラブルシューティングでき、そのステータスを評価してセッションがアクティブであるか、ユーザーのデバイスが特定のゾーンに分類されている理由、そしてどのポリシールールが適用されているかを確認でき、必要に応じて編集できます。

ユーザー セッションの詳細を表示するには、

1 メイン ナビゲーション メニューから、[**User Sessions (ユーザ セッション)**] をクリックします。

2 詳細を表示するセッションの [username] リンクをクリックします。必要に応じて、フィルタを設定して、表示するリストを絞り込み、[**Refresh (再表示)**] をクリックします。

- リソースへのアクセスをトラブルシューティングするには、[**Access requests (アクセス要求)**] リストを確認します。リストの項目を展開して、特定の接続要求を許可または拒否するかどうかを決定するアクセス制御ルールを表示できます。ルールが存在している場合、項目を編集するためのリンクも表示されます。
- アプリケーション アクセス制御を使用してアクセスされるリソースの情報は、セッションのクライアント ソフトウェアとプラットフォーム、リソースへのアクセスに使用されたアプリケーション、およびアクセスを許可または拒否するルールを識別します。
- End Point Control ゾーンは、デバイス プロファイルの存在の有無を基準として接続要求を分類します。[**Zone classification (ゾーン分類)**] ページでは、どの EPC ゾーン (存在する場合) がセッション中に評価されたのか、そして、各評価の結果を表示できます。この例では、モバイル デバイスが *Pocket PC* ゾーンに配置されましたが、*Equipment ID* デバイス プロファイルと一致しませんでした。
- ユーザー セッションに、現在、Connect Tunnel 接続がある場合、[**Active connections (アクティブな接続)**] ページに IP アドレスごとにセッションが表示されます。その他のアクセス エージェントは、VPN 接続をオープンのままにしないため、ここには表示されません。
- ユーザーが個人用デバイスを使用して接続した場合、デバイスと認証情報は [**Device Authorization (デバイス認証)**] ページで提供されます。承認条件に同意しなかったためにアクセスが拒否されたユーザーも、このページで識別されます。
- ユーザーがアプリケーション アクセス コントロールを使用して接続している場合は、エンドポイント上で見つかったアプリケーションに関する情報も特定されます。

ユーザー セッション データのエクスポート

ユーザー セッション データは、AMC からカンマ区切りのファイル (CSV) にエクスポートして、Microsoft Excel で表示および編集できます。ユーザー セッション データを CSV ファイルにエクスポートすると、ユーザー セッション データを無期限にアーカイブして、Secure Mobile Access Advanced Reporting (AAR) を使用しなくてもカスタム レポートを作成したり、その他の特別な目的にファイルを使用できます。

ユーザー セッション データを CSV ファイルにエクスポートするには、

1 メイン ナビゲーション メニューから、[**User Sessions (ユーザ セッション)**] をクリックします。

2 オプションで、表示するユーザー データをフィルタリングして、エクスポートしたいデータだけを表示できます。フィルタリングの詳細については、ユーザー セッションの表示を参照してください。

3 ユーザー セッション データの上にある [**Export (エクスポート)**] ボタンをクリックします。

> ⓘ **メモ**：管理者が [**User Sessions (ユーザ セッション)**] ページを表示するアクセス権限がある場合にのみ、[Export (エクスポート)] ボタンが表示されます。

4 Windows のファイルのダウンロード ダイアログが表示されたら、[**Save (保存)**] ボタンをクリックします。

5 ユーザー データを保存するローカル コンピュータの場所とファイル名を選択するか、デフォルトの設定を使用します。デフォルトのファイル名は、UserSessions.csv で、デフォルトの場所はユーザーの「Downloads (ダウンロード)」フォルダです。

6 [**Save (保存)**] ボタンをクリックして、ユーザー セッション データを csv ファイルにエクスポートします。現在のフィルタ条件に一致するすべてのユーザー セッションがエクスポートされます。

使用するフィルタによって、CSV ファイルには、各セッションの ユーザー セッション データ に示された情報が含まれる場合があります。

ユーザー セッション データ

データのタイプ	説明
システム バージョン	Secure Mobile Access バージョン番号
セッション ID	セッションを内部的に特定する一意の数字の ID
状況	ユーザー セッションの状態: **Login Failed (ログイン失敗)**、**Licensed (購読済)**、**Idle (アイドル)**、または **Ended (終了)** があります。
ユーザ名	簡単なユーザー名
長いユーザ名	完全なユーザー名とレルム、AD/LDAP セッションの共通名 (CN) が含まれます。
開始時刻	MM/DD/YYYY HH:MM:SS の形式のセッションの開始時間。アプライアンスのローカル時間が使用されます。
終了時刻	MM/DD/YYYY HH:MM:SS 形式のセッションの終了時間。セッションが待機中またはライセンスされている場合は空欄になります。
経過時間秒	セッションが開始してから終了するまでの秒数、またはアクティブおよび待機中のセッションが開始されてからの秒数
1 分あたりの平均バイト数 (過去 1 時間)	この 1 時間でセッションによって使用された 1 分あたりの平均バイト数 (アップロードおよびダウンロード)。これは利用率の高いユーザーとセッションを決定するために使用されます。
バイト合計	セッションによってアップロードおよびダウンロードされたバイト数
レルム	ユーザーの認証に使用されたレルム名
コミュニティ	ユーザーが配置されたコミュニティ名
ゾーン	ユーザー/デバイスが配置されたゾーン
EPC エージェント	使用された End Point Control エージェント: Cache Cleaner
アクセス エージェント	使用されたアクセス エージェント: Web のみ、Tunnel、Tunnel (ESP)、OnDemand、Web Proxy、または Exchange
リモート アドレス	クライアント コンピュータの IP アドレス
ローカル アドレス	クライアント接続に割り当てられたローカル アドレス。トンネル セッションではない場合は空欄になります。

次は、AMC によって生成されるユーザー セッション csv ファイルの例です。

Version,SessionID,State,Username,LongUsername,StartTime,EndTime,ElapsedSeconds,AverageBytesPerMinute LastHour,TotalBytes,Realm,Community,Zone,EPCAgent,AccessAgents,RemoteAddress,LocalAddress

```
10.6.1-auto404320,7,Ended,"ljones@am.us.sonicwall.com","(ljones)@(snwl) (CN=Laura Jones,OU=Users,OU=Engineering,OU=AM Domain Users,DC=am,DC=us,DC=sonicwall,DC=com)",03/09/2012 03:35:05,03/09/2012 03:36:41,96,120750,205276,"snwl","Default community","Default Zone","","Web only",10.10.10.1,
```

SNMP の構成

SNMP (Simple Network Management Protocol) ツールがある場合、これらのツールを使用することにより、アプライアンスを SNMP エージェントとして監視できます。このアプライアンスでは、SNMP

バージョン 2 および 3 をサポートしており、さまざまな管理データを Management Information Base (MIB) II 形式で提供します。

SNMPv2 または SNMPv3 を有効にできますが、同時に両方を有効にすることはできません。SNMPv2 を有効にすると、SNMPv3 の要求は無視されます。SNMPv3 を有効にすると、SNMPv2 の要求は無視されます。SNMP サポートを完全に無効にすることもできます。この場合は、システムから指示されるすべての SNMP 要求が無視され、トラップは生成されません。

SNMPv3 は、SNMPv1 と SNMPv2 の両方で発生したセキュリティの問題を解決しています。SNMPv3 は、バージョン 1 と 2 で定義されているすべてのオペレーションをサポートします。SNMPv3 で提供されるこの新しいセキュリティ機能は、認証、プライバシー (暗号化)、およびアクセス制御の 3 つのエリアに一般的に分けられます。

SNMPv2 での認証は、テキスト形式の「コミュニティ文字列」で安全ではない方法で提供されていますが、SNMPv3 での認証では、SHA アルゴリズムが使用され、安全な認証が提供されます。各 SNMP「ユーザー」について、ユーザー名とパスコードの両方、および使用するアルゴリズムがエージェントで構成され (この場合、SMA アプライアンス)、アプライアンスと通信する管理ソフトウェアに対して提供されるユーザー名、パスコード、およびアルゴリズム選択と一致する必要があります。

SNMPv3 の前は、すべての通信が暗号化されていませんでした。SNMPv3 では、AES アルゴリズムが使用され、SNMP メッセージが暗号化および復号化されます。認証では、ユーザー名、パスワード、および暗号化アルゴリズムが、暗号のシード作成に使用され、エージェントと管理ステーションの両方で構成される必要があります。

Secure Mobile Access で SNMPv3 でサポートされる認証および暗号化レベルの組み合わせは、認証レベルと暗号化レベルの組み合わせ で示されています。

認証レベルと暗号化レベルの組み合わせ

レベル	認証	暗号化	効果
noAuthNoPriv	ユーザ名	いいえ	認証の一致にユーザー名を使用します。
authNoPriv	SHA	いいえ	HMAC-SHA アルゴリズムを基準とする認証を行います。
authPriv	SHA	AES	HMAC-SHA アルゴリズムを基準とする認証を行います。認証の他に AES 暗号化を提供します。

SMA EX シリーズは、管理上の複雑さを最小化しながら、プロトコルのセキュリティの利点を活用するように設計されたSNMPv3 機能のサブセットをサポートします。現時点では、SNMPv3 の仕様で定義されているアクセス制御はサポートされません。SNMPv3 機能が追加されても、アプライアンスによって管理情報が報告される方法は変更されません。前のリリースと同じ方法で報告されます。

トピック:

- SNMP の構成
- MIB ファイルのダウンロード
- SNMP を使用した管理データの取得
- MIB データ

SNMP の構成

このセクションでは、AMC で SNMP を設定する方法について説明します。

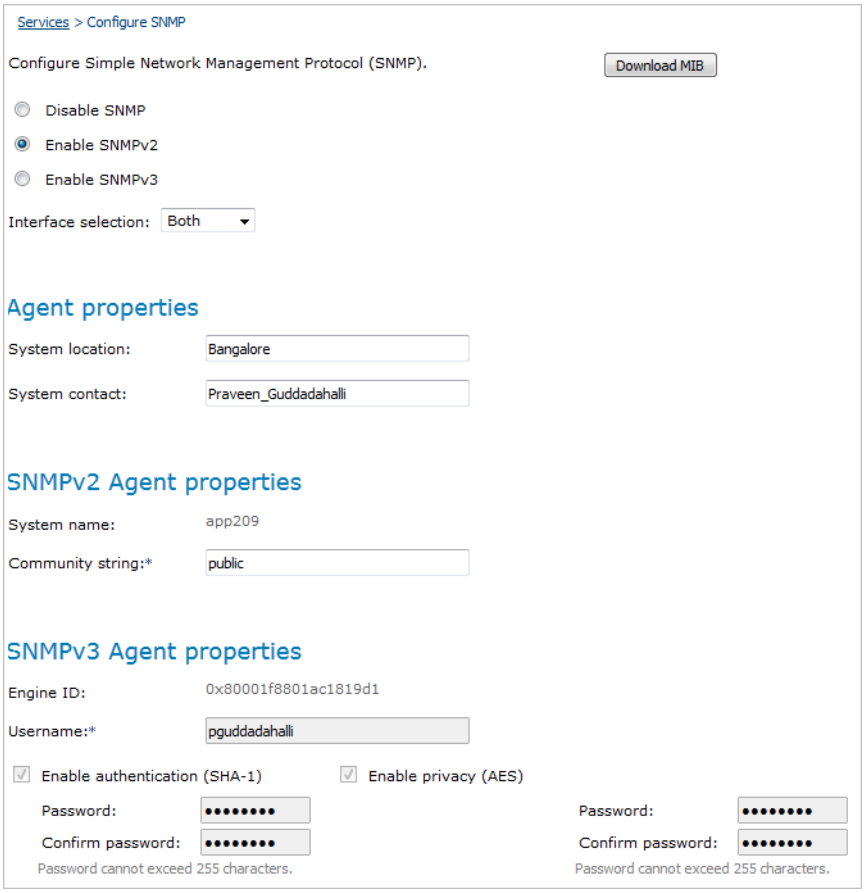
メモ：

- アプライアンスによって使用される管理情報ベース (MIB) を使用して SNMP マネージャを構成する必要があります。アプライアンスでは、カリフォルニア大学、Davis (UCD) MIB のバージョン 4.2.3および MIB II がサポートされます。SNMPv2 については、アプライアンスを照会するために必要なコミュニティ文字列を使用して SNMP マネージャを構成する必要もあります。SNMPv3 については、アプライアンスで構成されているのと同じユーザー名、パスコード、アルゴリズム選択を使用して、SNMP マネージャを構成します。
- 内部のファイアウォールがポート 161/udp トラフィックを許可するように構成されていることを確認してください。

SNMP を構成するには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Network Services (ネットワーク サービス)**] の [**SNMP**] に対応する [**Configure (設定)**] リンクをクリックします。



3 SNMP を有効にするには、[**Enable SNMPv2 (SNMPv2 を有効にする)**] または [**Enable SNMPv3 (SNMPv3 を有効にする)**] ラジオ ボタンのいずれかを選択します。(**Save (保存)** をクリックしないまま、SNMP ホストを構成するためにこのページを離れた場合、この設定のステータスは保存されません)。SNMP を無効にするには、[**Disable SNMP (SNMP を無効)**] ラジオ ボタンを選択してから、[**Save (保存)**] をクリックします。

4 [**Interface selection (インターフェイスの選択)**] ドロップダウン メニューから適切なオプション ([**Internal (内部)**]、[**External (外部)**]、[**Both (両方)**]) を選択して、SNMP で使用するネットワーク インターフェースを選択します。

5 [**Agent properties (エージェント プロパティ)**] の [**System location (システムの場所)**] および [**System contact (システムの連絡先)**] フィールドでアプライアンス エージェントを記述します。例えば、アプライアンスの物理的な場所 (*Server lab*)」など) やシステム管理者の連絡先 (「*Jim Jamerson, 206-555-1212*)」など) を指定できます。

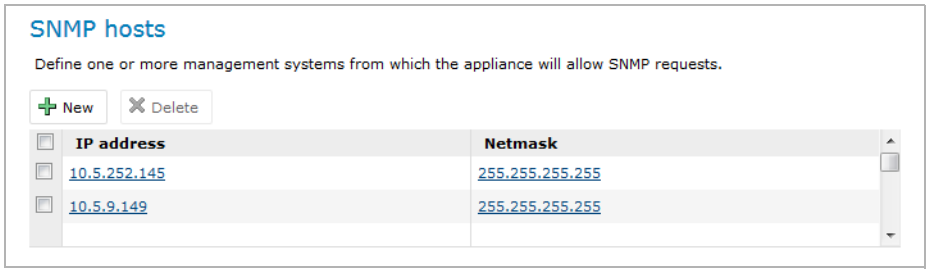
6 SNMPv2 を使用している場合、[**SNMPv2 Agent properties (SNMPv2 エージェント プロパティ)**] で、ネットワーク管理ツールが SMA アプライアンスを照会するときに使用する文字列を [**Community string (コミュニティ文字列)**] ボックスに入力します。このフィールドは必須で、デフォルトでは「**public (公開)**」に設定されます。「**public (公開)**」は安全ではないため、セキュリティを向上させるための習慣として、コミュニティ文字列に異なるパスフレーズを設定するようにします。

7 SNMPv3 を使用している場合、[**SNMPv3 Agent properties (SNMPv3 エージェント プロパティ)**] で、ネットワーク管理ツールが SMA アプライアンスを照会するときに使用する文字列を [**ユーザー名**] フィールドに入力します。

8 安全な認証を有効にするには、[**Enable authentication (SHA-1) (認証を有効化 ((SHA-1)))**] チェックボックスを選択して、[**Password (パスワード)**] および [**Confirm password (パスワードの確認)**] フィールドにパスワードを入力します。SHA-1 がより安全であるため、MD5 はサポートされていません。

9 プライバシーのための暗号化を有効にするには、[**Enable privacy (AES) (プライバシーを有効化 (AES))**] チェックボックスを選択して、[**Password (パスワード)**] および [**Confirm password (パスワードの確認)**] フィールドにパスワードを入力します。AES がより安全であるため、DES はサポートされていません。

10 [**SNMP Hosts (SNMP ホスト)**] で、アプライアンスが SNMP 要求を許可する管理システムを定義します。IP アドレスとサブネット マスクの両方に「`0.0.0.0`」と入力することで、任意のホストからの要求を許可できます。ただしその場合、アプライアンスのセキュリティが低下するという欠点もあります。



a [**SNMP hosts (SNMP ホスト)**] エリアで [**New (新規)**] をクリックします。

b ホストの [**IP address (IP アドレス)**] と [**Netmask (ネットマスク)**] を入力して、[**OK**] をクリックします。

11 [**Trap receivers (トラップの受信者)**] で、[**Enable support for SNMP traps (SNMP トラップのサポートを有効化)**] チェックボックスを選択して、トラップの送信を有効にします。チェックボックスをオフにすると、トラップが送信されなくなります。

トラップが有効な場合、すべてのトラップはリストで定義されているすべてのホストに送信されます。トラップが無効である場合、ホストのリストは無視されます。

12 SNMP トラップを送信する管理システムを定義します。

a [**Trap receivers (トラップの受信者)**] エリアの [**New (新規)**] をクリックします。

b ホストの [**IP address (IP アドレス)**] と [**Netmask (ネットマスク)**] を入力して、[**OK**] をクリックします。

13 [**Save (保存)**] を選択します。

MIB ファイルのダウンロード

AMC を使用して、Secure Mobile Access SRA MIB ファイルをダウンロードできます。これにより、すでにサポートされている MIB に VPN 固有のデータが追加されます。MIB によって提供される情報の詳細は、MIB データを参照してください。

MIB をダウンロードするには:

1 メイン ナビゲーション メニューから [**Services (サービス)**] をクリックします。

2 [**Network Services (ネットワーク サービス)**] の [**SNMP**] に対応する [**Configure (設定)**] リンクをクリックします。

3 [**Download MIB (MIB をダウンロード)**] ボタンをクリックします。ファイル ダウンロードのメッセージが表示されます。

4 [**Save (保存)**] をクリックして、正しいディレクトリをブラウズします。ここで設定したディレクトリに `SMA1000CustomMibs.tar` ファイルが保存されます。

SNMP を使用した管理データの取得

SNMP データは、標準化された階層構造に編成され、それを構成する構造化テキスト ファイルに、価値のある管理データが記述されています。これらのテキスト ファイル (MIB と呼ばれる) には、システム情報やステータスなどの固有のデータ変数が記述されています。

メモ：MIB II の詳細 (MIB II 変数名の説明も含まれる) については、http://www.ietf.org/rfc/rfc1213.txt を参照してください。

SNMP を介して情報を取得する場合、システムで「オブジェクト識別子」(OID) を照会します。それぞれの OID には、テキスト名も含まれますが、通常は番号で参照されます。例えば、システム アップタイム (**sysUpTime**) の OID は `1.3.6.1.4.1.674.3` になります。

SNMP 管理パッケージがない場合は、アプライアンスに接続して *root* としてログインし **snmpwalk** または **snmpget** コマンドを実行することによって、SNMP データを取得できます。例えば、ディスク容量についての情報を取得する場合、次の **snmpwalk** コマンドを入力することで、`1.3.6.1.4.1.2021.9:` を照会します。

```
# snmpwalk -v 2c -c public localhost 1.3.6.1.4.1.674.9
```

すべての MIB 変数のリストを表示するときは、次のコマンドを入力します。

```
snmpwalk -v 1 -O n localhost -c public |more
```

このコマンドにより、次のようなリストが表示されます。

```
.1.3.6.1.2.1.1.1.0 = Linux E-Class SRAvpn 2.4.20_004 #1 SMP Thu Apr 10 14:35:50 PDT
2017 i686
.1.3.6.1.2.1.1.2.0 = OID:.1.3.6.1.4.1.2021.250.10
.1.3.6.1.2.1.1.3.0 = Timeticks: (1707979) 4:44:39.79
.1.3.6.1.2.1.1.4.0 = Root < root@localhost> (configure /etc/snmp/snmp.local.conf)
.1.3.6.1.2.1.1.5.0 = E-Class SRAvpn
.1.3.6.1.2.1.1.6.0 = Unknown (configure /etc/snmp/snmp.local.conf)
.1.3.6.1.2.1.10.8.0 = Timeticks: (7) 0:00:00.07
```

```
.1.3.6.1.2.1.1.9.1.2.1 = OID:.1.3.6.1.2.1.31
..
```

すべての MIB 名のリストを表示するとき (**snmpget** コマンドを使用するときに便利です) は、次のコマンドを入力します。

```
snmpwalk -O S localhost -c public |more
```

このコマンドにより、次のようなリストが表示されます。

```
SNMPv2-MIB::sysDescr.0 = Linux E-Class SRAvpn 2.4.20_004 #1 SMP Thu Apr 10 14:35:50
PDT 2003 i686
SNMPv2-MIB::sysObjectID.0 = OID : SNMPv2-SMI::enterprises.2021.250.10
SNMPv2-MIB::sysUpTime.0 = Timeticks: (1712451) 4:45:24.51
SNMPv2-MIB::sysContact.0 = Root (configure /etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysName.0 = E-Class SRAvpn
SNMPv2-MIB::sysLocation.0 = Unknown (configure /etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (7) 0:00:00.07
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
..
```

MIB データ

MIB モジュールは、SMA アプライアンスに関する情報を提供する、オブジェクト識別子 (OID) やテキスト名を参照します。MIB データ を参照してください。

MIB データ

MIB データ	詳細情報
システム情報	MIB データ : システム情報モジュール
システム ヘルス	MIB データ : システム ヘルス モジュール
サービス ヘルス	MIB データ : サービス ヘルス
セキュリティ履歴	MIB データ : セキュリティ履歴モジュール
ネットワーク トンネル サービス	MIB データ : ネットワーク トンネル サービス モジュール
システム トラップ	MIB データ : トラップ
その他の SNMP データ	MIB データ : その他の SNMP データ

MIB データ : システム情報モジュール

システム情報モジュールの OID では、アプライアンスに関する基本情報が提供されます。

MIB データ : システム情報モジュール

項目	OID	説明
バージョン	1.3.6.1.4.1.674.1.1.0	このノード上で動作する Secure Mobile Access ファームウェアのバージョンで、major.minor.micro-hotfix-build の形式 (例えば「12.1.1.1-128」) になります。
ハードウェア モデル	1.3.6.1.4.1.674.1.2.0	アプライアンスのモデル番号です (例えば EX9000、EX7000、EX6000、SMA 7200、または SMA 6200)。今後新しいモデル番号が追加される場合があります。

MIB データ : システム ヘルス モジュール

システム ヘルス モジュールの OID では、アプライアンスの動作ステータスに関する情報が提供されます。

MIB データ : システム ヘルス モジュール

項目	OID	説明
現在のログイン	1.3.6.1.4.1.674.2.1.1.0	現在認証されているアクティブ ユーザー セッションの数。
最大ライセンス ユーザー	1.3.6.1.4.1.674.2.1.3.0	このアプライアンス (アプライアンスのクラスタ) でライセンスされているアクティブ ユーザー セッションの最大数。
現在の接続	1.3.6.1.4.1.674.2.2.1.0	このアプライアンス (アプライアンスのクラスタ) によって現在サービスが提供されている同時接続の数。
CPU 利用	1.3.6.1.4.1.674.2.3.0	5 秒間における、単一のアプライアンス ノードでの CPU の利用率 (デュアルプロセッサ マシンの場合、CPU の合計利用率)。
RAM 利用	1.3.6.1.4.1.674.2.4.1.0	現在使用中の仮想メモリ (RAM) の利用率。
スワップ利用	1.3.6.1.4.1.674.2.4.2.0	現在使用中の仮想メモリ (スワップ) の利用率。
ログ利用率	1.3.6.1.4.1.674.2.9.0	使用されているログ ファイル ディスク パーティションの割合。
ピーク ログイン	1.3.6.1.4.1.674.2.1.2.0	前回のリセット以降、認証されたアクティブ ユーザー セッションの最大数。リセット間隔は 24 時間です。
ピーク接続	1.3.6.1.4.1.674.2.2.2.0	前回のリセット以降のアプライアンスへの同時接続の最大数。リセット間隔は 24 時間です。
内部インターフェースの現在のスループット	1.3.6.1.4.1.674.2.5.1.0	5 秒間における、現在の VPN スループット (インバウントおよびアウトバンド) で、内部インターフェースで計測された値であり、秒あたりのメガビット数単位になります。
内部インターフェースのピーク スループット	1.3.6.1.4.1.674.2.5.2.0	前回のリセット以降の、ピーク VPN 内部インターフェース スループット (インバンドおよびアウトバンド)。秒あたりのメガビット数単位になります。
外部インターフェースの現在のスループット	1.3.6.1.4.1.674.2.5.3.0	5 秒間における、ノードの外部インターフェースで計測された、現在の VPN スループット (インバンドおよびアウトバンド)。秒あたりのメガビット数単位になります。
外部インターフェースのピーク スループット	1.3.6.1.4.1.674.2.5.4.0	前回のリセット以降の、ピーク VPN 外部インターフェース スループット (インバンドおよびアウトバンド)。秒あたりのメガビット数単位になります。

MIB データ : システム ヘルス モジュール

項目	OID	説明
クラスタ インターフェースの現在のスループット	1.3.6.1.4.1.674.2.5.5.0	5 秒間における、現在の平均 VPN クラスタ インタ フェース スループット (インバンドおよびアウトバンド)。秒あたりのメガビット数単位になります。リセット間隔は 24 時間です。
クラスタ インターフェースのピークスループット	1.3.6.1.4.1.674.2.5.6.0	前回のリセット以降の、ピーク VPN クラスタ インターフェース スループット (インバンドおよびアウトバンド)。秒あたりのメガビット数単位になります。リセット間隔は 24 時間です。

MIB データ : サービス ヘルス

MIB データ : サービス ヘルス モジュール で示されたサービス ヘルス モジュールの OID では、アプライアンスで動作する各サービスのステータスに関する情報が提供されます。MIB では、サービスごとに、サービス ID、サービスの記述、サービスの状態 (「稼働中」または「休止中」) について通知します。

MIB データ : サービス ヘルス モジュール

項目	OID	説明
サービス ID	1.3.6.1.4.1.674.3.1.1.1.1	AMC のサービス ID は 1 です。
	1.3.6.1.4.1.674.3.1.1.1.3	SonicWall Web プロキシ サービスのサービス ID は 3 です。
	1.3.6.1.4.1.674.3.1.1.1.4	WorkPlace のサービス ID は 4 です。
	1.3.6.1.4.1.674.3.1.1.1.5	syslog-ng (E-Class SMA アプライアンス ログ ファイルに書き込むプロセス) のサービス ID は 5 です。
サービスの記述	1.3.6.1.4.1.674.3.1.1.2.1	アプライアンス管理コンソール (AMC)
	1.3.6.1.4.1.674.3.1.1.2.2	(廃止) クライアント/サーバー アクセス サービス (AVPN)
	1.3.6.1.4.1.674.3.1.1.2.3	セキュア Web アクセス サービス (ExtraWeb)。「Web プロキシ サービス」とも呼ばれます。
	1.3.6.1.4.1.674.3.1.1.2.4	ASAP WorkPlace。Work Place と同じです。
	1.3.6.1.4.1.674.3.1.1.2.5	Syslog-ng (E-Class SMA アプライアンス ログ ファイルに書き込むプロセス)
サービスの状態	1.3.6.1.4.1.674.3.1.1.3.1	AMC の現在の状態 : **1** (アップ) または **2** (ダウン)。
	1.3.6.1.4.1.674.3.1.1.3.3	Web プロキシ サービスの現在の状態 : **1** (アップ) または **2** (ダウン)。
	1.3.6.1.4.1.674.3.1.1.3.4	WorkPlace の現在の状態 : **1** (アップ) または **2** (ダウン)。
	1.3.6.1.4.1.674.3.1.1.3.5	syslog-ng の現在の状態 : **1** (アップ) または **2** (ダウン)。

MIB データ : セキュリティ履歴モジュール

セキュリティ履歴モジュールの OID では、ログインおよびアクセス拒否に関する情報が提供され ます。

MIB データ : セキュリティ履歴モジュール

項目	OID	説明
ログイン拒否の回数	1.3.6.1.4.1.674.4.1.0	最近の 24 時間におけるログイン拒否の回数。
前回ログインが拒否されたユーザー	1.3.6.1.4.1.674.4.2.1.0	前回認証が拒否されたユーザー。「user@realm」の形式になります。
前回ログインが拒否された時刻	1.3.6.1.4.1.674.4.2.2.0	前回ユーザーのアクセスが拒否された日付と時刻。この文字列の形式は、Wed May 30 21:49:08 2017 となり、アプライアンスが構成されているのと同じタイムゾーンになります。
アクセス拒否の回数	1.3.6.1.4.1.674.4.3.0	最近の 24 時間におけるアクセス拒否の回数。
前回アクセスが拒否されたユーザー	1.3.6.1.4.1.674.4.4.1.0	前回アクセスが拒否されたユーザー。「user@realm」の形式になります。
前回アクセスが拒否されたリソース	1.3.6.1.4.1.674.4.4.2.0	前回アクセスが拒否されたリソースの URL、ホスト : ポート、またはホスト
前回アクセスが拒否された時刻	1.3.6.1.4.1.674.4.4.3.0	前回ユーザーのアクセスが拒否された日付と時刻。この文字列の形式は、Wed May 30 21:49:08 2017 となり、アプライアンスが構成されているのと同じタイムゾーンになります。

MIB データ : ネットワーク トンネル サービス モジュール

NG サーバー モジュールの OID では、ネットワーク トンネル サービスのステータスに関する情報が提供されます。

MIB データ : ネットワーク トンネル サービス モジュール

項目	OID	説明
NG サーバーの状態	1.3.6.1.4.1.674.5.1.0	ネットワーク トンネル サービスの現在の状態 : 「Active」、「Down」、「Crashed」のいずれか。
クライアント アドレス プールの数	1.3.6.1.4.1.674.5.2.0	ネットワーク トンネル サービスに割り当てられているクライアント アドレス プールの数。
クライアント アドレス プール範囲テーブル	1.3.6.1.4.1.674.5.3	現在アクティブな IP アドレス プールの数とその IP アドレス範囲を示すテーブル。
クライアント アドレス プール エントリ	1.3.6.1.4.1.674.5.3.1	現在アクティブな IP アドレス プールの数。
クライアント アドレス プール ID	1.3.6.1.4.1.674.5.3.1.1.0	IP アドレス プールに割り当てられている ID 番号。
クライアント アドレス プール利用率	1.3.6.1.4.1.674.5.3.1.2.0	クライアント アドレス プールから発行されている仮想 IP アドレス (VIP) の割合。

MIB データ : ネットワーク トンネル サービス モジュール

項目	OID	説明
クライアント IP アドレス プール開始範囲	1.3.6.1.4.1.674.5.3.1.3.0	クライアント IP アドレス プール範囲の最初の IP アドレス。
クライアント アドレス プール終了範囲	1.3.6.1.4.1.674.5.3.1.4.0	クライアント IP アドレス プール範囲の最後の IP アドレス。
NG SLL トンネルの数	1.3.6.1.4.1.674.5.4.0	アクティブ ネットワーク トンネルの総数。
SSL トンネル テーブル	1.3.6.1.4.1.674.5.5	ネットワーク トンネル統計を示すテーブル。
SSL トンネル ID	1.3.6.1.4.1.674.5.5.1.1.0	ネットワーク トンネル セッションに割り当てられている ID 番号。
SSL トンネル ユーザー	1.3.6.1.4.1.674.5.5.1.2.0	ネットワーク トンネル セッションに対応するユーザー名。
SSL トンネル VIP	1.3.6.1.4.1.674.5.5.1.3.0	ネットワーク トンネル セッションに対応する仮想 IP アドレス (VIP)。
トンネルあたりのフロー数	1.3.6.1.4.1.674.5.5.1.4.0	ネットワーク トンネル セッションのデータフローの数。
SSL トンネル アップタイム	1.3.6.1.4.1.674.5.5.1.5.0	ネットワーク トンネル セッションのアップタイム統計。

MIB データ : トラップ

トラップは、重要なイベントが発生した場合に、管理者に注意を促すために SNMP エージェントが送信するメッセージです。Secure Mobile Access の MIB をダウンロードするには、メインのナビゲーション メニューで [**Services (サービス)**] をクリックしてから、[**SNMP**] エリアで [**Configure (設定)**] をクリックします。[**Download MIB (MIB をダウンロード)**] をクリックして、ファイル (SMA1000CustomMibs.tar) のコピーを保存します。

MIB データ : トラップ

項目	MIB ファイル名	説明
ngServerStateChange	*SonicWallNGServer*	サーバーのコア機能は、ユーザー スペースのプロセス (*avssld* および *avpsd*) および 2 つの *avevent* カーネル スレッドによって変わります。SNMP エージェントは、これらのプロセスを監視しており、これらのプロセスのいずれかがダウンすると、トラップがトリガーされます。トラップの説明で、*avssld(0)* など、影響を受けるコンポーネントを確認できます。
ngclientAddrPoolUtilizationWarning	*SonicWallNGServer*	このトラップは、クライアント アドレス プールの使用量がしきい値を超えたときにトリガーされます。
asapServiceUp	SonicWallServiceHealth	単一ノード システムのサービス (トラップの送信元の IP アドレスで識別) が動作しています。このトラップと一緒に *serviceDescription* OID が送信されます。

MIB データ : トラップ

項目	MIB ファイル名	説明
asapServiceDown	SonicWallServiceHealth	単一ノード システムのサービス (トラップの送信元の IP アドレスで識別) がダウンしています。このトラップと一緒に *serviceDescription* OID が送信されます。
cpuCapacityWarning	SonicWallSystemHealth	ヒューリスティックに判定された、単一ノード システムに対する CPU 容量の割合が、単一ノードの容量 (*cpuCapacityUtilization*) を超えました。このトラップと一緒に *cpuCapacityUtilization* OID が送信されます。
memoryCapacityWarning	SonicWallSystemHealth	ヒューリスティックに判定された、単一ノード システムに対するメモリ容量の割合が容量 (*memoryCapacityUtilization*) の 90% を超えました。このトラップと一緒に memoryCapacityUtilization OID が送信されます。
logCapacityWarning	SonicWallSystemHealth	単一ノード システムで使用されるログ ファイル ディスク スペースが、総容量の 90% を超えました。このトラップと一緒に logUtilization OID が送信されます。
userLimitWarning	SonicWallSystemHealth	単一ノード システムにおける認証ユーザーの同時接続数 (*currentlyLoggedIn*) がライセンス数制限の 90% を超えた場合に、通知が生成されます。
userLimitReached	SonicWallSystemHealth	単一ノード システムで現在認証されているアクティブ ユーザー セッション数が、現在のライセンス制限 (*currentlyLoggedIn*) に達しました。このトラップと一緒に currentlyLoggedIn OID が送信されます。
userLimitExceeded	SonicWallSystemHealth	単一ノード システムにおける認証ユーザーの同時接続数が、現在のライセンス制限 (*currentlyLoggedIn*) に達しました。このトラップと一緒に currentlyLoggedIn OID が送信されます。
asapSystemUp	SonicWallSystemInfo	HA ペアではなく単一のアプライアンス : アプライアンス (トラップの送信元の IP アドレスで識別) が再びオンラインになりました。
asapSystemDown	SonicWallSystemInfo	HA ペアではなく単一のアプライアンス : アプライアンス (トラップの送信元の IP アドレスで識別) がオフラインになりました。

MIB データ : その他の SNMP データ

SNMP を使用して標準 MIB ファイルから取得可能な、アプライアンスに関するその他の情報を、MIB データ : その他の SNMP データ で示しています。

MIB データ : その他の SNMP データ

項目	OID	説明
サービス ステータス テーブル	1.3.6.1.4.1.674.2	次のいずれかのサービスのステータスをチェックします。戻りデータは、次のプロセス名になります。プロセス ステータスが「非動作」としてリストされている場合、エラーが出されます。 • apache2 (Web プロキシ サービス) • logserver (ログ サーバー) • syslog-ng (syslog) • policyserver (ポリシー サーバー) アプライアンスのバージョン 8.9.0 以降では、srvcmond (クラスタ マネージャ) が、AVFM (Secure Mobile Access フロー マネージャ) に置き換わりました。AVFM は、カーネル モジュールとして実行されるため、アプライアンスのプロセス リストには表示されません。
利用可能なディスク容量テーブル	1.3.6.1.4.1.674.9	「/」、「/var/log」、「/upgrade」の各パーティションについて、ディスク容量の可用性をチェックします。いずれかのパーティションのディスク容量が 10MB 以下になっている場合、エラーが出されます。
負荷平均チェック テーブル	1.3.6.1.4.1.674.10	1 分、5 分、15 分間隔で負荷平均をチェックします。負荷平均が 1 分間隔で 12 以上、5 分間隔および 15 分間隔で 14 以上の場合、エラーが出されます。
ソフトウェア バージョン番号テーブル	1.3.6.1.4.1.674.50	SonicWall システム ソフトウェアの現在のバージョンをチェックします。
システム名	1.3.6.1.4.1.674.0	システムの名前をチェックします。

構成データの管理

アプライアンスの構成データは、単一のエクスポート アーカイブ (.aea) ファイルに保管されます。このファイルには、データ タイプの設定 で示された構成データが含まれています。

データ タイプの設定

構成データのタイプ	説明
アクセス ポリシー	ルール、リソース、ユーザーとグループ、WorkPlace ショートカット、EPC 署名、ゾーンが含まれます。
証明書	証明書、プライベート キー、証明書パスワードが含まれます。
WorkPlace スタイルのカスタマイズ	一般的な表示設定、カスタム コンテンツ、カスタム テンプレートが含まれます。
ノード固有およびネットワーク固有の設定	ホスト名、IP アドレス、デフォルト ルート情報、DNS 設定、クラスタ設定が含まれます。

特に、システム変更を行った後、前の構成に戻す必要があるような場合、アプライアンスの構成データを定期的にバックアップすることが推奨されます。例えば、新しいアクセス制御ルールを追加する場合、最初に構成を保存しておき、変更するようにします。こうしておくと、新しいルールが予定通り動作しない場合でも、保存している (動作中の) 構成に戻すことができます。

構成データを保存、復旧する場合、次のようにいくつかの方法があります。

- 構成データをローカル マシンにエクスポートして、その後それをインポートします。エクスポートでは、構成データ全体が対象になりますが、インポートは部分的に実行することもできます。詳細については、ローカル マシンへの現在の構成のエクスポートと構成データのインポートを参照してください。
- 構成データ ファイルをアプライアンスに保存してリストアします。この場合、構成データ全体が対象になります。部分的に構成を保存したりリストアしたりすることはできません。詳細については、現在の構成のアプライアンスへの保存 およびアプライアンスに保管された構成データのリストアまたはエクスポート を参照してください。
- 古い SonicWall Secure Mobile Access アプライアンスからポリシーをエクスポートし、新しいアプライアンスにインポートできます。ただし古いアプライアンスのバージョンが、通常、新しいアプライアンスより 3 バージョン以上下まわることはできません。サポートされるプラットフォームについては『*SMA 12.1 アップグレード ガイド*』を、SonicWall によって使用されるバージョン番号の規則については システムのアップデート を参照してください。

注意：AMC で生成された構成データのみが保存またはエクスポートされます。(アプライアンス内デレクトリにある SonicWall のファイル群を直接編集することにより) 手動で構成ファイルを編集した場合、その変更は対象になりません。手動による変更は通常あまり行うことはなく、SonicWall テクニカル サポートが指示した場合に限って行います。

トピック:

- ローカル マシンへの現在の構成のエクスポート
- 現在の構成のアプライアンスへの保存
- 構成データのインポート
- アプライアンスに保管された構成データのリストアまたはエクスポート
- 構成データの保存とリストア

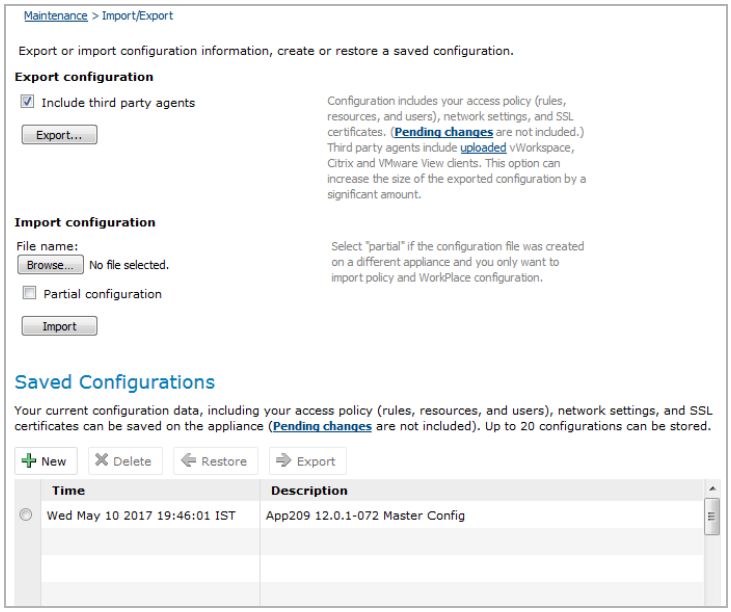
ローカル マシンへの現在の構成のエクスポート

アプライアンスの構成データ全体をローカル マシンにエクスポートできます (構成を部分的にエクスポートすることはできません)。その場合は、保存した変更のみが対象となります。構成をエクスポートする時点で保留中だった変更は破棄されます。

現在の構成をエクスポートするには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Maintenance (メンテナンス)**] をクリックします。

2 「**System Configuration (システム設定)**」エリアで、「**Import/Export (インポート/エクスポート)**」をクリックします。



3 [**Export (エクスポート)**] を選択します。この操作により、[**Export Configuration (設定をエクスポート)**] ページが表示されます。[**File Download (ファイルのダウンロード)**] ダイアログ ボックスで、`SonicWallSMAAppliance-<date>-<nnn>.aea` ファイルを開くかこれをハード ディスクに保存するよう求められます。

4 [**Save (保存)**] をクリックして、正しいディレクトリをブラウズします。ここで設定したディレクトリに `.aea` ファイルが保存されます。

5 [**Export (エクスポート)**] ページで [**OK**] をクリックします。

現在の構成のアプライアンスへの保存

構成データの保存の場合、エクスポートと異なり、アプライアンス上にデータが保管されます (最大で 20 の構成を保管できます)。構成を部分的にエクスポートすることはできず、適用済みの変更のみがエクスポートの対象になります。

構成データをアプライアンスに保存するには、

1 メイン ナビゲーション ページから、[**Maintenance (メンテナンス)**] をクリックします。

2 「**System Configuration (システム設定)**」エリアで、「**Import/Export (インポート/エクスポート)**」をクリックします。

3 [**Saved Configurations (保存済みの構成)**] リストで [**New (新規)**] をクリックします。

4 [**Description (説明)**] フィールドにこの構成についての説明を記述します。(複数の管理者がいる場合) 保存した管理者を識別しておくと良いでしょう。例えば、エントリは次のようになります。「`Saved by MIS before adding access control rules for mobile devices` (モバイル デバイス用のアクセス制御ルールを追加する前に `MIS` によって保存)」。

5 [**Save (保存)**] を選択します。現在の構成データがアプライアンスに保管され、[**Saved Configurations (保存済みの構成)**] リストに追加されます。

構成データのインポート

エクスポートでは、常に構成データ全体がその対象になりますが、インポートは部分的に実行することもできます (例えばポリシーおよび WorkPlace 設定のみのインポートも可能)。

インポート用のデータの設定では、既存の AMC 構成にインポートできるデータのタイプをまとめています。

インポート用のデータの設定

構成データのタイプ	説明
構成の一部	• **アクセス ポリシー :** ルール、リソース、ユーザーとグループ、EPC デバイス プロファイル、ゾーンが含まれます。 • **WorkPlace スタイルのカスタマイズ:** 一般的な表示設定、カスタム コンテンツ、ショートカット、カスタム テンプレートが含まれます。 • **CA 証明書 :** SSL で、認証サーバー接続またはバックエンド Web リソースを保護するために使用される CA 証明書が含まれます。 • **End Point Control:** デバイス プロファイルでクライアント証明書を使用する場合、部分的な構成には、ユーザーに証明書を発行した CA が含まれます。
構成のすべて	• 部分構成データ (構成の一部参照)。 • **SSL 証明書 :** プライベート キーおよびパスワードを伴う AMC およびアプライアンス証明書が含まれます。 • **ノード固有およびネットワーク固有の設定:** ホスト名、IP アドレス、デフォルト ルート情報、DNS 設定、管理者のアカウント、クラスタ設定が含まれます。

構成のすべてまたは一部をインポートするには、

1 メイン ナビゲーション ページから、[**Maintenance (メンテナンス)**] をクリックします。

2 「**System Configuration (システム設定)**」エリアで、「**Import/Export (インポート/エクスポート)**」をクリックします。

3 [**File name (ファイル名)**] ボックスで、適切なファイル (`SonicWallSMAApplianceVPN-<date>-<nnn>.aea`) のパスを指定するか、[**Browse (参照)**] をクリックしてこのファイルを指定します。

4 上記の表にリストされている項目のみをインポートする場合は、[**Partial configuration (構成の一部)**] をクリックします。

5 「**インポート**」を選択します。インポートした構成を有効にするには、変更を適用しなければなりません。詳細については、構成変更の適用を参照してください。

メモ :

- インポートが失敗した場合、管理メッセージ ログ ファイルで詳細について調べることができます。
- AMC で他の構成変更を保留している状態で、構成をインポートすると、保留中の変更が上書きされてしまいます。
- 古い Secure Mobile Access アプライアンスからポリシーをインポートできます。ただし古いアプライアンスのバージョンが、新しいアプライアンスより 3 バージョン以上下まわることはできません。例えば、11.4 より前のバージョンのポリシー構成を 12.1 のアプライアンスにインポートすることはできません。
- 構成を単一ノードからハイアベイラビリティ クラスタへインポートすることはできません。またクラスタ構成から単一ノードへインポートすることもできません。

アプライアンスに保管された構成データのリストアまたはエクスポート

アプライアンスに保管されている構成ファイルをリストアする場合は、以下の手順を実行します。(アプライアンスではなくローカル マシンに保管された構成データを指定する場合はインポート機能を使用します。詳細については、構成データのインポートを参照してください)。リストアできるのは構成データ全体のみです。構成を部分的にリストアすることはできません。

アプライアンスに保管されている構成データをリストアまたはエクスポートするには、

1 メイン ナビゲーション ページから、[**Maintenance (メンテナンス)**] をクリックします。

2 「**System Configuration (システム設定)**」エリアで、「**Import/Export (インポート/エクスポート)**」をクリックします。

3 [**Saved Configurations (保存済みの構成)**] リストから構成データを選択します。

4 構成データをリストアするか、ローカル マシンにエクスポートします。

- [**Restore (復旧)**] をクリックします。選択した構成のリストアがすぐに始まります。リストアが終わったら、[**Pending changes (保留中の変更)**] をクリックして、新しい構成を適用します。リストアされた構成はリストにそのまま残されます。
- 構成のコピーをローカル マシンに保存するときは、[**Export (エクスポート)**] をクリックします。

システムのアップグレード、リセット、またはロールバック

SonicWall では、サーバーに新しい機能を追加したり既存の問題に対応したりする目的で、ソフトウェア アップデートを定期的に提供します。アップデートは圧縮済みの `.bin` ファイルで提供され、次の形式になります。

- *ホットフィックス*は、アプライアンス ソフトウェアの特定バージョンに存在する問題に対応するもので、通常は、元のバージョンから変更されたファイルのみが含まれます。
- *Upgrade (アップグレード)* は、新しいバージョンのソフトウェアです (アプライアンスのバージョン番号が増加します)。

アップグレードのインストールや前バージョンへのロールバックは、AMC を使用します。

システムの現在のバージョンを表示するときは、メイン ナビゲーション メニューから [**System Status (システム状況)**] または [**Maintenance (メンテナンス)**] をクリックします。ホットフィックスが適用されている場合は、[**hotfixes (ホットフィックス)**] リンクをクリックすることで、リストを参照できます。

トピック:

- システムのアップデート
- 前のバージョンへのロール バック
- アプライアンスのリセット

システムのアップデート

MySonicWall Web サイトで、システムのアップデート (ホットフィックスとアップグレード) を見つけることができます。www.mysonicwall.com にアクセスするには、MySonicWall アカウントを作成するの説明に従って、最初にアカウントを作成する必要があります。アカウントを作成したら、新しいシステム アップデートとドキュメントが Web サイトの [**Download Center (ダウンロード センター)**] で入手できるようになります。

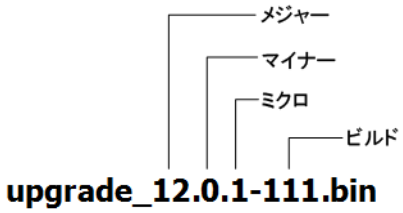
トピック:

- アップグレードの命名規則
- ホットフィックスの命名規則
- システム アップデートのインストール

アップグレードの命名規則

SonicWall では、アップグレードの命名規則 で説明された構文を使用して、アップグレード ファイルのバージョン番号が記述されます。

```
upgrade-<major>.<minor>.<micro>-<build>.bin
```



メモ：適用されているホットフィックスを確認するには、メイン ナビゲーション メニューから [**System Status (システム状況)**] または [**Maintenance (メンテナンス)**] をクリックします。

AMC (すべての AMC ページの左下隅に表示) およびクライアント ソフトウェアのバージョン番号も、同様のパターンを踏襲しています。

```
<major>.<minor>-<micro>-<build>
```

アップグレードの命名規則

名前	説明
major	メジャー リリース番号。この番号のみが存在する場合、このリリースには、重要な新しい機能とバグ フィックスが含まれていることになります。また同時に、システム全体のフル イメージが含まれていることになります。
minor	マイナー リリース番号。このアップデートのマイナー リリース番号。バージョン番号にメジャー番号とマイナー番号のみが含まれている場合、このリリースには、追加機能とバグ フィックスが含まれていることになります。また同時に、システム全体のフル イメージが含まれていることになります。
micro	マイクロ リリース番号。バージョン番号にメジャー番号、マイナー番号、マイクロ番号が含まれている場合、このリリースには、ごくわずかの追加機能とバグ フィックスが含まれていることになります。また同時に、システム全体のフル イメージが含まれていることになります。
build	SonicWall で使用される内部ビルド番号。すべてのリリースにはビルド番号が含まれます。

ホットフィックスの命名規則

SonicWall では、リリースとリリースの間に、SMA アプライアンス上のソフトウェア ファイルの一部を置換するホットフィックスを発表することがあります。修正プログラムのファイル名は、次の命名規則を使用します。

```
<component>-hotfix-<version>-<hotfix number>
```

ホットフィックスの命名規則は *<component>* を定義します。

ホットフィックスの命名規則

コンポーネント	説明
Pform	アプライアンス管理コンソール
clt	クライアント ソフトウェア

メモ：どのホットフィックスが適用されているか確認するには、メイン ナビゲーション メニューから [**System Status (システム状況)**] または [**Maintenance (メンテナンス)**] をクリックします。ホットフィックスが適用されている場合には、バージョン番号の横の [**hotfixes (ホットフィックス)**] リンクが表示されます。このリンクをクリックすると、適用されているホットフィックスの詳細が表示されます。

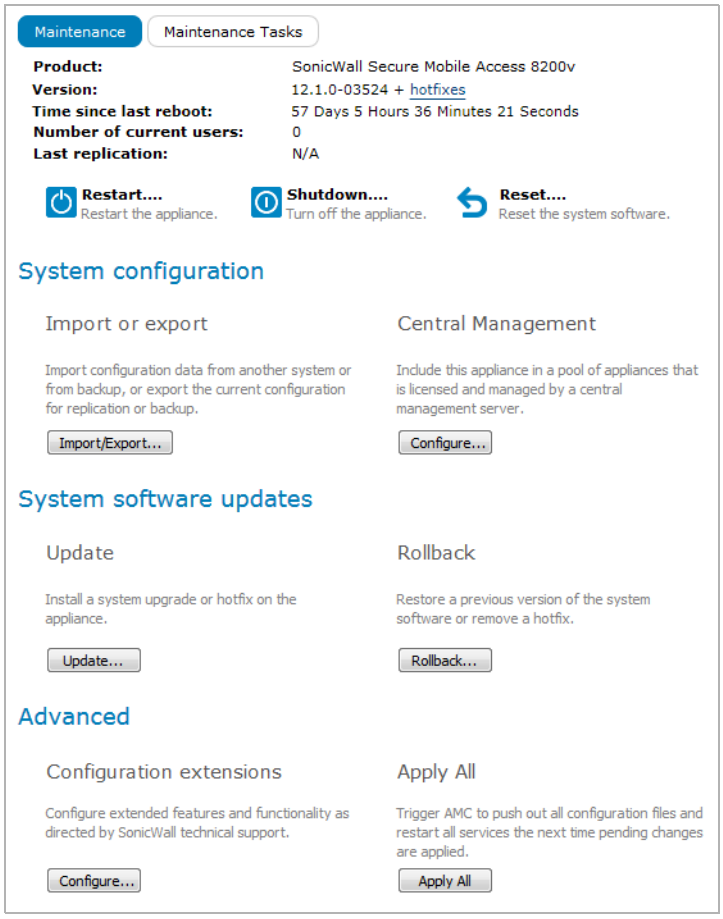
例えば、`Pform-hotfix-12.1.1,1-279` は、アプライアンス管理コンソールの問題を修正するバージョン 12.1 のホットフィックス 001 です。

システム アップデートのインストール

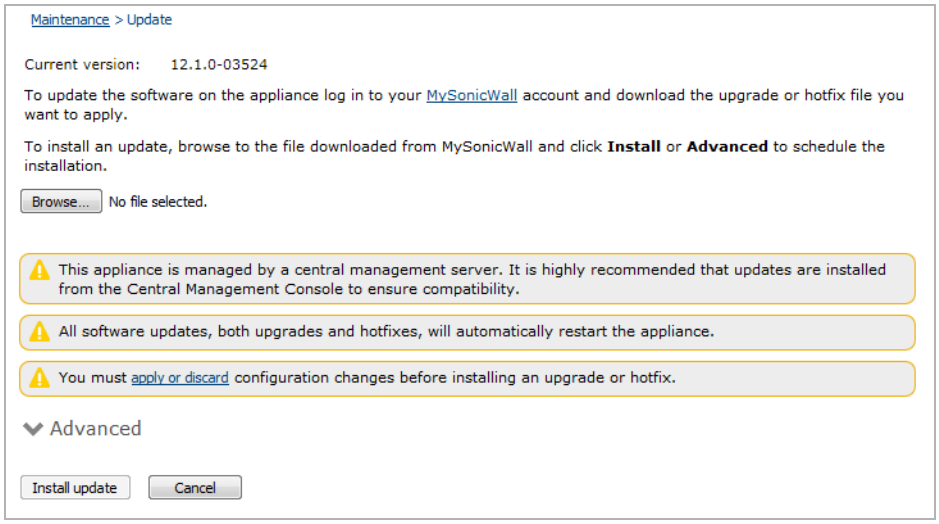
バージョン アップグレードおよびホットフィックスを手動または決められた日時に自動的にインストールする場合は、AMC を使用できます。

システム アップデートおよびホットフィックスを手動でダウンロードしてインストールするには

1 AMC のメイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Maintenance (メンテナンス)**] をクリックします。



2 [**System software updates (システム ソフトウェアの更新)**] エリアで、[**Update (更新)**] をクリックします。



3 アップグレードまたはホットフィックスファイルをまだダウンロードしていない場合は、Web サイトのリンクをクリックして、www.mysonicwall.com から対応するファイルをローカル ファイル システムにダウンロードします。

4 アップデート ファイルのパスを入力するか、[**Browse (参照)**] をクリックして、適切なファイルをブラウズします。

5 「**Install Update (更新のインストール)**」を選択します。ファイル アップロード ステータス インジケータが表示されます。必要であれば、[**Cancel (キャンセル)**] をクリックしてアップロード プロセスを停止できます。

ファイル アップロード プロセスが完了したら、アップデートがアプライアンスに自動的にインストールされます。インストール プロセスはキャンセルできません。インストール プロセスが完了したら、アプライアンスが自動的に再起動します。

6 アプライアンスが再起動したら、AMC にログインして、AMC ホーム ページの左下隅に表示されている新しいバージョン番号を確認します。

メモ：アップグレード ファイルが不正または破損しているというエラー メッセージが表示されたら、ダウンロード済みのアップグレード ファイルの確認の手順に従って、ファイルのチェックサムが正しいか確認してください。

前のバージョンへのロール バック

AMC からも、システムにインストールした最新のアップデートを取り消すことができます。アップデートの完了後、問題が発生した場合は、この機能を使用して、問題がなかった状態までロールバックできます。ソフトウェア イメージのロールバックを行うたびに、最新のシステム アップデートが削除されます。

注意：システムをアップデートした後なんらかの構成変更を行っている場合、ソフトウェア イメージを前にバージョンにリストアすると、このような構成変更も消去されます。一方で、ホットフィックスを削除するときには、構成変更は保存されます。

前のバージョンにロール バックするには、以下の手順に従います。

1 AMC のメイン ナビゲーション メニューから、「**Maintenance (メンテナンス)**」をクリックします。

2 [**System configuration (システムの設定)**] エリアで [**Rollback (ロールバック)**] をクリックします。

3 [**Rollback (ロールバック)**] ページに表示されているバージョンにロールバックするときは [**OK**] をクリックします。ロールバック プロセスが完了すると、装置が自動的に再起動され、変更が適用されます。

4 装置の再起動後、AMC ホーム ページの左下隅で新しいバージョン番号を確認します。

アプライアンスのリセット

AMC から、3 つのリセット レベルのいずれかを使用してアプライアンスをリセットできます。最も簡易なリセット レベルでは、構成情報、ログ ファイル、現在のファームウェアが消去されますが、前のバージョンにロールバックするオプションを利用できます (前のバージョンがロードされている場合)。

2 番目のレベルでは、すべての構成、ログ ファイル、およびファームウェアがアプライアンスから削除されます。このオプションでは、前のバージョンにはロールバックできません。

3 番目のレベルでも、すべての構成、ログ ファイル、およびファームウェアが削除され、ハード ドライブが安全な方法で消去されます。この操作には最大で 45 分かかる場合があります。このオプションを選択する場合、前のバージョンにはロールバックできません。

次のようにリセットが必要となるシナリオがいくつかあります。

- マシンを完全にきれいな状態にして、別の場所で再利用したい場合。
- アプライアンスが、取り返しの付かない状態になった場合。この場合は、SonicWall のテクニカル サポートにお問い合わせいただき、他に問題を解決する方法がないかを確認してください。アプライアンスを稼働できる状態に復旧するための最後の手段として、リセットは使用する必要があります。

リセットの後にアプライアンスを構成するには、LCD パネルまたはシリアル コンソールを使用する必要があります。

アプライアンスをリセットするには、

1 アプライアンスの構成データをバックアップします。次でこれを行うことができます:
   - AMC 内 (ローカル マシンへの現在の構成のエクスポート を参照)。
   - バックアップツールを使用 (構成データの保存 を参照)。
2 AMC のメイン ナビゲーション メニューから、「**Maintenance (メンテナンス)**」をクリックします。
3 ページの上の部分で、[**Reset (リセット)**] をクリックします。
4 **Maintenance (メンテナンス) > Reset (リセット)**ページで、[**Reset Options (オプションのリセット)**] の下にある次の 3 つのラジオ ボタンのいずれかを選択します。
   - [**Reset the current configuration (現在の構成をリセットする)**] - このオプションによって現在の構成が消去されます。前のバージョンからアップグレードしている場合、このオプションを選択すると、前のバージョンにロールバックできます。
   - [**Reset the entire appliance (アプライアンス全体をリセットする)**] - このオプションによって、構成が消去され、アプライアンスのすべてのファームウェア バージョンが削除されます。このオプションを選択する場合、前のバージョンにはロールバックできません。
   - [**Securely erase the hard drive and reset the entire appliance (ハード ドライブを安全に消去し、アプライアンス全体をリセットする)**] - このオプションによって、構成が消去され、すべてのファームウェア バージョンが削除され、ハード ドライブが安全に消去されます。このオプションを選択する場合、前のバージョンにはロールバックできません。

     メモ：ハード ドライブを安全に消去するには、最大で 45 分ほどかかります。
5 このページの下にある [**Reset (リセット)**] をクリックして、リセット操作を続行します。リセットをキャンセルするには、[**Cancel (キャンセル)**] をクリックします。

異なるバージョンのファームウェアを使用してアプライアンスをリセットするには:

メモ：ファームウェアのダウングレード機能の目的は、アプライアンスを別のベース ファームウェア バージョンに「ダウングレード」することです。したがって、既存の設定を移行したり、アプライアンスからデータやファイルを保存したりは**しません**。完全に新しいファームウェア ベースへの完全な工場出荷状態へのリセットと同じです。アプライアンスに保存されているすべてのファイルと設定は完全に上書きされ、アプライアンスは工場出荷時の既定値に設定されます。

ファームウェアのダウングレードの詳細および手順については、
https://www.sonicwall.com/ja-jp/support/knowledge-base/170502558229507 を参照してください。

SSL 暗号化

アプライアンス上のすべてのトラフィックでデータのセキュリティを保証するため、暗号が使用されます。アプライアンスは SSL で使用するすべてのデータを暗号化します。ネットワーク トラフィックを SSL で保護するには、最低でも 1 つの暗号を使用するよう構成しなければなりません。セキュリティ効果とパフォーマンスのバランスをよく考え、使用可能なものの中から「最上の」暗号を選択します (パフォーマンスよりセキュリティに重点を置くことが必要です)。

SSL では軽度の攻撃についてある程度保護できますが、一般的には、ユーザーの必要性に合った強力な暗号を許可するようサーバーを構成する必要があります。暗号には次のようなものがあります。最も優れたものから順に並んでいます。

- AES 256 ビット (SHA-256 付き)
- AES 128 ビット (SHA-256 付き)
- AES 256 ビット (SHA-1 付き)
- AES 128 ビット (SHA-1 付き)
- トリプル DES、SHA-1

メモ：AMC は、選択された暗号に関係なく、SSL ハンドシェークに常に AES 256 ビット SHA256 暗号を使用しているように見えることがあります。ただし、AMC は実際に選択されている暗号にかかわらず、SSL ハンドシェイクに最高の安全な暗号を使用します。

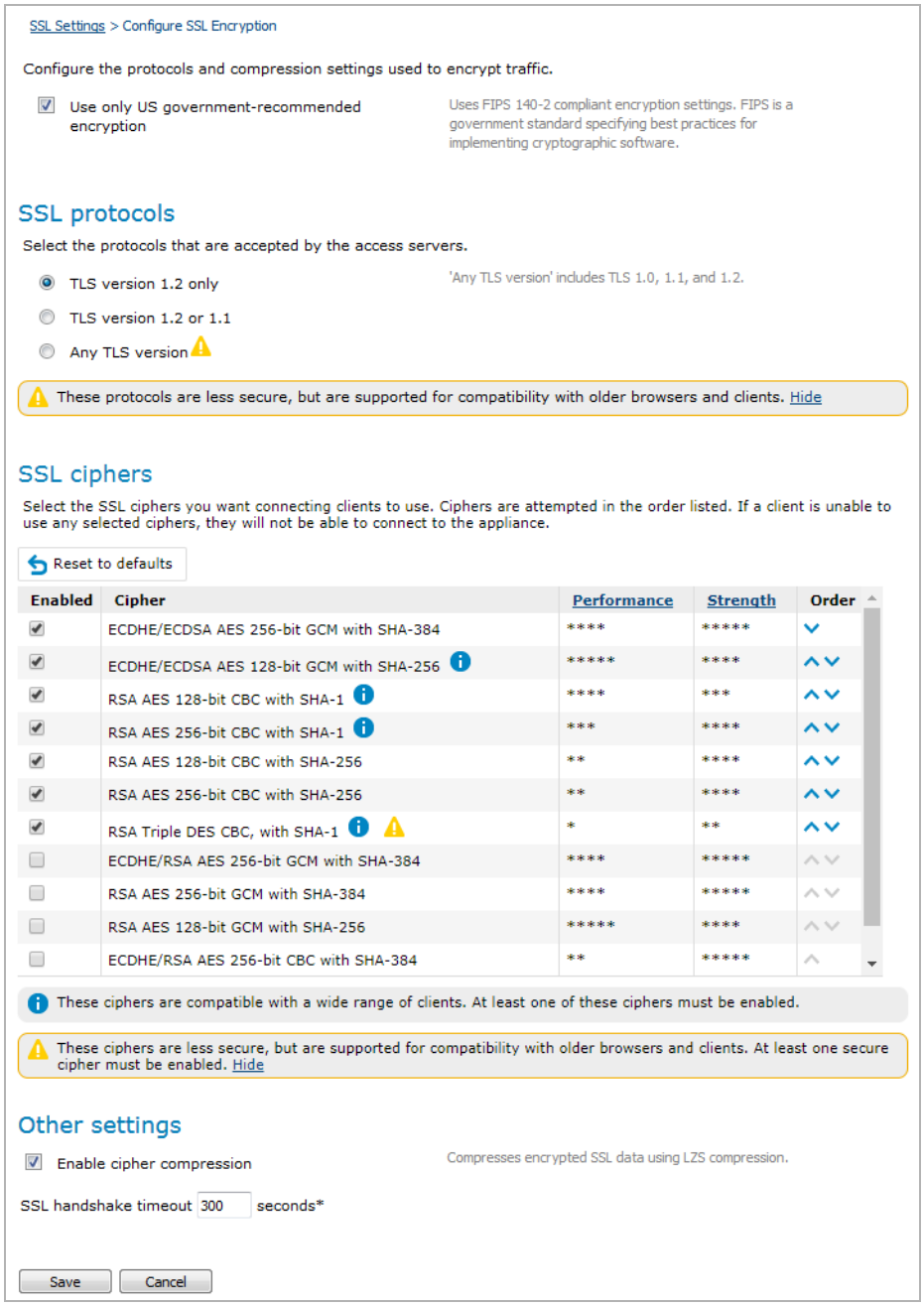
SSL 暗号化の構成

このアプライアンスでは、SSL 暗号化などの暗号アルゴリズム (つまり暗号) を使用して、データ転送を保護します。アプライアンスの暗号化設定を構成するときは、ネットワーク トラフィックを保護するため、最低でも 1 つの暗号を SSL と組み合わせて使用できるようにします。通常、ほとんどのインストールの場合、デフォルト設定で間に合います。

SSL 暗号化設定を構成するには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**SSL Settings (SSL 設定)**] をクリックします。

2 [**SSL encryption (SSL 暗号化)**] エリアの [**Edit (編集)**] リンクをクリックします。[**Configure SSL Encryption (SSL 暗号化の構成)**] ページが表示されます。



3 [Use only government-recommended encryption (政府推奨の暗号化のみを使用)] チェックボックスを選択して、FIPS 140-2 と互換性のある暗号化設定を有効にします。これにより、TLS プロトコルのみを使用して FIPS 互換の暗号だけを有効にするようにアプライアンスが構成されます。

このオプションは、SSL および CA 証明書が TLS 1.0 からアップグレードされていないときに、TLS 1.1 および 1.2 と対応する証明書通知を無効にするために使用されることが多くあります。

4 FIPS 140-2 互換の暗号化を有効にするには、トラフィックを暗号化するために使用する転送プロトコルをチェックします。これにより、TLS プロトコルのみを使用して FIPS 互換の暗号だけを有効にするようにアプライアンスが構成されます。

5 アプライアンスが使用する TLS 転送プロトコルのバージョンを選択します。

6 アプライアンスのアクセス サービス (Web プロキシ、ネットワーク プロキシ、およびネットワーク トンネル) が SSL 接続を受け入れる暗号を選択します。

7 LXS 圧縮を使用して暗号化された SSL データを圧縮するには、[**Enable cipher compression (暗号圧縮を有効化)**] チェックボックスを選択します。

8 [**SSL handshake timeout (SSL ハンドシェークのタイムアウト)**] ボックスで、SSL ハンドシェークがタイムアウトするまでの秒数を入力します。デフォルトは **300** です。

9 [**Save (保存)**] を選択します。

FIPS 認定

このセクションでは、FIPS モードを使用するように SMA アプライアンスを構成する方法について説明します。

FIPS (Federal Information Processing Standard) 140-2 Level 2 は、暗号モジュールを評価するための検証標準であり、暗号セキュリティ製品に関するソース コード、アルゴリズム、物理的なセキュリティ、および運用テストが含まれます。米国連邦政府は、FIPS 140-2 標準に対して検証を受けている暗号製品を購入することを求めています。国際的な市場では、ISO19790 が標準として採用されていますが、これは FIPS 140-2 と同じものです。

SonicWall E-Class SMA EX9000、EX7000、EX6000、SMA 7200、および SMA 6200 アプライアンスは FIPS 140-2 Level 2 認定を NIST (National Institute of Standards and Technology、United States FIPS 140-2 Cryptographic Module Validation Authority) と CSE (Communications Security Establishment、Canadian FIPS 140-2 Cryptographic Module Authority) から受けています。

メモ：バージョン 10.7.2 以降は FIPS 認定を受けています。

FIPS モードは、エンド ユーザーに透過的となっています。内部的には、FIPS モードによって、安全な通信とシステムの整合性が強制されます。

トピック:

- FIPS の要件
- FIPS 互換の証明書の管理
- FIPS の違反
- FIPS の有効化
- FIPS 互換の証明書のエクスポートとインポート
- FIPS の無効化
- 秘密情報の消去

FIPS の要件

次の項目は、完全準拠の FIPS を適切に構成するために必要です。

- EX9000、EX7000、EX6000、SMA 7200、またはSMA 6200 アプライアンス。その他のアプライアンスは、FIPS の認定を受けていません。

注意：140-2 Level 2 FIPS 認定を受けた EX9000、EX7000、EX6000、SMA 7200、または SMA 6200 アプライアンスを購入している場合は、改変防止のスティッカーがそのまま張り付けられたままになっている必要があります。

- FIPS を実行するライセンス
- 認証サーバーへの安全な接続
- 少なくとも 14 文字以上で、句読文字、数字、および大文字と小文字からなる文字が含まれる強力な管理者パスワード。さらに、レルムをセットアップするときに認証サーバーを指定する必要があります。「`null auth`」は許可されません。
- FIPS モードの場合、Grub シェルへユーザーが不正にアクセスできないように、Grub シェルを無効する必要があります。

注意：Grub 構成ファイルの変更は許可されません。変更すると、デバイスが FIPS 互換ではなくなり、デバイスが稼働しなくなります。

次の状態になっていると、FIPS を有効または完全互換にできません。

- 認証サーバーとの安全ではない接続
- RADIUS 認証サーバーの使用
- FIPS で承認されていない暗号を使用する SSL 接続を使用する LDAP 認証サーバーの使用
- FIPS で承認されていない暗号を使用する SSL 接続を使用する Active Directory 単一ドメイン認証サーバーの使用
- FIPS で承認されていない暗号を使用する SSL 接続を使用する RSA ClearTrust 認証サーバーの使用
- 共有シークレットとして強力なパスワードを使用しない RSA Authentication Manager 認証サーバーの使用
- 任意の目的での USB デバイスの使用
- シェル コマンドラインからのカーネル モジュールのロードまたはアンロード
- シェル コマンドラインからのサードパーティ ソフトウェアのインストール
- シェル コマンドラインからのファームウェア アップグレード
- デバッグ 1、デバッグ 2、デバッグ 3 またはテキスト形式のロギングの使用
- FIPS と互換性のないシステムによって生成されるプライベート/パブリックのキー ペアがある証明書の使用
- 秘密情報の消去手順の使用 (手順が完了するまで、物理的に存在しているプライマリ管理者がいない)、秘密情報の消去 を参照

FIPS モードは、ライセンスをインポートした後に自動的に有効にはなりません。FIPS の有効化 の説明に従ってセットアップする必要があります。

FIPS 互換の証明書の管理

FIPS モードで実行している EX9000、EX7000、EX6000、SMA 7200、または SMA 6200 アプライアンスで生成される鍵は、FIPS 互換になります。証明書 (および関連するパブリック キーとプライベート キー) をアプライアンスにインポートする場合、ユーザーが責任を持って、これらも FIPS 互換であることを確認する必要があります。FIPS モードをオンまたはオフにするときには、証明書はエクスポートして、再インポートする必要があります。エクスポートとインポートの手順については、FIPS 互換の証明書のエクスポートとインポートを参照してください。

使用している証明書が FIPS 互換であることを確認する最良の方法は、FIPS が有効なアプライアンスですべての CSR (証明書署名要求) を生成することです。

FIPS の違反

アプライアンスの整合性はいくつかの方法で検証できます。

- すべての FIPS 認定の暗号アルゴリズムが正しく稼働していることを検証するために、セルフテストが各パワーオン サイクルの段階で実行されます。いずれかのセルフ テストが失敗する場合、前面パネルの **Alarm LED (アラーム LED)** は点灯したままになります。特定のエラーの詳細を説明するメッセージが、シリアル コンソールに表示され、`/var/log/aventail/fips.log` に記録され、アプライアンスは停止します。復旧したかどうかを確認するためには、アプライアンスを一度パワーサイクルする必要があります。復旧していない場合、SonicWall のカスタマ サポートにお問い合わせいただき、詳細な指示を得る必要があります。
- 連続するセルフ テストが乱数生成器および新しい認証鍵の生成時に実行され、暗号操作の整合性が検証されます。これらのセルフ テストが失敗する場合、特定のエラーの詳細を示すメッセージがシリアル コンソールに表示され、`/var/log/aventail/fips.log` に記録され、システムの整合性を確認するための厳格なセルフ テストを実施するために、アプライアンスは再起動され直ちにパワーサイクルされます。
- 最重要のすべてのセキュリティ バイナリが署名されハッシュされます。これらのバイナリへの改変は、実行中のシステムの各再起動時に直ちに検出されます。パワーサイクル テストでこの問題が発生する場合、前面パネルの **Alarm LED (アラーム LED)** は点灯したままになります。特定の改変の詳細を説明するメッセージが、シリアル コンソールに表示され、`/var/log/aventail/fips.log` に記録され、システムは停止します。この場合は、SonicWall カスタマ サポートにお問い合わせいただき、詳細な指示を得る必要があります。実行中のシステムでこの改変が検出されると、システムの整合性を検証する厳格なセルフ テストを実行するために、アプライアンスは直ちに再起動してパワーサイクルされます。
- 最重要のすべてのセキュリティ構成ファイルが署名されハッシュされます。構成ファイルのいずれかを手動で変更すると (AMC を使用して変更するのではなく)、アプライアンスが直ちにエラー状態に移行します。実行中のシステムでこの改変が検出されると、システムの整合性を検証する厳格なセルフ テストを実行するために、アプライアンスは直ちに再起動してパワーサイクルされます。また、パワーサイクル セルフテスト中に改変が検出された場合、特定の改変の詳細を示すメッセージがシリアル コンソールに表示され、`/var/log/aventail/fips.log` に記録されます。前面パネルの **Test LED (テスト LED)** が点灯したままになり、システムのネットワークが無効になりシングル ユーザー モードになります。プライマリ管理者が、シリアル コンソール経由でログインして、有効なバックアップ コピーを使用して改変されたファイルをリストアするか、アプライアンスをパワーサイクルする前に構成リセットを実行します。
- ファームウェア アップグレード ファイルは署名されハッシュされます。アップグレード ファイルの整合性チェックに失敗する場合、アプライアンスの状態は変更せずに、アップグレード プロセスは中断されます。エラーの詳細を示すメッセージが AMC Web ページに表示され、アプライアンスは完全に機能した状態のままになります。

FIPS の有効化

FIPS モードを有効にする前に、強力なパスワード、認証サーバーへの安全な接続、および有効なライセンスが必要となります。

ソフトウェア ライセンスの説明に従って FIPS ライセンスを取得します。

FIPS 互換にするためには、パスワードの長さを少なくとも 8 文字以上にする必要がありますが、少なくとも 14 文字を使用することを推奨します。この要件はソフトウェアによって強制されませんが、強度の低い管理者パスワードにすると攻撃に対して脆弱なままになります。強力なパスワードにするには、文字、数字、および記号を含めます。これは単なるパスワードではなく、フレーズとして考え

ます。例えば、「I never saw @ purple cow, I never hope 2C1.」には、これら 3 つのすべての文字の組み合わせがあります。

システム権限を持つ管理者だけが FIPS モードを変更できます。FIPS モードになっている場合、SSL と互換性のないアルゴリズムを選択することはできません。

FIPS モードで既存の FIPS 互換の証明書を使用するには、FIPS を有効にする前に証明書をエクスポートして、FIPS を有効にした後に再度インポートします。FIPS 互換の証明書のエクスポートとインポートを参照してください。

FIPS を有効にするには、

1 メイン ナビゲーション メニューで、[**General Settings (一般設定)**] をクリックし、[**FIPS Security (FIPS セキュリティ)**] をクリックします。

2 「**編集**」を選択します。

3 ライセンスをインポートしている場合には、[**Enable FIPS mode (FIPS モードを有効にする)**] チェック ボックスを選択します。

ⓘ **メモ：**既存の証明書は、次の手順でシステムから削除されます。FIPS 互換の証明書を保持するには、必ずエクスポートしておいてください。

4 [**Save (保存)**] をクリックして、保留中の変更を適用します。

△ **注意：FIPS モードに一度すると、システム構成ファイルを編集できなくなります。**

アプライアンスの構成が FIPS 互換ではない場合、**FIPS 互換に関する警告**を表示するアラート リンクが上右隅に表示されます。リンクをクリックすると、アプライアンスの構成を FIPS 互換にするための詳細を確認できます。

△ **注意：このアラートが表示されていない場合でも、ユーザーの環境が FIPS 互換であることを意味しません。FIPS 互換にするためには、ユーザーが責任を持ってすべての FIPS 前提条件を確認してください。**

FIPS 互換の証明書のエクスポートとインポート

既存の証明書鍵が FIPS 互換のシステムで生成されていることが分かっており、FIPS が有効化された後にこの証明書鍵を使用する場合には、この証明書鍵を FIPS を有効にする前にエクスポートして、FIPS が有効化された後にインポートする必要する必要があります。

同じように、システムで FIPS モードを無効にする計画があり、FIPS を無効にした後で FIPS 互換の証明書を使用するには、FIPS を無効化する前に証明書をエクスポートして FIPS を無効にした後でインポートする必要があります。

FIPS モードに移行する前に証明書をエクスポートするには、

1 AMC で、**SSL Setting (SSL設定) > SSL Certificates (SSL 証明書)** に移動します。

2 エクスポートする各証明書について、次の操作を実行します。

a [**Certificates (証明書)**] の表で、証明書を選択して [**Export (エクスポート)**] ボタンをクリックします。

b エクスポートされる .p12 ファイルを暗号化するためのパスワードを入力します。

c [**Save (保存)**] ボタンをクリックします。

FIPS モードに移行した後に証明書をインポートするには、

1 AMC で、**SSL Settings (SSL設定) > SSL Certificates (SSL 証明書)** に移動します。

2 インポートする各証明書について、次の操作を実行します。

a [**Certificates (証明書)**] の表で、**New (新規) > Import certificate... (証明書のインポート...)** を選択します。

b インポートする証明書ファイルを選択します。

c `.p12` ファイルを暗号化したときに使用したパスワードを入力します。

d 「**インポート**」ボタンを選択します。

FIPS の無効化

FIPS をオフにすると、FIPS の機能が無効になり、FIPS モードの前提条件によって強制されるすべての制約が取り除かれます。

△ 注意：**警告: 完全に FIPS 互換にするためには、FIPS の重要なセキュリティ パラメータを FIPS で承認される操作モード以外で使用することはできません。これらのパラメータのいくつかは、ファームウェア自身に焼き付けられているため、完全互換にするためには、秘密情報の消去を実行する必要があります。秘密情報消去のためにハードウェアを SonicWall に返却するのではなく、システムの使用を継続したい場合には、秘密情報消去の手順を意図的に省略して、FIPS モードを AMC で無効にできます。これによって、論理的にはすべての構成可能なパラメータが破壊されます。**

FIPS モードを無効にした後で既存の FIPS 互換の証明書を使用するには、FIPS を無効にする前に証明書をエクスポートして、FIPS を無効にした後に再度インポートします。FIPS 互換の証明書のエクスポートとインポートを参照してください。

FIPS を無効にするには、

1 メイン ナビゲーション メニューで、[**General Settings (一般設定)**] をクリックし、[**FIPS Security (FIPS セキュリティ)**] をクリックします。

2 「**編集**」を選択します。

3 [**Enable FIPS mode (FIPS モードを有効にする)**] の横のボックスをクリアします。

ⓘ **重要**：既存の証明書は、次の手順でシステムから削除されます。FIPS 互換の証明書を保持するには、必ずエクスポートしておいてください。

4 [**Save (保存)**] をクリックして、**保留中の変更**を適用します。

△ 注意：**アプライアンスが再起動して、これらの変更が適用されます。すべての接続は終了します。**

秘密情報の消去

*秘密情報の消去*は、重要なすべてのセキュリティ パラメータを永久に破壊する操作です。これは、ディスク全体を完全に消去することで実行されます。秘密情報の消去により、アプライアンスから機密情報を取得することが極めて困難になります。ハードウェアをリサイクルする前や、データの保持よりもデータのセキュリティが重要となるほかの場合に、この操作を実行します。この操作が完了すると、アプライアンスはユーザー環境では使用することはできなくなります。サービスをリストアするためには、SonicWall にアプライアンスを返却して、ハードウェアを交換する必要があります。

アプライアンスの秘密情報を消去するには、

1 管理コンソールのメイン ナビゲーション ペインから [**Maintenance (メンテナンス)**] を選択します。

2 [**Reset (リセット)**] を選択します。

3 [**Reset (リセット)**] ページで、アプライアンスをリセットするには、の説明にあるように実行するリセットのタイプを選択します。

4 リセット操作が開始したら、アプライアンスが停止するまで、アプライアンスの前で物理的に待機してください。

△ **注意：アプライアンスが、秘密情報の消去プロセスを完了するまでには最大で 45 分かかる場合があります。**

ソフトウェア ライセンス

このセクションでは、アプライアンス コンポーネントのソフトウェア ライセンスを管理する方法について説明します。SMA アプライアンスのライセンスには、異なる種類があります。

- **管理テスト ライセンス:** SMA アプライアンスを受け取ったら、MySonicWall にログインして、初期のユーザー ライセンスを取得する必要があります。このライセンスは無期限で 1 ユーザー (管理者と 1 人のエンド ユーザー) が利用できます。このライセンスを使用して、AMC の操作に習熟できます。また、ユーザー数やその他のコンポーネントを追加するためのアプライアンス ライセンス ファイルをアップロードするために使用できます。
- **アプライアンス ライセンス:** このアプライアンスは、同時実行ユーザー数を監視および強制するために使用されます。アクティブな同時実行ユーザー数の上限を超過すると、アクティブなユーザー数がライセンスされているユーザー数の上限を下回るまで、ユーザー アクセスが制限されます。

  SMA アプライアンスによる同時ユーザー サポートは、SMA アプライアンスによる同時ユーザー サポート に示されています。

  SMA アプライアンスによる同時ユーザー サポート

装置	サポートされる最大同時ユーザー数
EX9000	20,000
EX7000	5,000
SMA-8200v	5,000
SMA-7200	10,000
SMA-6200	2,000

  しかし、ライセンス契約によっては、特定のユーザー セッション数までこの上限を超過することが許可される場合があります。この場合には、ユーザー アクセスは許可されますが、超過した利用について記録されます。

  ユーザー アクセスが制限されると、VPN へのログインを試行するユーザーには、ライセンスの上限数を超過している可能性があることを示すエラー メッセージが表示され、ネットワークへのアクセスが拒否されます。
- **コンポーネント ライセンス:** アプライアンスのコンポーネントのライセンスが失効している場合、このコンポーネントの使用を試行するユーザーには、WorkPlace でエラー メッセージが表

示されます。Spike ライセンスの場合には、残り日数と、このライセンスで対応可能なユーザー数が AMC に表示されます。

- **プールされたライセンス**: プールされたライセンス モデルにより、管理対象アプライアンス間で中央ユーザ ライセンスを共有できるため、中央ユーザ ライセンスが CMS またはいずれかのアプライアンスの障害 (または通信損失) への耐性ができます。詳細については、*SMA 12.1 CMS 管理ガイド* の「Central User Licensing (中央ユーザー ライセンス)」を参照してください。

ライセンスの管理の説明に従って、すべてのライセンス ファイルを www.mysonicwall.com から取得して、アプライアンスにインポートする必要があります。

トピック:

- ライセンスの計算方法
- ライセンス詳細の表示
- ライセンスの管理

ライセンスの計算方法

アプライアンスのユーザー ライセンスは、ユーザーではなく、ユーザー認証が単位となります。例えば、ユーザーがデスクトップ コンピュータで WorkPlace にログインし、モバイル デバイスからもログインする場合、ユーザーがアプライアンスによって保護されているリソースにアクセスするとすぐに、2 つのライセンスが消費されます。

接続が 15 分間アクティブではない状態が継続すると、ライセンスは解放されます。アクティブではない時間の計算方法は、ユーザーのアクセス方法によって異なります。

- 変換、カスタム ポート マッピング、またはカスタム FQDN マッピング Web アクセスの場合には、リソースがアクセスされなくなってから 15 分後にライセンスが解放されます。
- Connect Tunnel が実行中の場合には、アプライアンスへの接続は開いたままになり、トンネルが稼働している限りはライセンスは使用中になります。トンネルが切断されると、15 分後にライセンスが解放されます。

セッションを制限または終了する方法はいくつかあります。

- ユーザーがコミュニティ ベースで利用できるライセンス数を制限します。上限に達すると、それ以上はアプライアンスのセッション (およびリソースへのアクセス) は許可されません。既存のすべてのセッションを終了しない限り、新しいセッションをユーザーは開始できません。[**Maximum active sessions (最大アクティブ セッション)**] 設定の説明については、を参照してください。コミュニティへのメンバーの割り当て
- [**Credential lifetime (クレデンシャル存続期間)**] ([**Configure General Appliance Options (一般装置オプションの設定)**] ページの) に設定されている期間に達したときに、コミュニティ ベースでトンネル クライアント セッションを終了する。[**Limit session length to credential lifetime (セッションの長さをクレデンシャルの有効期間に制限)**] 設定の説明については、ユーザー セッションの終了を参照してください。

- ユーザー セッションを手動で終了する。AMC でユーザー セッションを終了する方法については、ユーザー セッションの表示を参照してください。また、各セッション タイプの詳細については、オープン セッションとライセンスを消費するセッションの違いを参照してください。

メモ：アプライアンス ライセンスの上限に達したユーザーが、クライアント証明書のみを使用して認証を試行すると、既存のすべてのセッションを終了するように求められません。このようなユーザーがライセンスを開放して新しいセッションを開始するには、既存のセッションを終了する必要があります。セッションを終了するための最良の方法はログアウトすることです。そうしない場合は、セッションがタイムアウトしてライセンスが解放されるまで 15 分間待機する必要があります。

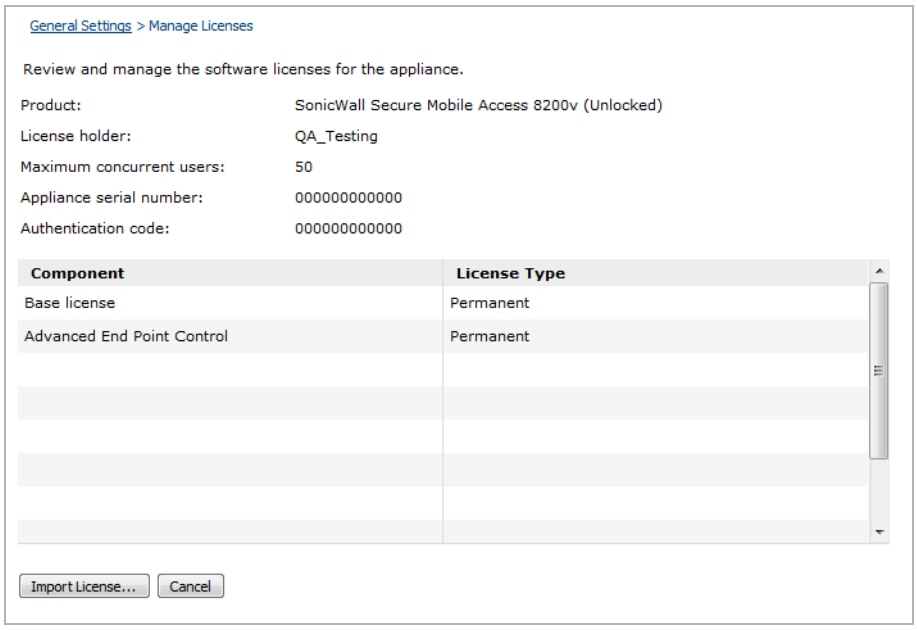
ライセンス詳細の表示

AMC では、ベース アプライアンス ライセンスと、OnDemand や Spike ライセンスなどの購入ししている可能性があるその他のアプライアンス コンポーネントのライセンスの状態を表示できます。このセクションでは、ライセンスの状態の詳細を表示する方法について説明します。

ライセンスの詳細を表示するには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**General Settings (一般設定)**] をクリックします。

2 [**Licensing (購読中)**] エリアの [**Edit (編集)**] リンクをクリックします。「**ライセンスの管理**」ページが表示されます。



3 ライセンス情報 に示すように、提供された情報を確認します。

ライセンス情報

ライセンスの情報	説明
製品	ライセンスが適用される SMA アプライアンスのタイプ。
[License holder]	アプライアンスのライセンスを受けているエンティティの名前。

ライセンス情報

ライセンスの情報	説明
最大同時実行ユーザー	ベース アプライアンス ライセンスによって許可される最大同時実行ユーザー セッションの数。同時実行ユーザーとは、1 つの IP アドレスからの 1 回のログインです。一度ログオフしたり、クレデンシャルが失効すると、ユーザーはカウントされません。 Spike ライセンスが有効な場合、許可されるユーザーの合計数、ライセンスの残り日数、および次の日が開始する時刻が表示されます。例えば、 `Spike license: 100 users, 60 days Active: Currently on day 2 of 60.Day 3 will begin at 10:15 PM on 9/23/09.` 必要に応じて Spike ライセンスを一時停止できます。詳細については、Spike ライセンスの管理を参照してください。
装置のシリアル番号	アプライアンスにインポートされたライセンス ファイルにあるシリアル番号。この番号は、AMC のメイン ナビゲーション メニューの下部に表示されます。シリアル番号は、テクニカル サポートに問い合わせるときに必要となります。
認証コード	これはアプライアンスのハードウェア ID です。www.mysonicwall.com から取得したライセンスは、この認証コードがあるアプライアンスでのみ有効になります。ライセンス ファイルの取得については、ライセンスの管理を参照してください。
コンポーネントとライセンス種別	個々のソフトウェア コンポーネント ライセンスの詳細。ライセンスが一時または評価ライセンスである場合は、失効日が表示されます。ライセンスの失効日が近づいている場合、またはライセンスが失効した場合、このエリアと AMC の状態エリアに警告メッセージが表示されます。

ライセンスの管理

このセクションでは、アプライアンスのライセンスを www.mysonicwall.com から入手する方法を説明します。例えば、アプライアンスを購入することを決定した後に評価ライセンスを永久ライセンスに置換する場合などは、ベース アプライアンス ライセンス ファイルが必要です。Connect および Spike ライセンスなど別途購入とライセンスが必要となるコンポーネントがいくつかあります。

別途購入またはライセンスが必要なアプライアンスやコンポーネントを有効にする前に、次の手順を実行しなければなりません。

1 MySonicWall アカウントを作成していない場合には、作成します。アプライアンスを登録するためのアカウントが必要です。(MySonicWall の登録情報は、売却されたり、他社と共有されることはありません。)詳細については、MySonicWall アカウントを作成するを参照してください。

2 装置を MySonicWall に登録します。登録すると、ライセンス ファイル、ファームウェア アップデート、テクニカル サポート情報などの重要なリソースにアクセスできます。詳細については、SMA アプライアンスの登録を参照してください。

3 MySonicWall アカウントを使用して、アプライアンスにライセンスを適用します。ハイアベイラビリティ クラスタ環境の場合、各アプライアンスに別々のライセンスを適用する必要があります。詳細については、Secure Mobile Access ライセンスの取得を参照してください。

4 AMC でライセンス ファイルを適用します。詳細については、SMA ライセンスの適用 を参照してください。

注意：ライセンス ファイルをインポートする前に、アプライアンスの日付と時刻の設定がタイムゾーンに合わせて正しく構成されていることをあらかじめ確認してください。システム クロック設定の構成の詳細については、時刻設定の構成を参照してください。

トピック:

- MySonicWall アカウントを作成する
- SMA アプライアンスの登録
- Secure Mobile Access ライセンスの取得
- SMA ライセンスの適用
- Spike ライセンスの管理

MySonicWall アカウントを作成する

MySonicWall アカウントを作成するには、簡単なオンラインの登録フォームに情報を入力します。登録情報が、別の企業に販売されたり共有されたりすることはありません。

MySonicWall アカウントを作成するには、以下の手順に従います。

1 Web ブラウザで、MySonicWall Web サイト https://www.mysonicwall.com/ にアクセスします。

2 [**User Login (ユーザ ログイン)**] セクションで、登録していないユーザーの方のためのリンクをクリックします。

3 アカウント情報、個人情報、各種の設定情報を入力して、[**Submit (適用)**] をクリックします。必ず有効な電子メール アドレスを使用してください。

4 画面の指示に従ってアカウントの作成を完了します。SonicWall により、ステップ 3 で入力した電子メール アドレスに購読コードが送信されます。

5 ログイン画面に戻ったら、新しいユーザ名とパスワードでログインを行います。

6 電子メールで受け取ったサブスクリプション コードを入力して、アカウントを確認します。

SMA アプライアンスの登録

登録すると、ライセンス ファイル、ファームウェアの更新、ドキュメント、テクニカル サポート情報などの必須のリソースにアクセスできます。

MySonicWall アカウントにログインして、アプライアンスを登録するには

1 Web ブラウザで MySonicWall Web サイト https://www.mysonicwall.com/ にアクセスして、ユーザー名とパスワードを入力してログインします。

2 ソフトウェア **シリアル番号**を確認します。シリアル番号は、SMA アプライアンスの背面に記載されています。

3 シリアル番号を入力し、[**Next (次へ)**] をクリックします。画面の指示に従います。

4 **シリアル番号**を確認します。

5 登録する装置の名前を入力します。

6 このアプライアンスの認証コードを入力します。これは、購入したアプライアンスのハードウェア ID に相当します。認証コードは AMC に表示されます。メイン ナビゲーション メニューの [**General Settings (一般設定)**] をクリックして、[**Licensing (購読中)**] エリアを確認します。

7 「**Register (登録)**」を選択して続行します。

オンライン プロンプトに従って、アンケートに情報を入力して、登録プロセスを完了させます。

Secure Mobile Access ライセンスの取得

アプライアンスのライセンス ファイルを取得するには、MySonicWall アカウントにログインします。ハイアベイラビリティ クラスタ環境の場合、各アプライアンスに別々のライセンスをダウンロードする必要があります。

装置のライセンス ファイルを取得するには、以下の手順に従います。

1 Web ブラウザで次の Web サイトにアクセスして、ユーザー名とパスワードを入力してログインします: https://www.mysonicwall.com/

2 ライセンスが必要なアプライアンスのリンクをクリックします。

3 [**Service Management (サービス管理)**] ページで、取得するライセンスのアプライアンス ソフトウェア バージョンをドロップダウン リストから選択します。

4 ライセンス ファイル (`.xml`) のリンクをクリックして、コンピュータに保存します。アプライアンスを稼働して実行したら、このライセンス ファイルを AMC を使用してインポートする必要があります。

SMA ライセンスの適用

SMA アプライアンスは、1 ユーザーを無期限でサポートする 1 つの管理テスト ライセンスが付属して出荷されています。これは、複数ユーザー環境でアプライアンスをテストおよび展開したり、Spike ライセンスなど別のコンポーネントを有効にしたりする場合は、有効なライセンス ファイルを適用する必要があります。MySonicWall アカウントにログインして、ライセンス ファイルを取得して、AMC でインポートします。

MySonicWall からライセンス ファイルを取得してインポートするには、

1 Web ブラウザで MySonicWall Web サイト https://www.mysonicwall.com/ にアクセスして、ユーザー名とパスワードを入力してログインします。

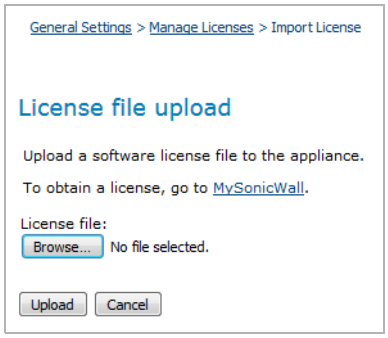
2 ライセンスが必要なアプライアンスのリンクをクリックします。

3 [**Service Management (サービス管理)**] ページで、取得するライセンスのアプライアンス ソフトウェア バージョンをドロップダウン メニューから選択します。

4 ライセンス ファイル (`.xml`) のリンクをクリックして、コンピュータに保存します。

5 AMC のメイン ナビゲーション メニューで、「**一般設定**」をクリックし、「**ライセンス**」領域の「**編集**」リンクをクリックします。「**ライセンスの管理**」ページが表示されます。

6 「**ライセンスのインポート**」をクリックします。



7 [**License file (ライセンス ファイル)**] フィールドで、ライセンス ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルを指定します。

8 「**アップロード**」をクリックし、右上隅にある「**保留中の変更**」リンクをクリックして変更内容を適用します。

Spike ライセンスの管理

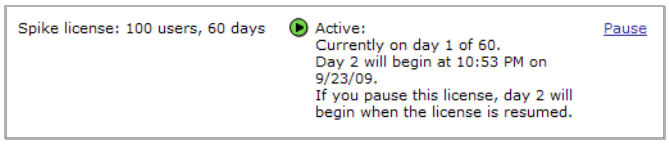
Spike License によって、災害発生時やその他のビジネス中断イベントが発生したときに、サポートできるリモート ユーザー数を一時的に増加させることができます。個別にライセンスされるこの機能は、予定された、または予定していないイベントの間、リモート アクセス トラフィックの増加に対応する手助けをします。

Spike ライセンスを購入いただくと、指定されたユーザー数および日数についてライセンスが有効になります (これは、Spike ライセンスを有効化したときにサポートされるユーザー数の合計であり、ベース ライセンス数への追加ではありません)。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。

Spike ライセンスを有効、一時停止、再開するには:

1 MySonicWall から Spike ライセンスを取得して、SMA ライセンスの適用で説明されているように、アプライアンスにインポートします。

2 Spike ライセンスが、AMC の [**Manage Licenses (ライセンスの管理)**] ページで**使用可能**と表示されます。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。対応が可能なユーザーの最大数が更新され、Spike ライセンスのタイムラインが表示されます。



3 [**Pause (停止)**] をクリックして、Spike ライセンスの使用を一時停止します。また、[**Resume (再開)**] をクリックして使用を再開できます。

メモ：

- アプライアンスには 1 つ以上の Spike ライセンスをアップロードできますが、有効にできるライセンスは 1 つのみです。
- Spike ライセンスを有効化または一時停止すると、毎回、24 時間が経過していなくても、有効な日数が 1 日分減ることになります。

第 6 部

アクセス制御

- エンド ポイント制御

8

エンド ポイント制御

End Point Control について

SMA アプライアンスでは、End Point Control がサポートされています。これによって、重要なデータを保護し、ネットワークが信頼されない環境のデバイスからアクセスを受けてもセキュリティが脅かされることがないように対応できます。End Point Control は、次のように機能します。

- ユーザーの環境が安全であることを確認
- セッション後、ユーザー データを PC から削除
- 重要なリソースへのアクセスを制御

従来の VPN ソリューションでは通常、企業のノート型 PC からの比較的安全なアクセスのみを許可しています。このような環境で、セキュリティ上大きな懸念になるのが、許可されていないネットワーク アクセスです。一方 SSL VPN は、信頼されていない環境のデバイスを含むあらゆる Web 対応システムからのアクセスを可能にします。空港やホテルのキオスク端末、従業員が所有する PC などからのアクセスにより、ネットワーク リソースに対する危険性は増大します。

End Point Control では、次の 3 つの方法で、信頼されていない環境からのアクセスを防止します。

- **ユーザーの環境が安全であることを確認** - 企業の IT 部門では、アンチウイルス ソフトウェアやファイアウォールや、その他の不正ソフトウェア (マルウェア) から保護するためのセーフガードを使用して、コンピュータを管理下に置いています。一方、管理されていないコンピュータの場合、キーストローク レコーダー、ウイルス、トロイの木馬など、ネットワークを危険に陥れる因子が簡単に入ってきます。

  Secure Mobile Access では、ユーザーのエンド ポイントで信頼レベルに応じて異なるアクセス レベルを割り当てる「信頼ゾーン」を定義できます。接続要求は AMC で設定されたデバイス プロファイルと比較され、適切なゾーンに割り当てられます。
- **セッション後、ユーザー データを PC から削除** - 重要なデータを、信頼されていない PC に不用意に残してしまう可能性があります。例えば、キオスク端末からログインしたユーザーは、ログアウトした後も、PC のキャッシュにパスワード、ブラウザのクッキー、ブックマークした URL などのさまざまなデータを残します。また、ファイルや電子メールの添付ファイルをハード ディスク上にうっかりと残してしまうこともあります。Secure Mobile Access のデータ保護エージェントは、PC からセッション データを自動的に削除します。
- **重要なリソースへのアクセスを制御** - End Point Control ゾーンは、アクセス制御ルールで参照できます。例えば、信頼性の低い EPC ゾーンから接続が試みられた場合は、重要なリソースへのアクセスを拒否できます。

End Point Control と OESIS

OESIS フレームワークは、インフラストラクチャに接続されたエンドポイントを保護および管理するために Secure Mobile Access 内で使用するクロスプラットフォームのソフトウェア開発キットです。Secure Mobile Access 12.1 では、OESIS フレームワークがバージョン 4 にアップグレードされました。これにより、コードをより高速に実行し、より頻繁に更新を行い、帯域外の定義を更新できるようになります。バージョン 11.4.x および 12.0.x を使用しているユーザは、これらの利点を活かすために 12.1 に更新してください。

新たに作成するプロファイルはすべて OESIS V4 準拠になりますが、以前のバージョンからアップグレードした場合は、既存のプロファイルも V4 準拠になるように、プロファイルを削除して作り直すことをお勧めします。業務上の理由で OESIS V3 準拠のデバイス プロファイルを使い続ける必要がある場合は、管理コンソールでMGMT_ALLOW_NEW_OPSWAT_V3=true という CEM 値を追加することにより、既定の動作を無効にすることができます。ただし、これは推奨されません。

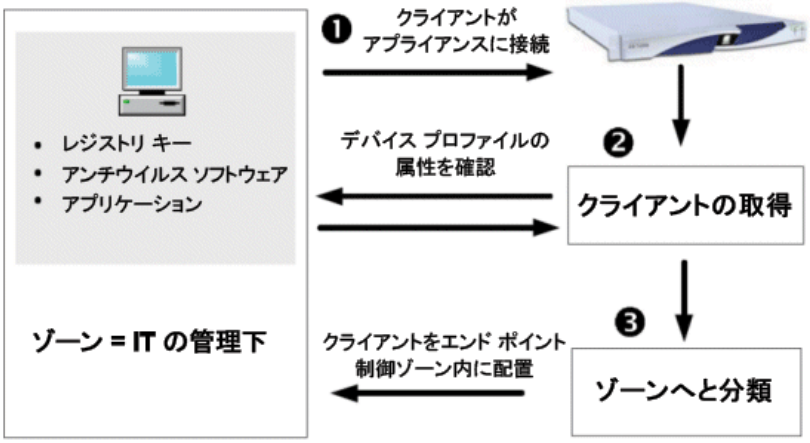
OESIS V4 では、**Anti-Malware Program (アンチマルウェア プログラム)**という新しい種別が策定されています。これはアンチウイルス プログラムとアンチスパイウェア プログラムに取って代わるものです。最近は多くの製品がこの両方の種別に該当するためです。

メモ：OPSWAT は、OESIS V3 ライブラリのサポートの終了をすでに公表しています。ただし、SonicWall のような既存顧客には、一定期間のサポートを継続します。詳細については、以下のナレッジ ベースを参照してください。
https://www.sonicwall.com/ja-jp/support/knowledge-base/171004181702551。

アプライアンスが End Point Control でゾーンとデバイス プロファイルを使用する方法

アプライアンスでは、End Point Control がコミュニティ レベルで管理および展開されます。認証レルム (ユーザーがアプライアンスに入るときの入口) は、1 つまたは複数のコミュニティ (同様のアクセス要件を持つユーザーまたはグループの集まり) を参照します。一方でコミュニティは、1 つまたは複数の EPC ゾーンを参照します。EPC ゾーンは、1 つまたは複数のデバイス プロファイルを参照できます。デバイス プロファイルは、クライアント コンピュータ上に存在する属性を定義するものです。EPC プロセスは次のように機能します。

IT の管理下にあるゾーンの End Point Control



1 ユーザーがアプライアンスに接続します。

a ユーザーが認証レルムにログインします。

b アプライアンスが、そのレルムに所属するコミュニティにユーザーを割り当てます。

2 アプライアンスは、ユーザーのコンピュータに照会することにより、コミュニティのいずれかの EPC ゾーンで定義されている属性と一致する属性 (デバイス プロファイルに含まれている) があるかを判定します。

3 デバイスがプロファイルと一致する場合、アプライアンスは、そのコンピュータを特定の EPC ゾーンに分類し、そのゾーンに構成されている EPC ツールを展開します。

4 ユーザーが個人用機器に接続すると、必要に応じて VPN 接続を許可するよう求められます。

ここでは、ユーザーのデバイス プロファイルが、*IT-managed* という End Point Control ゾーンと一致しています。このプロセスの詳細については、シナリオ 1: IT の管理下にあるノート型 PC から従業員が接続する場合を参照してください。

メモ：

- End Point Control では、特定の Web ブラウザ要件があります (Macintosh システムでは Mozilla Firefox よりも Safari が推奨されるなど)。詳細な要件については、クライアント コンポーネントを参照してください。
- ログ レベルが verbose に設定されている場合、クライアント インタロゲーションの間、アプライアンスがチェックしているデバイス プロファイル属性の他、それが見つかったかどうかがシステム メッセージ ログに記録されます。詳細については、End Point Control インタロゲーションを参照してください。

ゾーンの定義

カスタマイズ可能な 3 種類のゾーンに加えて、組み込みのゾーン (**Default (デフォルト)**) があります。ゾーンの種別を参照してください。コミュニティには、**Deny (拒否)**、**Standard (標準)**、**Quarantine (隔離)** の各ゾーンを入れることができます。一方、**Default (デフォルト)** ゾーンはグローバルです。コミュニティの詳細については、レルムへのコミュニティの追加を参照してください。

ゾーンの種別

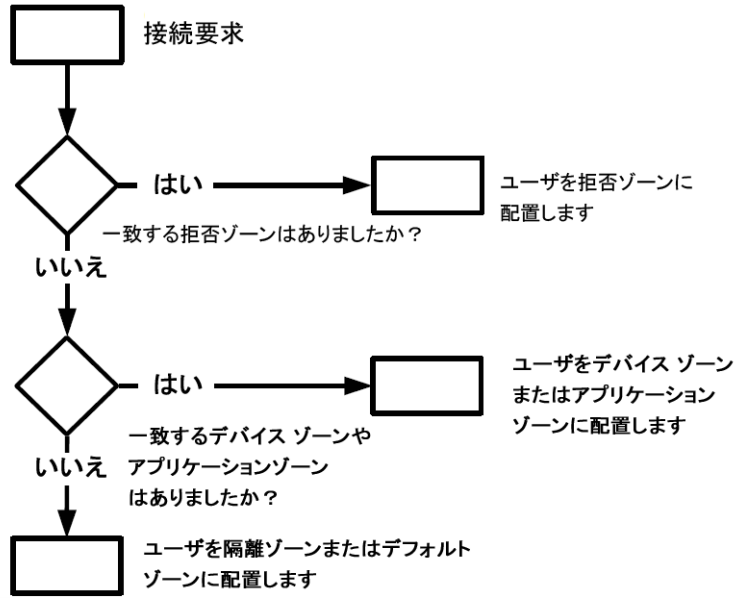
ゾーン タイプ	説明
拒否	拒否ゾーンは最初に評価されます。アプライアンスは、**Deny (拒否)** ゾーンのリストで、上から順に一致を見つけようとします。いずれかのデバイス プロファイルが一致した場合 (例えばデバイス上に特定のファイルがあった場合)、そのユーザーは、ネットワークへのアクセスが拒否されます。詳細については、拒否ゾーンの作成を参照してください。
デバイス	デバイスが**Deny (拒否)** ゾーンの基準と一致しない場合、アプライアンスは標準ゾーンのリストで、上から順に一致を見つけようとします。機器標準ゾーン カテゴリは **Device (デバイス)**ゾーンを含みます。デバイスが基準に一致する場合は、信頼ゾーンに配置されます。 一致が見つからない場合、デバイスは **Default (デフォルト)** ゾーンまたは **Quarantine (隔離)**ゾーン (定義されている場合) に入れられます。詳細については、デバイス ゾーンの作成を参照してください。

ゾーンの種別

ゾーン タイプ	説明
アプリケーション	デバイスが **Deny (拒否)**ゾーンの基準と一致しない場合、アプライアンスは標準ゾーンのリストで、上から順に一致を見つけようとします。標準ゾーン カテゴリはアプリケーション ゾーンを含みます。アプリケーションが基準に一致する場合は、信頼ゾーンに配置されます。 一致が見つからない場合、デバイスはデフォルト ゾーンまたは隔離ゾーン (定義されている場合) に入れられます。詳細については、アプリケーションケーションゾーンの作成を参照してください。
隔離	プロファイルが一致しないデバイスは、デフォルト ゾーンまたは隔離ゾーンに入れられます。ユーザーに提示されるメッセージをカスタマイズすることも可能です。例えば、ユーザーのシステムをセキュリティ ポリシーに準拠させる上での必要事項を説明できます。コミュニティには、隔離ゾーンを 1 つだけ入れることができます。詳細については、隔離ゾーンの作成を参照してください。
既定	このゾーンはグローバルであり、AMC で構成されたあらゆるコミュニティに暗黙的に存在します。デバイスが他のプロファイルと一致しない場合、そのデバイスをデフォルト ゾーンに「送り込む」か、隔離ゾーンに入れるかを選択します。デフォルト ゾーンは、ある程度カスタマイズできますが、削除できません。詳細については、デフォルト ゾーンの構成を参照してください。

ゾーン評価順序は、ゾーンが評価される順序を示しています。**デフォルト** ゾーンのみが必須になります。

ゾーン評価順序



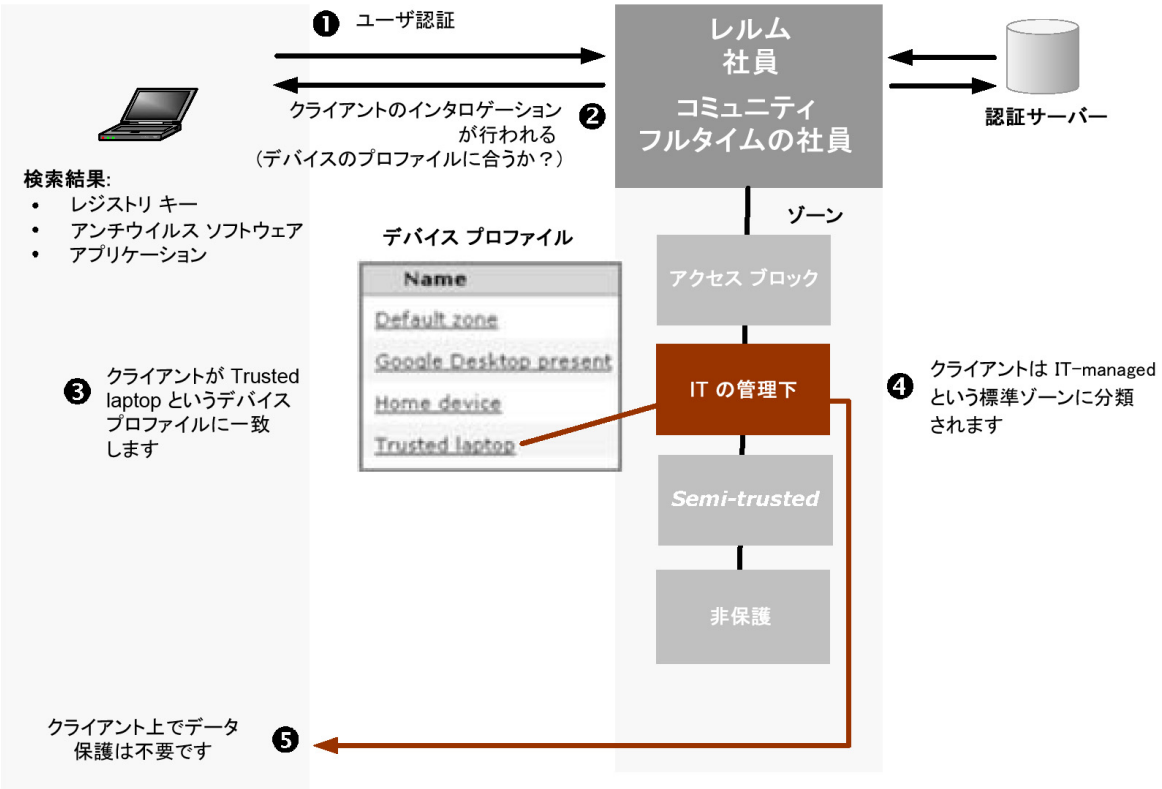
End Point Control のシナリオ

このセクションでは、ゾーンとデバイス プロファイルを使用して、接続要求を分類し End Point Control ツールをクライアントにインストールする、一般的な End Point Control シナリオについて説明します。

トピック:

- シナリオ 1: IT の管理下にあるノート型 PC から従業員が接続する場合
- シナリオ 2: ホーム PC から従業員が接続する場合
- シナリオ 3: キオスク端末から従業員が接続する場合
- シナリオ 4: Google Desktop が動作している PC から従業員が接続する場合
- シナリオ 5: 従業員がモバイル デバイスから接続する場合

シナリオ 1: IT の管理下にあるノート型 PC から従業員が接続する場合



このシナリオでは、最初に従業員が、IT の管理下にあるノート型 PC からアプライアンスに接続します。

1 ユーザーがアプライアンスに接続して *Employees* レルムにログインし、*Full-time employees* コミュニティに割り当てられます。

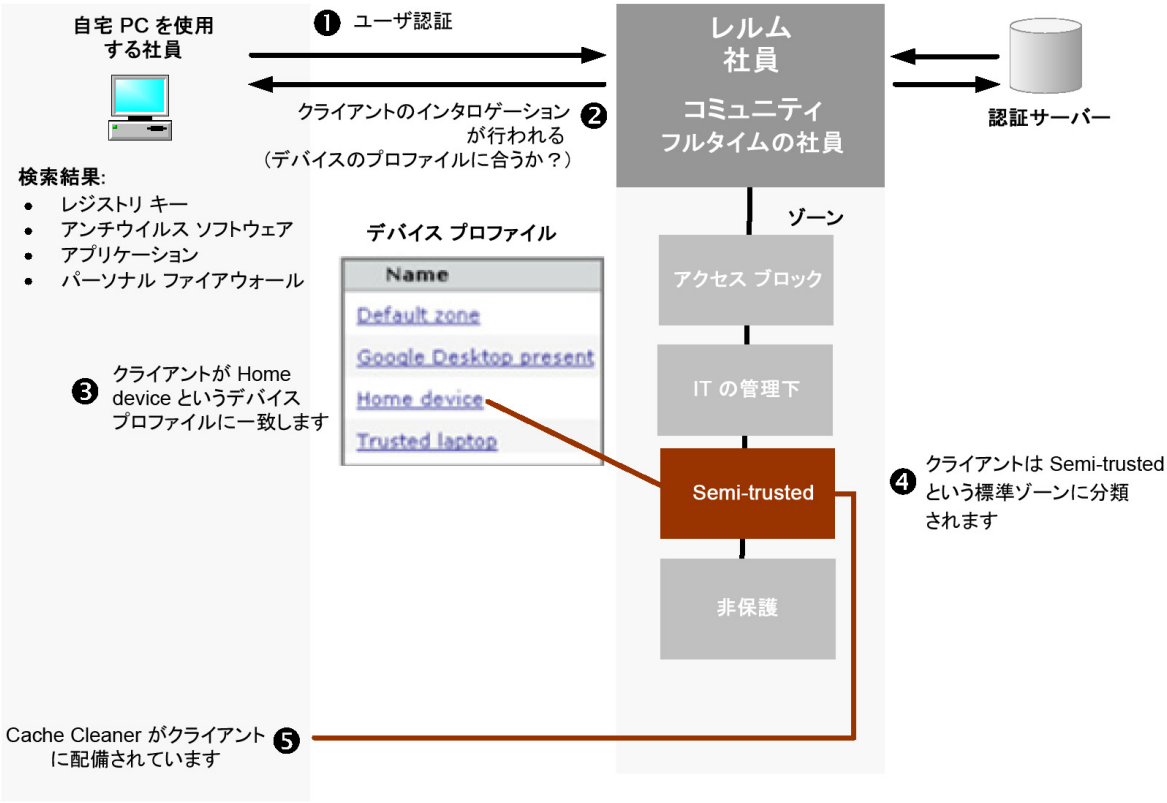
2 ユーザーが認証されると、クライアント デバイスのインタロゲーションが行われ、*Full-time employees* コミュニティが参照するゾーンに属するいずれかのデバイス プロファイルに一致するかが判定されます。デバイス プロファイルはゾーンごとに評価され、拒否ゾーンから開始して、コミュニティにリストされているゾーンが順にチェックされます。

3 アプライアンスは、クライアントが **Deny (拒否)**ゾーン (*Block-access*) のデバイス プロファイルと一致しないことを検出し、*IT-managed* ゾーンのプロファイルのチェックに進みます。*IT-managed* ゾーンは、*Trusted laptop* という名前のデバイス プロファイルを参照します。アプライアンスは、ユーザーのデバイス属性が、このデバイス プロファイル (レジストリ キー エントリ、アンチウイルス ソフトウェア、アプリケーション) と一致していると判定します。

4 アプライアンスは、その一致に基づいて、このデバイスを *IT-managed* ゾーンに分類し、このコミュニティでリストされているそれ以降のゾーンについては評価しません。

5 *IT-managed* ゾーンの場合は、クライアント側にデータ保護ツールがなくてもかまいません。次にアプライアンスは、*Full-time employees* コミュニティ用に構成されているアクセス エージェントのプロビジョニングを行います。これにより、ユーザーは適切なネットワーク リソースにアクセスできるようになります。

シナリオ 2: ホーム PC から従業員が接続する場合



このシナリオでは、最初に従業員が、ホーム PC からアプライアンスに接続します。

1 ユーザーがアプライアンスに接続して *Employees* レルムにログインし、*Full-time employees* コミュニティに割り当てられます。

2 ユーザーが認証されると、クライアント デバイスのインタロゲーションが行われ、*Full-time employees* コミュニティが参照するゾーンに属するいずれかのデバイス プロファイルに一致するかが判定されます。デバイス プロファイルはゾーンごとに評価され、拒否ゾーンから開始して、コミュニティにリストされているゾーンが順にチェックされます。

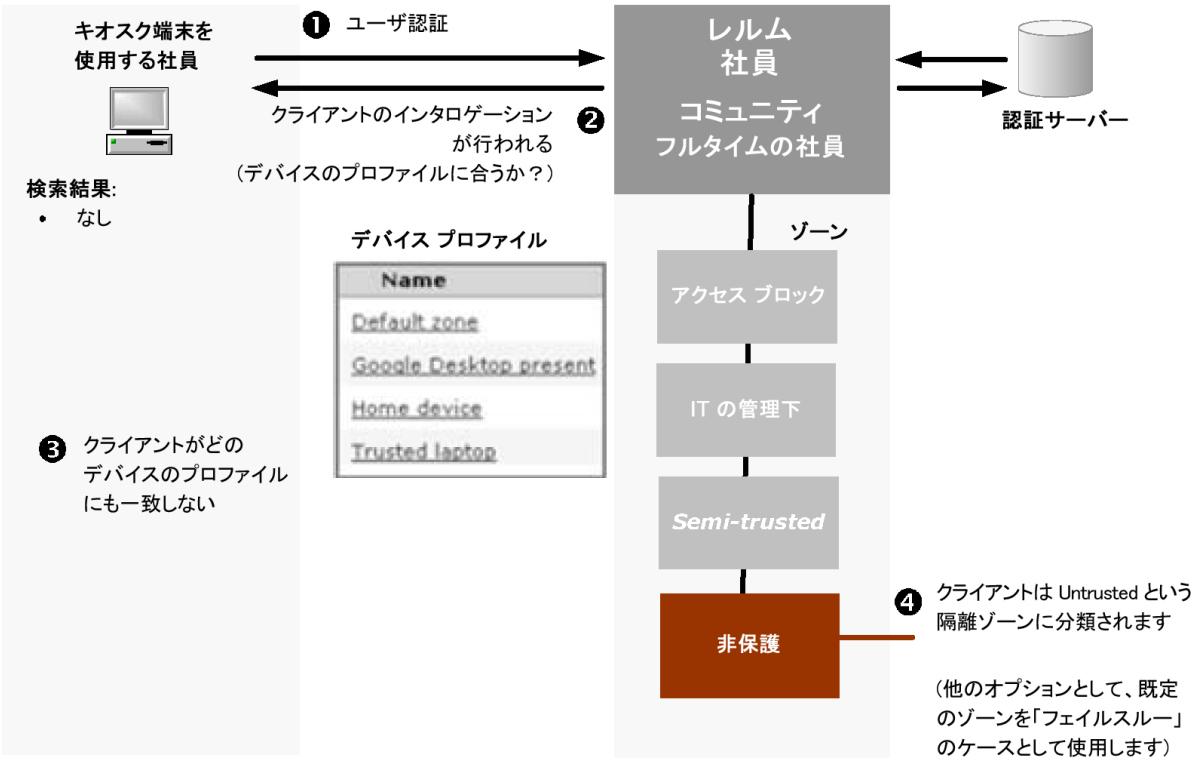
3 このシナリオでは、クライアントが拒否ゾーン (*Block-access*) および標準ゾーン (*IT-managed*) のデバイス プロファイルと一致しないことが検出され、リスト内の次のプロファイル。(*Semi-Trusted*) のチェックに進みます。

4 *Semi-trusted* ゾーンは、*Home device* という名前のデバイス プロファイルを参照します。アプライアンスは、ユーザーのデバイス属性 (レジストリ キー エントリ、アンチウイルス ソフトウェア、アプリケーション) が、このデバイス プロファイルと一致していると判定します。

5 アプライアンスは、その一致に基づいて、このデバイスを *Semi-trusted* ゾーンに分類し、このコミュニティのそれ以降のゾーンについては評価しません。

6 *Semi-trusted* ゾーンの場合は、クライアント側にデータ保護ツールが必要となるため、アプライアンスはクライアントに Cache Cleaner を展開します。次にアプライアンスは、*Full-time employees* コミュニティ用に構成されているアクセス エージェントのプロビジョニングを行います。これにより、ユーザーは適切なネットワーク リソースにアクセスできるようになります。

シナリオ 3: キオスク端末から従業員が接続する場合



このシナリオでは、最初に従業員がキオスク端末からアプライアンスに接続します。

1 ユーザーがアプライアンスに接続して *Employees* レルムにログインし、*Full-time employees* コミュニティに割り当てられます。

2 ユーザーが認証されると、クライアント デバイスのインタロゲーションが行われ、*Full-time employees* コミュニティが参照するゾーンに属するいずれかのデバイス プロファイルに一致するかが判定されます。拒否ゾーンから開始して、コミュニティにリストされているゾーンが順にチェックされます。

3 このシナリオでは、クライアントが構成されているどのゾーンとも一致しないことが検出されます。このような状況の場合の処理する方法としては、クライアントを **Quarantine (隔離)**ゾーンに分類するか、**Default (デフォルト)** ゾーンに分類するかの 2 種類があります。この例では **Quarantine (隔離)**ゾーン *Untrusted (非保護)*が使用されます。この場合にユーザーがアクセスできるリソースは、ユーザーが設定したリソースだけです。例えば、システムがセキュリティ ポリシーに準拠する上で必要な Web リソースに対するリンクを含むカスタマイズされたページを表示することもできます。

   a 信頼されていないデバイス (キオスク端末の PC など) で Windows 7、Windows Vista、または Windows 2008 Server が動作し、サポート されているブラウザが使用されている場合、

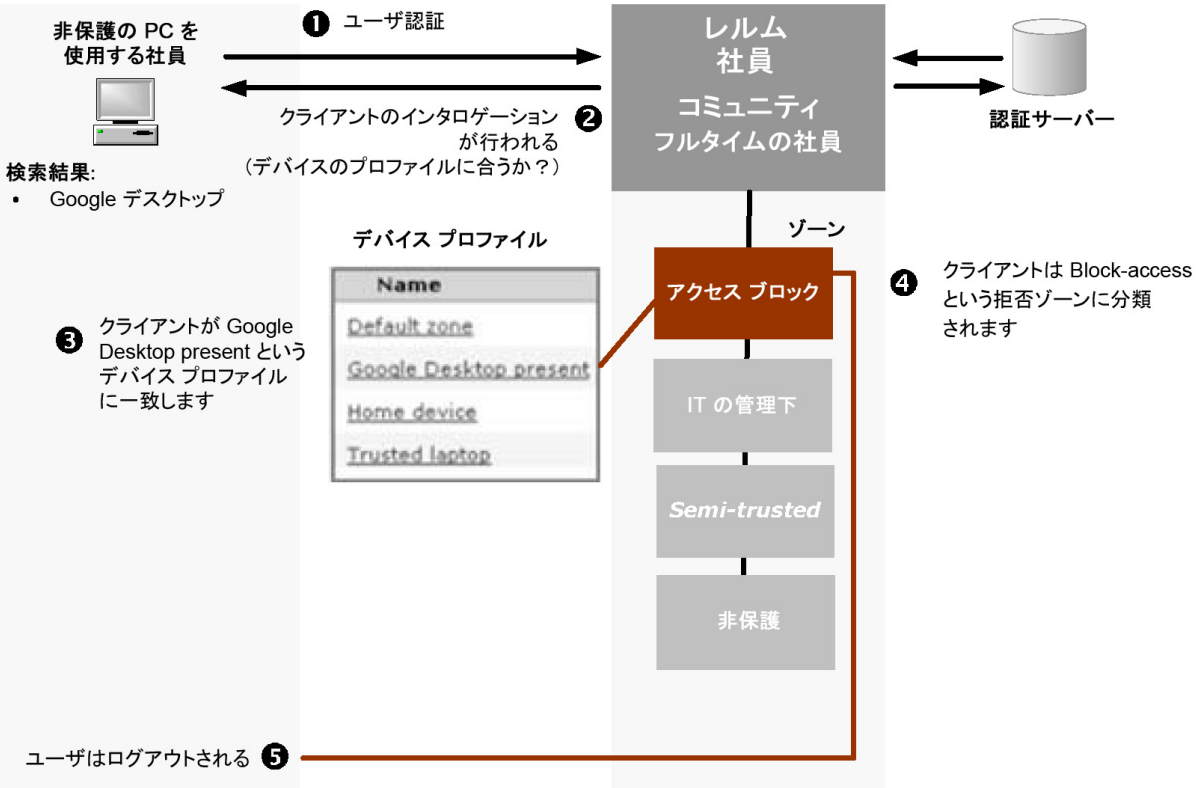
ユーザーはクライアント コンポーネント マネージャーの Secure Endpoint Manager をダウンロードしてインストールする必要があります。クライアント コンポーネント マネージャにより、ユーザー向けに Cache Cleaner が自動展開されます。次にアプライアンスは、*Full-time employees* コミュニティ用に構成されているアクセス エージェントのプロビジョニングを行います。これにより、ユーザーは適切なネットワーク リソースにアクセスできるようになります。

b デバイスのオペレーティング システムおよびブラウザが Cache Cleaner と互換性を持たない場合は、メッセージが表示されます。

c Cache Cleaner をクライアントに展開できない場合、ユーザーの接続要求は拒否されます。

このゾーンの設定オプションについては、デフォルト ゾーンの構成を参照してください。

シナリオ 4: Google Desktop が動作している PC から従業員が接続する場合



従業員が、企業のオフィス外の PC からアプライアンスに接続します。

1 ユーザーがアプライアンスに接続して *Employees* レルムにログインし、*Full-time employees* コミュニティに割り当てられます。

2 ユーザーが認証されると、クライアント デバイスのインタロゲーションが行われ、*Full-time employees* コミュニティが参照するゾーンに属するいずれかのデバイス プロファイルに一致するかが、拒否ゾーンから順に判定されます。

3 このシナリオでは、PC で Google Desktop が動作していることが判定され、Google Desktop present デバイス プロファイルに一致します。デバイスは *Block-access* という拒否ゾーンに分類されます。

4 他のゾーンは評価されず、ユーザーのアクセス要求は拒否されます。

5 ユーザーはログアウトさせられます。

シナリオ 5: 従業員がモバイル デバイスから接続する場合

このシナリオでは、従業員が企業のオフィス外のモバイル デバイスからアプライアンスに接続します。特定のユーザーと使用デバイスの間の関連付けを確立するために (デバイスを置き忘れたり失ったりした場合に備えて)、管理者はユーザー名と各デバイスの IMEI (International Mobile Equipment Identity) 番号を収集し、ユーザー アカウント向けの IMEI 番号を Active Directory サーバーに追加しています。また管理者は、ユーザーと IMEI の関連付けを検証するための *Mobile resources* というデバイス プロファイルを作成しています。

ユーザーがログインするとき、次のようにイベントが発生します。

1. ユーザーがアプライアンスに接続して、ユーザー名とパスワードを入力して *Employees* レルムにログインし、*Mobile employees* コミュニティに割り当てられます。
2. ユーザーの認証後、クライアント デバイスのインタロゲーションが行われ (*Mobile employees* コミュニティにより参照されるゾーン向けのデバイス プロファイルを使用して)、IMEI 番号が判定されます。
3. IMEI 番号は、AD ディレクトリのユーザーに関連付けられている番号と比較されます。番号が一致する場合、ユーザーはモバイル デバイス専用リンクへのアクセスを許可されます。一致しない場合は、アクセスが拒否されます。
4. 必要に応じて、ユーザーは個人用機器から VPN 接続を許可するよう求められます。

メモ：IMEI 番号のチェックは、WiFi ではなく WAN (Wide Area Network) でのみ機能します。また、認証後プロセスでモバイル デバイス上の IMEI 番号を識別するために WAN サービスがオンになっていなければなりません。

モバイル デバイスとユーザー別にサービスを追跡するため、ネットワーク プロキシ、Web プロキシ、またはトンネル クライアント向けの監査ログ ファイルを処理できます。

ゾーンおよびデバイス プロファイルによる EPC の管理

デバイス プロファイルは、次の属性を任意の組み合わせで含めて、クライアントを識別して「信頼ゾーン」に割り当てたり、隔離したり、アクセスを完全に拒否したりすることができます。

- アプリケーション
- クライアント証明書
- ディレクトリ名
- 機器 ID (モバイル デバイスの IMEI 番号などのデバイスの識別子)
- ファイル名、サイズ、またはタイムスタンプ
- Windows ドメイン
- Windows レジストリ エントリ
- Windows バージョン

Advanced EPC を使用する場合は、クライアント デバイスのセキュリティ プログラムを識別するために次の属性も使用できます。

- アンチウイルス プログラム

- アンチスパイウェア プログラム
- パーソナル ファイアウォール プログラム

また、EPC ライブラリを使用すると、これらのタイプのセキュリティ プログラムについてフォールバック検出を定義できます。構成方法については、Advanced EPC: フォールバック検出の使用を参照してください。

1 つの EPC ゾーンからは、1 つまたは複数のデバイス プロファイルを参照できます。同様の VPN アクセス要件を持ち、異なるコンピュータ プラットフォームを利用している複数のユーザーが存在する場合に、複数のデバイス プロファイルを使用すると便利です。例えば、Windows コンピュータのデバイス プロファイルを参照する EPC ゾーンと、Macintosh コンピュータ向けのゾーンを構成できます。AMC は、Windows、Macintosh、Linux、Windows Mobile 搭載デバイス、その他のモバイル デバイス (PDA やスマートフォンなど) のデバイス プロアイルをサポートします。ゾーンとデバイス プロファイルは、さまざまなアクセス シナリオと信頼レベル に対応するために、必要に応じていくらでも作成できます(従業員、ビジネス パートナー、請負業者向けの個別ゾーンなど)。

AMC には、定義済みのゾーンといくつかのデバイス プロファイルが用意されています。

- **Default (デフォルト)** ゾーンは、ある程度カスタマイズできますが、削除できません。構成したゾーンに分類できないデバイスは、**Default (デフォルト)** ゾーンまたは**Quarantine (隔離)**ゾーンに入れられます(コミュニティを構成する際に「フォールバック」ゾーンを指定できます。方法についてはコミュニティでの End Point Control 制約の使用を参照してください)。詳細については、デフォルト ゾーンの構成を参照してください。
- アプライアンスでは、Advanced EPC の使用開始を支援するため、一般的なアクセス シナリオ向けのデバイス プロファイルがいくつか事前定義されています。これらのプロファイルはそのまま使用できるほか、必要性に合わせてカスタマイズできます (詳細はAdvanced EPC: 構成済みのデバイス プロファイルの使用を参照)。

ユーザーの認証後、そのユーザーが使用できるゾーンを指定する場合は、コミュニティを使用します。ゾーン をコミュニティにリンクする方法については、コミュニティでの End Point Control 制約の使用を参照してください。また、ユーザー、グループ、リソースと同じように、ゾーンをアクセス ポリシーと連携させることも可能です。

トピック:

- End Point Control の有効化と無効化
- ゾーンおよびデバイス プロファイルの設定と使用
- 特殊な状況向けのゾーンの作成
- End Point Controlエージェントの使用

End Point Control の有効化と無効化

AMC では End Point Control をグローバルに有効化または無効化できます。ここでは、End Point Control を一時的に無効にする例を 2 つ示します。

- 会社全体でアンチウイルス ソフトウェアをバージョン 2.x から 3.x にアップグレードした場合。アンチウイルス ソフトウェアを指定したデバイス プロファイルを変更するために、End Point Control を一時的に無効化します。
- ユーザーの作業を中断させることなく、実稼働アプライアンスで新しいデバイス プロファイルとゾーンを作成できます。

End Point Control が無効 (デフォルト設定) になっているとき、アプライアンスは次の EPC アクションを実行しません。

- クライアント デバイスの属性の評価
- ゾーンへの接続要求の分類
- アクセス制御ルールのゾーン制約の強制

End Point Control を有効にするには、

1 メイン ナビゲーション メニューから [**End Point Control**] をクリックします。

2 一般セクションの [**Edit (編集)**] リンクをクリックします。[**Configure End Point Control (エンド ポイント制御 の設定)**] ページが表示されます。

3 [**Enable End Point Control (エンド ポイント制御を有効にする)**] チェックボックスを選択します。

4 「**Save (保存)**」を選択します。

メモ：EPC が有効になっている場合は、ゾーンごとに EPC のチェック頻度を 1 度だけ (ログイン時) 実行するか、またはログイン時とその後のセッションで *<n>* 分おきに実行するように指定できます。詳細については、「デバイス ゾーンの作成」または「デフォルト ゾーンの構成」を参照してください。

ゾーンおよびデバイス プロファイルの設定と使用

トピック:

- 表ゾーン
- 表示デバイス プロファイル
- デバイス ゾーンの作成
- アプリケーションケーション ゾーンの作成
- 拒否ゾーンの作成
- 隔離ゾーンの作成
- デフォルト ゾーンの構成
- ゾーンに対するデバイス プロファイルの定義
- デバイス プロファイルの属性
- Advanced EPC: セキュリティ プログラムの拡張リスト
- Advanced EPC: フォールバック検出の使用
- Advanced EPC: 構成済みのデバイス プロファイルの使用
- デバイス プロファイル属性での比較演算子の使用
- Connect Tunnel クライアントでの End Point Control の使用
- 反復 EPC チェックの実行: 例

表ゾーン

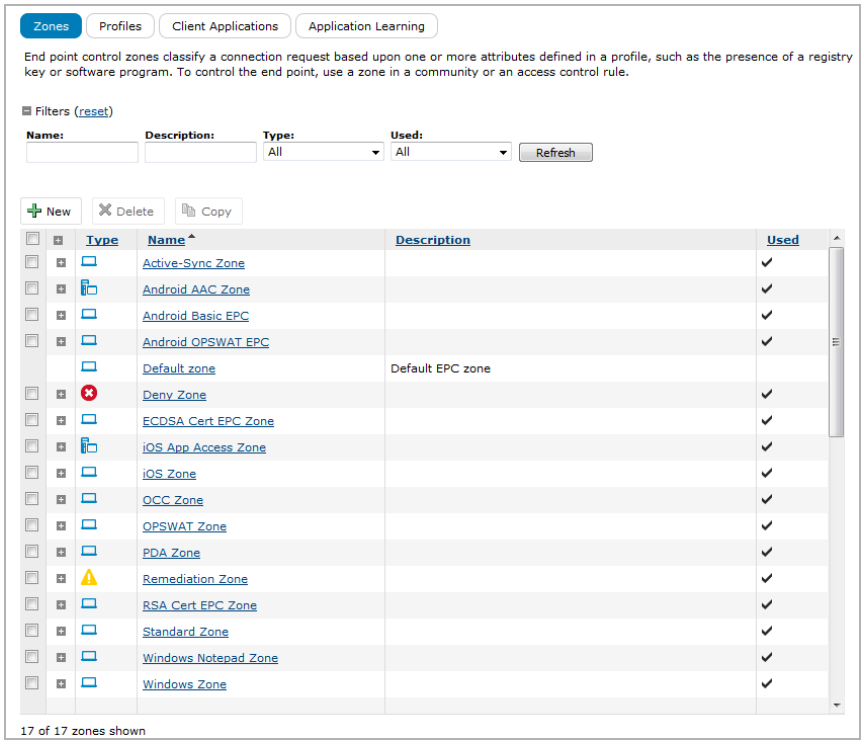
AMC で End Point Control ゾーンのリストを参照し、どのようなタイプで関連するコミュニティがあるかどうかを迅速に判定できます。

構成済みのゾーンを表示するには、

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Zones (ゾーン)**] の横にある [**Edit (編集)**] リンクをクリックします。

3 [**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されて、AMC で構成されているゾーンのサマリ、および EPC エージェントのステータスのサマリも表示されます。SMA アプライアンスでは、**Default zone (デフォルト ゾーン)** というゾーンがあらかじめ構成されています。



リスト内のそれぞれのゾーンに関する情報を参照できます。

- プラス記号 (+) の列をクリックすると、選択したゾーンが拡大され、関連するデバイス プロ ファイルとコミュニティが表示されます。テーブル見出しにあるプラス記号をクリックすると、すべてのゾーンの表示が展開されます。
- **Type (種別)**列には、そのゾーンが**Default (デフォルト)** ゾーン、**Standard (標準)**ゾーン、**Deny (拒否)**ゾーン、**Quarantine (隔離)**ゾーンのいずれかが示されます (これらのゾーン タイプについてゾーンの定義を参照)。
- [**Name (名前)**] 列には、ゾーンを作成するときに割り当てた名前が表示されます。ゾーンを編集するときは、名前をクリックします。
- [**Description (説明)**] 列には、ゾーンに対する説明テキストがリストされます。

- [**Used (使用中)**] 列には、ゾーンがコミュニティによって参照されているかどうかが示されます。青いドットは、ゾーンが 1 つまたは複数のコミュニティによって使用されていることを示します。ゾーンが参照されていない場合、このフィールドは空白です。

4 ゾーンの設定を表示または編集するときは、ゾーンの名前をクリックします。

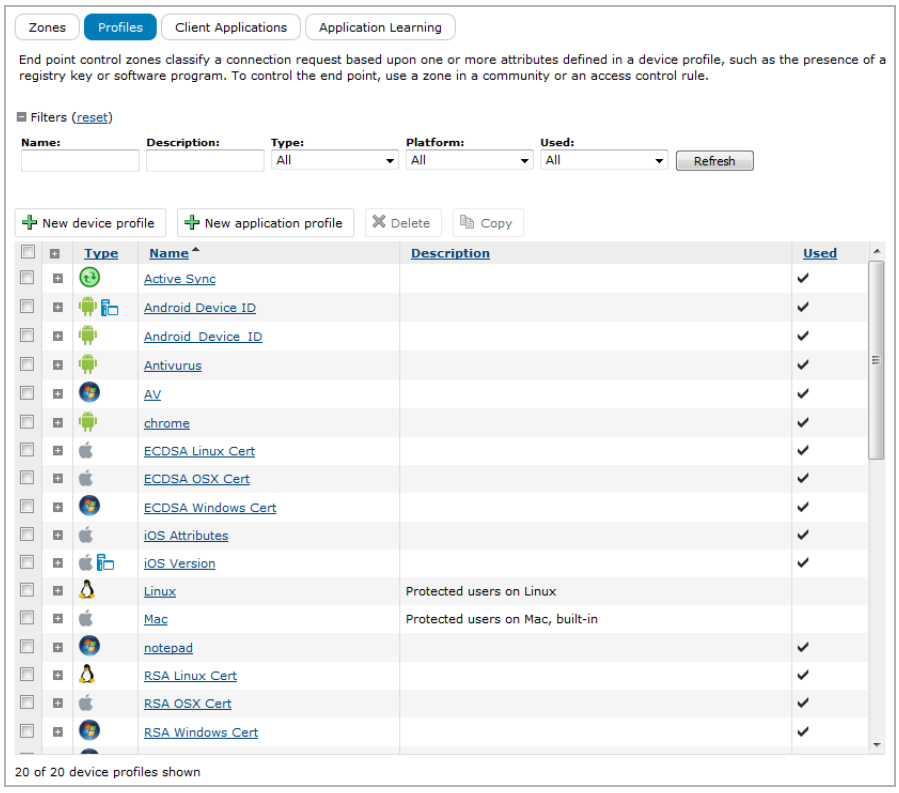
表示デバイス プロファイル

デバイス プロファイルは、クライアントを識別するときに使用される属性 (レジストリ キーやソフトウェア プログラムの存在など) を指定します。End Point Control ゾーンにより参照されます。

構成済みのデバイス プロファイルを表示するには、

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Profiles (プロファイル)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。



- [**Name (名前)**] 列には、デバイス プロファイルを作成するときに割り当てた名前が表示されます。デバイス プロファイルを編集するには名前をクリックします。
- [**Description (説明)**] 列には、デバイス プロファイルに冠する説明テキストがリストされます。
- [**Type (種別)**] 列には、デバイス プロファイル *e* がサポートするプラットフォームを表すアイコンが表示されます。**Microsoft Windows**、**Mac OS X**、**Linux**、**Windows Mobile**、および**その他のモバイル デバイス**。

- [**Used (使用中)**] 列には、プロファイルがクライアントによって参照されているかどうかが示されます。青いドットは、ゾーンが 1 つまたは複数のクライアントによって使用されていることを示します。ゾーンが参照されていない場合、このフィールドは空白です。

3 [**Device Profiles (デバイス プロファイル)**] タブで、構成済みのプロファイルのリストを確認します。Advanced EPC を使用している場合は、このリストには構成済みのデバイス プロファイルがいくつか含まれます。

デバイス ゾーンの作成

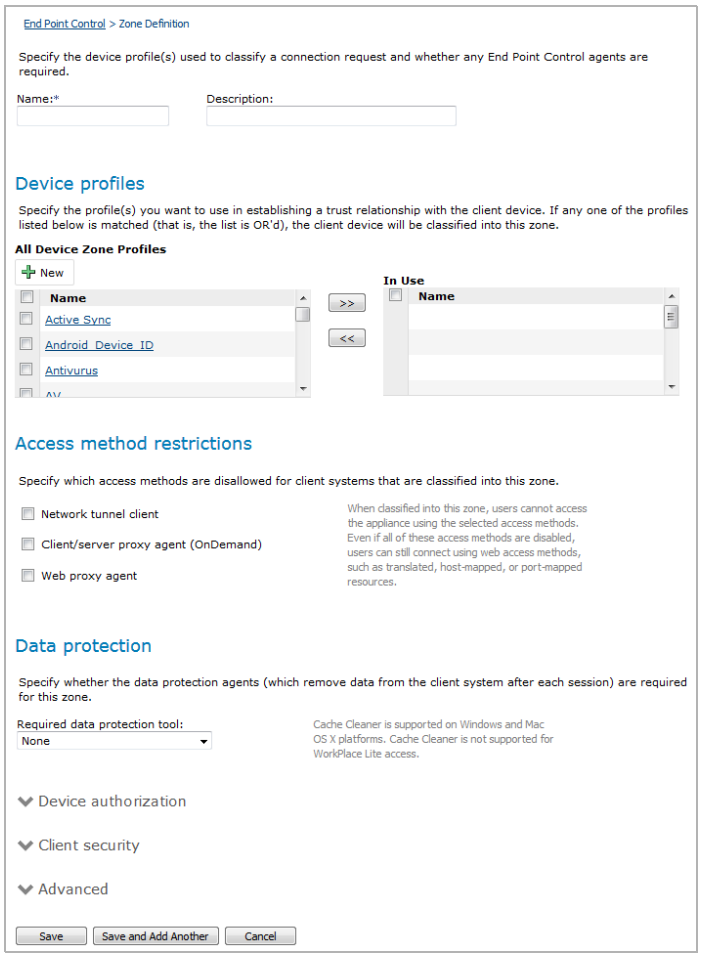
デバイス ゾーンは、**Deny (拒否)**ゾーンの後に評価されます。例えば、*Windows firewall* という名前で、パーソナル ファイアウォールの動作を求めるデバイス プロファイルを作成できます。この End Point Control ポリシーが存在する場合、この条件と一致するデバイスは「信頼ゾーン」に入れられます。

デバイス ゾーンを定義するには:

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Zones (ゾーン)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。

3 [**New (新規)**] をクリックし、ドロップダウン メニューから [**Device zone (デバイス ゾーン)**] を選択します。[**Zone Definition - Device Zone (ゾーン定義 - 機器ゾーン)**] ページが表示されます。



4 **Name (名前)**フィールドに、ゾーン名を分かりやすい名前で入力します (*Windows firewall required* など)。ゾーンがモバイル デバイス ユーザーにより参照される場合は、モバイル デバイス上で全体が表示されるように短い名前を指定します。

5 (オプション) [**Description (説明)**] フィールドに、ゾーンについての分かりやすいコメントを入力します。

6 [**All Device Zone Profiles (すべてのデバイス ゾーン プロファイル)**] リストで、ゾーンに入れたいデバイス プロファイルに対応するチェック ボックスを選択して、右矢印 (>>) ボタンをクリックします。デバイスが作成中のゾーンに入るために一致する必要があるのは、[**In Use (使用中)**] リストのプロファイルのいずれか 1 つだけです。

7 このゾーンにデバイス プロファイルが存在しない場合は、[**New (新規)**] をクリックして 1 つ追加します。プロファイル作成の詳細については、ゾーンに対するデバイス プロファイルの定義を参照してください。

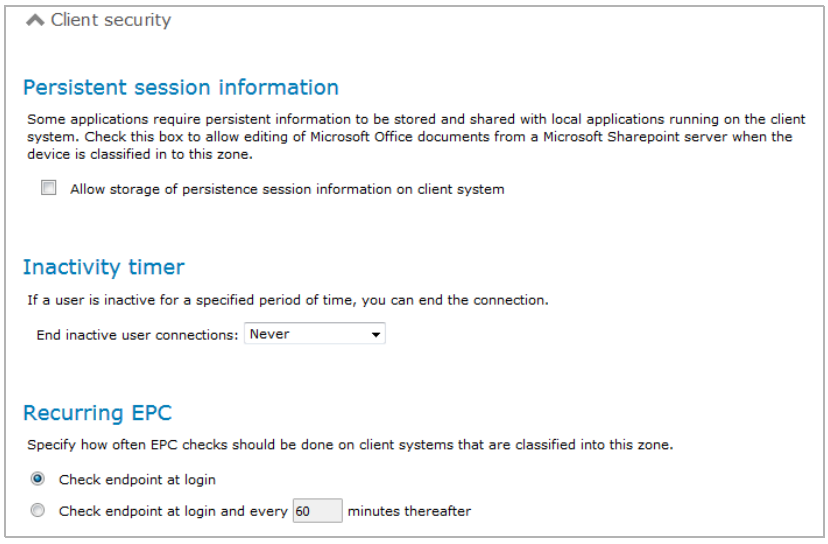
8 [**Access method restrictions (アクセス方法の制限)**] エリアで、このゾーンに分類されるクライアントに許可しないアクセス方法を指定します (ある場合)。

9 [**Data protection (データ保護)**] エージェントが必要かどうか指定します。Cache Cleaner は Linux プラットフォーム以外のすべてのプラットフォームで強化された保護機能を提供します。

10 [**Device Authorization (機器の認証)**]エリアの一番上のチェックボックスをオンにして、VPN 接続が確立される前にユーザーに個人用機器の認証を要求します。デフォルトでは、このチェックボックスは、デバイス ゾーンに対して EPC が有効になっている場合にチェックされています。

11 ユーザーが同意する必要がある承認条件を変更するには、[**Device Authorization (機器の認証)**]エリアの[**Terms (条件)**]セクションに必要な承認条件を入力します。条件を編集するには、[**Device Authorization (機器の認証)**]チェックボックスをオンにする必要があります。

12 [**Client security (クライアント セキュリティ)**] エリアを展開します。



13 デフォルトでは、ユーザー認証は、機器が最後に使用された 180 日後に失効します。機器の認証が有効になっている場合は、有効期限チェックボックスをオフにするか、期限が切れるまでのお好みの日数を入力して変更することで、ゾーン認証の有効期限を無効にすることができます。

14 デフォルトでは、接続がアクティブでない場合にデバイス ゾーンへのユーザー接続は破棄されません。ただし、[**Inactivity timer (休止タイマー)**]エリアで休止タイマーを設定して、一定時間休止した後に接続を終了することができます。無効休止タイマー間隔は 3 分から 10 時間まで設定できます (既定は**Never (無効)**)。

メモ：以前のリリースでは、休止タイマーはコミュニティ属性の一部でした。

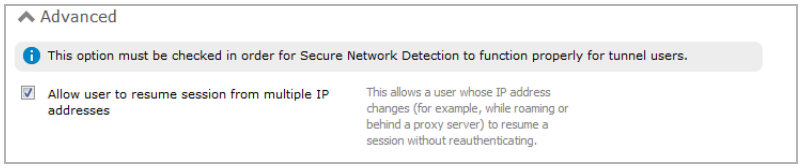
15 [**Recurring EPC (EPC の周期)**] エリアでは、EPC のチェック頻度を選択できます。

- [**Check endpoint at login (ログイン時にエンド ポイントを確認する)**] (既定) - 一度だけ (ログイン時)
- [**Check endpoint at login and then every <*n*> minutes for the duration of the session (ログイン時にエンド ポイントを確認し、セッション中は <n> 分ごとに確認する)**]

反復 EPC チェックの実行: 例では、アプライアンスが USB デバイスの存在を繰り返しチェックし、チェックが失敗するとセッションが終了するシナリオについて説明しています。既定では、エンド ポイントはログイン時に確認されます。

16 デバイスとアプライアンスの間の接続は、デバイスが同一の IPv4 または IPv6 IP アドレスを使用している限りは、中断 (セッションの一時停止と再開、一時的な接続の喪失など) が発生してもユーザーの再認証を要求せずに処理できます。

ユーザーが別の IP アドレスからセッションを再開できるように許可するには (例えば、ネットワークの異なる部分に接続して、異なる IP サブネット間でローミングする場合)、[**Advanced (詳細)**] エリアの [**Allow user to resume session from multiple IP addresses**] チェック ボックスを選択します。



17 ゾーンの構成が終わったら、[**Save (保存)**] をクリックします。

メモ：EPC ゾーンをコピーまたは削除する方法については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

アプリケーションケーション ゾーンの作成

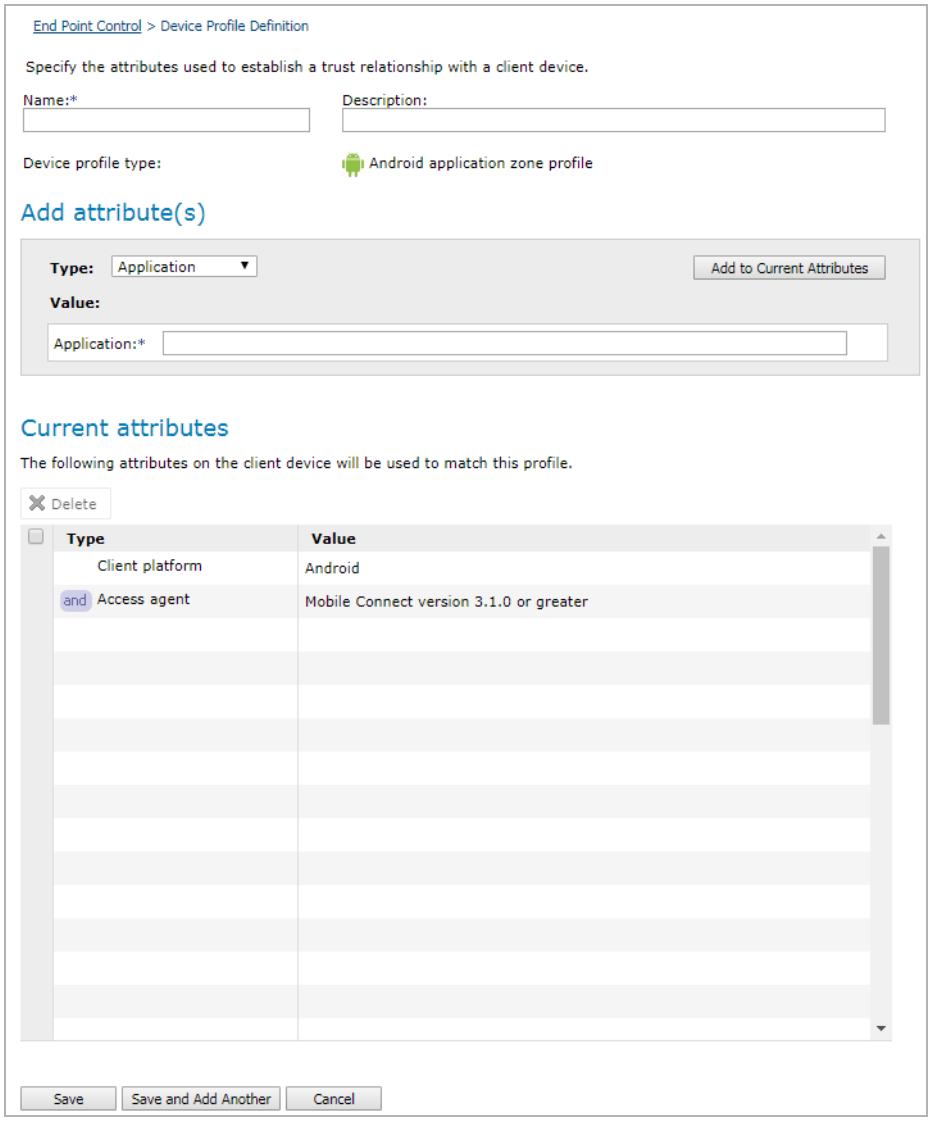
アプリケーション ゾーンは、**Deny (拒否)**ゾーンと**Device (デバイス)**ゾーンの後に評価されます。特定のアプリケーションの稼働中は、企業ネットワークへのアクセスを特定のユーザーにしか許可しないアプリケーション ゾーンを作成できます。この End Point Control ポリシーが存在する場合、この条件と一致するデバイスは「信頼ゾーン」に入れられます。

アプリケーションケーション ゾーンを定義するには:

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Profiles (プロファイル)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。

3 **Profiles (プロファイル)** テーブルの上の[**New application profile (新しいアプリケーションのプロファイル)**] をクリックしてからドロップダウン メニューから [**Android**] を選択すると、[**Device Profile Definition (デバイス プロファイルの定義)**] ページが表示されます。



4 [**Name (名前)**] フィールドに、プロファイルのわかりやすい名前を入力します (例えば、*Unmanaged Android Devices*)。

5 (オプション) [**Description (説明)**] フィールドに、ゾーンについての分かりやすいコメントを入力します。

6 必要な属性が [**Current attributes (現在の属性)**] セクションにリストされない場合は、[**Type (種別)**] ドロップダウン メニューからアプリケーションの種別を選択します。属性をいくつでも組み合わせて定義に関連付けることができます。アプリケーション ゾーンの属性を参照してください。[**Add attributes (属性の追加)**] セクションの残りの部分は、選択した種別によって異なります。

アプリケーション ゾーンの属性

種別	属性
アンチウィルス アプリ	• [**Product Name (製品名)**] ドロップダウン メニューからアプリを選択する または 指定したベンダーのすべての製品を追加するには、[**Any product from this vendor (このベンダーのすべての製品)**] チェックボックスを選択します。 • [**Product version (製品バージョン)**] フィールドで、ドロップダウン メニューから許可するバージョン番号と限定子 (>、>=、=、<、<=) を選択します。 • アプリをアプリ動作時のフィルターとしてのみ使用するには、[**App must be running (アプリが動作していること)**] チェックボックスを選択します。
パーソナル ファイアウォール アプリ	• [**Product Name (製品名)**] ドロップダウン メニューからアプリを選択する または 指定したベンダーのすべての製品を追加するには、[**Any product from this vendor (このベンダーのすべての製品)**] チェックボックスを選択します。
アプリケーション	• [**Application (アプリケーション)**] ドロップダウン メニューからデバイス プロファイルの定義を選択します。
クライアント証明書	• [**CA certificate (CA 証明書)**] ドロップダウン メニューを選択します。必要な証明書が表示されない場合は、新しい証明書のインポートか、既存の証明書の変更が必要な場合があります。
ディレクトリ名	• [**Directory Name (ディレクトリ名)**] フィールド**にディレクトリ名を入力します。**
周辺機器 ID	• ユーザーが登録済みデバイスを使用していない場合は、デバイス識別子 (あるいは、実行時に評価された変数のリテラル値) がプロファイルと一致するかどうかを選択します。例えば、周辺機器 ID を使用する場合、周辺機器 ID と一致するすべてのデバイスによるアプリケーションへのアクセスを制御するのに、デバイス プロファイルが使われます。
ファイル名	• [**File name (ファイル名)**] フィールドにファイル名を入力します。
Android バージョン	• [**Operator (演算子)**] フィールドで、ドロップダウン メニューから限定子 (>、>=、=、<、<=) を選択します。 • [**Major (メジャー)**] フィールドに、フィルターとして使用するメジャーバージョン番号を入力します。 • 必要に応じて、[**Minor (マイナー)**] フィールドに、フィルターとして使用するマイナーバージョン番号を入力します。 • 必要に応じて、[**Build (ビルド)**] フィールドに、フィルターとして使用するビルド番号を入力します。

7 [**Add to Current Attributes (現在の属性に追加)**] ボタンをクリックすると、属性がページの [**Current attributes (現在の属性)**] セクションに転送されます。

8 [**Save (保存)**] を選択します。

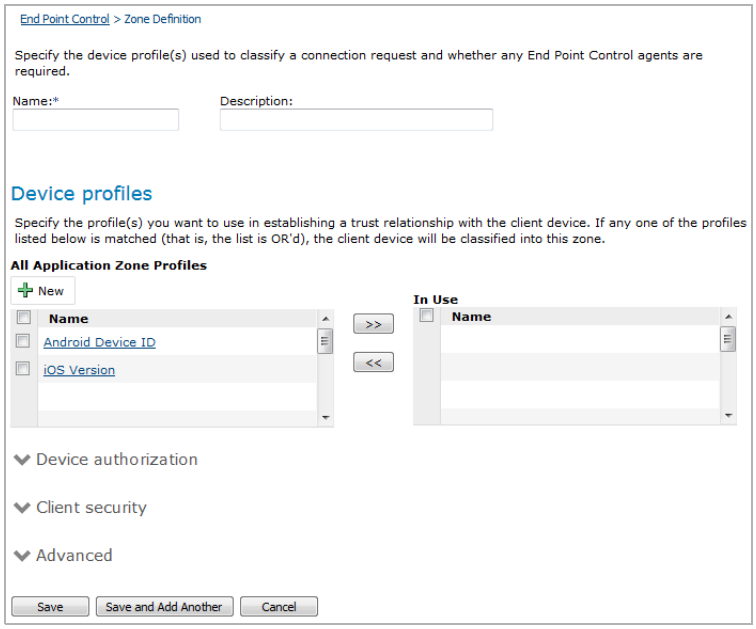
アプリケーション ゾーンを作成するには:

メモ：すべてのアプリケーション ゾーンは、少なくとも 1 つのアプリケーション ゾーン プロファイルが割り当てられている必要があります。接続デバイスがアプリケーション制御対応かどうか、ポリシーが強制されるのはデバイス レベルか、またはアプリケーション レベルかを判断するのに、プロファイルが使用されます。

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Zones (ゾーン)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。

3 [**New (新規)**] をクリックし、ドロップダウン メニューから [**Application zone (アプリケーション ゾーン)**] を選択します。 [**Zone Definition - Device Zone (ゾーン定義 - アプリケーション ゾーン)**] ページが表示されます。



アプリケーション アクセス制御対応のもののみがプロファイルに含まれます。

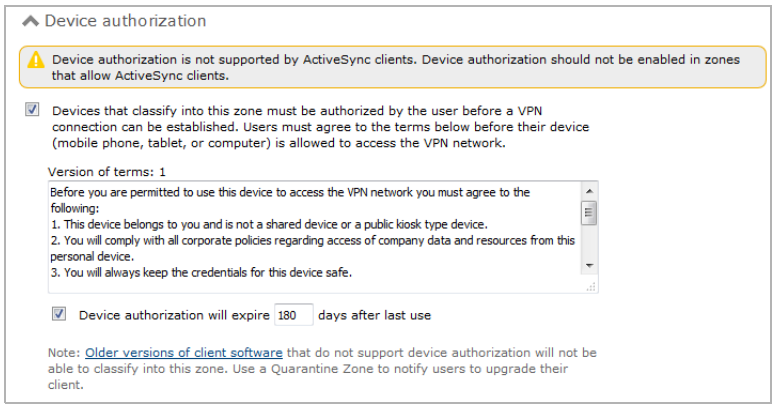
4 [**Name (名前)**] フィールドに、わかりやすいゾーン名を入力します。ゾーンがモバイル デバイス ユーザーにより参照される場合は、モバイル デバイス上で全体が表示されるように短い名前を指定します。

5 (オプション) [**Description (説明)**] フィールドに、ゾーンについての分かりやすいコメントを入力します。

6 [**All Application Zone Profiles (すべてのアプリケーション ゾーンのプロファイル)**]リストで、ゾーンに必要なプロファイルのチェックボックスを選択して、右矢印 (>>) ボタンをクリックします。アプリケーションが作成中のゾーンに入るために一致する必要があるのは、[**In Use (使用中)**]リストのプロファイルのいずれか 1 つだけです。

7 このゾーンにデバイス プロファイルが存在しない場合は、[**New (新規)**] をクリックして 1 つ追加します。プロファイル作成の詳細については、ゾーンに対するデバイス プロファイルの定義を参照してください。

8 [**Device Authorization (機器の認証)**] エリアを展開します。

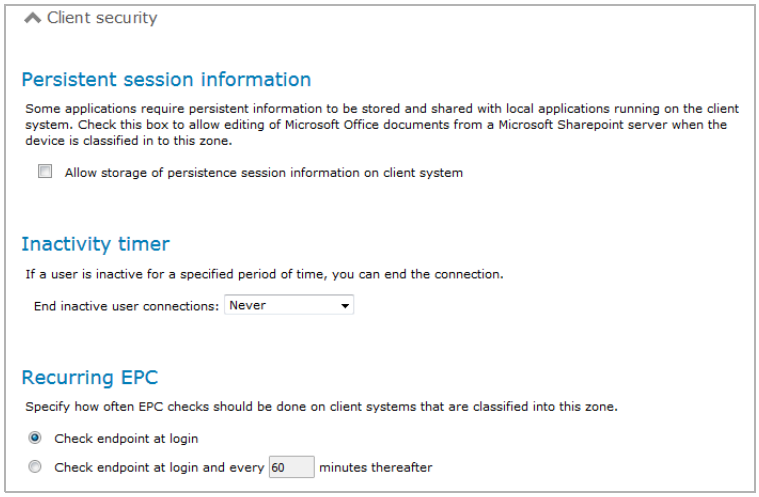


9 [**Device Authorization (機器の認証)**]エリアの一番上のチェックボックスをオンにして、VPN 接続が確立される前にユーザーに個人用機器の認証を要求します。デフォルトでは、このチェックボックスは、アプリケーション ゾーンに対してEPC が有効になっている場合にチェックされています。

10 ユーザーが同意する必要がある承認条件を変更するには、[**Device Authorization (機器の認証)**]エリアの[**Terms (条件)**]セクションに必要な承認条件を入力します。条件を編集するには、[**Device Authorization (機器の認証)**]チェックボックスをオンにする必要があります。

11 デフォルトでは、ユーザー認証は、機器が最後に使用された 180 日後に失効します。機器の認証が有効になっている場合は、有効期限チェックボックスをオフにするか、期限が切れるまでのお好みの日数を入力して変更することで、ゾーン認証の有効期限を無効にすることができます。

12 [**Client security (クライアント セキュリティ)**] エリアを展開します。

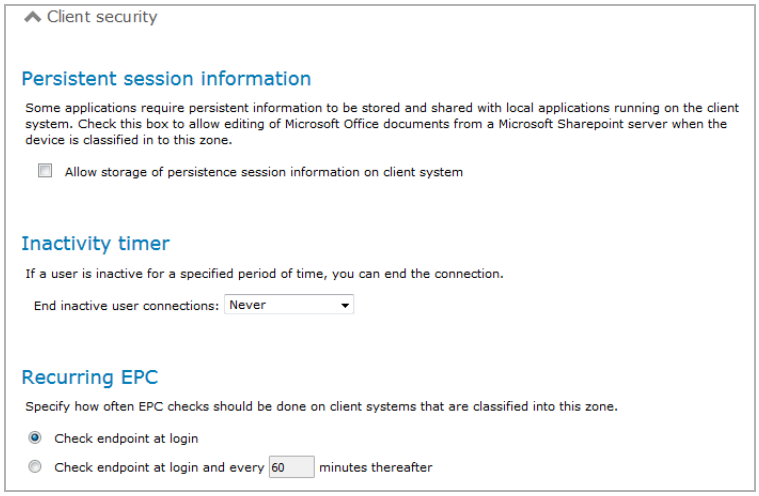


13 デフォルトでは、接続がアクティブでない場合、ゾーンへのユーザー接続は破棄されません。ただし、[**Inactivity timer (休止タイマー)**]エリアで休止タイマーを設定して、一定時間休止した後に接続を終了することができます。休止タイマー間隔は 3 分から 10 時間まで設定できます。

14 [**Recurring EPC (EPC の周期)**] エリアでは、EPC のチェック頻度を 1 度だけ (ログイン時) 実行するか、またはログイン時とその後のセッションで *<n>* 分おきに実行するように指定できます。反復 EPC チェックの実行: 例では、アプライアンスが USB デバイスの存在を繰り返しチェックし、チェックが失敗するとセッションが終了するシナリオについて説明しています。

15 デバイスとアプライアンスの間の接続は、デバイスが同一の IPv4 または IPv6 IP アドレスを使用している限りは、中断 (セッションの一時停止と再開、一時的な接続の喪失など) が発生してもユーザーの再認証を要求せずに処理できます。

ユーザーが別の IP アドレスからセッションを再開できるように許可するには (例えば、ネットワークの異なる部分に接続して、異なる IP サブネット間でローミングする場合)、[**Advanced (詳細)**] エリアの [**Allow user to resume session from multiple IP addresses**] チェック ボックスを選択します。



16 ゾーンの設定が終了したら、[**Save (保存)**] をクリックします。

拒否ゾーンの作成

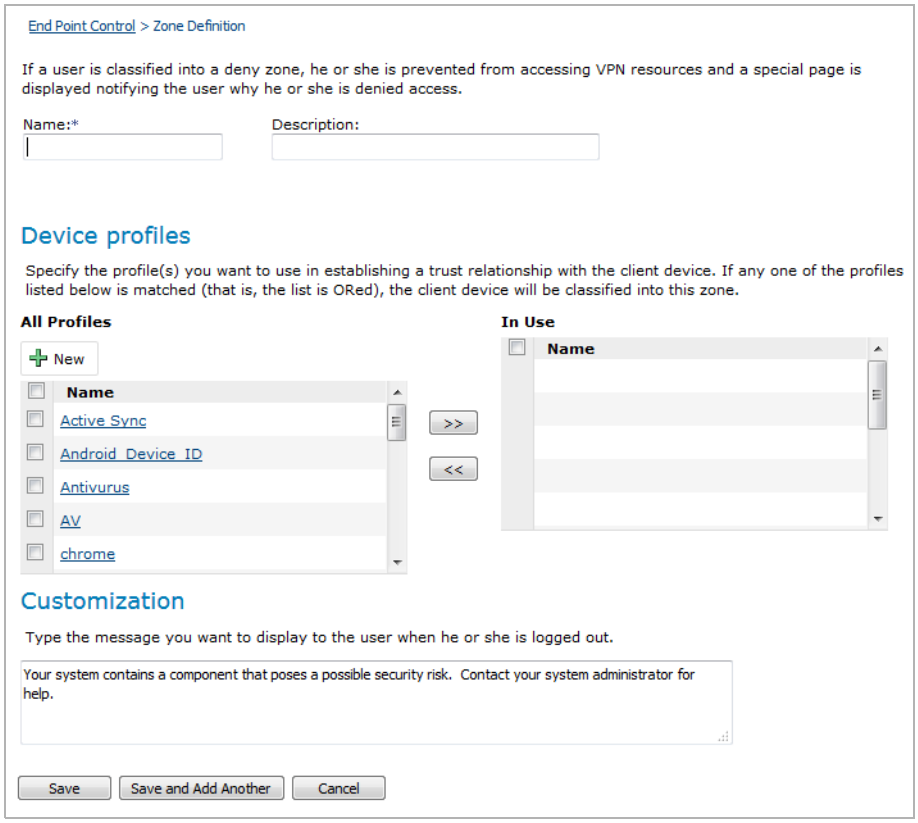
拒否ゾーンは最初に評価されます。いずれかのデバイス プロファイルが一致した場合 (例えば、デバイス上に特定のファイルまたはレジストリ キーがある場合)、そのユーザーはアクセスが拒否され、ログアウトさせられます。

拒否ゾーンを定義するには、

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Zones (ゾーン)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。

3 [**New (新規)**] をクリックし、メニューから [**Deny zone (拒否ゾーン)**] を選択します。[**Zone Definition - Deny Zone (ゾーン定義 - 禁止ゾーン)**] ページが表示されます。



4 [**Name (名前)**] フィールドに、ゾーン名を分かりやすい名前で入力します (*Google Desktop present* など)。

5 (オプション) [**Description (説明)**] フィールドに、ゾーンについての分かりやすいコメントを入力します。

6 [**All Profiles (すべてのプロファイル)**] リストで、ゾーンに入れたいデバイス プロファイルに対応するチェック ボックスを選択して、右矢印 (>>) ボタンをクリックします。(デバイスが作成中の拒否ゾーンに入るために一致する必要があるのは、[**In Use (使用中)**] リストのプロファイルのいずれか 1 つだけです。)

例えば、デバイス プロファイルの定義で、*GoogleDesktop.exe* アプリケーションの実行を求めるように設定していると仮定します。デバイスに *GoogleDesktop.exe* が見つかった場合、そのデバイスは *Google Desktop present* という名前の**Deny (拒否)**ゾーンと一致し、ユーザーはアクセスを拒否され、ログアウトさせられます。

7 このゾーンに適切なデバイス プロファイルが存在しない場合は、[**New (新規)**] をクリックして 1 つ追加します。プロファイル作成の詳細については、ゾーンに対するデバイス プロファイルの定義を参照してください。

8 [**Zone Definition (ゾーン定義)**] ページ下部の [**Customization (カスタマイズ)**] セクションでは、拒否されたユーザーがログアウトさせられるときに表示されるメッセージをカスタマイズできます (例えば、「`Your system is running Google Desktop, which poses a security risk (システムで Google Desktop が動作しています。セキュリティ上危険です。)`」)。

9 ゾーンの設定が終了したら、[**Save (保存)**] をクリックします。

EPC ゾーンをコピーまたは削除する方法については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

隔離ゾーンの作成

分類できない (**Deny (拒否)**ゾーンや**Standard (標準)**ゾーンのプロファイルに一致しない) デバイスを入れるために、**Quarantine (隔離)**ゾーンを作成できます。このゾーンに分類されるデバイスのユーザーには、Web リンクと説明を提供できます (例えば、デバイスをセキュリティ ポリシーに準拠させるための方法や、システムを EPC インタロゲーション向けに構成する方法など)。

Quarantine (隔離)ゾーンは、コミュニティあたり 1 つだけ定義できます (**Deny (拒否)**ゾーンと**Standard (標準)**ゾーンは複数作成できます)。

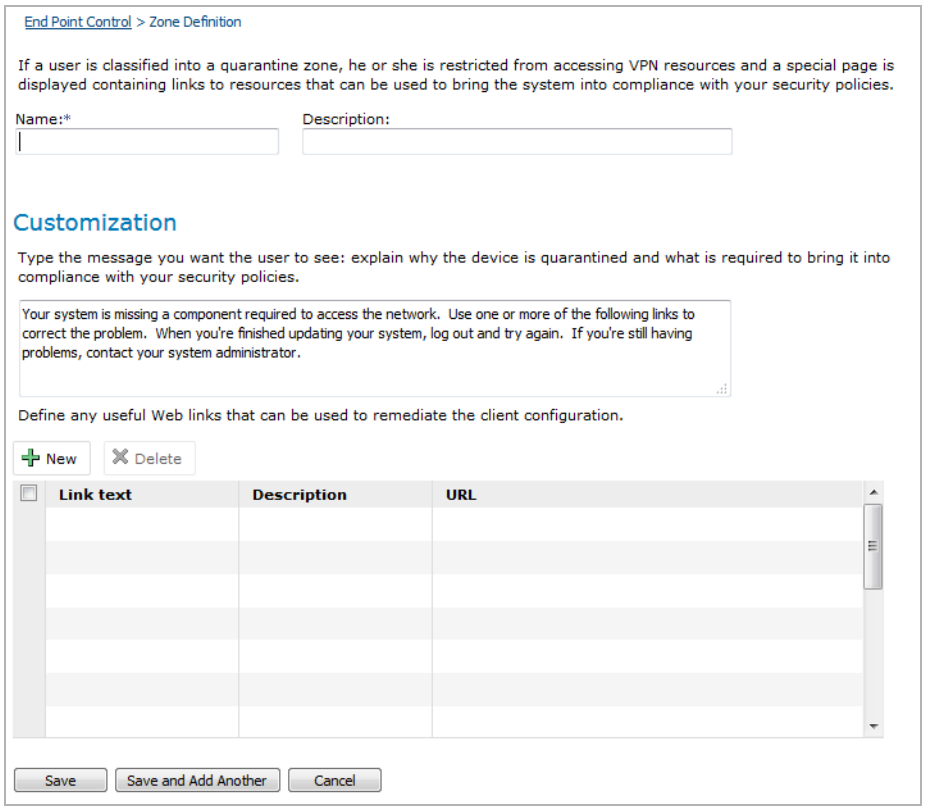
コミュニティを構成するときは、分類できないデバイスを入れるための「フォールバック」ゾーンを選択します。このようなデバイスは、**Default (デフォルト)** ゾーンまたは**Quarantine (隔離)**ゾーンに入れられます。詳細については、コミュニティでの End Point Control 制約の使用を参照してください。

隔離ゾーンを定義するには、

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Zones (ゾーン)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。

3 [**New (新規)**] を選択し、メニューから [**Quarantine zone (隔離ゾーン)**] を選択します。[**Zone Definition - Quarantine Zone (ゾーン定義 - 隔離ゾーン)**] ページが表示されます。



4 [**Name (名前)**] フィールドに、わかりやすいゾーン名を入力します。

5 (オプション) [**Description (説明)**] フィールドに、ゾーンについての分かりやすいコメントを入力します。

6 [**Customization (カスタマイズ)**] エリアに、隔離されたユーザーに提示するメッセージを入力します。デバイスが隔離ゾーンに入れられた理由や、セキュリティ ポリシーに準拠する上での要件などを記述できます。

Quarantine (隔離)ゾーンに入れられたデバイスの矯正方法としては、システムを EPC インタロゲーション向けに構成する方法についての情報を含めることが考えられます。ほとんどのユーザーの場合、これはブラウザで Java を有効にする、ActiveX を有効にする、または Java Runtime Environment (JRE) をダウンロードすることを意味します。ユーザー向けのメッセージには、次のいずれか、またはすべてを入れることができます。

- Verify that Java or JavaScript is enabled in the Web browser on the computer (in most browsers, Java is enabled by default). (コンピュータの Web ブラウザで Java または JavaScript が有効であることを確認してください (ほとんどのブラウザでは Java はデフォルトで有効)。)End point interrogation can't take place if ActiveX and Java are both disabled in the user's browser. (ユーザーのブラウザで ActiveX および Java の両方が無効になっている場合は、エンド ポイント インタロゲーションが動作することはありません。)
- If you are using Microsoft Windows and Internet Explorer, verify that ActiveX is enabled: start Internet Explorer, and then click **Internet Options** on the **Tools** menu. (Microsoft Windows および Internet Explorer をお使いの場合は、ActiveX が有効であることを確認してください。Internet Explorer を起動し、[ツール] メニューの [インターネット オプション] をクリックします。) On the **Security** tab, click the Internet logo at the top of the tab, and then click **Custom Level** to configure ActiveX controls and plug-ins. ([セキュリティ] タブで、このタブの上部にある [インターネット] のロゴをクリックして、[レベルのカスタマイズ] をクリックし、ActiveX コントロールとプラグインを構成します。)
- JRE allows Java applications or Java applets to run on personal computers. (JRE は、Java アプリケーションまたは Java アプレットが PC 上で動作できるようにするソフトウェアです。)To see if it is running on your machine, type `java -server` at the command prompt. (マシン上で JRE が動作しているか確認するには、コマンド プロンプトで java -server と入力します。)

7 ユーザーが、使用中のデバイスを準拠させる上で利用できる Web リンクを追加します。この場合、パブリック URL とプライベート URL を混在させることができます。

- パブリック アドレスは、ユーザーが Java Virtual Machine などのソフトウェア コンポーネントをダウンロードできるインターネット URL などを参照します。パブリック リソースは、通常アプライアンスを介してリダイレクトされます。このリダイレクトは、リソースを排除リストに追加することで禁止できます。手順については、リソース排除リストの使用を参照してください。
- プライベート アドレスは、最新のウイルス定義を含むイントラネット URL などを参照します。この場合、指定した URL にユーザーがアクセスでき、他のリソースにアクセスできないようにするためのルールが自動的に作成されます。

8 [**Save (保存)**] または [**Save and Add Another (保存して他を追加)**] をクリックします。

デフォルト ゾーンの構成

AMC には、グローバルの **Default (デフォルト)** ゾーンがあり、他の設定済みのゾーンに一致しない接続要求の VPN アクセスを許可またはブロックするための安全装置として機能します。アプライアンスが、ゾーンに分類できない (つまりクライアント デバイスのオペレーティング システム、ブラウザ、その他の属性などを識別できない) 接続要求を受け取った場合、デバイスは自動的に **Default (デフォルト)** ゾーンに入れられます。デバイスが **Default (デフォルト)** ゾーンに割り当てられたユーザーについては、VPN アクセスを許可するか拒否するかを選択できます。

Default (デフォルト) ゾーンは、他のゾーンと違ってデバイス プロファイルを含みませんが、データ保護エージェントの存在を求めるように構成できます。**Default (デフォルト)** ゾーンは、AMC で構成されたすべてのコミュニティに暗黙的に存在します。

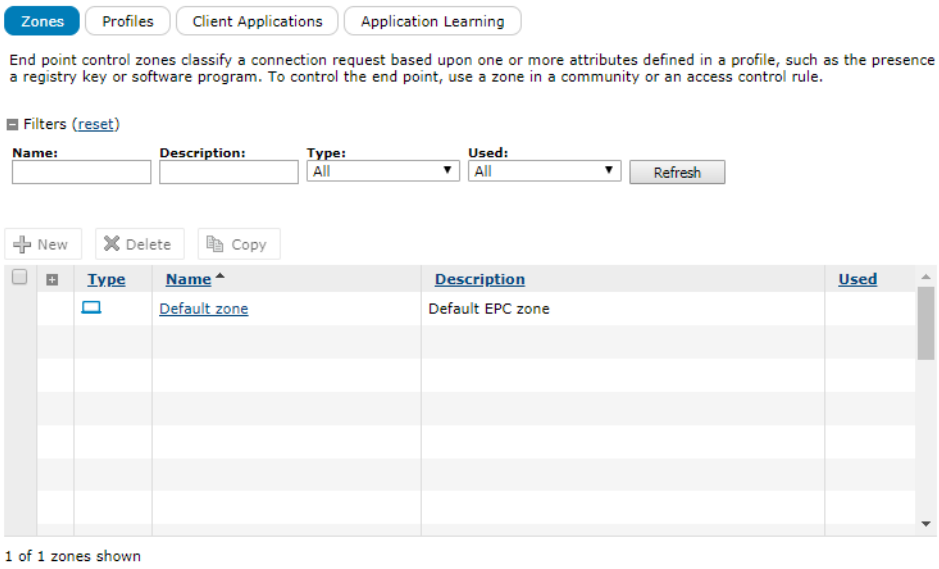
接続要求が信頼関係の基準と合致しないユーザーのアクセスを制限する場合、**Default (デフォルト)** ゾーンを制約のあるアクセス制御ルールに入れることができます。例えば、Outlook Web Access に接続する Web ブラウザに限定された「permit」アクセス制御ルールに **Default (デフォルト)** ゾーンを入れることで、これらのユーザーが自分の電子メールにアクセスできるようになります。

高レベルの信頼性に基づく制約のあるアクセス ポリシーを設け、明示的に定義されているものを除いて接続要求を認めないようにする場合は、**Default (デフォルト)** ゾーンを [**Block VPN access (VPN アクセスを遮断)**] に設定することが最善策となります。ただし、他のゾーンやアクセス制御ルールで、正当なユーザーが誤って排除される場合、**Default (デフォルト)** ゾーンが例外なくこれらのユーザーをブロックすることに注意してください。

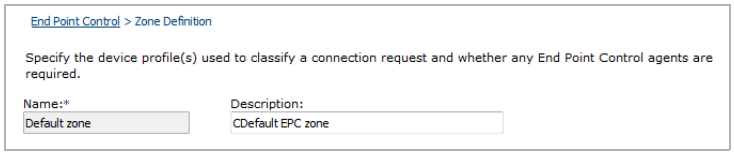
デフォルト ゾーンを構成するには、

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Zones (ゾーン)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。



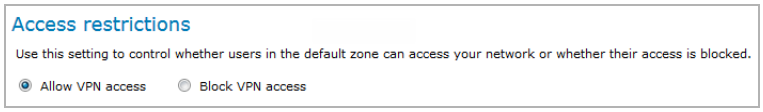
3 [**Zone (ゾーン)**] テーブルで [**Default zone (デフォルト ゾーン)**] をクリックします。[**Zone Definition - Deny Zone (ゾーン定義 - デフォルトゾーン)**] ページが表示されます。



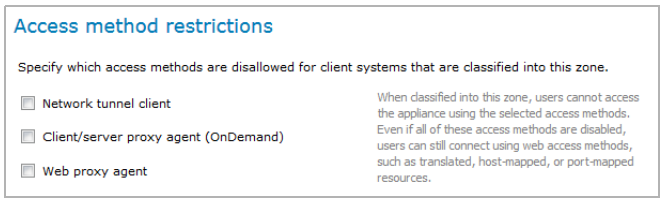
このゾーンの名前は変更できないので、[**Name (名前)**] フィールドはグレー表示です。

4 [**Access restrictions (アクセスの制限)**] セクションで、**Default (デフォルト)** ゾーンに入れられているデバイスに VPN アクセスを許可するか ([**Allow VPN access (VPN アクセスの許可)**])、またはブ

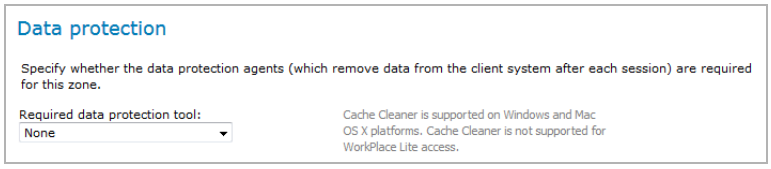
ロックするか ([**Block VPN access (VPN アクセスを遮断)**]) を指定します。[**Block VPN access (VPN アクセスを遮断)**] を選択すると、**Default (デフォルト)** ゾーンに割り当てられたユーザーはアプライアンスからログアウトさせられます。



5 [**Access method restrictions (アクセス方法の制限)**] セクションで、このゾーンに分類されるクライアントに許可されるアクセス方法を指定します (ある場合)。



6 [**Data protection (データ保護)**] セクションで、[**Default (デフォルト)**] ゾーンに入れられたクライアント デバイスが *Cache Cleaner* を使用して接続する必要があるかどうかを指定します。Cache Cleaner は Linux プラットフォーム以外のすべてのプラットフォームで強化されたデータ保護機能を提供します。



7 [**Client security (クライアント セキュリティ)**] セクションを展開します。

8 [**Recurring EPC (EPC の周期)**] セクションでは、EPC のチェック頻度を指定できます。選択:

- EPC チェックを一度だけ (ログイン時) 行う [**Check endpoint at login (ログイン時にエンド ポイントを確認する)**]
- ログイン時とその後のセッションで *<n>* 分おきに行う [**Check endpoint at login and every** *<n>* **minutes thereafter (ログイン時にエンド ポイントを確認し、セッション中は <n> 分ごとに確認する)**]

9 [**Advanced (詳細設定)**] セクションを展開します。

10 デバイスとアプライアンスの間の接続は、デバイスが同一の IPv4 または IPv6 IP アドレスを使用している限りは、中断 (セッションの一時停止と再開、一時的な接続の喪失など) が発生してもユーザーの再認証を要求せずに処理できます。

ユーザーが別の IP アドレスからセッションを再開できるように許可するには (例えば、ネットワークの異なる部分に接続して、異なる IP サブネット間でローミングする場合)、[**Advanced (詳細)**] エリアの [**Allow user to resume session from multiple IP addresses (複数の IP アドレスからのセッションの再開を許可)**] チェック ボックスを選択します。

メモ：Secure Network Detection が機能するには、このチェック ボックスを選択して、ユーザーが複数の IP アドレスからセッションを再開できるようにする必要があります。

11 [**Save (保存)**] を選択します。

ゾーンに対するデバイス プロファイルの定義

デバイス プロファイルは、アンチウイルス プログラム、アプリケーション、Windows レジストリ エントリなど、1 つまたは複数の属性を検索することにより、クライアント デバイスとの間に信頼関係を確立します。デバイス プロファイルは1 つまたは複数のゾーンから参照されます。

デバイス プロファイルは、クライアント コンピュータ上の 1 つの属性のみを検出するように定義したり、複 数の属性を必要とするように設定したりできます。デバイス プロファイルが複数の属性を参照するとき、一致するためにはクライアント コンピュータ上にすべての属性が存在しなければなりません。

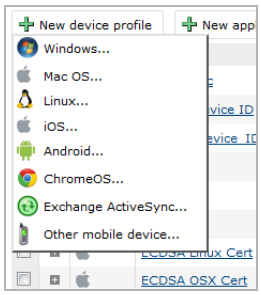
メモ：デバイス プロファイルをコピーまたは削除する方法については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

デバイス プロファイルをゾーンに定義するには、

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 このページの [**Zones and Profiles (ゾーンとプロファイル)**] エリアで、[**Profiles (プロファイル)**] の横にある [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Profiles (ゾーンとプロファイルの設定)**] ページが表示されます。

3 [**New device profile (新しいデバイス プロファイル)**] ボタンをクリックします。



4 [**New device profiles (新しいデバイス プロファイル)**] メニューから、SMA EPC 対応 デバイス プロファイルの 1 つを選択します。

- Microsoft Windows
- Apple Mac OS
- Linux オペレーティング システム
- Apple iOS モバイル オペレーティング システム
- Android モバイル オペレーティング システム
- Google ChromeOS

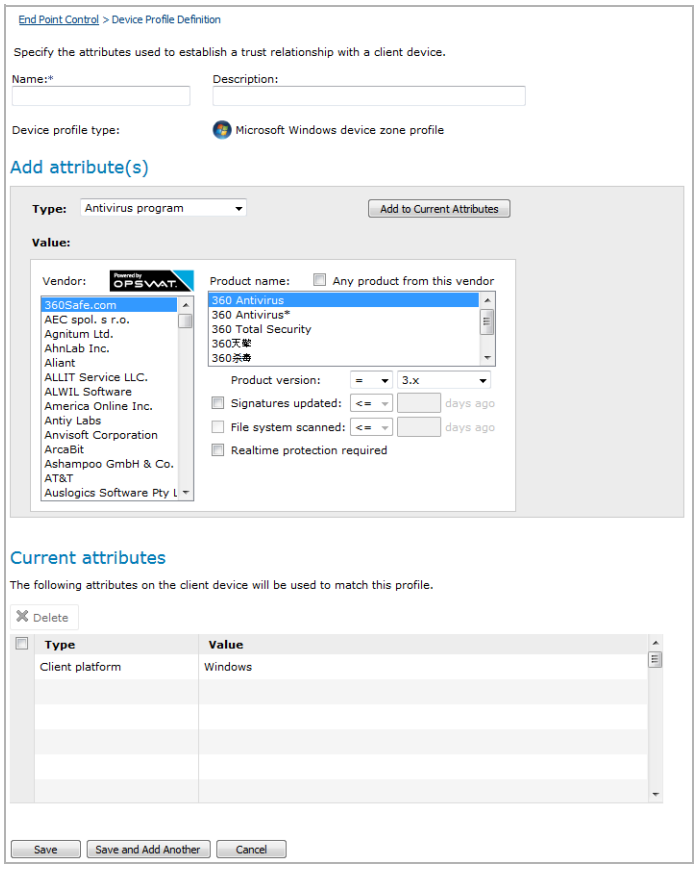
  メモ：アクセス制御ルールのプラットフォームとして、End Point Control を必要としない **ChromeOS** のポリシーを一致させることもできます。

- Exchange ActiveSync
- その他のモバイル デバイス

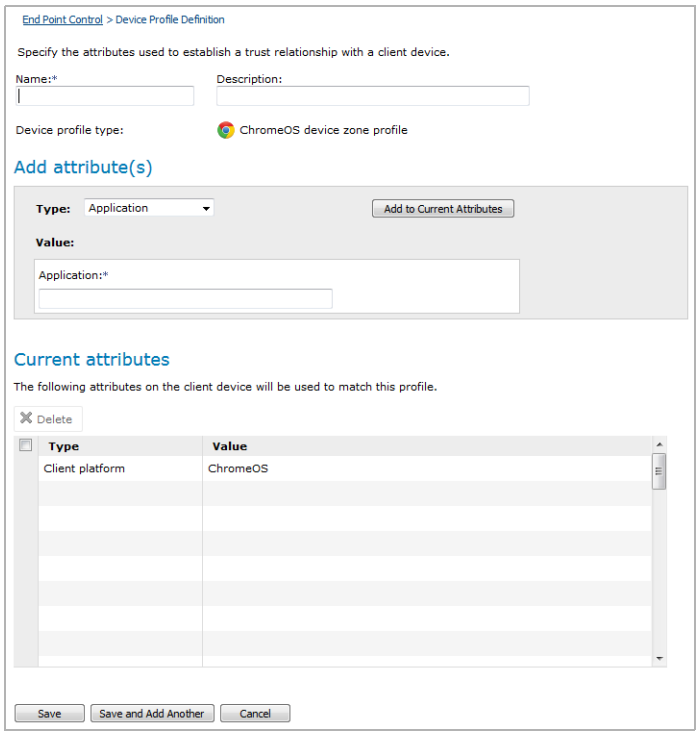
そのデバイスの [**Device Profile Definition (デバイス プロファイル定義)**] ダイアログが表示されます。例:

- Microsoft Windows のデバイス プロファイル定義
- ChromeOS のデバイス プロファイル定義

Microsoft Windows のデバイス プロファイル定義



ChromeOS のデバイス プロファイル定義



5 [**Name (名前)**]フィールドに、デバイス プロファイルの名前を入力します。

6 (オプション) [**Description (説明)**] フィールドに、デバイス プロファイルについて説明するコメントを入力します。

7 [**Value (値)**] セクションから、そのデバイス プロファイルに必要な属性を選択します。

8 各属性を選択したら、[**Add to Current Attributes (現在の属性に追加)**] をクリックします。属性は [**Current attributes (現在の属性)**] リスト (ページ下部) に追加されます。

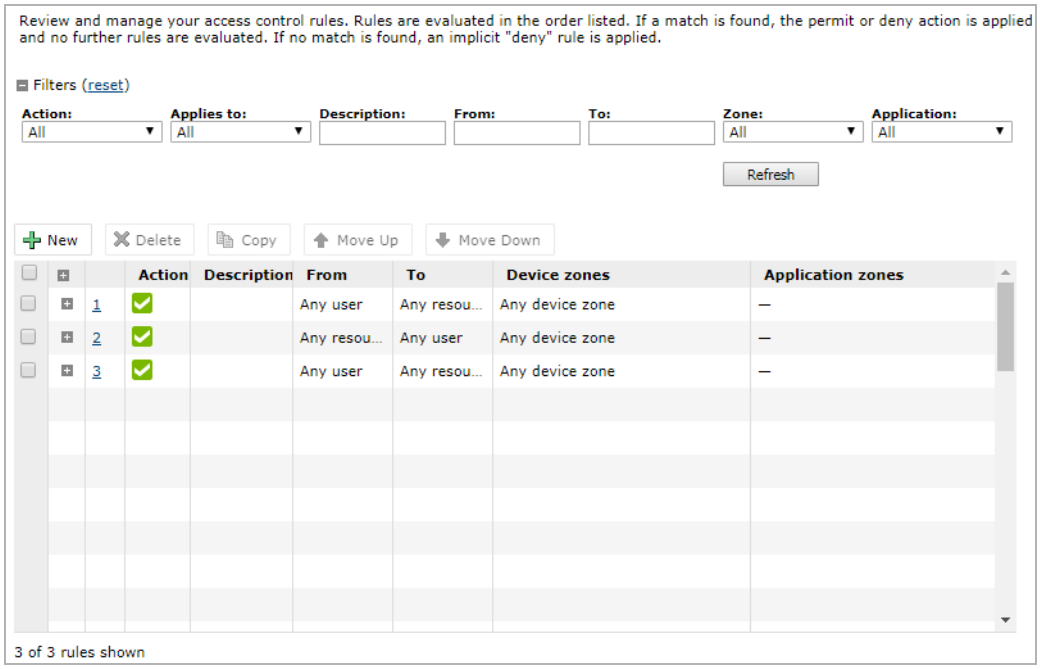
- 利用可能な属性は、選択したデバイス プロファイルに応じて異なります。例えば、*クライアント証明書*は *Linux* プロファイルの属性としては使用できず、*アンチスパイウェア プログラム*は Advanced EPC を使用するユーザーのみが使用できます。
- 1 つの属性に複数のエントリが許可される場合、デバイス プロファイルはデバイスの *すべて* (**and**) の項目に一致するか、または*いずれか* (**or**) の項目に一致する必要があります。

属性、および属性が提供されるプラットフォームの詳細については、デバイス プロファイルの属性を参照してください。

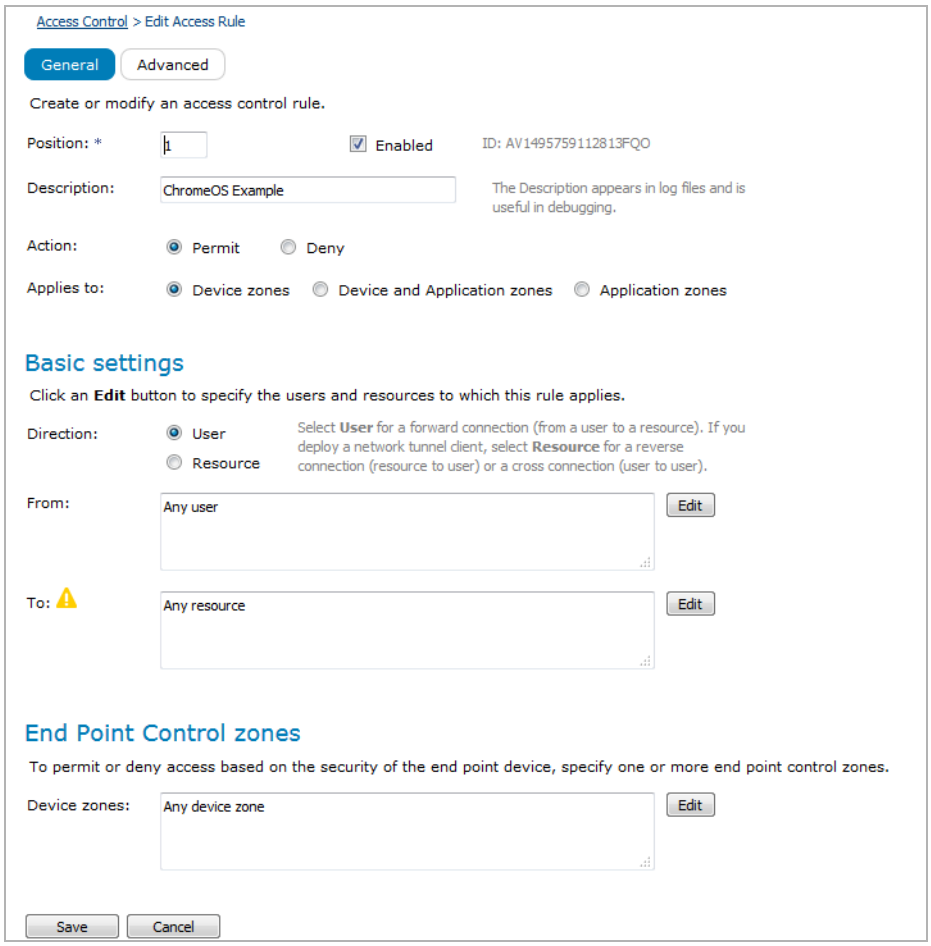
9 [**Save (保存)**] を選択します。

アクセス制御ルールのプラットフォームとして ChromeOS を設定するには:

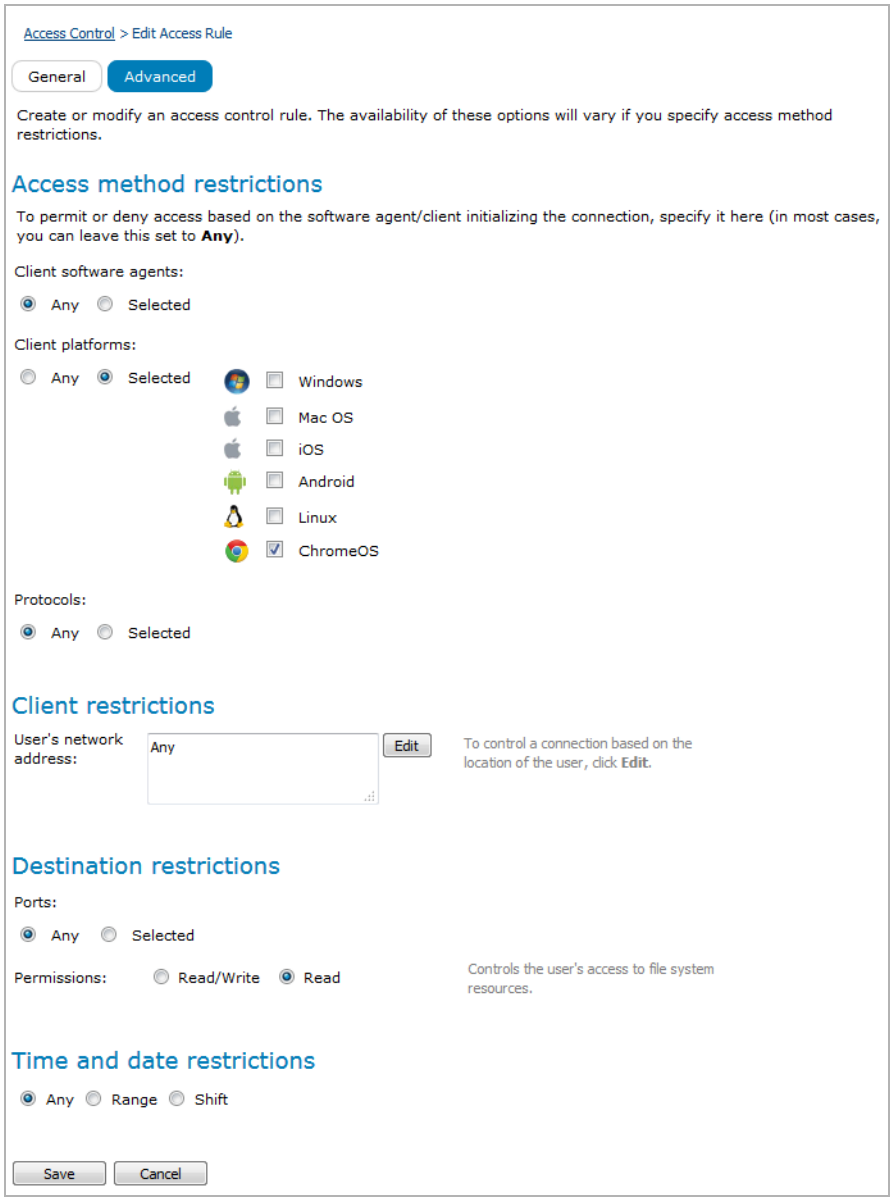
1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。[**Access Control (アクセス制御)**] ページが表示されます。



2 編集する**アクセス制御ルール**をクリックします。 [**Edit Access Rule > General (アクセス ルールの編集 > 一般)**] ページが表示されます。



3 「**詳細**」タブを選択します。[**Edit Access Rule (アクセス ルールの編集) > Advanced (詳細)**] ページが表示されます。



4 **クライアント プラットフォーム**で、[**Selected (選択済み)**] を選択してから [**ChomeOS**] を選択します。

5 [**Save (保存)**] を選択します。

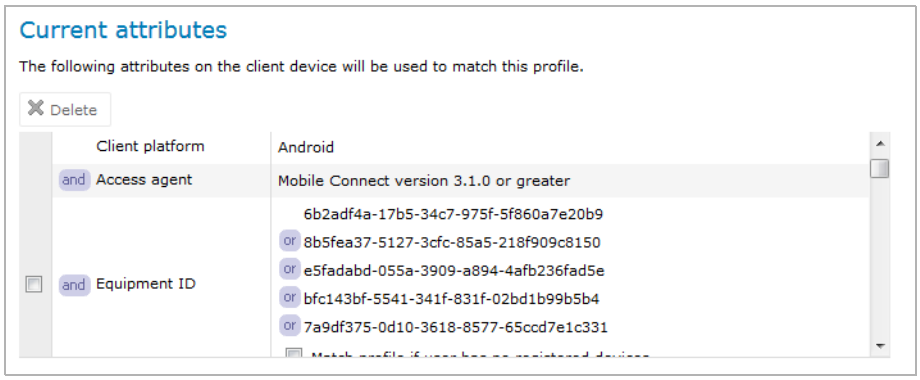
デバイス プロファイルの属性

デバイス プロファイルには、使用できるプラットフォーム、同じ種別の複数の属性 (可能な場合) が OR になるか AND になるかなど、いくつかの属性があります。

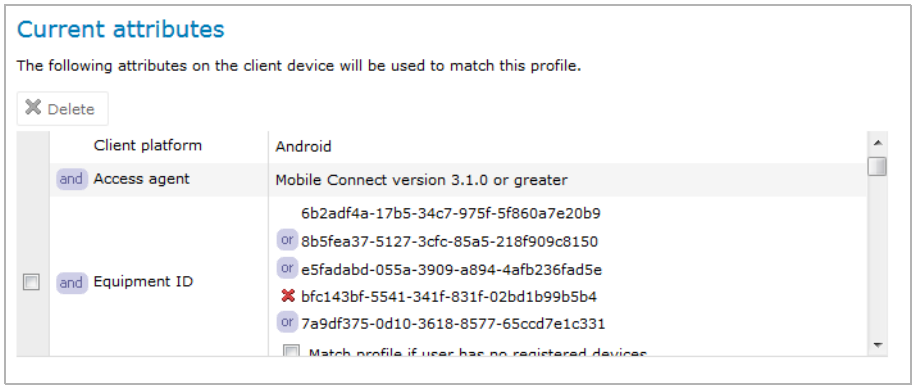
- デバイス プロファイルの属性: ChromeOS バージョン
- デバイス プロファイルの属性: Android アプリケーション
- デバイス プロファイルの属性: Android バージョン
- デバイス プロファイルの属性: アンチウイルス プログラム (Advanced EPC のみ)
- デバイス プロファイルの属性: アンチスパイウェア プログラム (Advanced EPC のみ)
- デバイス プロファイルの属性: クライアント証明書
- デバイス プロファイルの属性: ディレクトリ名
- デバイス プロファイルの属性: iOS バージョン
- デバイス プロファイルの属性: Mac OS X バージョン
- デバイス プロファイルの属性: パーソナル ファイアウォール プログラム (Advanced EPC のみ)
- デバイス プロファイルの属性: Windows ドメイン
- デバイス プロファイルの属性: Windows レジストリ エントリ

ただしこの属性については、いくつか留意しなければならない点があります。

- 選択できる属性は、デバイス プロファイルに選択したプラットフォームによって異なります。
- Advanced EPC を所有しているユーザーは、広範囲のセキュリティ プログラムから選択できます。
- 1 つの属性に複数のエントリが可能な場合、デバイス プロファイルがデバイスの *すべて* (**and**) の項目に一致するか、*いずれか* (**or**) の項目に一致するかを指定しなければなりません。



- リスト内の項目を削除するには、左の列のチェック ボックスを選択して、[**Delete (削除)**] をクリックします。単一 (**or**) の項目を削除するには (例えば、*Norton AntiVirus* を削除して *eTrust EZ Antivirus* を削除しない場合)、削除対象の左にポインタを移動して、表示される赤い「**X**」 をクリックします。



デバイス プロファイルの属性: ChromeOS バージョン

ChromeOS バージョン	プラットフォーム
オペレーティング システムのメジャー バージョン、マイナー バージョン、およびビルド番号を入力します。 [**Operator (演算子)**] の比較演算子は、3 つの値すべてに適用されます。すべてのバージョンを指定するには、[**Operator (演算子)**] に >= (以上) と入力し、[**Major (メジャー)**] フィールドにメジャー バージョン番号、および [**Minor (マイナー)**] フィールドにマイナー バージョン番号を入力します。**ビルド**番号と**パッチ**番号も指定することができます。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。	ChromeOS

デバイス プロファイルの属性: Android アプリケーション

Android アプリケーション	プラットフォーム	一致
このプロファイルについて EPC がチェックする 1 つまたは複数の Android アプリケーションを選択します。そのためには、[**Vendor (ベンダー)**] リストからベンダーを選択します。これにより、ベンダーのモバイル セキュリティ製品と現行バージョンの番号が表示されます。ベンダーが複数のモバイル セキュリティ製品を提供している場合は、すべてのモバイル セキュリティ製品が [**Product name (製品名)**] リストにリストされます。このアプリケーションで EPC がチェックするモバイル セキュリティ製品を選択します。次に、選択した製品の最新バージョンが表示されます。製品バージョン番号の比較に使用する [**Operator (演算子)**] を選択します。 デフォルトは、最新バージョンより後のすべてのバージョンです。現行バージョンと将来のすべてのバージョンを指定するには、[**Operator (演算子)**] ドロップダウン メニューから >= (以上) を選択します。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。	Android	or (いずれかに一致) and (すべてに一致)

デバイス プロファイルの属性: Android バージョン

Android バージョン	プラットフォーム
オペレーティング システムのメジャー バージョン、マイナー バージョン、およびビルド番号を入力します。 [**Operator (演算子)**] の比較演算子は、3 つの値すべてに適用されます。すべてのバージョンを指定するには、[**Operator (演算子)**] に >= (以上) と入力し、[**Major (メジャー)**] フィールドにメジャー バージョン番号、および [**Minor (マイナー)**] フィールドにマイナー バージョン番号を入力します。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。	Android

デバイス プロファイルの属性: アンチウイルス プログラム (Advanced EPC のみ)

アンチウイルス プログラム	プラットフォーム	一致
(この属性は Advanced EPC を使用している場合のみ使用できます。)EPC がこのプロファイルでチェックするアンチウイルス プログラムを選択します。詳細については、Advanced EPC: セキュリティ プログラムの拡張リストを参照してください。 Advanced EPC を使用していない場合、またはユーザーが必要とするセキュリティ プログラムが表示されない場合は、*アプリケーション*や *Windows レジストリ エントリ*などの別の属性を使用してデバイス プロファイルに追加することで、プログラムを指定できます。	Windows Mac OS Linux	or (いずれかに一致)

デバイス プロファイルの属性: アンチスパイウェア プログラム (Advanced EPC のみ)

アンチスパイウェア プログラム	プラットフォーム	一致
(この属性は Advanced EPC を使用している場合のみ使用できます。)左側でアンチスパイウェア ベンダー、右側でプログラムの名前とパラメータを選択します。 Advanced EPC を使用していない場合、またはユーザーが必要とするセキュリティ プログラムが表示されない場合は、*アプリケーション*や *Windows レジストリ エントリ*などの別の属性を使用してデバイス プロファイルに追加することで、プログラムを指定できます。	Windows Mac OS X	複数のアンチスパイウェア プログラムを追加する場合は、リスト内の*いずれか*の項目に一致すべきか (**or**) か、*すべて*の項目に一致すべきか (**and**) を指定します。

デバイス プロファイルの属性: クライアント証明書

クライアント証明書	プラットフォーム	一致
[**CA certificate (CA 認証)**] エリアのドロップダウン メニューから認証局を選択します。(希望する CA がリストされていない場合は、CA 証明書のインポートを参照)クライアント証明書をユーザーに発行した CA のルート証明書によりアプライアンスが構成されている限り、クライアント デバイスはこのプロファイルに一致します (中間証明書は機能しません)。 検索する証明書ストアを選択します。 • [**System store only (システム ストアのみ)**] は、システム ストア (*HKLM\SOFTWARE\Microsoft\SystemCertificates*) のみを検索するように指定します。 • [**System store and user store (システム ストアとユーザ ストア)**] は、システム ストアを最初に検索し、次にユーザー ストア (*HKCU\Software\Microsoft\SystemCertificates*) を検索するように指定します。 **メモ：** • デバイス プロファイルに含めることができるクライアント証明書は 1 つだけです。 • Windows Mobile 搭載デバイスには、1 ユーザーしか入れることができません。つまり、ローカル ユーザー ストアのクライアント証明書は常に同じになります。(デスクトップまたはラップトップ デバイスには複数のユーザーを設定できます)。 • ユーザーがクライアント　デバイス上で管理権限を持っていない限り、システム ストアは検索できません。	Windows Mac OS X Windows Mobile Apple iOS Android	or (いずれかに一致)

デバイス プロファイルの属性: ディレクトリ名

ディレクトリ名	プラットフォーム	一致
デバイスのハード ディスク上に存在しなければならないディレクトリの名前を入力します。ディレクトリ名は大文字小文字が区別されません。 • ジェイルブレイクされた Apple iOS デバイスの場合、ディレクトリ名は「`/Applications/Cydia.app`」になります。 **メモ：**ジェイルブレイクされた iOS デバイスのデバイス プロファイルを作成する場合は、プロファイルに拒否 EPC ゾーンを必ず構成し、このゾーンを少なくとも 1 つのコミュニティに関連付けます。	Windows Mac OS X Linux Windows Mobile Apple iOS Android	and (すべてに一致)

デバイス プロファイルの属性: 周辺機器 ID

周辺機器 ID	プラットフォーム	一致
ユーザー属性に基づいて識別子を定義するには、デバイスの識別子を入力するか、変数を使用します。 登録デバイスを 1 つも持たないユーザーに外部 AD/LDAP サーバーへのアクセスを許可するために、選択します。通常これは、デバイスの識別子をまだ登録できないユーザーにアクセスを許可するために行われます。アクセスを許可するかどうかにかかわらず、未登録デバイスからのすべてのアクセス要求は、Unregistered Device Log (未登録デバイスログ) に記録されます。	Windows Mac OS X Linux Windows Mobile Apple iOS Android	and (すべてに一致)

デバイス プロファイルの属性: ファイル名

ファイル名	プラットフォーム	一致
デバイスのハード ディスク上に存在しなければならないファイルの名前 (拡張子と完全なパスを含む) を入力します。ファイル名は大文字小文字が区別されません。環境変数 (`%windir%`、`%userprofile%` など) やワイルドカード文字 (`*` および `?`) を使用できます。 オプションで、[**File size (ファイル サイズ)**] にファイル サイズを指定でき、[**Last modified (最終更新)**] にファイルが最後に変更された日時 (GMT) を指定できます。両方のオプションとも、[**Operator (演算子)**] に比較演算子を指定できます。詳細および例については、デバイス プロファイル属性での比較演算子の使用を参照してください。ファイルの変更日時は、[**絶対値**] または [**相対値**] を選択して絶対値または相対値で指定できます。 **ファイルの整合性**の検証に MD5 または SHA-1 ハッシュを使用 (すべてのプラットフォームで有効) したり、Windows システム ファイルの検証に Windows カタログ ファイルを使用したりするように、デバイス プロファイルを構成できます。 ジェイルブレイクまたはルート化されたデバイスにより使用されるファイルの名前をチェックするデバイス プロファイルには、次のものが含まれます。 • ジェイルブレイクされた Apple iOS デバイスの場合、ファイル名は「`cydia`」になります。 • ルート化された Android デバイスの場合、ファイル名は「`/system/bin/su`」と「`/system/xbin/su`」になります。 **メモ**：ジェイルブレイクされた iOS デバイスまたはルート化された Android デバイスのデバイス プロファイルを作成する場合は、各プロファイルに拒否 EPC ゾーンを必ず構成し、これらのゾーンをそれぞれ少なくとも 1 つのコミュニティに関連付けます。	Windows Mac OS X Linux Windows Mobile Apple iOS Android	and (すべてに一致)

デバイス プロファイルの属性: iOS バージョン

iOS バージョン	プラットフォーム
オペレーティング システムのメジャー バージョン、マイナー バージョン、およびビルド番号を入力します。例えば、iOS 5.0.1 build 9A405 については、[**Major (メジャー)**] に5、[**Minor (マイナー)**] に 0、[**Build (ビルド)**] に 9A405 と指定します。 [**Operator (演算子)**] の比較演算子は、3 つの値すべてに適用されます。例えば、5.0 のすべてのバージョンを指定するには、[**Operator (演算子)**] に >= (以上) と入力し、[**Major (メジャー)**] フィールドに 5、[**Minor (マイナー)**] フィールドに 0 と入力します。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。	Apple iOS

デバイス プロファイルの属性: Mac OS X バージョン

Mac OS X バージョン	プラットフォーム
オペレーティング システムのメジャー バージョン、マイナー バージョン、およびビルド番号を入力します。Mac OS のバージョンの例を次に示します。 • v10.2 (Jaguar) • v10.3 (Panther) • v10.4.4 (Tiger) • v10.5.6 (Leopard) [**Operator (演算子)**] の比較演算子は、3 つの値すべてに適用されます。例えば、Leopard のすべてのバージョンを指定するには、[**Operator (演算子)**] に >= (以上) と入力し、[**Major (メジャー)**] フィールドに 10、[**Minor (マイナー)**] フィールドに 5 と入力します。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。	Mac OS X

デバイス プロファイルの属性: パーソナル ファイアウォール プログラム (Advanced EPC のみ)

パーソナル ファイアウォール プログラム	プラットフォーム	一致
(この属性は Advanced EPC を使用している場合のみ使用できます。) EPC がこのプロファイルでチェックするファイアウォール プログラムを選択します。詳細については、Advanced EPC: セキュリティ プログラムの拡張リストを参照してください。 Advanced EPC を使用していない場合、またはユーザーが必要とするセキュリティ プログラムが表示されない場合は、*Application (アプリケーション)* や *File name (ファイル名)* などの別の属性を使用してデバイス プロファイルに追加することで、プログラムを指定できます。	Windows Mac OS X Linux	or (いずれかに一致)

デバイス プロファイルの属性: Windows ドメイン

Windows ドメイン	プラットフォーム	一致
コンピュータが属するドメイン名を、DNS 接尾辞を付けずに NetBIOS 構文で入力します (mycompany など)。複数のエントリは、セミコロンを使用して区切ります。ドメインにはワイルドカード文字 (* と ?) を使用できます。 **メモ**：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。	Windows	or (いずれかに一致)

デバイス プロファイルの属性: Windows レジストリ エントリ

Windows レジストリ エントリ	プラットフォーム	一致
[**Key name (キー名)**] にキー名を入力します。また、オプションで [**Value name (値名)**] に値、[**Data (データ)**] にデータを入力できます。[**Data (データ)**] フィールドでは [**Operator (演算子)**] に比較演算子を選択できます。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。 ワイルドカードは値とデータの指定に使用できますが、キーには使用できません。特殊文字 (ワイルドカードやバックスラッシュなど) を使用する場合は、その前にバックスラッシュを付ける必要があります。	Windows Windows Mobile	and (すべてに一致)

デバイス プロファイルの属性: Windows バージョン

Windows バージョン	プラットフォーム
オペレーティング システムのメジャー バージョン、マイナー バージョン、およびビルド番号を入力します。Windows のメジャー/ マイナー バージョンの例を次に示します。 • Windows Vista: 6/0 • Windows 2000: 5/0 [**Operator (演算子)**] の比較演算子は、3 つの値すべてに適用されます。詳細については、デバイス プロファイル属性での比較演算子の使用を参照してください。	Windows Windows Mobile

Advanced EPC: セキュリティ プログラムの拡張リスト

Advanced EPC は、セキュリティ プログラムの詳細な拡張リストを提供するオプション コンポーネント (別途のライセンス) です。EPC デバイス プロファイルを構成して、Microsoft Windows や Mac OS X を実行するクライアントでパーソナル ファイアウォール、アンチウイルスおよびスパイウェア プログラムをチェックしたり、Linux を実行するクライアントでパーソナル ファイアウォールやアンチウイルス プログラムをチェックしたりできます。

Advanced EPC には組み込みデバイス プロファイル リストが含まれ、そのままで、または変更して使用できます (詳細は Advanced EPC: 構成済みのデバイス プロファイルの使用を参照)。

メモ：クライアントの OESIS ライブラリのバージョンは、接続するアプライアンスで設定される OESIS ライブラリのバージョンと常に同じになります。バージョンの不一致がある場合は、クライアントはアプライアンスから OESIS ライブラリをプロビジョニングします。

Advanced EPC を使用して属性を追加するには、

1 AMC のメイン ナビゲーション メニューから、「**エンド ポイント制御**」をクリックします。

2 [**Zones and Device Profiles (ゾーンとデバイスのプロファイル)**] セクションの [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Devices (ゾーンとデバイスの設定)**] ページが表示されます。

3 [**Device Profiles (デバイス プロファイル)**] セクションで [**New (新規)**] をクリックして、リストから任意のオペレーティング システム を選択します

4 [**Name (名前)**] にプロファイル名を指定したら ([**Description (説明)**] はオプション)、[**Type (種別)**] に EPC がチェックするプログラムの種別タイプ (*アンチウイルス プログラム*など) を選択します。(Linux プラットフォームでは *アンチスパイウェア プログラム* を選択できません。)

5 [**Vendor and Product name (ベンダーと製品名)**] にベンダーと製品名をそれぞれ選択します。Windows デバイス プロファイルでは、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム ベンダーについて [**Any product from this vendor (このベンダーのすべての製品)**] チェックボックスを選択し、すべての製品名を選択して、ベンダーが新バージョンをリリースするたびに更新する必要がないプロファイルを作成します。このオプションを選択する場合でも、リスト内のすべての製品のすべてのバージョンが当該機能をサポートする限り、更新されたシグネチャ、スキャンされたファイル システム、有効なリアルタイムの保護などの追加条件を指定する必要があります。

6 [**Product version (製品バージョン)**] に製品バージョンを絶対値または相対値で指定します。

一部の製品はいくつかの異なる名称で知られています。例えば、McAfee 社は *McAfee VirusScan* というコア製品を提供していますが、これは *McAfee VirusScan 2004* および *McAfee VirusScan 2005* という名称でも知られています。(アスタリスクが付いた製品名を選択すると、その「コア」製品名を示す補足情報が表示されます)。補足情報に示された名前を使用することが推奨されます。これにより、コア製品が新しい名称で販売されるたびに、デバイス プロファイルを更新する必要がなくなります。

7 デバイス プロファイルで必要なセキュリティ プログラム設定をより細かく定義できるように、次のようなオプション パラメータが提供されます (各プログラムですべてのパラメータが選択可能なわけではありません。選択できないパラメータはグレー表示されています)。

- **シグネチャ更新**: クライアント デバイスで、アンチスパイウェアまたはアンチウイルスのシグネチャのリストがどの程度最近更新されたかを定義します。
- **スキャンされたファイル タイプ**: このアンチスパイウェアまたはアンチウイルス プログラムを使用して、クライアント デバイスのディスクがどの程度最近スキャンされたかを定義します。

- **リアルタイム防御要件**: デバイス プロファイルでウイルスやスパイウェアのリアルタイム スキャンを有効にすることを要求する場合は、このチェック ボックスを選択します。

8 [**Add to Current Attributes (現在の属性に追加)**] ボタンをクリックして、エントリをリスト (ページ下部) に追加します。他のプログラムを追加する場合 (例えばデバイス プロファイルが複数のプログラムをチェックするように指定する場合)、デバイス プロファイルはデバイス上の *すべて* (**and**) または*いずれか* (**or**) の項目に一致しなければなりません。

- 追加のアンチウイルス プログラムはグループ化されますが、デバイス プロファイルではいずれか 1 つのプログラムに一致することだけが求められます。
- 複数のアンチスパイウェア プログラムを指定する場合は、すべてが必須か (**and**) 、いずれか 1 つだけが必要か (**or**) を指定できます。

9 「**Save (保存)**」を選択します。

メモ：選択できる製品名には、極東言語の文字を使用しているものも含まれます。オペレーティング システム でインターナショナル サポートが有効になっていない場合、これらの文字はボックスや疑問符で表示されることがあります。例えば Symantec 製品の中には、適切なフォントがサポートされていない場合に次のように表示される製品名があります。

Symantec AntiVirus Client
Symantec AntiVirus □□□
Symantec AntiVirus Server

インターナショナル サポートが有効な場合は、次のように表示されます。

Symantec AntiVirus Client
Symantec AntiVirus 用戶端
Symantec AntiVirus Server

Advanced EPC: フォールバック検出の使用

フォールバック検出は、Advanced EPC を使用して、OESIS で識別されるよりも新しいベンダー ソフトウェア バージョンを検出します。これにより、ゾーンの分類が継承されます。フォールバック検出は、すべて検出したいバージョンについて、EPC 定義を使用して完全に信頼するプロファイルを補完します (例えば、Microsoft Security Essentials バージョン 4.x 以降)。Windows Security Center (WSC) を使用するフォールバック検出は、Windows ベースのアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール製品向けに構成できます。

例えば、ユーザーは McAfee Antivirus を使用してログインする際に信頼ゾーンに入れられます。より新しいバージョンの McAfee に更新してログインすると、WSC のフォールバック機能により信頼フォールバック ゾーンに一致し、アクセスが許可されます。

Secure Mobile Access が McAfee の新しいバージョンをサポートするようになると、信頼ゾーンのポリシーを更新するだけで新しいバージョンを含めることができます。これにより、管理者はアンチウイルスの特定バージョンに一致するデバイスと、特定バージョンに一致せずにフォールバック ロジックに一致するデバイスを簡単に区別できます。

メモ：フォールバック検出を使用するには、プライマリ EPC ゾーンのデバイス プロファイルの構成で [**Any product from this vendor (このベンダーのすべての製品)**] オプションを「非選択」にして、アンチウイルス、アンチスパイウェア、およびファイアウォール製品の特定バージョンを含める必要があります。

フォールバック検出を構成するには:

1 これらの値を使用して、信頼されるフォールバック用に新しいデバイス プロファイルを作成します。

a AMC のメイン ナビゲーション メニューから、「**エンド ポイント制御**」をクリックします。

b [**Zones and Device Profiles (ゾーンとデバイスのプロファイル)**] セクションの [**Edit (編集)**] リンクをクリックします。[**Configure Zones and Devices (ゾーンとデバイスの設定)**] ページが表示されます。

c [**Device Profiles (デバイス プロファイル)**] セクションで [**New (新規)**] をクリックしてから [**Microsoft Windows**] を選択します

d [**Name (名前)**] に新しいデバイス プロファイルの名前を入力します。

e [**Type (種別)**] ドロップダウン メニューから、[**Antivirus program (アンチウイルス プログラム)**]、[**Antispyware program (アンチスパイウェア プログラム)**]、または [**Personal firewall program (パーソナル ファイアウォール プログラム)**] を選択します。

f [**Vendor (ベンダー)**] ドロップダウン メニューから、その製品を提供するベンダーを選択します。

g [**Product (製品)**] ドロップダウン メニューから、[**Other (その他)** <***vendor (ベンダー)***> <***type (種別)***>] (「**Other Aliant Firewall (その他の Aliant ファイアウォール)**」など) を選択します。

[**Any product from this vendor (このベンダーのすべての製品)**] チェックボックスは**非選択**にします。

h [**Product version (製品バージョン)**] を >= *x* に設定します。

i [**Signatures updated (シグネチャ更新)**] と [**Realtime protection required (リアルタイム防御要件)**] を有効にします (該当する場合)。

j [**Save (保存)**] を選択します。

2 信頼フォールバック ゾーンを作成して、このゾーンに信頼フォールバック プロファイルを追加します。

オプションで、セキュリティ要件に応じて、信頼および信頼フォールバックのプロファイルを 1 つのゾーンに組み合わせることができます。ただし、個別の信頼フォールバック ゾーンを使用することで、ユーザーが信頼ゾーンに一致しないソフトウェアを更新するときに簡単に把握できるので、信頼ゾーンに新バージョンを追加するタイミングが分かります。

3 コミュニティで、信頼ゾーンのすぐ下にあるレルム リストに信頼フォールバック ゾーンを追加します。

Advanced EPC: 構成済みのデバイス プロファイルの使用

End Point Control の導入を支援するため、構成済みのデバイス プロファイルがいくつか用意され、オペレーティング システムごとにグループ化されています。これらのデバイス プロファイルはそのまま、またはアクセス ポリシーやリソース要件に合わせて変更して使用できます。AMC のメイン ナビゲーション メニューから [**End Point Control (エンド ポイント制御)**] をクリックして、[**Zones and Device Profiles (ゾーンとデバイスのプロファイル)**] セクションで [**Edit (編集)**]をクリックします。これにより、次のリストが表示されます。

構成済みのデバイス プロファイル

Windows	Mac OS X	Linux
Windows	MAC	Linux
Windows - Home Users	Mac OS X - Home Users	Linux - Antivirus
Windows - McAfee Corporate	Mac OS X - McAfee Corporate	
Windows - Norton Corporate	Mac OS X - Norton Corporate	
Windows - Sophos Corporate		
Windows - Trend Micro Corporate		

例えば *Windows - McAfee Corporate* という名前のデバイス プロファイルは、McAfee VirusScan Enterprise (バージョン 7.50.0 以降) の他、構成済み McAfee Corporate プロファイル に示す指定されたパーソナル ファイアウォール製品のいずれかが必要となるように、あらかじめ構成されています。

構成済み McAfee Corporate プロファイル

属性タイプ	製品名
アンチウイルス プログラム	McAfee VirusScan Enterprise バージョン 7.5.0.x 以降
および	
パーソナル ファイアウォール	McAfee Personal Firewall Express バージョン 5.x 以降
	または
	McAfee Personal Firewall Plus バージョン 5.x 以降

これらの構成済みプロファイルを元にして、独自のプロファイルを作成できます。環境にもっとも近いプロファイルをコピーして変更します。例えば、承認できる製品バージョンや、クライアント デバイスでアンチスパイウェアまたはアンチウイルスのシグネチャのリストがどの程度最近更新されていなければならないかという要件などを変更できます。現在の属性リスト内の行全体を削除するには、その行に対応するチェックボックスを選択して、[**Delete (削除)**] をクリックします。OR リストの項目 (例えば、*McAfee Corporate* プロファイルのパーソナル ファイアウォール製品の 1 つ) を削除する場合は、マウスのカーソルを「or」の上に動かして、表示される赤の「X」をクリックします。

デバイス プロファイル属性での比較演算子の使用

一部のデバイス プロファイル属性は、利用可能な比較演算子 に示す比較演算子を使用して変更できるので、次のような状況で使用すると便利です。

- クライアント デバイス上のソフトウェアが自動的に更新される場合、そのソフトウェアに合わせてデバイス プロファイルが更新されるようにする場合。ソフトウェアが更新されるたびに手動でプロファイルを変更する必要がありません。
- 特定の日時よりも新しいタイムスタンプを持つファイルのみがクライアント マシン上で検出されるよう指定する場合。
- 特定のバージョン以降の Windows オペレーティング システムがクライアント デバイス上で検出されるよう指定する場合。

利用可能な比較演算子

演算子	説明
<	より小さい
<=	以下
=	等しい
>=	以上
>	より大きい
!=	等しくない

比較演算子は、次のデバイス プロファイル属性と組み合わせて使用できます。

- 特定ファイルの日付もしくはタイムスタンプ
- 特定ファイルのサイズ

- レジストリ エントリ (レジストリ キーに値データが選択されている場合)
- Windows バージョン
- 高度な End Point Control

例

この例では、Microsoft Windows が動作するパソコンで、最近更新されたファイルを検出する方法を説明します。

相対または絶対ファイル日付を指定するには、

1 AMC のメイン ナビゲーション メニューから、「**エンド ポイント制御**」をクリックします。

2 [**Zones and Device Profiles (ゾーンとデバイスのプロファイル)**] セクションで [**Edit (編集)**] リンクをクリックし、[**Device Profiles (デバイス プロファイル)**] セクションで [**New (新規)**] をクリックします。

3 メニューから [**Microsoft Windows**] を選択します。

4 [**Name (名前)**] フィールドに、わかりやすいデバイス プロファイル名を入力します。

5 (オプション) [**Description (説明)**] フィールドに、デバイス プロファイルについての分かりやすいコメントを入力します。

6 [**Add attribute(s) (属性の追加)**] エリアで、[**Type (種別)**] リストから [**File name (ファイル名)**] を選択します。

7 [**File name (ファイル名)**] フィールドに `weekly_timesheet.xls` と入力します。ファイルのタイム スタンプを指定する方法の 2 つの例を示します。

   - *weekly_timesheet.xls* が過去 5 日以内に更新されていることを指定する場合、[**Last modified (最終更新)**] リストから <= を選択し、[**Relative (相対関係)**] をクリックしてフィールドに `5` と入力します。
   - このファイルが 2017 年 6 月 1 日以降に更新されたことを指定する場合、[**Last modified (最終更新)**] リストから >= を選択し、[**Absolute (絶対値)**] をクリックしてフィールドに `06/01/2017` と入力します。

8 [**Add to Current Attributes (現在の属性に追加)**] をクリックし、[**Save (保存)**] をクリックします。

Connect Tunnel クライアントでの End Point Control の使用

Connect Tunnel クライアントを使用してアプライアンスに接続するデバイスで、End Point Control を使用できます。Connect Tunnel クライアントの EPC の場合も、他の方式の場合と同様にデバイス プロファイルと EPC ゾーンの使用がサポートされています。ただし、Connect Tunnel クライアントでは、Cache Cleaner がサポートされません。これらのデータ保護オプションは、Connect Tunnel クライアントでは無視されます。

反復 EPC チェックの実行: 例

接続要求は、デバイス プロファイルに定義された属性に基づいて EPC ゾーンに分類されます。このチェックは、ユーザーのログイン時に常に実行されます。さらに、特定のゾーンについてデバイスがプロファイルに一致し続けているかどうかを一定間隔でチェックするオプションも使用できます。

この設定の使用方法を、例で説明します。このシナリオでは、システム管理者が組織内の各システム エンジニアに USB デバイスを提供しています。このデバイスは、SMA アプライアンスにより保護さ

れるリソースへのアクセスを提供します。これにより、2 要素認証が提供されます。ユーザーのセッション中に、アプライアンスは USB デバイスに関連付けられているクライアント証明書の存在を繰り返しチェックします。チェックが失敗するとセッションが終了します。ユーザーの認証の基本部分 (クライアント証明書) は USB デバイス上に存在するため、システム エンジニアがキーを取り外すと認証データはシステムに残りません。

システム エンジニアから見た場合は、次のように認識されます。

1 自分の USB デバイスを任意のデスクトップやラップトップ デバイス (信頼されるか信頼されないかを問わず) に挿入します。デバイスで Windows Vista と Internet Explorer 7 が実行されている場合は、保護モードをオフにする必要があります。

2 自分の PIN を入力します。

3 VPN にアクセスするためにログインし、認証します。ログイン時、およびその後定期的な間隔で、SMA アプライアンスが自分のクライアント証明書をチェックします (チェック間隔は SMA アプライアンスの管理者が設定します)。USB デバイスを取り外すと、チェックが失敗して接続が終了します。

メモ：接続に USB デバイスの存在が必要であることを、ユーザーが理解することが重要です。このため、USB デバイスを挿入したまま放置してはなりません。

管理者が実行する必要のある構成手続きの概要は、次のとおりです。

1 USB デバイスとアプライアンスの間の信頼関係を確立するには、EPC デバイス プロファイルのルート CA の証明書を参照する必要があります。証明書がすでに存在しない場合は、アプライアンスに証明書をインポートします (メイン ナビゲーション メニューの [**SSL Settings (SSL 設定)**] をクリックして、[**CA Certificates (CA 証明書)**] エリアで [**Edit (編集)**] をクリックします)。

2 アプライアンス管理コンソール (AMC) を使用して、Windows、Mac、または Linux デバイス向けデバイス プロファイルを作成します。これにより、配布予定の USB デバイスでクライアント証明書の存在がチェックされます。証明書は、ステップ 1 のルート証明書に由来するものでなければなりません。Windows 向けデバイス プロファイルを作成する際は、システムとユーザー証明書の両方のストアを必ず検索対象とします。

3 前の手順からのデバイス プロファイルを必要とする EPC 標準ゾーンを作成します。

4 ゾーンを定義する際に、このゾーンに分類されるクライアント システムに対する EPC のチェック間隔を、[**Recurring EPC (EPC の周期)**] エリアで指定します。このケースでは、頻繁なチェック (例えば、毎分のチェック) を実行するように指定します。

5 一致するプロファイルがないデバイス (クライアント証明書が手順 1 で特定されたルート CA 証明書に由来しない、または USB デバイスに証明書がない) は、**Default (デフォルト)** ゾーンまたは **Quarantine (隔離)**ゾーンのいずれかに「送り込まれる」ことになります。

- 設定した条件を満たさない接続要求に対してアクセスを拒否するには、デフォルト ゾーンが単純にアクセスを拒否するように構成します。[**Zone Definition (ゾーン定義)**] ページの [**Access restrictions (アクセスの制限)**] エリアで、[**Block VPN access (VPN アクセスを遮断)**] を選択します。
- 必要に応じて、**Quarantine (隔離)**ゾーンを作成し、ユーザーに提示されるメッセージをカスタマイズすることも可能です。例えば、ユーザーのシステムをセキュリティ ポリシーに準拠させる上での必要事項を説明できます。

特殊な状況向けのゾーンの作成

大部分の接続要求 (Microsoft Windows と Internet Explorer、Google Chrome または Mozilla Firefox を使用する要求) は、標準のゾーン構成で対応できますが、他のオペレーティング システムやブラウザ、または定義済みのゾーンのいずれにも一致しない接続要求といった特殊な状況に対応しなければならない場合もあります。ゾーンとデバイス プロファイルを使用すると、次のような状況に対応できます。

- 定義されているゾーンやデバイス プロファイルの基準に一致しないクライアント。
- クライアントを EPC ゾーンに分類する上で必要な EPC インタロゲーションをサポートしていないクライアント。
- Windows で特定の Web ブラウザ (Internet Explorer、Google Chrome、および Firefox 以外) を実行するクライアント、 または以前のバージョンの Windows を実行するユーザー。
- 実行するクライアント デバイスに関係なくアクセスを必要とする特殊なクラスのユーザー。

また、グローバルの**Default (デフォルト)** ゾーンを構成し、AMC で構成されているすべてのコミュニティに暗黙的に存在するようにします。

トピック: 。

- 特定のブラウザまたは以前のバージョンの Windows に対するゾーンの定義
- 未登録デバイスからの機器 ID の収集
- 特殊なクラスのユーザーに対するゾーンの定義

特定のブラウザまたは以前のバージョンの Windows に対するゾーンの定義

ユーザーが SMA アプライアンスに接続する場合、アプライアンスはユーザーのコンピュータのインタロゲーションを実行し、(例えば) 動作中のオペレーティング システムおよび使用中の Web ブラウザを判定します。EPC では、Windows 7 (またはそれ以降) と Internet Explorer が必要ですが、このような要件に一致しないユーザー向けに特殊なゾーンを定義できます。これにより、ユーザーがデフォルト ゾーンに配置され、アクセスがブロックされることがないように対処できます。このゾーンのタイプを区別するための唯一の属性は、Windows システムの存在です。

この構成は、Windows XP よりも前のバージョンの Microsoft Windows を実行するユーザー向けにゾーンを定義するときにも使用できます。

非標準ブラウザを使用するクライアント向けのゾーンを定義するには、

1 AMC のメイン ナビゲーション メニューから、「**エンド ポイント制御**」をクリックします。

2 [**End Point Control Settings (エンド ポイント制御設定)**] ページの [**Zones and Device Profiles (ゾーンとデバイスのプロファイル)**] セクションで、[**Edit (編集)**] リンクをクリックします。[**Configure Zones and Devices (ゾーンとデバイスの設定)**] ページが表示されます。

3 [**Zones (ゾーン)**] セクションで [**New** (新規)] をクリックして、メニューから [**Standard zone (標準ゾーン)**] を選択します。[**Zone Definition (ゾーン定義)**] ページが表示されます。

4 [**Name (名前)**] フィールドに、わかりやすいゾーン名を入力します。

5 [**Description (説明)**] フィールドに、特殊ブラウザ ゾーンについての分かりやすいコメントを入力します。

6 [**Device Profiles (デバイス プロファイル)**] セクションで [**New (新規)**] をクリックし、メニューから [**Microsoft Windows**] を選択します。[**Device Profile Definition (デバイス プロファイルの定義)**] ページが表示されます。

7 [**Name (名前)**] フィールドに、わかりやすいデバイス プロファイル名を入力します。

8 [**Description (説明)**] フィールドに、デバイス プロファイルについての分かりやすいコメントを入力します。

9 [**Add attribute (属性の追加)**] エリアで、[**Type (種別)**] リストから [**Windows version (Windows バージョン)**] を選択して、[**Add to current attributes (現在の属性に追加)**] をクリックします。他の属性設定は指定しないでください。

10 [**Save (保存)**] を選択します。

11 このゾーンに入れたいブラウザの**デバイス プロファイル**に対応するチェック ボックスを選択します。

12 >> ボタンを使用して、項目を [**In use (使用中)**] リストに移動させます。

13 このデバイス プロファイルでデータ保護コンポーネントの存在を要求する場合は、[**Required data protection tool (必須データ保護ツール)**] リストから、[**Cache Cleaner (キャッシュ クリーナー)**] を選択します。

Cache Cleaner は Linux プラットフォームではサポートされていません。

14 ゾーンの設定が終了したら、[**Save (保存)**] をクリックします。

未登録デバイスからの機器 ID の収集

Windows デスクトップおよびモバイル デバイスは、それぞれ一意の識別子を持ちます。この識別子をデバイス プロファイルで使用することにより、特定デバイスだけが保護されたリソースにアクセスできるように保証できます。ただし、機器 ID データをディレクトリ サーバーにユーザー属性として追加するには、まずデータを収集する必要があります。これには、いくつかの方法があります。

- 未登録デバイスのデバイス プロファイルを作成し、ユーザーのログインを実行する。これにより、デバイス ID が登録されていないデバイスログに収集されます。未登録デバイスを許可するデバイス プロファイルの作成を参照してください。
- デバイス ID を使用するが [**Match Profile if user has no registered devices (ユーザーが登録デバイスを持たない場合はプロファイルを一致させる)**] オプションが有効化されていないデバイス プロファイルを作成する。デバイス プロファイルでの [Match Profile if user has no registered devices (ユーザーが登録デバイスを持たない場合はプロファイルを一致させる)] の無効化を参照してください。
- 未登録デバイスを使用してログインするユーザーに一致するデバイス プロファイルに関連付けられた隔離ゾーンを作成する。未登録デバイスの隔離を参照してください。
- 未登録デバイスを使用してログインするユーザーに一致するデバイス プロファイルに関連付けられた拒否ゾーンを作成する。未登録デバイスのロック アウトを参照してください。
- 未登録デバイスによるログインの試行についてのログ メッセージを、外部マシンにエクスポートする。外部マシンでは、IT 管理者がリストを表示してデバイスを登録するか、またはデバイスが自動的に登録されます。外部処理向けとしての未登録デバイス ログのエクスポートを参照してください。

メモ：バックエンド AD または LDAP サーバーに登録されているデバイスをユーザーが使用していず、またデバイス プロファイルにハード コーディングされたデバイスがない場合、[**Match profile if user has no registered devices (ユーザーが登録デバイスを持たない場合はプロファイルを一致させる)**] チェック ボックスが選択されていれば適用可能になります。

例えば、AD/LDAP サーバーでユーザー *test* 向けに 2 つの属性が作成されている場合、これらの属性は 2 つのポリシー変数にマッピングされます。デバイス プロファイルが作成され、これら 2 つの変数と機器 ID の *4JV5DQH1* が含まれます。チェックボックスが選択されます。デバイス プロファイルは、*std_desc* というゾーンの一部です。ユーザー *test* とは異なり、ユーザー *test1* はバックエンドの LDAP/AD サーバーに設定されていません。

ユーザー *test* は、バックエンド サーバーに登録されているデバイスを使用してログインします。ゾーンの分類は *std_desc* です。一方、ユーザー *test1* は同じデバイスでログインしても、デフォルト ゾーンに分類されます。この場合、ユーザー *test1* に対してチェック ボックスは適用されません。

ただし、デバイス プロファイルから デバイス IDである *4JV5DQH1* を削除し、2 つのポリシー変数のみを残すと、ユーザー *test1* に異なるゾーン分類が適用されます。この場合、ユーザー *test* は登録デバイスを使用してログインし、*std_desc* ゾーンに分類されます。ユーザー *test1* がログインすると、やはり *std_desc* ゾーンに分類されます。ここでは、ユーザー *test1* が登録デバイスを持たず、ゾーンのデバイス プロファイルに含まれる 2 つのポリシー変数が NULL 値を戻し、デバイス プロファイルにハード コーディングされた第 3 のデバイスが存在しないために、チェックボックスが適用されます。

モバイル デバイスを使用している場合、デバイス IDがすでにデータベースに入力されている可能性があります。この場合は、プロファイル内で参照できます。これらのデバイスのいずれかからログインするユーザーは、このプロファイルに一致し、関連ゾーンの条件を満たします。

通常、デバイス識別子は、認証ディレクトリに含まれる属性であり、変数で表されます ({`device_identity`} など)。識別子の形式は、使用されるデバイスの種類に応じて異なります。

- Microsoft Windows デバイスの場合、識別子はハード ドライブの一意のシリアル番号です (*WD-WMAM9SK79685* など)。
- Mac OS X デバイスの場合、Universal Unique Identifier (UUID) が使用されます。UUID は、UUID を生成したホストのネットワーク アドレス、タイムスタンプ、およびランダムな数字への参照を組み合わせた 128 ビットの数値です。UUID は、*951A240E-F502-5632-BDAB-D1ECA43FA371* のようになります。
- Linux デバイスの場合、UUID がデバイス識別子になります。
- 仮想マシンの場合、UUID がデバイス識別子になります。
- Windows Mobile 6 デバイスの場合、識別子はデバイスの一意の 15 桁の IMEI (International Mobile Equipment Identity) コードです。例えば、*350077-52-323751-3* のようになります。
- Nokia Symbian デバイスの場合、識別子は一意の 15 桁の IMEI です。
- Google Android デバイスの場合、デバイスのシリアル番号が識別子になります。
- Apple iPhone/iPad の場合、デバイスのシリアル番号が識別子になります。
- Apple iPhone の場合、Exchange サーバーと通信する際に、デバイスはそのデバイス ID やシリアル番号の先頭に「`Appl`」 を付けます。例えば、*Appl828315FLY7H* となります。

スマートフォンの正しいデバイス ID を取得する別の方法としては、デバイスがアプライアンスへの接続を試みた後に、AMC ログの POST メッセージを表示する操作があります。[**Logging (ログ)**] ページに移動して、[**View Logs (ログの表示)**] タブの [**Log file (ログ ファイル)**] ドロップダウン メニューで [*Web proxy audit log (Web プロキシ監査ログ)*] を選択します。POST メッセージは次のように表示されます。

```
http://10.10.11.12/Microsoft-Server-ActiveSync?User=jt&DeviceId=Appl828315FLY7H&DeviceType=iPhone&Cmd=Sync
```

データベース内の DeviceId の値を、プロファイルの参照用として使用します。

ディレクトリ サーバーは、これらのタイプの ID に異なる属性を使用してセットアップしたり、単一の属性にデータを格納したりできます。この例では、単一の属性と変数が使用されています。

未登録デバイスを許可するデバイス プロファイルの作成

未登録デバイスから機器 ID を収集するには、デバイス プロファイルとともにデバイス ID 変数を使用します。

1 未登録デバイスを使用するユーザーがログインする AD または LDAP 認証サーバーとレルムを、識別またはセットアップします。ゼロから開始する場合の詳細については、レルムの作成を参照してください。この例では、レルムの名前は *Employees* です。

2 ステップ 1 で指定したディレクトリ サーバーの属性を指す *device_identity* という変数を作成します (指定先の属性がまだ存在しない場合でも、変数を作成してデータをキャプチャできます)。

   a AMC のメイン ナビゲーション メニューから [**Resources (リソース)**] をクリックします。

   b [**Variables (変数)**] タブで [**New (新規)**] をクリックして、変数名 (`device_identity` など) を入力します。

   c [**Type (種別)**] リストから [**User attribute (ユーザ属性)**] を選択し、[**Realm (レルム)**] リストで [**Employees (従業員)**] が選択されていることを確認します。

   d デバイス ID のデータを保持するユーザー属性がすでに存在する場合は、[**User (ユーザー)**] フィールドに有効なユーザー名を入力して、[**Attribute (属性)**] リストから属性を選択します。まだ存在しない場合は、[**Attribute (属性)**] フィールドに属性名を入力します。

   e 複数のデバイス (デスクトップやラップトップなど) に関連付けられるユーザーがいる可能性がある場合は、[**Output (出力)**] リストで [**Multiple results (複数の結果)**] を選択します。

3 未登録デバイス向けのデバイス プロファイルとゾーンを作成します。3 種類のデバイスすべてからデータを収集している場合は、各デバイスに 1 つのデバイス プロファイルが必要となります。

   a AMC のメイン ナビゲーション メニューから [**End Point Control**] をクリックし、EPC が有効になっていることを確認します。

   b [Device Profiles (デバイス プロファイル)] ページの [Zones and Device Profiles (ゾーンとデバイスのプロファイル)] セクションで [**Profiles (プロファイル)**] の隣にある [**Edit (編集)**] リンクをクリックし、[Profiles (プロファイル)] タブで [**New device profile (新しいデバイス プロファイル)**] をクリックし、新しいデバイス プロファイルを作成するプラットフォームを選択します。

   c デバイス プロファイルに名前 (Unregistered - Windows など) を指定し、属性の [**Type (種別)**] リストで [**Equipment ID (周辺機器 ID)**] を選択します。

   d [**Value (値)**] として [**Matches (一致)**] を選択します。標準ゾーンは、後ほどこの手順の中で作成します。

   e [**Device identifier (デバイス識別子)**] フィールドの横の [**{variable} (変数)**] ボタンをクリックし、手順 2 で作成した変数を選択し、[**Insert (挿入)**] をクリックします。再び [**{variable}**] をクリックして、リストを閉じます。

   f [**Unregistered devices (未登録デバイス)**] エリアで、[**Match profile if user has no registered devices (ユーザーが登録デバイスを持たない場合はプロファイルを一致させる)**] チェックボックスを選択します。外部 AD/LDAP サーバーにまだ登録されていないデバイスはこのプロファイルに一致し、識別子が *Unregistered device log* に記録されます。変数をまだ定義していない場合は、警告 (*Undefined: {device_identity}*) が表示されますが、この時点では無視してかまいません。

   g [**Add to Current Attributes (現在の属性に追加)**] ボタンをクリックし、[**Save (保存)**] をクリックします。

h 対応する他のタイプのデバイスについて、それぞれデバイス プロファイルを追加します (Unregistered - WinMobile、Unregistered - ActiveSync など)。

4 作成したデバイス プロファイルを使用する、*Data collection* という名前の標準ゾーンを作成します。詳細については、デバイス ゾーンの作成を参照してください。

5 *Employees* レルムに *New devices* という名前のコミュニティを作成します。そのコミュニティの [**End Point Control Restrictions (End Point Control の制限)**] ページで、*Data collection (データ収集)* ゾーンを [**In use (使用中)**] リストに移動します。コミュニティのセットアップ方法の詳細については、コミュニティの作成と構成を参照してください。

6 変更を適用して保存したら、メイン ナビゲーション メニューで [**End Point Control (エンド ポイント制御)**] をクリックします。

7 ログイン中に未登録デバイスが検出されると、デバイスが *Unregistered (未登録)* プロファイルに一致するため、ユーザーは *Data collection (データ収集)* ゾーンに入れられます。デバイス ID の詳細を表示するには、AMC の [**Logging (ログ)**] ページで [**Unregistered device log (未登録デバイス ログ)**] を選択します。

8 [**Device count (デバイス カウント)**] リストで [**No devices (デバイスなし)**] を選択し、[**Refresh (更新)**] をクリックします。これにより、すべての新しいユーザーをキャプチャできます。

9 ロギングされたデータをさらに分析する必要がある場合は、XML ファイルにエクスポートします。最初にフィルタや検索条件を適用することで、エクスポート ファイルのサイズを小さくすることができます。[**Show last <n> messages (最近の <n> 件のメッセージを表示)**] 設定で、エクスポートするログ ファイルに含まれる最大メッセージ数が決定されます。

デバイス プロファイルでの [Match Profile if user has no registered devices (ユーザーが登録デバイスを持たない場合はプロファイルを一致させる)] の無効化

デバイス ID を使用するデバイス プロファイルを作成し、[**Match Profile if user has no registered devices (ユーザーが登録デバイスを持たない場合はプロファイルを一致させる)**] オプションを無効にする場合、新しいデバイスを使用するユーザーは (一部のデバイスがそのユーザーに登録されている場合でも) このプロファイルに一致せず、このゾーンに入れられません。ユーザーがプロファイルに一致するための他 (デバイス以外) の条件をすべて満たしている場合、未登録のデバイス ID は収集され、未登録デバイス リストに入れられます。管理者は、未登録デバイス リストからデバイス情報を収集して、半自動的にデバイスを登録できます。このように、ユーザーの操作を伴わずに、ユーザーが次回デバイスを使用してログインを試みた際に、このゾーンに分類されるようになります。

未登録デバイスの隔離

ユーザーが現在登録されているデバイス ID のいずれにも一致しないことを指定するデバイス プロファイルを作成できます。新しいデバイスを使用するユーザーはこのプロファイルに一致し、隔離ゾーンに入れられます。ユーザー向けのメッセージを構成して、現在のデバイスが未登録であるが、ログイン試行からデバイス情報が収集されてユーザー向けにデバイスが登録されるため、次回のログインで通常の (隔離でない) ゾーンに入れられることを通知できます。

未登録デバイスのロック アウト

拒否ゾーンを使用して、特定のデバイスをロック アウトできます。そのためには、機器 ID の属性を含むデバイス プロファイルを作成し、デバイス識別子を追加する際に [**Does not match (一致しません)**] チェック ボックスを選択します。この機能により、デバイスを所有するユーザーを完全にロック ア

ウトせずに、セキュリティのリスクがあると疑われるデバイスなどをロック アウトすることが可能になります。デバイス情報は、ログインの試行から収集されます。

外部処理向けとしての未登録デバイス ログのエクスポート

未登録デバイスでログインが試行されるたびに、未登録デバイスのログ メッセージが作成されます。このようなメッセージは、XML 形式で外部マシンにエクスポートできます。このとき、AMC の [**Logging (ログ)**] ページから操作したり、外部マシンから *curl* または *wget* コマンドを使用したりすることで、エクスポートを実行します。詳細については、未登録デバイスのログ メッセージを参照してください。このエクスポート機能でメッセージを収集することにより、各デバイスを自動的に登録したり、各ユーザーが新規に使用した未登録デバイスについてヘルプ デスクに通知したりできます。

- **Advanced (詳細)**: 未登録デバイスを使用してユーザーがログインを試行するときに、即座に通知を受ける必要がある場合は、AMC の [Configure Logging] ページで Syslog サーバーを構成します。ログインまたはログイン試行が行われると、アプライアンスは次の形式でログ メッセージを生成します。
- **New Equipment**: user '#1', platform '#2', device '#3', existing Devices '#4' where:
  - #1 は、ユーザー名
  - #2 は、プラットフォーム名
  - #3 は、このデバイスまたはユーザー機器の ID
  - #4 は、このユーザーに対して登録済みのデバイスの番号

特殊なクラスのユーザーに対するゾーンの定義

信頼されている特殊なクラスのユーザーが **Default (デフォルト)** ゾーンに割り当てられ (アクセスが拒否され) ないようにするために、デバイス プロファイルが含まれないゾーンを作成し、そのゾーンを信頼されているユーザーのみが所属するコミュニティに割り当てるという方法もあります。

例えば、使用するクライアント デバイスに関係なくシステム管理者がネットワーク リソースにアクセスできるようにしたい場合に、システム管理者をプロファイルがないゾーンを含むコミュニティに割り当てます。その後、システム管理者がそのコミュニティを参照するレルムを選択してログインすると、プロファイルがないこのゾーンに入れられます。これにより、承認されないクライアントをブロックするためのグローバルの**Default (デフォルト)** ゾーンに入れられることを回避できます。

プロファイルがないゾーンを作成するには、

1. AMC のメイン ナビゲーション メニューから、「**エンド ポイント制御**」をクリックします。[**End Point Control Settings (End Point Control 設定)**] ページが表示されます。
2. [**Zones and Device Profiles (ゾーンとデバイスのプロファイル)**] セクションで、[**Edit (編集)**] をクリックします。
3. [**Zones (ゾーン)**] セクションで [**New (新規)**] をクリックし、作成対象として [**Standard** zone (標準ゾーン)] を選択します。[**Zone Definition (ゾーン定義)**] ページが表示されます。
4. [**Name (名前)**] フィールドに、わかりやすいゾーン名を入力します。
5. [**Description (説明)**] フィールドに、ゾーンについての分かりやすいコメントを入力します。
6. オプションで、このゾーンに対して [**Required data protection tool (必須データ保護ツール)**] を選択できます。ただし、このような信頼されている特殊クラスのユーザーに、接続で使用するデバイスのタイプについて柔軟性を持たせたい場合は、このフィールドを **None (なし)** のままにしておきます。

7 [**Save (保存)**] を選択します。

プロファイルがないゾーンを定義したら、このような信頼されているユーザーの特殊クラスに特化したレルムを作成します。その上で、この特殊クラスのみがログインできるように、レルムに専用コミュニティを構成します。詳細については、コミュニティへのメンバーの割り当てを参照してください。

End Point Controlエージェントの使用

End Point Control エージェントを使用して、一般的な EPC タスク (仮想キーボードの有効化/無効化、各ユーザー セッション後にクライアント システムからのリモート データの消去など) を実行できます。

End Point Control タスク

項目	説明
Enable virtual keyboard (仮想キーボードを有効にする)	
Require use of keyboard (キーボードの使用を要求する)	
End inactive user connections (非アクティブ ユーザー接続の終了)	接続が非アクティブになってから切断されるまでの時間を選択します。3 分から切断なしの範囲で選択でき、デフォルト設定は **10** 分です。
Enable Cache Cleaner (キャッシュ クリーナーを有効にする)	このチェック ボックスを選択して Cache Cleaner を有効にし、各ユーザー セッション後にブラウザのキャッシュを消去します。Cache Cleaner は、End Point Control が有効になっている場合に限り、Windows および Mac プラットフォームのみで使用できます。
Allow user to disable Cache Cleaner (ユーザーにキャッシュ クリーナーの無効化を許可する)	このチェック ボックスを選択することにより、ユーザーは Cache Cleaner を終了して、キャッシュ消去機能を迂回できます。
Clean session items only (セッション項目のみクリア) Clean all items (すべての項目をクリア)	すべてのブラウザ項目を消去するか、または現在のセッションに関連する項目のみを消去するかを指定します。

仮想キーボードを使用したクレデンシャルの入力

クレデンシャルが盗まれる懸念がある場合、WorkPlace にログインするユーザーに対して、クレデンシャルを入力する代わりに、画面に表示されたキーボード上の文字をポイントする方法を提示 (または強制) できます。

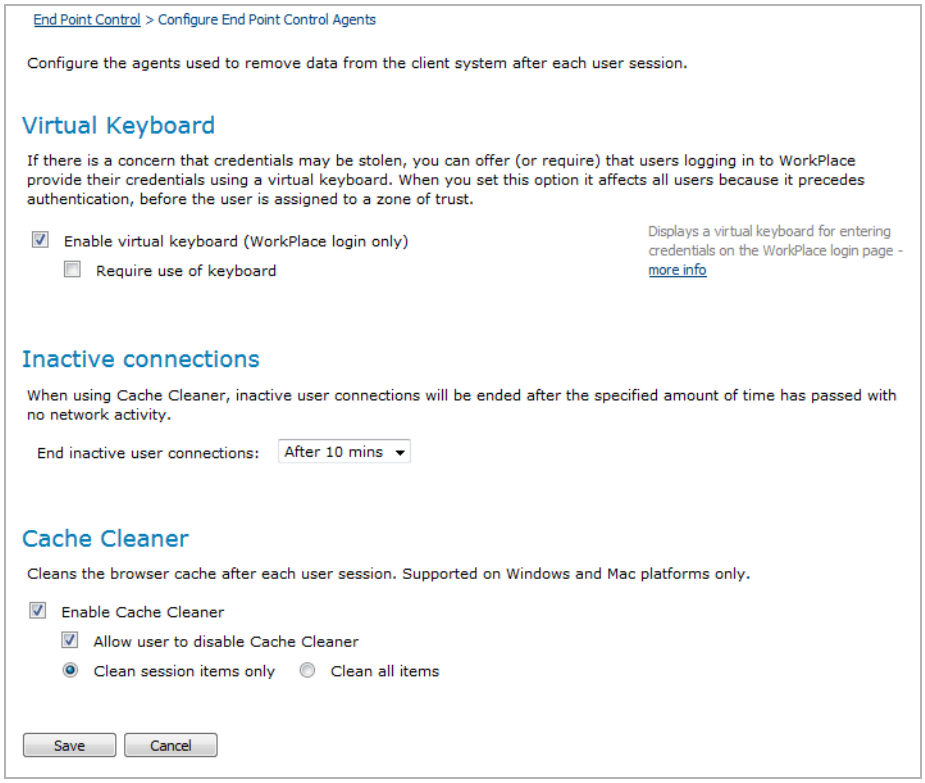
仮想キーボードは、ユーザーが認証される前 (レルムが選択される前) に使用されるため、その構成はすべてのレルムに適用されます。特定のユーザー グループのみに仮想キーボードを提供したり、特定の状況に限って要求することはできません。仮想キーボードを使用するために、End Point Control を有効にする必要はありません。

仮想キーボード設定は、小型携帯端末 (スマートフォンなど) には適用されません。これらのデバイス向けの WorkPlace の最適化については、小型携帯端末での表示用に WorkPlace を最適化するを参照してください。

WorkPlace で仮想キーボードを設定するには:

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 [**End Point Control agents (エンド ポイント制御エージェント)**] セクションで、[**Edit (編集)**] をクリックします。[**Configure End Point Control Agents (エンド ポイント制御エージェントの設定)**] ページが表示されます。



3 ユーザーが、WorkPlace ログイン ページでクレデンシャルを入力するときに仮想キーボードを使用できるようにするには、[**Enable virtual keyboard (Workplace login only) (仮想キーボードを有効にする(Workplace ログインのみ))**] チェックボックスを選択します。これにより、クレデンシャルが盗まれるリスクを低減できます。この設定を有効にすると、ログイン レルムに関係なく、すべての WorkPlace ユーザーにこのオプションが割り当てられます。

4 仮想キーボードが有効化されている場合、[**Require use of keyboard (キーボードの使用を要求する)**] チェックボックスを選択すると、ユーザーが WorkPlace ログイン クレデンシャルを入力する際に仮想キーボードを強制的に使用させることができます。

5 [**Save (保存)**] を選択します。

データ保護の構成

Cache Cleaner は、アプライアンスのライセンスに含まれます。

重要：Cache Cleaner は Linux プラットフォームではサポートされていません。

Cache Cleaner について

Cache Cleaner が有効化され、ユーザーが WorkPlace にログインすると、Cache Cleaner アイコンがタスクバーの通知領域に表示されます。ユーザーは、必要に応じてネットワーク リソースにアクセスできます。

ユーザーが Cache Cleaner セッションを終了する際、Cache Cleaner によって、セッションに関連付けられているすべてのデータが削除されます。ログアウト時に、すべてのブラウザ ウィンドウが Cache Cleaner によって閉じられます。ログアウト時に、すべてのブラウザ ウィンドウが閉じられることを警告するダイアログが表示されます。

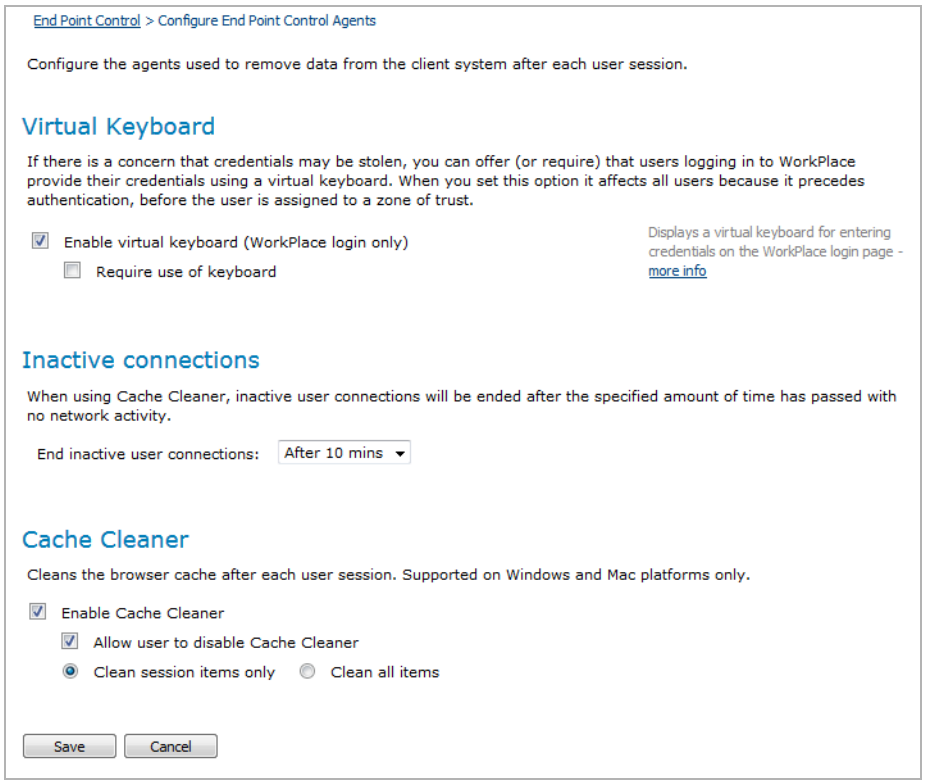
メモ：Cache Cleaner はログアウト時にすべてのブラウザ ウィンドウを閉じるため、ブラウザ ウィンドウが閉じるときに送信されていないデータ (入力中の伝票など) はすべて失われることについて、ユーザーが認識していることを確認してください。

データ保護設定の構成

WorkPlace にデータ保護を設定するには:

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 [**End Point Control agents (エンド ポイント制御エージェント)**] セクションで、[**Edit (編集)**] をクリックします。[**Configure End Point Control Agents (エンド ポイント制御エージェントの設定)**] ページが表示されます。



3 [**End inactive user connections (非アクティブなユーザー接続の終了)**] ドロップダウン リストで、非アクティブなユーザー接続を自動的に終了してクライアントからデータを削除するためのタイムアウトを選択します。この設定により、ユーザーがキオスク端末などの共有コンピュータからログアウトし忘れた場合のセキュリティのリスクを最小限に抑えることができます。

4 [**Enable Cache Cleaner (キャッシュ クリーナーを有効にする)**] チェック ボックスを選択して、各セッション後にユーザーのブラウザ キャッシュを消去します。

5 ユーザーが Cache Cleaner を終了してキャッシュ消去機能を迂回できるようにするには、[**Allow user to disable Cache Cleaner (ユーザーに Cache Cleaner の無効化を許可する)**] チェックボックスを選択します。

6 すべてのブラウザ項目を消去するか、または現在のセッションに関連する項目のみを消去するかを指定します。([**Clean session items only (セッション項目のみクリア)**] または [**Clean all items (すべての項目をクリア)**])。

7 [**Save (保存)**] を選択します。

アプリケーション アクセス 制御

個人用機器の使用により、時間と場所にかかわらず従業員の生産性と応答性を向上させることを、企業は望んでいます。しかし、企業はこの開放性と、確実な社内データとネットワークの保護、さらに企業のコンプライアンスと規制要件への適合性との間でバランスをとらなければなりません。企業は最大 BYOD 機器までオープンなので、以下のことを確実にする必要があります。

- 社内データとネットワーク リソースが安全であること。
- ユーザーが、社内ネットワークに接続する個人用機器に関する社内ポリシーとプライバシーの問題について注意を払い、同意していること。
- 管理者が従業員による個人用機器の使用を追跡し、監視できること。

アプリケーション アクセス制御がこれらのあらゆる問題に対処できること。これにより管理者は、クライアント上の SonicWall Mobile Connect とアプライアンス上の Secure Mobile Access の機能を組み合わせることで、個人用機器からエンタープライズ データ リソースにアクセスできるアプリケーションを制御することができます。

トピック:

- クライアント (SonicWall Mobile Connect)
- 装置 (SonicWall Secure Mobile Access)

クライアント (SonicWall Mobile Connect)

アプリケーション アクセス制御は、サポートされたクライアント デバイス (iOS/Mac OS/Android) 上の SonicWall Mobile Connect を使用して、以下のようにアプリケーションを処理します。

- アプリケーション リストから選択されたアプリケーション - これらのアプリケーションから社内ネットワークに宛てたトラフィックは、トンネルに入ることができます。アプリケーションを特定するために、情報がサーバに提供されます。
- 無効とされたリストにあるアプリケーション (または機器上のその他のアプリケーション) - 社内ネットワークに宛てたトラフィックは遮断され、Mobile Connect によって破棄され、トンネルに入ることはできません。
- すべてのアプリケーション (アプリケーション リストに掲載されているかどうかによらない) - トラフィックが社内ネットワーク宛ではない場合は、トラフィックは機器のデフォルト インターフェースを使用して送信されます。

装置 (SonicWall Secure Mobile Access)

アプリケーション ゾーンを作成し、適切な機器を持つユーザーをゾーンに分類できるようになったら、以下の設定を行います。

- 社内ネットワークへのアクセスを許可するべきアプリケーション、
- 各許可アプリケーションを使用できるユーザー、
- 各アプリケーションがアクセスできる社内ネットワーク上の送信先。

アプリケーション アクセス制御は、iOS 7+ 機器、Mac OS Mavericks 10.9+ 機器、および Android 4.0+ 機器で利用できます。

トピック:

- アプリケーション アクセス制御の動作
- アプリケーション制御の設定
- クライアント アプリケーション リストの作成
- 信頼済み学習機器の特定
- アプリの取得
- 取得済みアプリの承認
- ユーザー セッションの表示

アプリケーション アクセス制御の動作

Secure Mobile Access と Mobile Connect は以下のように共同して動作し、社内リソースに簡単にアクセスするために個人用機器を使用できる、安全で管理可能な環境を提供します。

1. 管理者は、アプライアンスが個人用機器に社内ネットワークとリソースへのアクセスを許可することができる、アプリケーション ゾーンを作成します。
2. ユーザーは、登録されていない個人用機器をアプライアンスと一緒に使用して接続します。ユーザーは、企業のリソースにアクセスするために機器の登録と個人用機器の企業ポリシーとプライバシーポリシーへの同意を求められます。

   ユーザーが機器の企業ポリシーに同意すると、機器の一意の機器 ID が決定され、装置によってその機器がユーザーに登録されます。この機器からの以降の接続には、機器の承認は必要ありません。
3. ユーザーは、アクセスを許可するのに使用されるアプリケーション ゾーンで許可されたネットワーク リソースにアクセスします。
4. 管理者は、アプライアンスにアクセスした個人用機器の使用状況を監視します。

アプリケーション制御の設定

アプリケーション制御を設定するには:

1. アプリケーションケーション ゾーンを定義するには: に説明するように、アプリケーション ゾーン プロファイルを作成します。
2. アプリケーション ゾーンを作成するには: に説明するように、アプリケーション ゾーンを設定します。

3 アプリケーション ゾーンをコミュニティに追加します。そのために、コミュニティの [**End Point Control Restrictions (エンド ポイント制御 の制限)**] ページで、*Application (アプリケーション)* ゾーンを [**In use (使用中)**] リストに移動します。コミュニティのセットアップ方法の詳細については、コミュニティの作成と構成を参照してください。

4 クライアント アプリケーション リストの作成 に説明するように、クライアント アプリケーション リストを作成します。

5 アプリケーションのアクセス制御用にアクセス制御ルールを追加するに説明するように、アプリケーション ゾーンのアクセス制御ルールを作成、または変更します。トンネルを介してデータを送信できるアプリケーションと、それらのアプリケーションがアクセスを許可される社内ネットワーク上の送信先を、アクセス制御ルールで制御します。

6 信頼済み学習機器の特定に説明するように、信頼済み学習機器を特定します。信頼済み学習機器は、学習アプリケーション バージョン情報の一部としてシグネチャ検索を行う特別な権利が与えられます。

7 アプリの取得に説明するように、アプリを学習します。

8 取得済みアプリの承認に説明するように、クライアント アプリケーション リストへの学習済みアプリの追加を承認します。

9 ユーザー セッションの表示に説明するように、ユーザーのアクセスを表示します。

クライアント アプリケーション リストの作成

クライアント アプリケーション リストには、アプリケーションとそのバージョン、認証するためにプラットフォームが使用するシグネチャのリストが含まれます。このリストのアプリケーションは、アクセス制御ルールで参照され、リストに定義され、アクセス制御ルールで参照されるアプリケーションを使用して、ユーザーがリモート ネットワークにアクセスしようとする際に、Mobile Connect によって強化されます。

Safari や電子メールのような、一部共通アプリは、すべてのリストに事前設定されます。追加のアプリを検索して、ゾーンで使用するクライアント アプリケーション リストに追加するには、最初に追加するアプリのアプリ ID を識別する必要があります。

トピック:

- アプリのダウンロード
- クライアント アプリケーション リストの作成

アプリのダウンロード

トピック:

- iOS 機器または Mac OS 機器から
- Android 機器から

iOS 機器または Mac OS 機器から

iOS アプリまたは Mac OS アプリを追加するには:

1 [**End Point Control > Add Client Application (エンド ポイント制御 > アプリ クライアント アプリケーション)**] ページの [**Search (検索)**] リンクを使用して、AMC 内からアプリを検索します。

2 または、https://itunes.apple.com で、アプリ用の iTunes ストアを検索します。

SMA は、アプリ ID 値として iTunes ストアから受信した *bundleid* フィールドを使用します。

3 アプリを iOS 機器または Mac OS 機器にダウンロードします。

Android 機器から

Android アプリを追加するには:

1 Android 機器上で、APK Extractor のようなアプリをダウンロードしてインストールします。このアプリはアプリから `Apk` ファイルを抽出して読み出します。Apk Extractor は Google Play ストアからダウンロードできる無料のアプリです。

2 抽出アプリを起動して、ゾーンに追加するアプリケーションが見つかるまで下にスクロールします。

例えば、Chrome を使用すると、アプリ ID は `com.android.chrome`です。

クライアント アプリケーション リストの作成

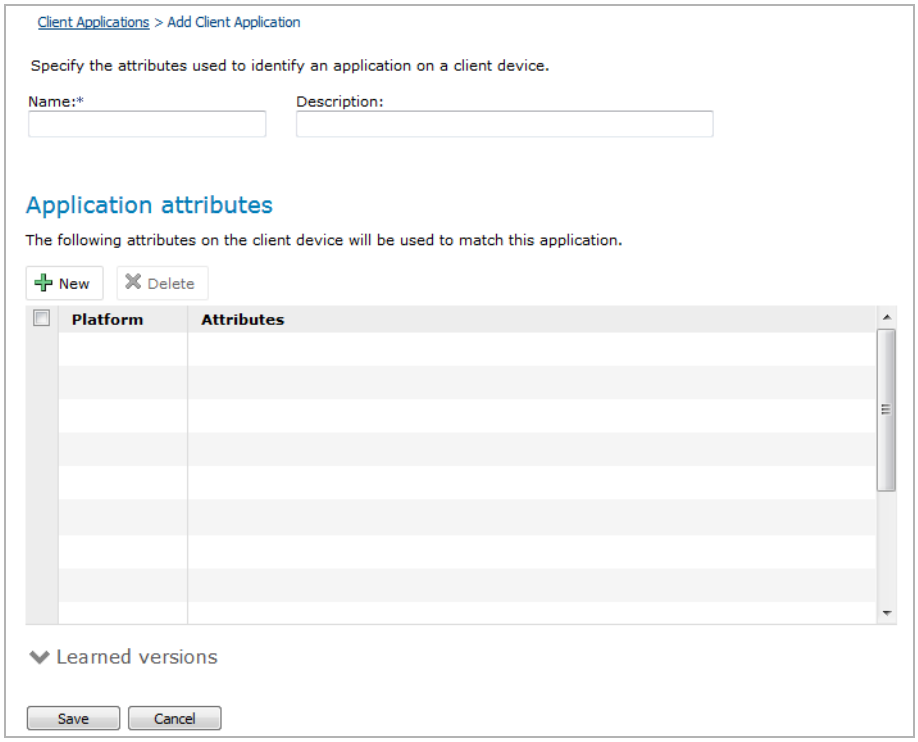
クライアント アプリケーション リストに追加するそれぞれのアプリのアプリ ID を識別してから、リストを作成します。

クライアント アプリケーション リストを作成するには:

1 [**User Access (ユーザー アクセス)**] の下の AMC のメイン ナビゲーション メニューで、[**End Point Control (エンド ポイント制御)**] をクリックします。[**End Point Control (エンド ポイント制御)**] ページが表示されます。

2 [**Application Control (アプリケーション制御)**] セクションで、[**Client Applications (クライアント アプリケーション)**] の横にある [**Edit (編集)**] をクリックします。

3 [**New (新規)**] をクリックします。[**Add Client Application (クライアント アプリケーションの追加)**] ページが表示されます。



4 [**Name (名前)**] フィールドに、アプリをユーザーに識別されるのに使用する、アプリのわかりやすい名前を入力します。

5 (オプション) [**Description (説明)**] フィールドに、アプリをさらに識別するための簡単な説明を入力します。

6 [**Add Client Application (クライアント アプリケーションを追加する)**] ページの [**Application attributes (アプリケーション属性)**] セクションで、[**New (新規)**] をクリックし、ドロップダウン メニューから シグネチャを (iOS、Mac OS、または Android) に適用するのに必要なプラットフォームを選択します。

7 アプリケーション ID フィールドに、リストに追加するアプリのアプリ ID を入力します。残りの属性は、アプリが取得されるときに検出されます。

メモ：アプリのすべてのバージョンがおなじシグネチャを共有する必要があります。

8 [**OK**] を選択します。

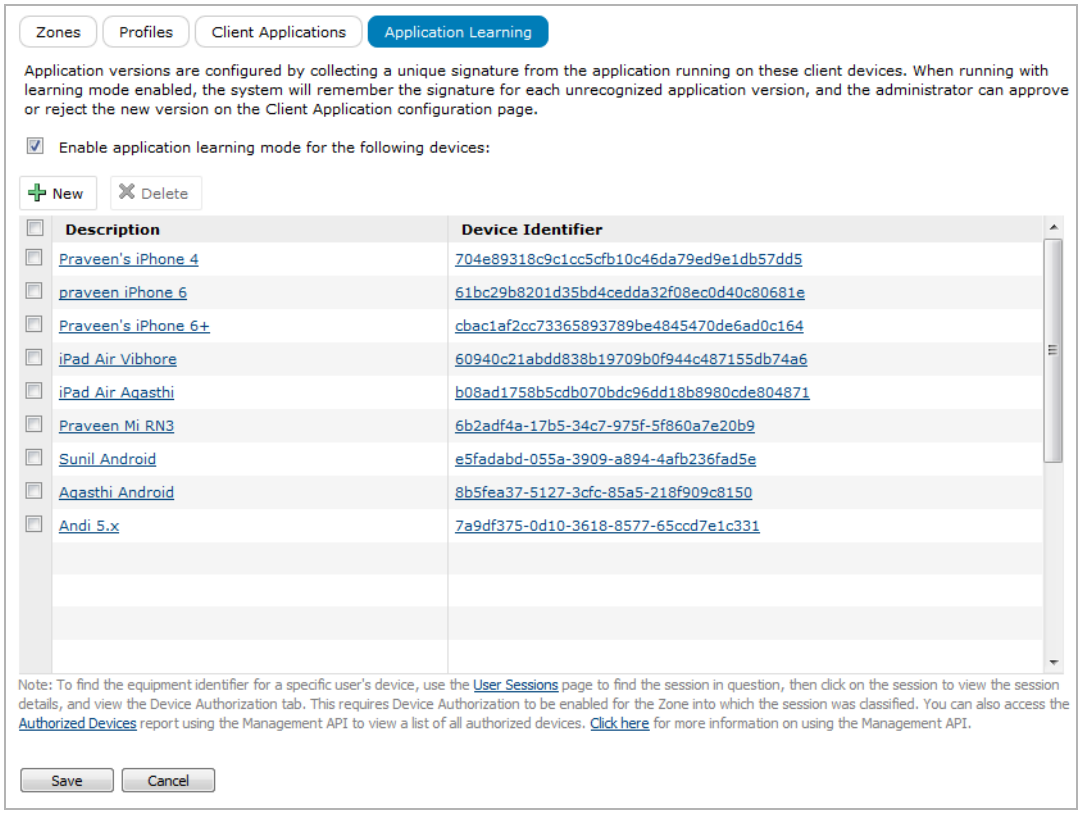
信頼済み学習機器の特定

信頼済み学習機器は、バージョン情報取得アプリケーションの一部としてシグネチャ検索を行う特別な権限が割り当てられます。信頼済み機器は、End Point Control でも使用され、 セキュリティ状態を検出するためにエンドポイント機器の属性を確認します。機器がアプリケーション学習タブに追加されると、その機器はアプリケーション バージョンを取得できます。

信頼済み学習機器を特定するには:

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**End Point Control**] をクリックします。

2 [**Zones and Profiles (ゾーンとプロファイル)**] の下の [**Profiles (プロファイル)**] セクションで [**Edit (編集)**] をクリックしてから、[**Application Learning (アプリケーション学習)**] タブをクリックします。



3 エントリ フィールドを表示するには、[**New (新規)**] をクリックします。

4 [**Description (説明)**] フィールドに、デバイスを識別するための簡単な説明を入力します。

5 [**Device Identifier (デバイス識別子)**] フィールドに、信頼済み学習機器にする機器のデバイス識別子を入力します。

6 機器を信頼済み学習機器として認識するためのアプライアンスを有効にするには、[**Enable application learning mode for the following devices (以下のデバイスのアプリケーション学習モードを有効にする)**] チェックボックスを選択します。

7 [**Save (保存)**] を選択します。

アプリの取得

アプリケーション アクセス制御を設定し、追加のアプリを追加し、学習機器を識別すると、アプリケーション アクセス制御で設定した各アプリを取得します。

メモ：アプリの制約により、iOS アプリのバージョンは信頼済み学習機器では取得できず、手動で設定する必要があります。バージョンはすべての AMC ページで **Unknown (不明)** として表示されます。

アプリを取得するには:

1 信頼済み機器上の Mobile Connect を起動して SMA アプライアンスに接続します。機器が正常に認証されると、バージョンを取得する必要のあるアプリケーションが表示されます。

2 リストにあるアプリケーションを起動します。

3 社内ネットワーク リソースにアクセスします。

4 表示を更新して [**Pending (保留)**] アイコンがアプリケーションの横に表示されていることを確認して、アプリケーションが承認保留のバージョンであることを検証します。

5 メイン画面をプルダウンして Mobile Connect 表示を更新します。

6 リストされたアプリケーションごとに ステップ 1 から ステップ 5 まで繰り返します。

7 バージョン番号が [**Pending Versions (保留バージョン)**] リストに表示されている場合は、アプリケーションを承認するために AMC にログインします。

   a [**User Access (ユーザー アクセス)**] > [**End Point Control (エンド ポイント制御)**] > [**Client Applications (クライアント アプリケーション)**] に移動します。

   b アプリケーションを選択します。

   c 取得済みバージョン リストから項目を選択して、[**Approve (承認)**] をクリックします。

   d [**Save (保存)**] クリックして、クライアント アプリケーションを保存します。

   e 承認待ちの各アプリケーションを承認します。

   f 変更を適用します。

8 クライアント アプリケーション バージョンを承認したら、信頼済み機器に戻って Mobile Connect 表示を更新します。[**Pending (保留)**] アイコンが [**Approved (承認済み)**] アイコンに代わっており、これはアプリケーションが一般に使用される準備ができたことを示しています。

取得済みアプリの承認

アプリは、取得されると、クライアント アプリケーション ページの取得済みバージョン セクションに追加されます。リストに追加できるようにするには、取得済みアプリを承認する必要があります。

取得済みアプリを承認するには:

1 AMC で、[**User Access > End Point Control > Client Applications (ユーザー アクセス > エンド ポイント制御 > クライアント アプリケーション)**] タブに移動します。

2 アプリが使用される [**Client Application List (クライアント アプリケーション リスト)**] を選択して、[**Edit Client Application (クライアント アプリケーションの編集)**] ページを表示します。

3 [**Learned.Versions (取得済みバージョン)**] セクションを展開して、取得済みアプリを選択し、[**Approve (承認)**] ボタンをクリックしてアプリケーション リストに追加します。それぞれのバージョンの最近のエントリーだけが表示されます。

4 (オプション) リストからアプリを削除するには、アプリを選択して [**Discard (破棄)**] をクリックします。

5 [**Save (保存)**] を選択します。

ユーザー セッションの表示

[**User Sessions (ユーザー セッション)**] ページは、アプライアンスにログインしたすべてのユーザーの統合表示を、各ユーザーのレルム、コミュニティ、EPC、アクセス エージェント、およびライセンス状況に関する情報と共に提供します。このページには、接続期間、平均速度、および転送した合計バイトも表示されます。

第 7 部

コンポーネント

- WorkPlace ポータル
- ユーザー アクセス コンポーネントおよびサービス

9

WorkPlace ポータル

WorkPlace の概要

このセクションで、ユーザーの観点からみた WorkPlace の概要について説明します。

WorkPlace ポータルは、Web ベース (HTTP) のリソースに対する、動的にパーソナライズされたアクセスをユーザーに提供します。また、Web ブラウザから Windows ファイル サーバー上のファイルやフォルダへのアクセスや、WorkPlace からインストール可能なSecure Mobile Access エージェントを介しての TCP/IP リソースへのアクセスも提供します。

SMA アプライアンスにはデフォルトの WorkPlace ポータルが含まれています (これは変更することができます)。各ユーザー向けに、独自の外観を備えたサイトを追加で設定できます。詳細については、WorkPlace サイトを参照してください。WorkPlace 用クライアントのシステム要件については、システム要件を参照してください。

ユーザーがブラウザで WorkPlace のアドレスにアクセスすると、認証ページが表示されます。**Authentication (認証)**ページに、ユーザー名とパスワードを使用してログインします。このページではパスワードを変更することもできます。

クライアント証明書を使用して認証するユーザに、このページが表示されない場合、[**Authentication (認証)**] ページが表示される代わりに、ワンタイム パスワードが要求される場合があります。パスワードはシステムが電子メールで送信します。ワンタイム パスワードの要求画面は次のとおりです。

メモ：システムで End Point Control を使用するよう構成している場合、システムへのユーザー アクセス方法に End Point Control がどのように影響するかについては、End Point Control とユーザー エクスペリエンスを参照してください。

ユーザーが認証クレデンシャルを入力すると、WorkPlace によって現在のライセンス契約がチェックされます。ライセンスに問題がある場合はメッセージが表示されます。メッセージでは、他の種類の認証エラー (パスワードの誤りなど) ではなくライセンス関連のエラーであることが示されます。その場合、ユーザーは管理者に連絡する必要があります。

システムの構成によっては、ユーザーは使用規定 (AUP) や他のライセンス契約への同意を求められる場合があります。

AUP では、ユーザーが同意する必要のある特定のメッセージや指示が表示されることがあります。ライセンス契約に同意しないと、ユーザーは WorkPlace にアクセスできません。

メモ：レルムに AUP が構成されている場合、バージョン 11.4 よりも古いトンネル クライアントからログインしようとするとログインは失敗します。クライアントをバージョン 12.1 またはその以上にアップグレードしてから接続する必要があります。AUP レルムでトンネル クライアントの自動アップグレードが有効になっている場合、ユーザーはアップグレードするために接続することができます。この場合、管理者は、(自動クライアント アップグレードを可能にするために) AUP なしの区切りレルムを構成するか、他の方法でクライアントをアップグレードする必要があります。

トピック:

- ホーム ページ
- イントラネット アドレス フィールド
- ブックマーク
- カスタム RDP ブックマーク
- ネットワーク エクスプローラ ページ

ホーム ページ

ユーザーが認証情報を入力した後、ライセンスが最新であれば、WorkPlace のホーム ページが表示されます。WorkPlace には、他の関連リソースへのリンクを含んだ個人用ブックマーク エリアを追加できます。このエリアには、管理者が事前に構成したブックマークを含めることができるほか、ユーザーがリソースや Web サイトへのリンクを独自に追加できます。

メモ：Java 1.7u71 をインストールした Linux システムで Firefox を使用している場合、Workplace を起動できません。次のエラー メッセージが表示されます。`Unable to authorize request.` (許可要求が無効です) `Zone classification process has not completed` (ゾーン分類処理が完了していません).

構成可能な WorkPlace 要素

ホーム ページの機能のほとんどが構成可能です。構成可能な WorkPlace 要素を参照してください。

構成可能な WorkPlace 要素

WorkPlace 要素	説明
レイアウト	WorkPlace ページのコンテンツとレイアウトは、コミュニティ ベースでカスタマイズできます。これらのレイアウト要素に含まれるものは以下のとおりです。 • コンテンツ (表示されるショートカットおよびショートカット グループ) • ページ (単一または複数) • 列 (単一または複数) • ナビゲーション (左または上部) 詳細については、WorkPlace の外観の変更を参照してください。
ショートカット ショートカット グループ	ユーザーにアクセスが許可されている Web リソース、ファイル システム リソース、およびターミナル サーバー リソースへの、管理者が定義するショートカットです。ショートカットは、ユーザーのアクセス ポリシーに基づいて動的に表示されます。各ユーザーには、自身が利用権限を持つリソースのみが表示されます。 ショートカットの動作は各タイプにより異なります。 • **Web リソース:** 新しいブラウザ ウィンドウで開きます。 • **ターミナル サーバー リソース:** 新しいブラウザ ウィンドウで開き、適切なグラフィカル ターミナル エージェントが自動的に開始されるか、必要な場合はインストールされます。 • **共有フォルダまたはファイル:** WorkPlace ネットワーク エクスプローラ ページを開きます (新しいブラウザ ウィンドウで表示されます)。ファイル システム リソースに対するすべてのアクセスを無効にしている場合、ファイル システム リソースをポイントしているネットワーク ショートカットは表示されません (ファイル システム リソースへのアクセスの無効化については、WorkPlace の一般設定の構成を参照してください)。 • **ブックマーク**: Workplace のユーザー定義ブックマークの基本的な機能 (RDP、Citrix、VNC、Telnet、および SSHv2) をすべて提供します。 • **カスタム ショートカット**: カスタム構成に応じて動作します。 ショートカットの作成については、WorkPlace ショートカットについての作業を参照してください。
Connect Tunnel	WorkPlace ポータルからの Connect Tunnel クライアントのカスタム接続を定義できます。
[ヘルプ] ボタン	WorkPlace に付属のヘルプ システムには、ユーザーに必要なすべての基本情報が含まれています。カスタムの HTML ヘルプ ファイルを作成してユーザーに提供する場合は、WorkPlace スタイルの構成時にファイルを指定できます。カスタム ヘルプの利用は、環境固有の情報 (VPN 上の利用可能なリソースについての情報や、テクニカル サポートの詳細など) を追加する場合に役立ちます。このファイルは、適切な規格の単一の HTML ファイルである必要があります。

組み込みの WorkPlace 要素

ユーザー向けの WorkPlace ポータルをセットアップする際、組み込みのリソースや WorkPlace 要素を選択してポータルに含めることができます。組み込みの WorkPlace 要素を参照してください。これらのリソースを提供するかどうかは、コミュニティ ベースで構成できます。

組み込みの WorkPlace 要素

WorkPlace 要素	説明
イントラネット アドレス	このボックスを表示するかどうかを指定できます。また、このボックスを使用して Web リソース (URL を入力)、ファイル システム リソース (UNC パス名を入力)、またはその両方にアクセスできるようにするかどうかを構成できます。 詳細については、イントラネット アドレス フィールドを参照してください。
個人用ブックマーク	ユーザーに対して、SMA アプライアンスによって保護された他のリソース (SMB ホストなど) や URL への個人用リンク (ブックマークに類似) の作成と管理を許可することができます。個人用リンクはアプライアンス上に保存されます。ユーザーは、WorkPlace にログインすればどのコンピュータからでも個人用リンクにアクセスできます。 詳細については、ブックマークを参照してください。
Connect Tunnel [Connect Tunnel]	組み込みの [**Install Connect Tunnel (Connect Tunnel のインストール)**] ショートカットを有効化して、ユーザーが WorkPlace ポータルから Connect Tunnel クライアントをダウンロードしてインストールできるようにすることができます。
ネットワーク エクスプローラ	共有フォルダおよびファイルを含む Windows ネットワークの参照を可能にすることができます。 詳細については、ネットワーク エクスプローラ ページを参照してください。

WorkPlace ステータス バー

WorkPlace ページには、ステータス バーがあります。WorkPlace ステータス バー要素を参照してください。

WorkPlace ステータス バー要素

WorkPlace 要素	説明
アクセス	ユーザーが現在実行中のアクセス方法を示します。 ユーザー アクセス エージェントについては、ユーザー アクセス コンポーネントおよびサービスを参照してください。
ユーザ	ログインに使用されたユーザー名。
セッション開始	現在のセッションの開始時刻 (24 時間形式)。

WorkPlace ステータス バー要素

WorkPlace 要素	説明
[**Log out (ログアウト)**] ボタン	ユーザーはこのボタンを使用して WorkPlace からログアウトできます。ただし、このボタンでログアウトしても、実行中のすべてのアプリケーションからログアウトするとは限りません (使用しているユーザー アクセス エージェントにより異なります)。セキュリティを高めるために、ユーザーはアプリケーションでの作業完了時 (特に、他のユーザーと共用しているコンピュータで作業している場合) に、アプリケーションからログアウトするか、アプリケーションを終了する必要があります。
詳細	ユーザーはこのボタンをクリックすると、次のシステム ステータス情報 (全ユーザーに表示される項目ではない) を表示できます。 • **ゾーン**: セキュリティ ゾーンを使用して、各コミュニティのメンバーに対してアクセスを許可または拒否します。 • **レルム**: レルムを使用すると、ユーザーは外部認証サーバーに保存されているクレデンシャルを使用して認証を行うことができます。 • **コミュニティ**: コミュニティを使用すると、さまざまなセキュリティ要件に基づいて、レルムのメンバーをグループ化できます。 • **データ保護**: Cache Cleaner[Cache Cleaner]

メモ：

- ユーザーが小型携帯端末で WorkPlace にアクセスする場合、デバイスの機能に応じてWorkPlace の外観が変わります。詳細については、End Point Control とユーザー エクスペリエンスを参照してください。
- Windows システムでは、ポップアップ ブロック機能が有効化された状態でブラウザ ツールバーを使用すると、メインの WorkPlace ウィンドウを閉じる際に、開いているネットワーク エクスプローラやグラフィカル ターミナル セッションのウィンドウを WorkPlace が閉じられない場合があります。
- WorkPlace セッション中に Outlook Web Access (OWA) からログアウトすると、ユーザーは WorkPlace からもログアウトします。これは、OWA のログオフ スクリプトによって、ブラウザのクッキーがすべて (WorkPlace で使用しているものも含む) クリアされるためです。OWA からログアウトする代わりに、単にブラウザのウィンドウを閉じることで、この問題を回避できます。

イントラネット アドレス フィールド

有効化されている場合、WorkPlace ページの下部に [**Intranet Address (イントラネット アドレス)**] フィールドが表示され (小型携帯端末の場合を除く)、ユーザーはこのボックスを使用して Web リソース、Windows ネットワーク リソース、およびターミナル サーバーにアクセスできます。

レルム内にコミュニティ (例えば、自社従業員のコミュニティと、パートナー向けのコミュニティ) を設定する際、WorkPlace のスタイルとレイアウトを使用して、各コミュニティごとに固有の外観を表示できます。WorkPlace レイアウトによって、当該コミュニティで [**イントラネット アドレス**] ボックスを表示するかどうかを制御します。詳細については、WorkPlace レイアウトの作成または編集を参照してください。

[**Intranet Address (イントラネット アドレス)**] フィールドの機能の構成は、グローバルな構成設定です。構成に応じて、ユーザーは WorkPlace が変換モードで実行されている場合に URL を入力して Web リソースにアクセスしたり、UNC パスを入力してファイル システム リソースにアクセスしたりすることができます。 (WorkPlace が変換モードで実行されていない場合は、ユーザーは Internet Explorer の [**Address (アドレス)**] ボックスに直接 URL を入力できます)。DNS や Windows ドメイン全体を単一の

リソースとして定義していて、ユーザーのグループにそのドメイン内の全リソースへの直接アクセス権を付与したい場合は、この方法が特に役立ちます。

WorkPlace が変換モードで実行されている際に Web リソースやターミナル サーバーにアクセスするには、ユーザーは [**Intranet Address (イントラネット アドレス)**] フィールドに URL を入力して [**Go (移動)**] をクリックします。ユーザーが適切なアクセス権限を有していれば、リソースが新しいブラウザ ウィンドウで開きます。

[**Intranet Address (イントラネット アドレス)**] フィールドでは、Web リソースやターミナル サーバーにアクセスするためのさまざまな入力を受け入れます。以下に、イントラネット アドレス入力ガイドライン に従ってガイドラインを示します。

イントラネット アドレス入力ガイドライン

要素	説明
リソース アドレス	ユーザーは、完全な URL (ドメインおよびホスト名) またはホスト名のみを入力して、リソースにアクセスできます。例えば、ユーザーは、「*fred*」 というホスト上にある「*CRM*」というリソースに、完全な URL (*http://fred.example.com/CRM/* など) またはホスト名 (*http://fred/CRM/* や *fred/CRM/* など) を使用してアクセスできます。
UNC パス	ファイル システム リソースにアクセスする場合、ユーザーは [**Intranet Address (イントラネット アドレス)**] フィールドに UNC パス (例えば、`\\jax\software\download`) を入力して [**Go (移動)**] をクリックします。ユーザーが適切なアクセス権限を有していれば、ネットワーク エクスプローラ ページが開き、要求したファイル システム リソースの内容が表示されます。
プロトコル	通常の Web リソースにアクセスする場合、ユーザーは `http://` プロトコル識別子を入力する必要はありません。ただし、安全な Web サイトにアクセスする場合は、`https://` プロトコル識別子を入力する必要があります。 ターミナル サーバーのリソース名を指定するとき、ユーザーは URL に適切なプロトコル識別子を加えなければなりません。サポートされているターミナル サーバーの種類は、`rdp://` 識別子を使用する Windows Terminal Services および `citrix://` 識別子を使用する Citrix です。
ポート番号	非標準ポート (ポート番号 80 以外) で Web リソースにアクセスする場合は、ユーザーはホスト名の後にポート番号を入力する必要があります。例えば、*fred:8080/SAP* と *https://fred:443/SAP* はいずれも有効な入力です。

UNC パス名、URL、またはその両方にアクセスできるように [**Intranet Address (イントラネット アドレス)**] フィールドを構成する方法については、WorkPlace の一般設定の構成を参照してください。

ブックマーク

ユーザーは、利用権限を持つあらゆるリソースへすばやくアクセスするために、WorkPlace に自分用のリンクを作成できます。これには、WorkPlace のユーザー定義 Web URL、RDP、VNC、Citrix、FTP、SSH、および Telnet ブックマークが含まれます。また、ユーザーは、自分のブックマーク リストの最小化、ブックマーク リストの編集、および、個々の RDP ブックマークの編集を行うことができます。

WorkPlace の個人用リンクは、一般的な Web ブラウザのブックマークやお気に入りリストに似ていますが、一般的なブラウザのブックマークは特定のコンピュータに保存されるのに対し、WorkPlace の自分用のリンクは SMA アプライアンスに保存されるという点が異なります。ユーザーは、WorkPlace にログインすると、どのコンピュータを使用していても自分の WorkPlace 個人用リンクにアクセスして管理できます。

レルム内にコミュニティ (例えば、自社従業員のコミュニティと、パートナー向けのコミュニティ) を設定する際、WorkPlace のスタイルとレイアウトを使用して、各コミュニティごとに固有の外観を表示できます。WorkPlace レイアウトによって、当該コミュニティで [*Personal Bookmarks*] グループを表示するかどうかを制御します。詳細については、WorkPlace レイアウトの作成または編集を参照してください。

メモ：WorkPlace ブックマーク経由で HTTP 以外のリソース (SMB ホストなど) にアクセスする場合、ユーザーは、アクセス エージェント (いずれかのトンネル クライアントなど) を実行している必要があります。詳細については、ユーザー アクセス エージェントを参照してください。

カスタム RDP ブックマーク

ユーザーのリモート デスクトップ リンク用のカスタム設定は、[Custom RDP Link] ウィンドウで管理します。ユーザーまたは管理者のどちらかが、画面解像度と色深度を管理できます。シングル サインオンでは、管理者がユーザーのサインオンをカスタマイズして、特定のクレデンシャルを要求したり、特定のドメインを有効化することができます。

ネットワーク エクスプローラ ページ

ユーザーがファイル システム リソースにアクセス (ネットワーク ショートカットをクリックする、[**Intranet Address (イントラネット アドレス)**] ボックスに UNC パスを入力する、または WorkPlace ホーム ページで [**Network Explorer (ネットワーク エクスプローラ)**] リンクをクリックするのいずれかの方法を使用) すると、ネットワーク エクスプローラ ページが表示されます。ネットワーク エクスプローラの機能は、Sun JRE Version 1.6 Update 34 以降がインストールされているかどうかによって異なります。このバージョンの Java がインストールされている場合、高機能のフォームが表示されます。これらのアップデートがインストールされていない場合は、HTML バージョンのネットワーク エクスプローラが表示されます。この HTML バージョンでは機能が制限されます。高機能版のネットワーク エクスプローラのメリットを最大限に活用するには、最新の Java アップデートをダウンロードしてください。ネットワーク エクスプローラ ページは、小型携帯端末では利用できません。

メモ：最新バージョンの Java および JRE は、http://www.java.com からダウンロードできます。

トピック:

- HTML ベースのネットワーク エクスプローラ
- Java ベースのネットワーク エクスプローラ

HTML ベースのネットワーク エクスプローラ

HTML ベースのネットワーク エクスプローラは、すべての機器で既定のインターフェースになっています。HTML ベースのネットワーク エクスプローラでは、ユーザーはネットワーク上でローカルに作業しているかのように、Web ブラウザを使ってネットワーク上のネットワーク ファイルとフォルダを操作することができます。ネットワーク エクスプローラ ページでユーザーがアクセス権を持つ共有フォルダまたはファイルを表示します。

- ユーザーは、ネットワーク エクスプローラ ページ上のリンクをクリックして、これらのドメイン、サーバー、共有、フォルダおよびファイルを参照できます。
- 左のナビゲーション ペインにネットワーク上で使用可能なリソースのリストが表示されます。

- 右のペインでフォルダおよびファイルを使って作業できます。
- 管理者がアップロード機能を有効化しており、ユーザーが書き込み権限を有している場合、ユーザーはファイルをアップロードできます。詳細については、WorkPlace の一般設定の構成を参照してください。

HTML ベースのネットワーク エクスプローラの詳細については、*Secure Mobile Access 12.1 WorkPlace ユーザー ガイド*を参照してください。

Java ベースのネットワーク エクスプローラ

Java ベースのネットワーク エクスプローラでは、Java プラットフォームのブラウザ プラグインを活用しており、ドラッグ アンド ドロップや複数ファイルの選択機能など、一般に利用されている Windows エクスプローラと同じような機能を利用できるようにして、操作性を向上しています。ネットワーク エクスプローラは、HTTPS プロトコルを利用し、暗号化されたファイルや情報を EX-Series アプライアンス間で安全に転送します。このアプライアンスは、リモート ネットワークにある個々のマシンとこのデータのやりとりを行います。

メモ：Java ベースのネットワーク エクスプローラを使用するには、JRE をローカル コンピュータにインストールする必要があります。JRE Version 1.6.0 Update 24 以降を推奨します。最新のバージョンの Java および JRE をダウンロードするには、http://www.java.com にアクセスします。

- Java ベースのネットワーク エクスプローラでは、左のペインにローカル マシンのファイル システムが表示され、右ペインにリモートの場所が表示されます。
- 右側のペインを使用すると、ネットワーク ドメインやコンピュータ、およびそれに関連するファイル共有を参照できます。
- この 2 つのウィンドウを使用すると、ファイルを操作したり、リモートやローカルのファイル システム間でコピーしたりできます。(リソースを移動すると、そのリソースの下のすべてのリソースも再帰的に転送されます。)
- また、ネットワーク エクスプローラ内でブックマークを作成すれば、ポータル レベルからネットワークをすぐに移動できます。

Java ベースのネットワーク エクスプローラの詳細については、*Secure Mobile Access 12.1 WorkPlace ユーザー ガイド*を参照してください。

HTML5 を使用した RDP、VNC、SSH および Telnet

トピック:

- HTML5 と RDP、VNC、SSH および Telnet について
- HTML5 を使用した RDP
- HTML5 を使用した VNC
- HTML5 を使用した SSH および Telnet

HTML5 と RDP、VNC、SSH および Telnet について

HTML5 クライアントは、RDP、VNC、SSH、および Telnet を使用してバックエンド システムに接続できます。HTML5 クライアントでは、シングル サインオン (SSO)、コピー アンド ペースト、複数の言語キーボードのサポート、バック スクロール、および動的なウィンドウ サイズ変更の各機能を使用できます。また、ユーザは、クロスブラウザやクロス OS のサポートなど、より広範囲の接続が可能です。

メモ：HTML5 を使用した RDP、VNC、SSH および Telnet は、SMA 1000 シリーズ装置上の SMA 12.1 または SMA 12.1 WorkPlace で設定できます。

HTML5 クライアントでは、Java や ActiveX など、エンドポイント クライアントの管理が削除されています。

HTML5 機能 は、RDP、SSH と Telnet、および VNC の HTML5 機能を示します。

HTML5 機能

RDP	SSH および Telnet	VNC
キーボード - AMC のサポート	SSO	SSO
キーボードの拡張	バック スクロール	Mac の画面共有でのパフォーマンス向上
TLS/NLA - AMC のサポート RDP 証明書の ID に関する警告	動的なウィンドウ サイズ変更 (ウィンドウ サイズに関する AMC オプションを削除)	ウィンドウ制御
コピー アンド ペースト	コピー アンド ペースト	エンコード、圧縮レベル、JPEG 画像品質、カーソル形状の更新、CopyRect の使用、制限された色数、表示のみ、デスクトップ共有
タブレット/電話向けの最適化	拡大および縮小	
機器単位ライセンス	ホストキー - SSH の既定のフォント サイズ	

HTML5 を使用した RDP

トピック:

RDP のサーバ認証

ユーザーが、意図したリモート コンピュータやサーバ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。

証明書の検証オプションを設定してサーバ認証に失敗した場合、システムが取る動作を選択することができます。

AMC の[**Graphical Terminal Shortcut > Advanced (グラフィカル ターミナル ショートカット > 詳細)**] ページで、次のオプションが選択できます。

- 接続して警告を表示しない
- 警告を表示する
- 接続しない

RDP デバイスの[**Remote Desktop Connection (リモート デスクトップ接続)**] ページで、次のオプションが選択できます。

- 接続して警告を表示しない
- 警告を表示する
- 接続しない

RDP のキーボード サポート

WorkPlace および AMC のキーボード サポートが強化され、対応言語が追加されています。キーボードの言語は、WorkPlace および AMC のドロップダウン メニューから選択できます。ブラウザの設定言語が既定のキーボード言語として使用されます。

SMA12.1 では、以下のキーボード言語がサポートされています。

- デンマーク語
- オランダ語
- 英語 (英国)
- 英語 (米国)
- フィンランド語
- フランス語 (ベルギー)
- フランス語 (カナダ)
- フランス語 (フランス)
- フランス語 (スイス)
- ドイツ語 (ドイツ)
- ドイツ語 (スイス)
- ハンガリー語
- イタリア語
- ルクセンブルク語
- ノルウェー語
- ロシア語
- スペイン語
- スウェーデン語

HTML5 RDP でのコピー アンド ペースト

次のような RDP 機器間でコピー アンド ペーストが可能です。

- ローカルからローカル
- ローカルからリモート
- リモートからローカル

HTML5 を使用した VNC

トピック:

- VNC オプションの追加と編集
- VNC 表示プロパティの設定
- VNC ウィンドウの縮尺

VNC オプションの追加と編集

[**Add Graphical Terminal Shortcut > Advanced (グラフィカル ターミナル ショートカットの追加 > 詳細)**] ページで、VNC シングル サインオン (SSO) オプションを追加または編集して、使用する VNC 表示パスワードの種類を選択できます。

- なし (prompt user)
- ユーザーのセッション パスワードを使用する
- 個別のパスワードを使用する

VNC 表示プロパティの設定

[**Add Graphical Terminal Shortcut > Advanced (グラフィカル ターミナル ショートカットの追加 > 詳細)**] ページで、以下の VNC 表示プロパティを設定できます。

- エンコード
- 圧縮レベル
- JPEG イメージ品質
- カーソル状態更新
- CopyRect の使用
- 制限された色数（256 色）
- 表示のみ
- デスクトップ共有

VNC ウィンドウの縮尺

以下のオプションから選択することで、VNC ウィンドウの縮尺を設定できます。

- **拡大/縮小を行わない**: VNC ウィンドウのサイズは固定です。ブラウザのウィンドウのサイズはユーザの操作によって変更できますが、VNC リモート デスクトップのウィンドウ サイズは VNC サーバによって指定された値のままで変化しません。
- **ウィンドウに合わせて拡大/縮小**: VNC ウィンドウのサイズは固定されません。ブラウザ ウィンドウのサイズに合わせて拡大/縮小されます。ブラウザのウィンドウのサイズを変えることで、VNC ウィンドウのサイズを変更することができます。
- **Full screen**: ブラウザが全画面表示の状態になると、VNC ウィンドウもブラウザのウィンドウ サイズに合わせて拡大/縮小されます。このオプションは、全画面表示モードをサポートしていないブラウザ (iOS の Safari など) には表示されません。
- **縦横比を保持**: VNC ウィンドウの縦横比は VNC サーバによって指定されているのと同じ値になります。このオプションは、**ウィンドウに合わせて拡大/縮小** または **全画面表示** が選択されている場合にのみ利用可能です。

HTML5 を使用した SSH および Telnet

トピック:

- SSH および Telnet のシングル サインオンの設定
- SSH および Telnet でのスクロールとズーム
- SSH および Telnet のコピー アンド ペースト
- SSH のホスト キーとフォント サイズの設定

SSH および Telnet のシングル サインオンの設定

[**Add Text Terminal Shortcut > Advanced (テキスト ターミナル ショートカット > 詳細)**] ページで、SSH または Telnet のシングル サインオン (SSO) の設定ができます。

以下のオプションを使って SSO の設定ができます。

- なし (prompt user)
- ユーザーのセッション クレデンシャルを転送
- 静的クレデンシャルを転送
  静的ユーザー名とパスワードを定義する必要があります。

SSH および Telnet でのスクロールとズーム

SSH と Telnet ではスクロールが可能です。前後にスクロールすることができ、現在の SSH または Telnet ウィンドウ セッションにある項目やテキストをすべて見ることができます。テキストを拡大/縮小することができ、ウィンドウ自体のサイズ変更もできます。

SSH および Telnet のコピー アンド ペースト

SSH ウィンドウまたは Telnet ウィンドウと他のウィンドウとの間でコピー アンド ペーストすることができます。

SSH のホスト キーとフォント サイズの設定

SSH だけで、以下のオプションを設定できます (WorkPlace または AMC で)。

- 自動的にホスト キーを受け入れる
- 既定のフォント サイズ

Web ショートカット アクセス

SMA アプライアンスでは、OnDemand Tunnel エージェントを実行しているユーザーへの、WorkPlace ショートカットを介した一般的な Web (HTTP) リソースへのアクセス方法として、次の 2 つのオプションを提供しています。

- **ネットワーク エージェントを通してリダイレクトする:** この方法が有効になっていると、OnDemand Tunnel エージェントを実行しているユーザーの場合、OnDemand Tunnel エージェントがロードされていれば、アプライアンスを介して Web コンテンツがプロキシされるようになります。この方法では、WorkPlace リンクからの Web トラフィックで変換が使用されず、シングル サインオンもサポートされません。また、アクセス制御のために URL ベースのルールが使用されることもありません。ただし、この方法は通常、[**Web content translation (ウェブ コンテンツの変換)**] オプションよりもアプリケーションの互換性が向上します。

  この設定を有効にした場合は、オプションで、選択した WorkPlace リソースにエイリアスを定義することによって、それらのリソースを変換するよう構成できます。また、この方法を使用してポリシーを URL レベルで適用し、シングル サインオンをサポートすることもできます。詳細については、Web アプリケーション プロファイルの追加を参照してください。

- [**ウェブ コンテンツの変換**]: Web コンテンツは Secure Mobile Access Web 変換エンジン (シングル サインオンと詳細なアクセス制御を提供するリバース プロキシ) を使用して変換されます。この方法を有効にすると、シングル サインオンが可能になり、アクセス制御のために URL ベースのルールを使用できるようになります。ただし、この方法では、[**Redirect through network agent (ネットワーク エージェントを通してリダイレクトする)**] オプションの場合と比較して、アプリケーションの互換性が制限されます。シングル サインオンを有効にするには、リソースに対してエイリアスを指定する必要があります。詳細については、リソースの追加を参照してください。

Web ショートカットのアクセス方式にどちらを選択するかは、アプリケーションで使用されるネットワーク プロトコル、セキュリティ要件、エンド ユーザーの利便性、対象のプラットフォームなどのさまざまな要素に応じて変わります。このオプションは、WorkPlace の [**Settings (設定)**] ページで構成します。

WorkPlace の一般設定の構成

このセクションでは、作成するすべての WorkPlace サイトに適用される、WorkPlace の一般設定の指定方法について説明します。[**Intranet Address (イントラネット アドレス)**] ボックスからの UNC パス名、URL、またはその両方へのアクセスを有効にするかどうかを、この一般設定で指定します。ただし、各コミュニティに対して [**Intranet Address (イントラネット アドレス)**] ボックスを表示するかどうかは WorkPlace レイアウトによって制御されます。

WorkPlace は、次のようにさまざまな度合いでカスタマイズできます。

- 特定のロゴ、色スキーム、メッセージ テキストを使用するスタイルをセットアップすることで、WorkPlace の外観を変更できます。外観の一貫性を保つために、この同じスタイルを、サイトのログイン、エラー、および通知の各ページに指定できます。詳細については、WorkPlace サイトを参照してください。
- WorkPlace のルック アンド フィールをより細かく制御する必要があるサイトの場合は、WorkPlace ページの全面的なカスタマイズを参照してください。

WorkPlace の一般設定を行うには:

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**WorkPlace**] の下にある [**Access services (アクセス サービス)**] セクションで、[**Configure (設定)**] をクリックします。**WorkPlace** の [**Settings (設定)**] タブが表示されます。

3 [**Web shortcut access (Web ショートカット アクセス)**] オプションのいずれかを選択します。この設定によって、WorkPlace がトンネル エージェントをアクティブにした場合の URL リソースへのアクセス方法が決まります。これらのオプションについては、Web ショートカット アクセスを参照してください。

   - **ネットワーク エージェントを通してリダイレクトする:** Web コンテンツは、OnDemand Tunnel エージェントを実行しているユーザーに代わりアプライアンスによってプロキシされます。
   - [**ウェブ コンテンツの変換を使用**]: Web コンテンツは Secure Mobile Access Web 変換エンジンを使用して変換されます。

4 WorkPlace サイトに指定したレイアウトに**Network Explorer (ネットワーク エクスプローラ)** リソースが含まれている場合、ユーザーは、WorkPlace のネットワーク エクスプローラ ページからファイル システム リソースにアクセスできます。[**Enable file uploads to < > megabytes**] を選択すると、ユーザーが Windows ファイル システム リソースにファイルをアップロードできるようになります。この設定は、ファイル システムのアクセス制御ルールに設定したあらゆる許可よりも優先されます。アクセス ルールにおいてファイル システムへの書き込みアクセスがユーザーに許可されていても、WorkPlace サービスでファイルのアップロードが無効化されている場合、そのユーザーが実行できるのはファイルの移動と削除のみとなり、ファイルへの書き込みはできません。

   1 回のファイル アップロードにおいて、指定されたメガバイト数を超えることはできません。ユーザーに対して大容量ファイルのアップロードを許可すると、アプライアンスのパフォーマンスが低下することがあります。

5 [**Intranet Address box (イントラネット アドレス ボックス)**] エリアで各項目を設定します。この設定は、WorkPlace の [**Intranet Address (イントラネット アドレス)**] ボックスの機能を制御します ([**Intranet Address (イントラネット アドレス)**] フィールドが表示されるかどうかは、WorkPlace レイアウトでの指定により制御されるほか、使用するデバイスによっても変わります。モバイル デバイスでは表示できません)。

ユーザーが WorkPlace の [**Intranet Address (イントラネット アドレス)**] フィールドに UNC パス名または URL を入力して Web リソースにアクセスできるようにするには、[**Enable access to UNC pathnames (UNC パス名へのアクセスを有効にする)**] と [**Enable access to URLs (URL へのアクセスを有効にする)**] を選択します。この方法は、例えば、DNS ドメイン全体を 1 つのリソースとして定義している場合に、そのドメイン内の個々の Web リソースを定義することなく、ドメイン内のすべての Web サーバーへのアクセスを提供したいときなどに役立ちます。この設定は、WorkPlace が変換モードで実行されている場合にのみ適用されます。

Web リソースの定義については、リソースの追加を参照してください。

メモ：

- [**Intranet Address (イントラネット アドレス)**] フィールド で指定した設定は、アクセス制御ポリシーには影響しません。この機能の詳細については、イントラネット アドレス フィールドを参照してください。
- ユーザー クレデンシャルが盗まれることが懸念される場合は、WorkPlace にログインするユーザーに、キーボードからの入力ではなく、画面上の仮想キーボードで文字を指定することによってクレデンシャルを入力できるようにする (またはこの方法を必須とする) ことができます。詳細については、仮想キーボードを使用したクレデンシャルの入力を参照してください。

トピック:

- WorkPlace ショートカットについての作業
- ショートカットの表示
- Web ショートカットの追加
- ショートカット グループの作成
- ネットワーク ショートカットの追加
- Web 専用アクセス
- Citrix の構成
- 仮想デスクトップ ショートカットの追加
- テキスト ターミナル ショートカットの追加
- ショートカットの編集

WorkPlace ショートカットについての作業

WorkPlace では、適切なアクセス権限を持つユーザーが、Web ブラウザを使用して、Web リソース、ターミナル サーバー、および Windows ファイル サーバー上のファイルやフォルダにアクセスできます。AMC にリソースが定義されていても、対応するショートカットを作成するまでは、それらのリソースは WorkPlace に表示されません。このセクションでは、WorkPlace にショートカットおよびショートカット グループを作成して管理する方法について説明します。

ファイル システム リソースへのアクセス、ファイル アップロード、および [**Intranet Address (イントラネット アドレス)**] フィールドの有効化については、WorkPlace の一般設定の構成を参照してください。

ショートカットの表示

管理者には、AMC で構成したショートカットの全リストが表示されます。ただし、ユーザーが WorkPlace にログインすると、このリストは、ショートカットが有効になっているデバイスの種類やポリシーに基づいてフィルタされ、そのユーザーに利用権限があるリソースのみが表示されます。すべての種類のショートカット (Web、ネットワーク、グラフィカル ターミナル) とショートカット グループが、AMC と WorkPlace に表示されます。表示レイアウトは、そのコミュニティで使用されている WorkPlace レイアウトによって決まります。

AMC でショートカットを表示するには、

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 オプションの [**Filters (フィルタ)**] 設定を使用すれば、表示させるオブジェクトを絞り込むことができます。フィルターの使用方法については、フィルタを参照してください。

3 [**Shortcuts (ショートカット)**] リストのデータを確認します。

4 チェック ボックスを使用して、移動または削除するショートカットを選択します。

- ショートカットの構成の詳細を表示するには、横にあるプラス記号 (+) をクリックします。説明、所属するショートカット グループ (該当する場合)、デバイスの種類による制約の有無、および、所属する WorkPlace レイアウト名が表示されます。
- 番号は、そのショートカットの WorkPlace での表示順序を示します。この画面で順序を変更できるほか、[**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページでレイアウトに関連付けられているショートカットのリストを編集することもできます。詳細については、WorkPlace レイアウトの作成または編集を参照してください。
- [**Link text (リンク テキスト)**] 列には、ユーザーに表示されるハイパーリンク テキストが示されます。
- [**Resource (リソース)**] 列には、AMC の [**Resources (リソース)**] ページで定義されているリソース名が示されます。リソースの構成については、リソースの作成と管理を参照してください。
- [**Type (種別)**] 列には、ショートカットの種類が示されます。サポートされているショートカットの種類は、Web、ネットワーク、およびグラフィカル ターミナルです。
- [**Used (使用中)**] 列には、ショートカットがグループや WorkPlace レイアウトに含まれているかどうかが示されます。

ショートカット グループの表示

AMC でショートカット グループを表示するには:

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**Shortcut Groups (ショートカット グループ)**] タブをクリックします。

3 オプションの [**Filters (フィルタ)**] 設定を使用すれば、表示させるオブジェクトを絞り込むことができます。フィルターの使用方法については、フィルタを参照してください。

4 グループのリストのデータを確認します。

5 チェック ボックスを使用して、移動または削除するグループを選択します。

- ショートカット グループの構成の詳細を表示するには、横にあるプラス記号 (+) をクリックします。グループに含まれるショートカットと、グループが属する WorkPlace レイアウトの名前が表示されます。
- 番号は、ショートカット グループの WorkPlace 内での表示順序を示しています。この画面で順序を変更できるほか、[**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページでレイアウトに関連付けられているグループのリストを編集できます。
- [**Name (名前)**] 列には、ユーザーに表示するグループの見出しが示されます。

- [**Description (説明)**] 列には、このグループについての説明が表示されます (指定されている場合)。
- [**Used (使用中)**] 列には、ショートカット グループが WorkPlace レイアウトに含まれているかどうかが示されます。

Web ショートカットの追加

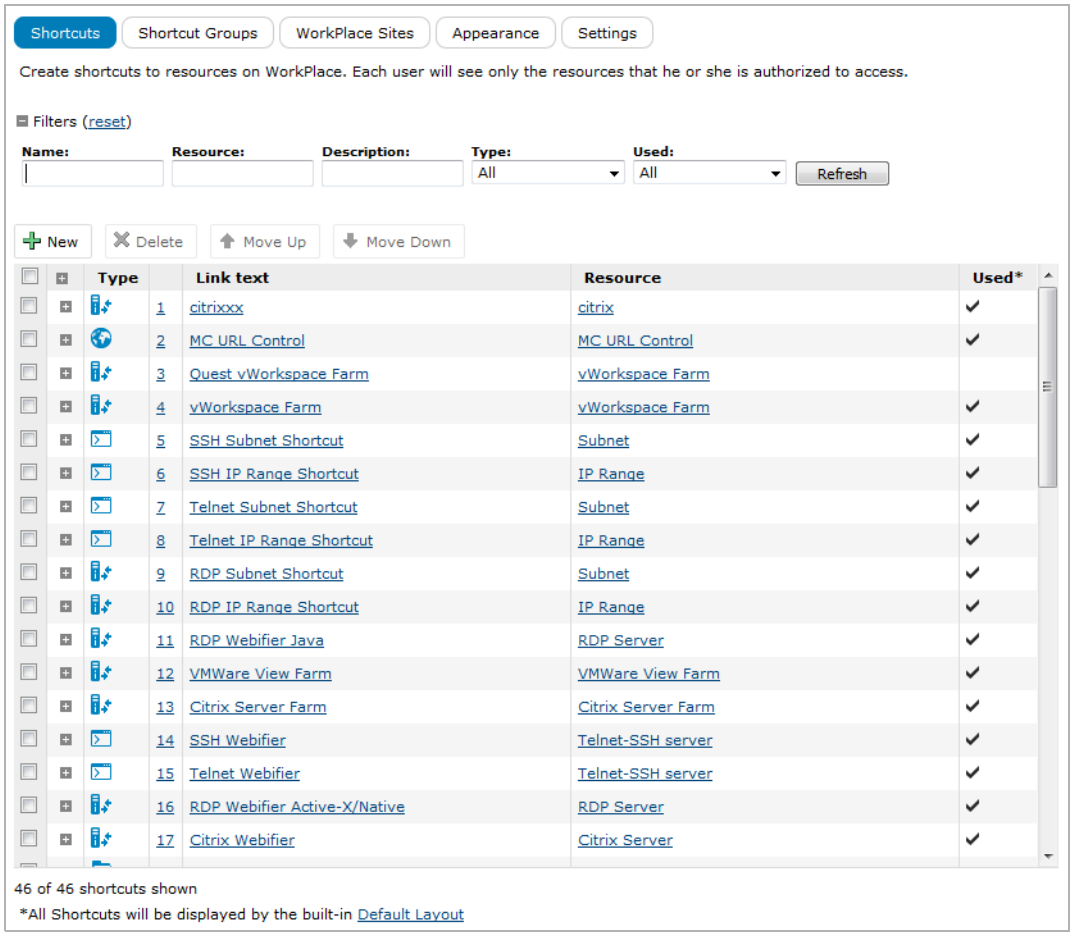
Web ショートカットを使用すると、ユーザーは Web リソースにすばやくアクセスできます。Web リソースへのショートカットを作成するには、まず、そのリソースを定義する必要があります。詳細については、リソースの追加を参照してください。

Web ショートカットを追加するには、

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 「**Shortcuts (ショートカット)**」 タブをクリックします。

3 「**New (新規)**」をクリックします。ドロップダウン メニューが表示されます。



4 リストから [**Web shortcut (Web ショートカット)**] を選択します。[**Add Web Shortcut (Web ショートカットの追加)**] ページが表示されます。

5 [**Position (位置)**] フィールドに、リスト内でのショートカットの順序を指定する番号を入力します。

6 [**Resource (リソース)**] ドロップダウン メニューで、このショートカットにリンクするリソースを選択します。このリストには、AMC の [**Resources (リソース)**] ページで定義されている、利用可能な URL リソースが表示されます。例えば、SharePoint へのショートカットを追加する際は、リソース名に「*SharePoint*」、リソースの URL に「*http://intranet.sharepoint.com*」と指定して URL リソースを定義します。そのうえで、[*Resource (リソース)*] ドロップダウンで [**SharePoint**] を選択します。

リソースの定義については、リソースの作成と管理を参照してください。

7 WorkPlace でユーザーに表示される、リンクおよび説明テキストを指定します。これらの入力内容に変数を使用して、各ユーザーやセッションに固有のリンクや説明テキストを表示することができます。詳細については、リソースと WorkPlace ショートカットの定義での変数の使用を参照してください。

- [**Link text (リンク テキスト)**] フィールドに、ハイパーリンク テキストを入力します。ユーザーはこのハイパーリンク テキストをクリックして Web リソースにアクセスします。[**Link text (リンク テキスト)**] に指定できるのは最大 25 文字です。
- [**Description (説明)**] フィールドに、ショートカットについての分かりやすいコメントを入力します。説明の入力はオプションですが、入力しておくとユーザーが Web リソースを識別しやすくなります。このコメントはリンクの横に表示されます。

8 [**Shortcut group (ショートカット グループ)**] エリアを使用して、既存グループまたは新しいグループにこのショートカットを追加します。グループは、WorkPlace レイアウトの構成要素の 1 つです。例えば、ユーザー向けのすべてのクライアントのダウンロードを 1 つのグループに含めたうえで、([**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページで) 列にグループを含めたり、独自の WorkPlace ページに含めることができます。

9 その他のオプションを指定するには、[**Next (次へ)**] をクリックします。[**Add Web Shortcut (Web ショートカットの追加)**] ページの [**Advanced (詳細)**] タブが表示されます。

10 [**Make link available to these devices (このデバイスでリンクを利用可能にする)**] の下で、WorkPlace ショートカットと、そのショートカットへのアクセスを利用可能にするデバイスの種類とを関連付けます。

- [**All devices (すべてのデバイス)**] を選択した場合は、リンク先の Web リソース自体がすべての種類のデバイスでサポートされているかどうかに関係なく、すべての種類のデバイスでそのショートカットが表示されます。
- 特定の種類のデバイスでのみショートカットが表示されるように制限するには、[**All devices (すべてのデバイス)**] チェック ボックスをオフにしてから、サポートされている種類のデバイスのみを選択します。

例えば、WorkPlace ではさまざまな小型携帯端末をサポートしていますが、すべての Web リソースがすべてのデバイスに対応しているわけではありません。Outlook Web Access は一般的なブラウザでのみ利用でき、また、Outlook Mobile は小型携帯端末でのみ利用できます。このため、Outlook Mobile をリソースとして設定している場合は、一般的なモバイル デバイスと高機能のモバイル デバイスの両方を選択する必要があります。

11 必要な場合は、[**Start page (開始ページ)**] フィールドを使用して、選択した URL に、より詳細な情報を追加します。例えば、そのリンクでルート以外のディレクトリやファイルをポイントしたい場合は、[**Start page (開始ページ)**] フィールドに相対パスを入力します。

これは、コンテンツをルート以外の場所に保存する Web アプリケーションなどの場合に役立ちます。例えば、選択した URL が Outlook Web Access の URL で、*mail.example.com* をポイントしている場合は、スタート ページを */exchange/root.asp* と設定します。最終的な URL は、*https://mail.example.com/exchange/root.asp* となります。

SharePoint の場合は、スタート ページに、*Pages/Default.aspx* や *SitePages/Home.aspx* などの拡張パスを指定します。SharePoint のショートカットの場合、SharePoint サーバーの基本ホスト名 /<IP アドレス> は AMC の [**Resources (リソース)**] ページで定義されます。拡張パスは [**Start Page (開始ページ)**] として構成されます。

ショートカット グループの作成

Web ショートカットやネットワーク ショートカットをグループ化して WorkPlace を整理すると、より合理的な外観とすることができます。WorkPlace ユーザーは、ファイル共有のグループをまとめることができます。

ユーザーには、自身がアクセス権限を持つグループのみが表示されます。グループを作成するには、既存の WorkPlace ショートカット (リソースではない) のなかから、ショートカットを選択します。ショートカットは、複数のグループに含めることができます。

ショートカットのグループを作成するには、

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**Shortcut Groups (ショートカット グループ)**] タブで、[**New (新規)**] をクリックします。

3 名前を入力し、オプションで、グループの説明を入力します。説明は、WorkPlace でグループ名の下に表示されます。上記の例では、「*Domain and stand-alone shares*」が説明になります。

4 [**Position (位置)**] フィールドに、リスト内でのショートカット グループの順序を指定する番号を入力します。ショートカットおよびグループの順序は、[**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページを使用して、この WorkPlace サイト用に選択するレイアウト内で後から変更できます。

5 既存のショートカットがリストされます。このグループに追加するショートカットを選択して、[**Save (保存)**] をクリックします。各ショートカットは複数のグループに含めることができます。空のグループ (ショートカットを選択していないもの) を保存して、後で編集することもできます。

ネットワーク ショートカットの追加

ネットワーク ショートカットを使用すると、ユーザーはファイル システム リソースにすばやくアクセスできます。ファイル システム リソースへのショートカットを作成するには、まず、そのリソースを定義する必要があります (詳細については、リソースの追加を参照してください)。

ネットワーク ショートカットを追加するには:

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 「**Shortcuts (ショートカット)**」 タブをクリックします。

3 「**New (新規)**」をクリックします。ドロップダウン メニューが表示されます。

4 メニューから [**Network shortcut (ネットワーク ショートカット)**] を選択します。[**Add Network Shortcut (ネットワーク ショートカットの追加)**] ページが表示されます。

5 [**Position (位置)**] フィールドに、リスト内でのショートカットの順序を指定する番号を入力します。

6 [**Resource (リソース)**] ドロップダウン メニューで、このショートカットにリンクするファイル システム リソースを選択します。このメニューには、AMC の [**Resources (リソース)**] ページで定義されたファイル システム リソースが含まれます。例えば、*ネットワーク エクスプローラ*は組み込みのリソースであり、ここでショートカットを構成できます。リソースの定義については、リソースの作成と管理を参照してください。

7 WorkPlace でユーザーに表示される、リンクおよび説明テキストを指定します。これらの入力内容に変数を使用して、各ユーザーやセッションに固有のリンクや説明テキストを表示することができます。

   - [**Link text (リンク テキスト)**] フィールドに、ハイパーリンク テキストを入力します。ユーザーはこのハイパーリンク テキストをクリックしてファイル システム リソースにアクセスします。[**Link text (リンク テキスト)**] に指定できるのは最大 25 文字です。
   - [**Description (説明)**] フィールドに、ショートカットについての分かりやすいコメントを入力します。説明の入力はオプションですが、入力しておくとユーザーがファイル システム リソースを識別しやすくなります。このコメントはWorkPlace でリンクの横に表示されます。

8 グループは、WorkPlace レイアウトの構成要素の 1 つです。[**Shortcut group (ショートカット グループ)**] エリアを使用して、既存グループまたは新しいグループにこのショートカットを追加します。例えば、ファイル システム関連のすべてのショートカットを 1 つのグループに含めたうえで、([**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページで) 列にそのグループを含めたり、独自の WorkPlace ページに含めることができます。

Web 専用アクセス

SMA の Web 専用アクセス機能は HTML5 をサポートしており、ユーザーは HTML5 Web サイトにアクセスすることができます。SMA の Web 専用アクセスを使うと、ユーザーは、ウェブ ブラウザのみを使ってオンデマンド コンピューティング サービスにアクセスすることもできます。ユーザーは Connect Tunnel (CT) とネイティブ アクセス方法 (NAMs) を使ってバックエンド アプリケーションにアクセスすることもできます。

SMA の Web 専用アクセスは、以下のクライアント不用の NAM アプリケーションをサポートしています。

- リモート デスクトップ プロトコル (RDP)

  メモ：ターミナル サーバ接続上では、HTML5 RDP ブックマークは、*デバイス毎*のライセンスでサポートされていません。HTML5 RDP ブックマークは、*ユーザー毎*のライセンスでのみサポートされます。ActiveX と Japa RDP ブックマークは、ターミナル サーバ接続上で*ユーザー毎*と *デバイス毎*の両方のライセンスでサポートされています。

- セキュア シェル (SSH)

- Telnet
- 仮想ネットワーク コンピューティング (VNC)
- Citrix

メモ：SMA 11.3 以上は Java クライアントをサポートしていません。Java 非推奨警告が AMC 画面に表示されます。

WorkPlace Lite は、Secure Mobile Access (SMA) 装置のアクセス モードの 1 つで、すべてのアクセス エージェントと EPC エージェントをバイパスして WorkPlace にログインします。WorkPlace Lite が有効になっている WorkPlace サイトにログインするために必要なことは、HTML5 をサポートしている 最新の Web ブラウザを使用することのみです。Web 限定アクセスは、一般にリバース プロキシ アクセスと呼ばれます。

AMC 管理者は次のことを制御できます。

- WorkPlace Lite へのアクセス権をユーザーに付与する。
- ユーザーの利用を WorkPlace Lite のみに制限する。
- ユーザーの WorkPlace Lite へのアクセスを無効にする。

ユーザーが Lite にアクセスするには、チェックボックスをオンにするか、特定の WorkPlace サイトに移動します。ユーザーが WorkPlace Lite モードをオンにすると、ブラウザ ベースのグラフィカル ターミナル ショートカット、テキスト ターミナル ショートカット、Web URL、および HTML ファイル共有ショートカットにアクセス可能になります。

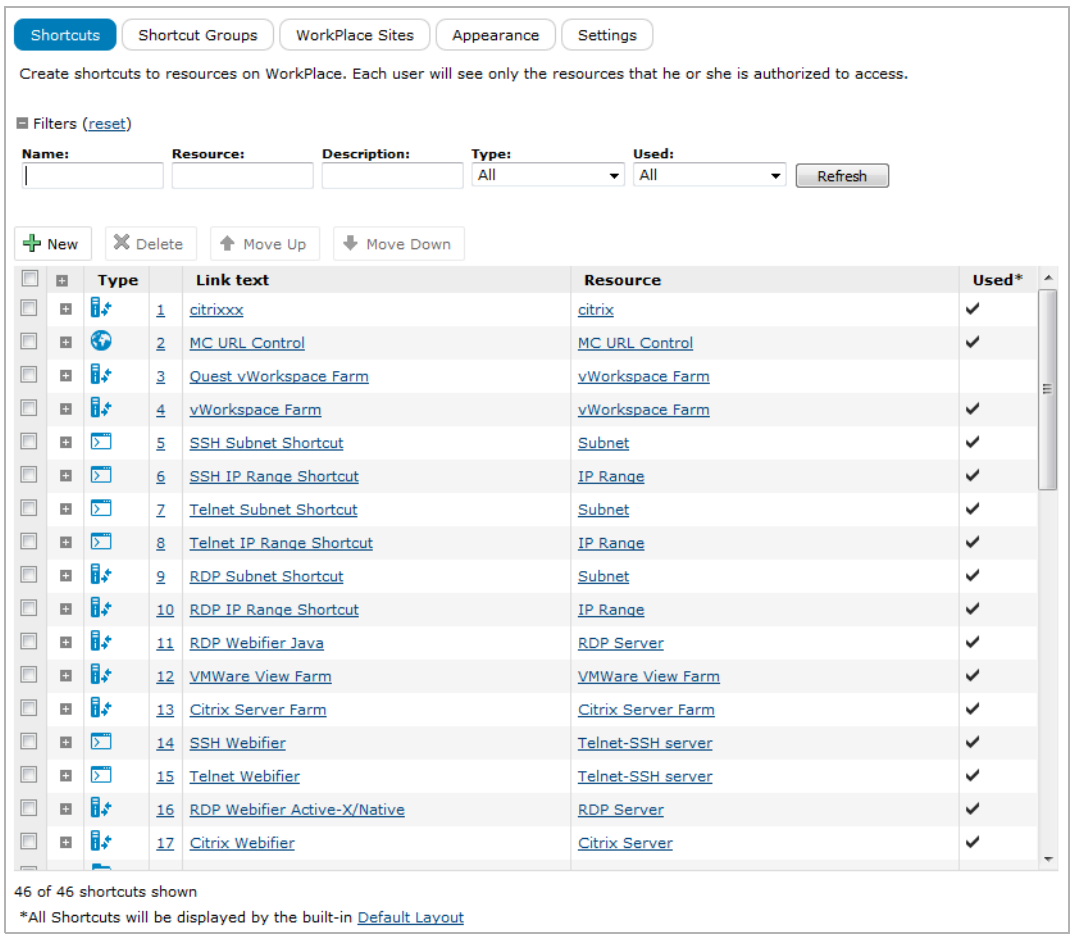
トピック:

- SSH または Telnet を使用するテキスト ターミナル ショートカットの追加
- VNC のグラフィカル ターミナル ショートカットの追加
- Windows Terminal Services の設定
- WorkPlace Lite の設定
- HTML5 RDP の TLS と NLA のサポート

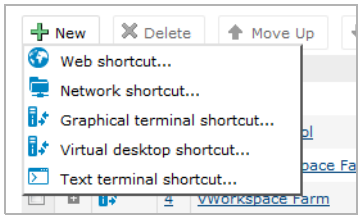
SSH または Telnet を使用するテキスト ターミナル ショートカットの追加

SSH または Telnet を使用するテキスト ターミナル ショートカットを追加するには:

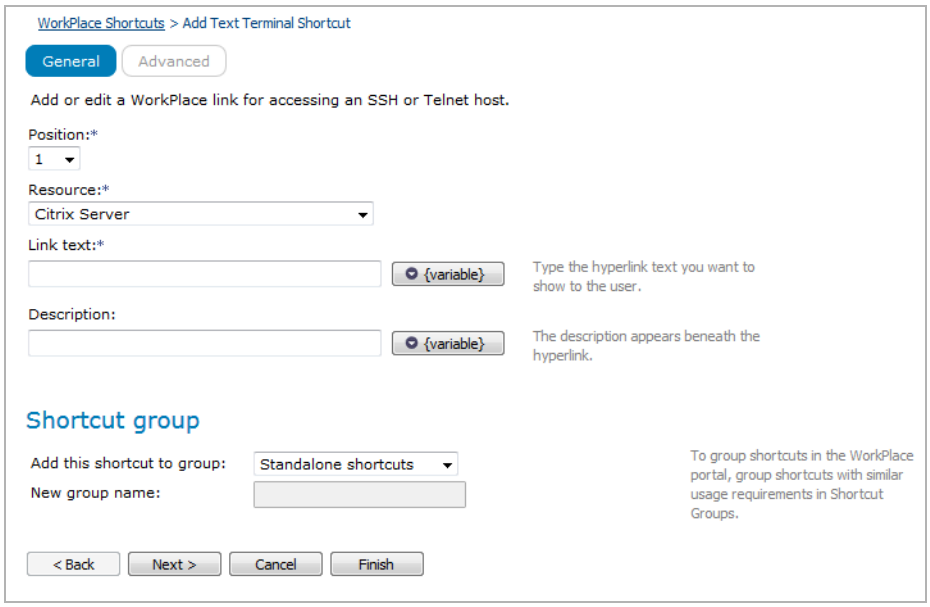
1 [**User Access > WorkPlace > Shortcuts (ユーザー アクセス > WorkPlace > ショートカット)**] ページに移動します。



2 [**New (新規)**] ボタンをクリックします。[**New (新規)**] ドロップダウン メニューが表示されます。



3 [**New (新規)**] ドロップダウン メニューから、[**Text Terminal Shortcut (テキスト ターミナル ショートカット)**] を選択します。[**Add Text Terminal Shortcut (テキスト ターミナル ショートカットの追加)**] ページが表示されます。



4 [**Resources (リソース)**] メニューから、このショートカットを追加したいリソースを選択します。

5 [**Link (リンク)**] テキスト フィールドに、このショートカットに表示したいテキストを入力します。

6 (オプション) [**Description (説明)**] フィールドに、このショートカットの説明を入力します。

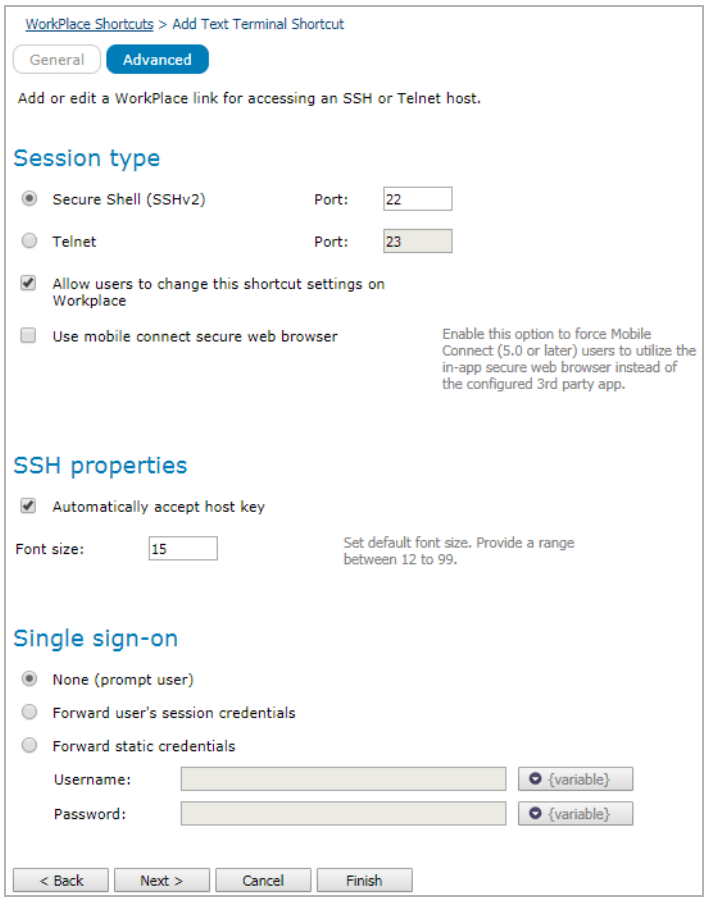
7 [**Add this shortcut to group (このショートカットをグループに追加する)**] ドロップダウン メニューで、次のオプションのうちの 1 つを選択します。

   a このショートカットをグループに含めない場合は、[**Standalone shortcuts (スタンドアロン ショートカット)**] を選択します。

   b このショートカットを既存のグループに含める場合は、リストから既存のグループの 1 つを選択します。

   c 新規のグループを作成する場合は、[**New group name (新規グループ名)**] フィールドに新規のグループの名前を入力します。

8 「**次へ**」を選択します。[**Add Text Terminal Shortcut > Advanced (テキスト ターミナル ショートカットの追加 > 詳細)**] ページが表示されます。



9 目的の**セッション 種別**、**保護Shell (SSHv2)** または **Telnet** を選択します。

10 [**Port (ポート)**] フィールドに、ポート番号を入力します。

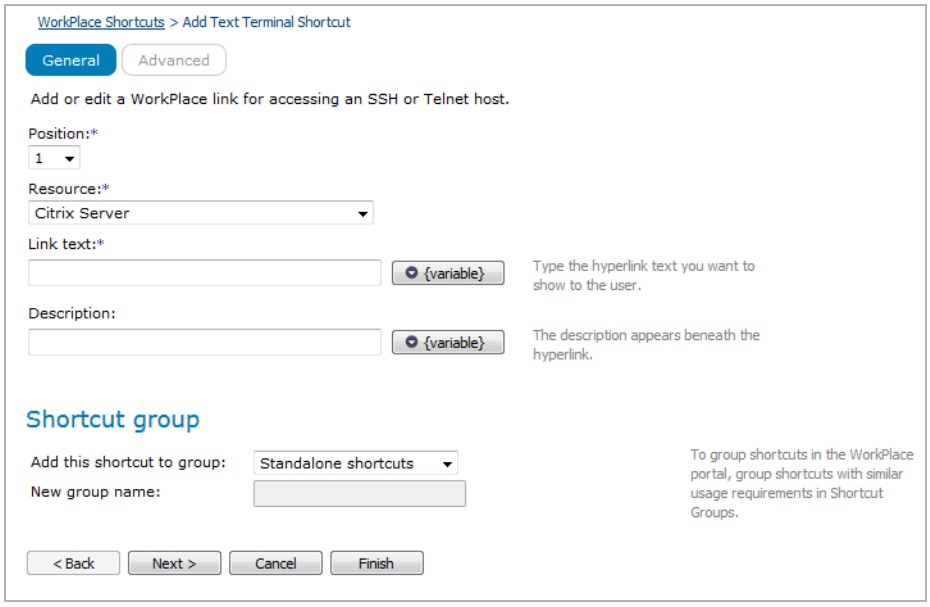
11 「**完了**」をクリックします。上部に新規のショートカットがリストされた、[**Shortcuts (ショートカット)**] ページが表示されます。

VNC のグラフィカル ターミナル ショートカットの追加

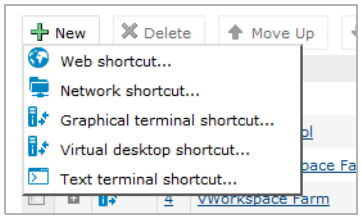
グラフィカル ターミナル ショートカットを使用すると、ユーザーは、転送方法 (プロキシまたはトンネル) に関係なく、バックエンド サーバー (Microsoft RDP、Citrix、VNC) にすばやく簡単にアクセスできます。ほとんどの場合、いずれかの種類のシングル サインオン (SSO) クレデンシャルが有効化されるため、ユーザーは GTS の起動後にユーザー名とパスワードを再入力しなくて済みます。グラフィカル ターミナル ショートカットのなかには、AMC 管理者によって構成されるごく基本的な機能 (IP/ホスト名およびポートなど) のみを持つものがあります。他には、非常に複雑な構成 (例えば、カスタム構成ファイルのアップロード (.RDP/.ICA)、複数モニタのサポート、高解像度ディスプレイのサポートなど) を持つものなどもあります。

VNC にグラフィカル ターミナル ショートカットを追加するには:

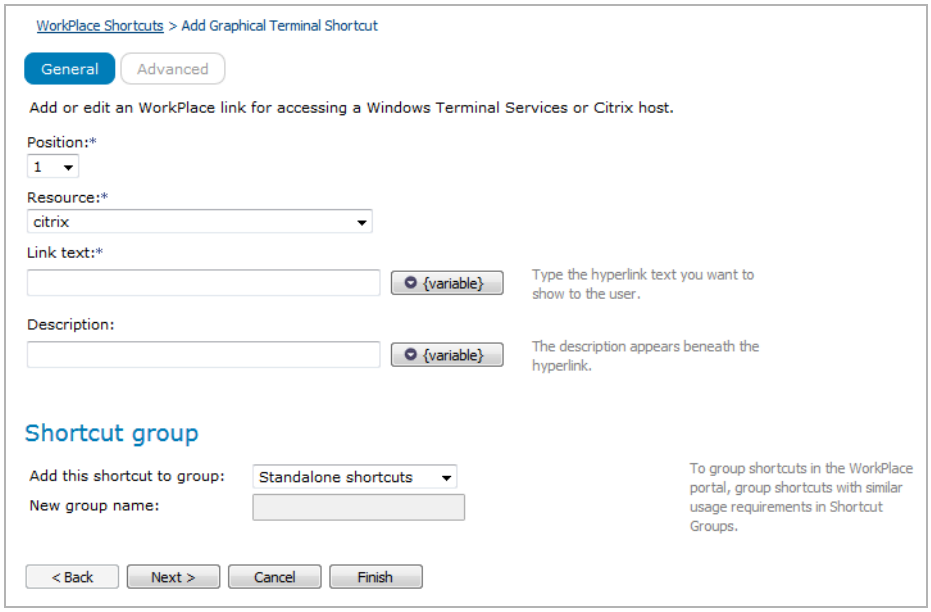
1 [**User Access > WorkPlace > Shortcuts (ユーザー アクセス > WorkPlace > ショートカット)**] ページに移動します。



2 [**New (新規)**] ボタンをクリックします。[**New (新規)**] ドロップダウン メニューが表示されます。



3 [**New (新規)**] ドロップダウン メニューから、[**Graphical terminal shortcut (グラフィカル ターミナル ショートカット)**] を選択します。[**Add Graphical Terminal Shortcut > General (グラフィカル ターミナル ショートカットの追加 > 一般)**] ページが表示されます。



4 [**Position (位置)**] ドロップダウン メニューから、そのリンクが WorkPlace に表示される順序を選択します。

5 [**Resources (リソース)**] ドロップダウン メニューから、このショートカットを追加したいリソースを選択します。必要に応じて、セキュリティ管理で説明されるように、リソースを設定します。

6 [**Link (リンク)**] フィールドに、このショートカットに表示したいハイパーリンク テキストを入力します。

7 (オプション) [**Description (説明)**] フィールドに、このショートカットの説明を入力します。

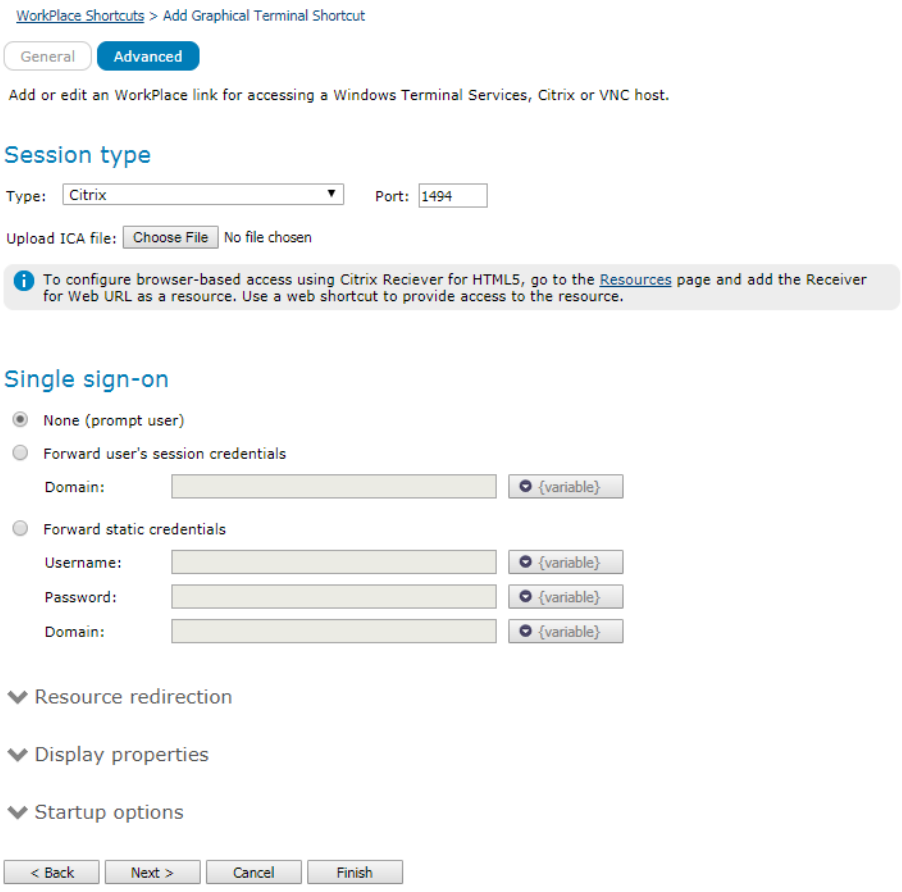
8 [**Add this shortcut to group (このショートカットをグループに追加する)**] ドロップダウン メニューで、次のオプションのうちの 1 つを選択します。

   a このショートカットをグループに含めない場合は、[**Standalone shortcuts (スタンドアロン ショートカット)**] を選択します。

   b このショートカットを既存のグループに含める場合は、リストから既存のグループの 1 つを選択します。

   c 新規のグループを作成する場合は、[**New group name (新規グループ名)**] フィールドに新規のグループの名前を入力します。

9 「**次へ**」を選択します。[**Add Graphical Terminal Shortcut > Advanced (グラフィカル ターミナル ショートカットの追加 > 詳細設定)**] ページが表示されます。



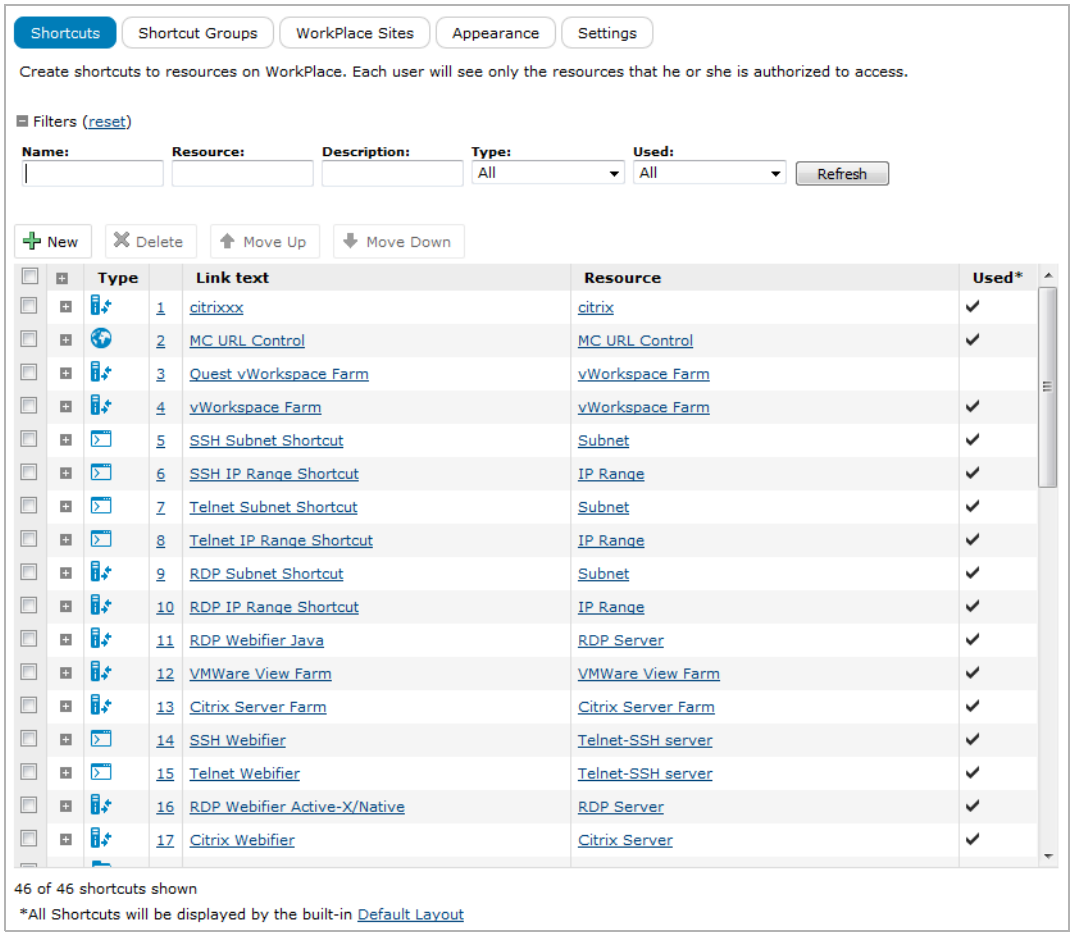
10 「**完了**」をクリックします。上部に新規のショートカットがリストされた、[**Shortcuts (ショートカット)**] ページが表示されます。

Windows Terminal Services の設定

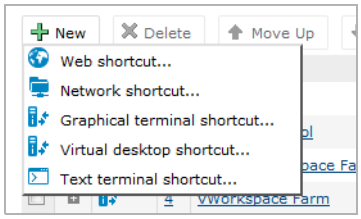
メモ：ActiveX と Japa RDP ブックマークは、ターミナル サーバ接続上で*ユーザー毎*と*デバイス毎*の両方のライセンスでサポート されています。

Windows Terminal Services を設定するには:

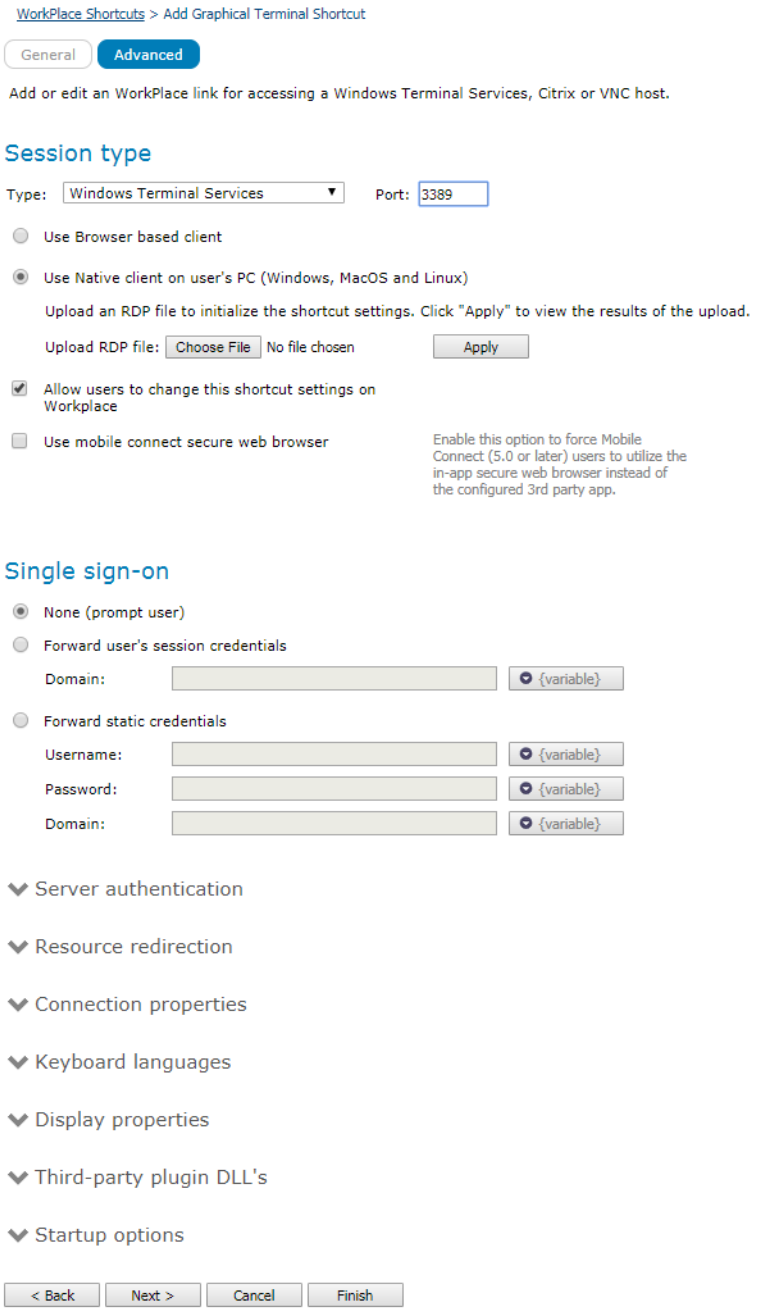
1 [**User Access > WorkPlace > Shortcuts (ユーザー アクセス > WorkPlace > ショートカット)**] ページに移動します。



2 [**New (新規)**] ボタンをクリックします。[**New (新規)**] ドロップダウン メニューが表示されます。



3 ショートカット ドロップダウン メニューから、[**Graphical terminal shortcut (グラフィカル ターミナル ショートカット)**] を選択します。[**Add Graphical Terminal Shortcut > General (グラフィカル ターミナル ショートカットの追加 > 一般)**] ページが表示されます。



4 [**Position (位置)**] ドロップダウン メニューから、そのリンクが WorkPlace に表示される順序を選択します。

5 [**Resources (リソース)**] ドロップダウン メニューから、このショートカットを追加したいリソースを選択します。必要に応じて、セキュリティ管理で説明されるように、リソースを設定します。

6 [**Link (リンク)**] フィールドに、このショートカットに表示したいハイパーリンク テキストを入力します。

7 (オプション) [**Description (説明)**] フィールドに、このショートカットの説明を入力します。

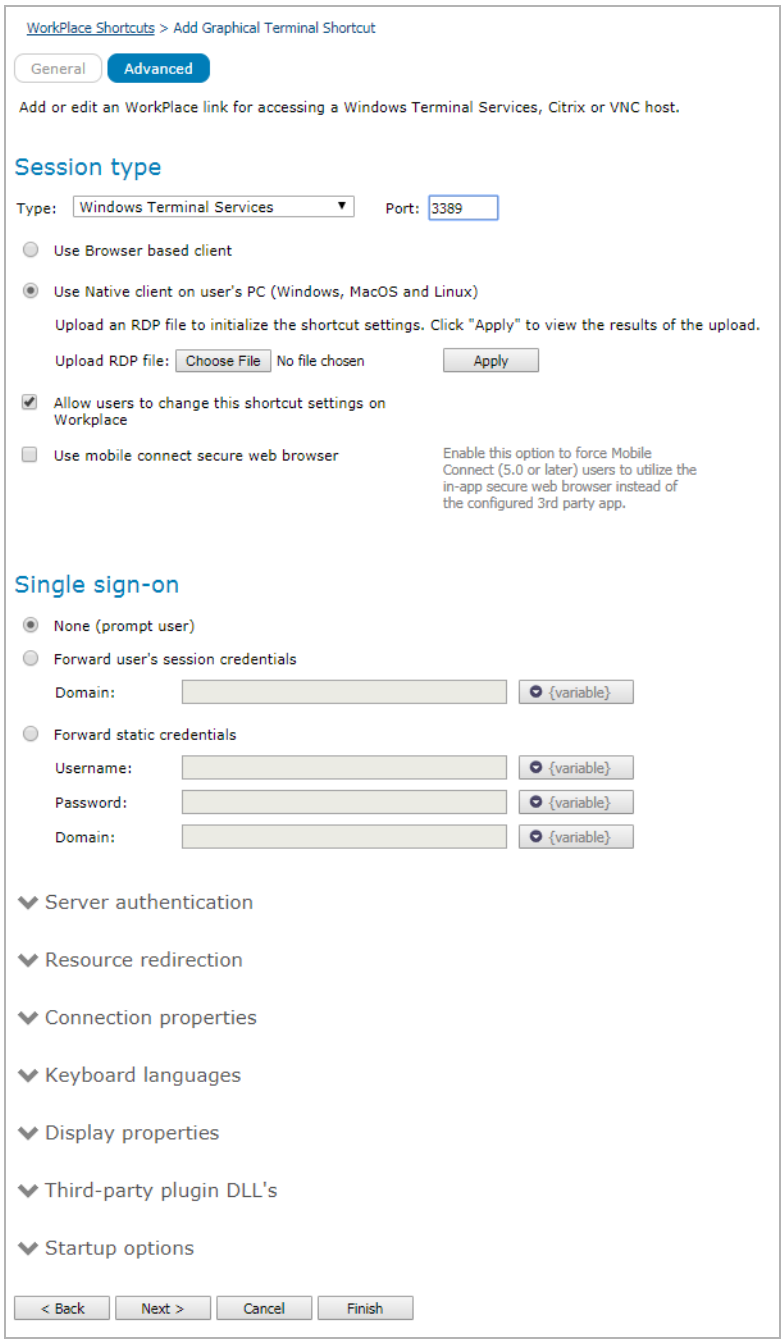
8 [**Add this shortcut to group (このショートカットをグループに追加する)**] ドロップダウン メニューで、次のオプションのうちの 1 つを選択します。

a このショートカットをグループに含めない場合は、[**Standalone shortcuts (スタンドアロンショートカット)**] を選択します。このオプションは既定の設定です。

b このショートカットを既存のグループに含める場合は、リストから既存のグループの 1 つを選択します。

c 新規のグループを作成する場合は、[**New group name (新規グループ名)**] フィールドに新規のグループの名前を入力します。

9 「**次へ**」を選択します。[**Add Graphical Terminal Shortcut > Advanced (グラフィカル ターミナル ショートカットの追加 > 詳細設定)**] ページが表示されます。



トピック:

- セッション種別
- シングル サインオン
- サーバ認証
- リソースのリダイレクト
- 接続プロパティ
- キーボード言語
- 表示プロパティ
- サードパーティ プラグイン DLLs
- 起動オプション

セッション種別

メモ：オプションは、[**General (一般)**] ページでの [**Resources (リソース)**] の選択によって変わります。選択の中には、[**Port (ポート)**] フィールドだけが有効なものもあります。

1 [**Type (種別)**] ドロップダウン メニューから、[**Windows Terminal Services (Windows ターミナル サービス)**] を選択します。

2 [**Port (ポート)**] フィールドに、RDP 通信に使用するポート番号を入力します。既定値は **3389** です。

3 ショートカットで使用する RDP クライアントの種別を選択します。

- **ブラウザ ベースのクライアントを使用する**-すべてのエンド ポイント デバイスが、ブラウザ ベースの RDP クライアントを使用します。ブラウザ ベースの RDP クライアントは、Forms などの詳細なセッションのオプションをサポートしていません。
- **PC のネイティブ クライアントを使用する (Windows/Mac/Linux)** - (既定値) このショートカットでは、ユーザーの PC 上にあるネイティブ RDP クライアントを使用するようにします。
  - **RDP ファイルのアップロード**- RDP ファイルがある場所を参照して RDP ファイルをアップロードします。

シングル サインオン

1 エンド ユーザーがサインオンする方法として、以下のいずれかのオプションを選択します。

メモ：ユーザー クレデンシャルが盗まれることが懸念される場合は、WorkPlace にログインするユーザーに、キーボードからの入力ではなく、画面上の仮想キーボードで文字を指定することによってクレデンシャルを入力できるようにする (またはこの方法を必須とする) ことができます。詳細については、仮想キーボードを使用したクレデンシャルの入力を参照してください。

- **なし (入力をユーザーに求める)** - エンド ユーザーにクレデンシャルの入力を求めるプロンプトを表示します。
- **Forward user's session credentials (ユーザーのセッション クレデンシャルを転送する)** - バックエンド RDP マシンにログインするのに、ユーザーのセッション クレデンシャル (ユーザー名/パスワード) を使用します。[**Domain (ドメイン)**] フィールドには、ログイン試行時にバックエンド RDP マシンに転送する必要のある Windows ドメインを指定します。

- [**Forward static credentials (静的クレデンシャルの転送)**] - ログオン要求時にバックエンドサーバに送信する静的クレデンシャルを (手動またはポリシー変数による設定のいずれかの方法で) 定義します。静的クレデンシャルを転送するには、使用する静的な**ユーザー名**、**パスワード**、および**ドメイン**を指定します。

サーバ認証

1 [**If the identity of the remote computer cannot be verified (リモート コンピュータの ID が確認できない場合)**] ドロップダウン メニューから、サーバ認証が失敗したときにリモート ユーザーのアクセスを許可するか、拒否するかを選択します。

- **接続して警告を表示しない**
- **警告を表示して、接続を続行するかどうかを選択する** (既定値)
- **接続しない**

リソースのリダイレクト

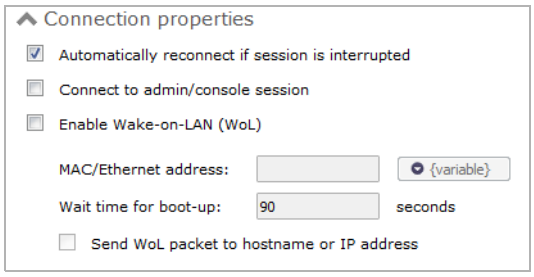
1 [**Bring remote audio to local computer (リモート デバイスの音声をローカル コンピュータ上で再生する)**] チェックボックスを選択すると、ユーザーはセッション中にリモートの音声にアクセスできるようになります。音声のリダイレクションはネットワーク リソースを多く消費するため、パフォーマンスが低下する可能性があることに注意してください。デフォルトではオフになっています。

2 [**Share clipboard between local and remote computers (ローカル コンピュータとリモート コンピュータでクリップボードを共有する)**] チェックボックスを選択すると、ユーザーは双方向でクリップボードの内容のコピーと貼り付けができるようになります。デフォルトでは、この機能が有効になっています。

3 [**Allow access to local (ローカルへのアクセスを許可する)**] で、セッション中にユーザーがアクセスできるデバイスのチェックボックスを選択します。

- ドライブ
- プリンタ
- SmartCards (認証用途)
- プラグ アンド プレイ デバイス
- ポート (ローカル コンピュータからリモート コンピュータへのポート リダイレクション)

接続プロパティ



1 [**Automatically reconnect if session is interrupted (セッションが中断された場合に自動的に再接続する)**] チェックボックスを選択すると、接続が切断された場合に、RDP クライアントはプロンプトを表示することなく再接続を行います。

2 [**Connect to admin/console session (管理/コンソール セッションに接続)**] チェックボックスを選択すると、AMC 管理者は接続の確立に AMC セッションを使用するかどうかを定義できます。

3 Wake-on-LAN パケットを対応する MAC アドレスやリソースのホスト名/IP アドレスに送信するには、[**Enable Wake-on-LAN (WoL) (Wake-on-LAN (WoL) を有効にする)**] チェックボックスを選択して、WoL パケットを送信することになる対応するハードウェアのアドレスを、[**Mac/Ethernet address (Mac/ イーサネット アドレス)**] に入力します。[**Wait time for boot-up (起動待ち時間)**] を変更するには、WoL パケットの送信後に、クライアント マシンが起動したかどうかを確認するまでの秒数 (既定値は 90) を入力します。

4 [**Send WoL packet to hostname or IP address (WoL パケットをホスト名/IP アドレスに送信)**] チェックボックスを選択すると、WoL パケットはこのリソースに関連付けられているホスト名/IP アドレスにも送信されます。

キーボード言語

1 [**Keyboard Layout (キーボード レイアウト)**] ドロップダウン メニューから、言語を選択します。デフォルトは**ブラウザのロケールを使用**です。

表示プロパティ

1 [**Screen resolution (画面解像度)**] ドロップダウン メニューから、目的の画面解像度を選択する、または[**Custom (ユーザー定義)**] を選択してユーザー定義の解像度を入力します (既定は、**1024 x 768 ピクセル**)。管理者は、Workplace ユーザーに解像度を選択させることもできます。

2 [**Color Depth (色深度)**] ドロップダウン メニューから、画面の色深度を選択します (既定は、**16-ビット**)。

3 適用したい他の画面プロパティも選択できます。

- **Show connection bar (接続バーを表示)** - AMC 管理者が、GTS セッションの確立後に画面上部に接続バーを表示するかどうかを定義できます。既定: **オン**
- **Multiple monitor support (マルチ モニタのサポート)** - RDP7 の複数モニタ サポートを有効にするかどうかを制御します。RDP7 が利用不可の場合、複数モニタが有効化されていると、GTS は RDP6 のデュアル モニタ モードにフォールバックします既定: **無効**
- **Remote application (リモート アプリケーション)** - AMC 管理者は (実際にターミナルを起動することなく) GTS セッションを介してアプリケーションをリモートで起動させることができます。既定: **無効**

  ⓘ **重要**：RDP ファイルを介するリモート アプリケーションは、ODMM または HTML5 でサポートされません。

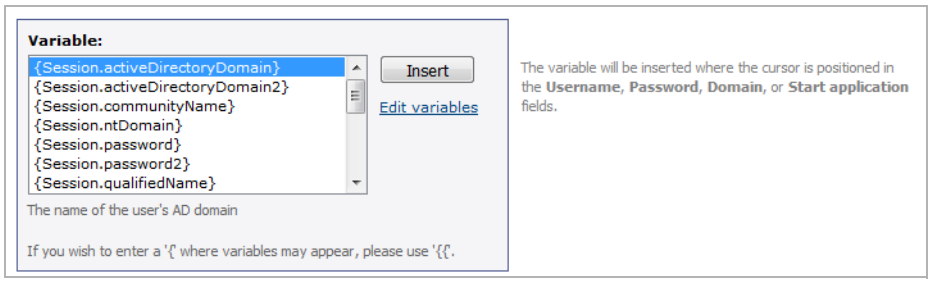
  ⓘ **メモ**：この項目を有効にした場合は、[**Startup Options (開始オプション)**] セクションで、[**Start application (開始アプリケーション)**]、[**Application Arguments (アプリケーション引数)**]、および [**Working directory (作業ディレクトリ)**] を定義する必要があります。

サードパーティ プラグイン DLLs

ⓘ **メモ**：DLL はクライアント マシンにあらかじめインストールされている必要があります。ターミナル サービスでは DLL のインストールは行いません。

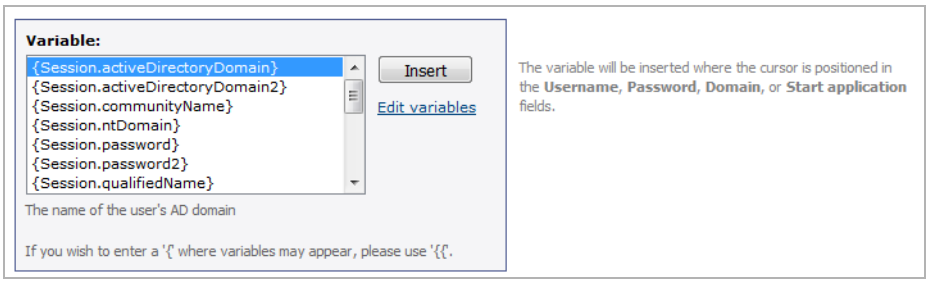
1 サードパーティ プラグイン DLLs を RDP GTS セッション開始時に読み込むには、[**Enable third-party plugin DLLs (有効サードパーティ プラグイン DLLs)**] チェックボックスを選択します。

2 読み込む DLL をカンマ区切りで入力します。**{variable (変数)}** ボタンをクリックすると、ポップアップ リストから予め定義した変数を選択できます。



起動オプション

メモ：これらのオプションについて、オプションに関連付けられた {variable (変数)} ボタンをクリックして、予め定義した変数を使用できます。



1 GTS RDP セッション開始時にアプリケーションを開始するには、[**Start application (開始アプリケーション)**] フィールドで、クライアント マシン上のアプリケーションの完全なパスを入力します。

2 アプリケーションを正常に開始するために指定する必要があるコマンドライン引数を追加するには、[**Arguments (引数)**] フィールドにアプリケーションの引数を入力します。

3 開始アプリケーションを指定する場合は、[**Working directory (作業ディレクトリ)**] フィールドにアプリケーションを起動するディレクトリを入力します。

4 設定を保存するには[**Finish (完了)**] をクリックし、項目を削除するには [**Cancel (キャンセル)**] をクリックし、[**General (一般)**] タブに戻るには [**Back (戻る)**] をクリックします。

メモ：起動オプションは HTML5 RDP 経由でサポート されます。

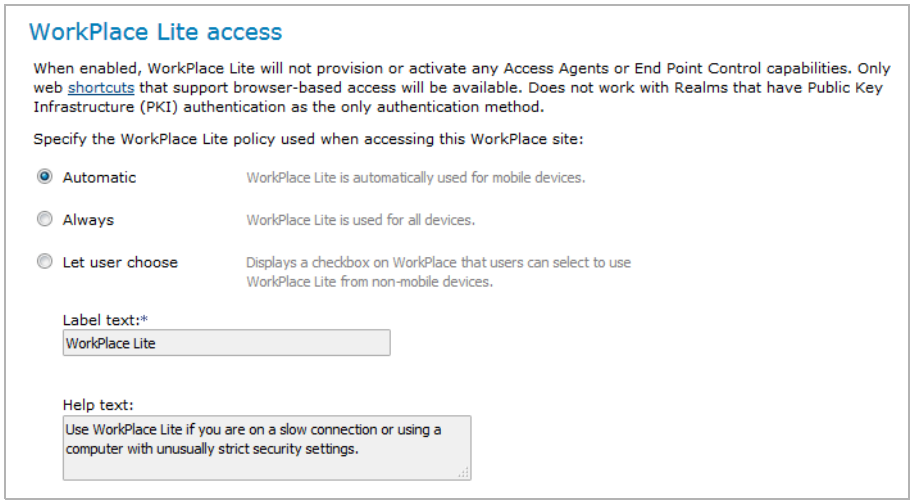
メモ：SMA 11.3 以上では、Java ベースの RDP はサポート されていません。

WorkPlace Lite の設定

WorkPlace Lite モードの設定は、各 WorkPlace サイト別に行います。

WorkPlace Lite を設定するには

1 AMC で、[**User Access > WorkPlace > WorkPlace Sites (ユーザー アクセス > WorkPlace > WorkPlace サイト)> *<Your WorkPlace Site (WorkPlce サイト)>* > Advanced (詳細)**] を参照します。



2 [**WorkPlace Lite access (WorkPlace ライト アクセス)**] で、これらのオプションを選択します。

- **Automatic** - WorkPlace に WorkPlace Lite モードのユーザー選択チェックボックスを表示せず、モバイル機器でのみ WorkPlace Lite アクセスを有効にします。以前のファームウェア バージョンからアップグレードした場合と新規インストールの場合は、この設定がデフォルトです。**ラベル** と **ヘルプ** テキストのコントロールは無効になります。
- **Always** - WorkPlace には WorkPlace Lite モードのユーザー選択チェックボックスを表示しませんが、この WorkPlace サイトにユーザーがログインすると、WorkPlace Lite アクセスは常に有効になります。**ラベル** と **ヘルプ** テキストのコントロールは無効になります。
- **Let user choose** - WorkPlace に WorkPlace Lite アクセスの有効と無効を選択するチェックボックスを表示し、ラベル テキストとヘルプ テキストも表示します。AMC 管理者は、必要に応じて**ラベル** と **ヘルプ** テキストを変更したり、調整したりできます。

3 「**Save (保存)**」を選択します。

HTML5 RDP の TLS と NLA のサポート

Secure Mobile Access (SMA) はリモート デスクトップ プロトコル (RDP) を介してリモート ホストに接続したい HTML5 ブラウザ クライアントの Transport Layer Security (TLS) とネットワーク レベル認証 (NLA) を提供します。

RDP はリモート クライアントと RDP ホスト サーバとの間の暗号化レベルをネゴシエートします。TLS を使用する RDP を設定すると、RDP セッションの安全性を強化して、RDP ホスト サーバを認証して RDP ホスト サーバとクライアントの間のすべての通信を暗号化することができます。NLA を使用する RDP を設定することもでき、これにより RDP ホスト サーバがユーザー向けのセッションを作成する前に、クライアントは認証用のユーザー クレデンシャルを提示することを強制されます。

RDP 用の HTML5 ブラウザ サポートの TLS と NLA を有効にするには、RDP ホスト サーバで TLS と NLA を設定して、WorkPlace の [**Manage Bookmarks (ブックマークの管理)**] ページでクライアントのブラウザ ロケール用のキーボード言語を設定する必要があります。

TS-Farm サーバは、負荷分散となる RDP セッションを有効にします。TS-Farm は、追加のライセンス機能とセッション ブローカを備える多くのリモート デスクトップ サーバ (ファーム サーバ) で構成されます。セッション ブローカはブック キーピングを行い、負荷分散判断を行います。

HTML5 RDP の TLS と NLA サポートの設定

RDP ホスト サーバで TLS と NLA を設定するには:

1 RDP ホスト サーバで、[**RDP-Tcp Properties (RDP-Tcp プロパティ)**] ダイアログを開きます。

2 [**Security layer (セキュリティ層)**] ドロップダウン メニューで、**SSL (TLS 1.0)** を選択します。

3 [**Allow connections only from computers running Remote Desktop with Network Level Authentication (ネットワーク レベル認証を使用してリモート デスクトップを実行しているコンピュータからのみ接続を許可)**] のチェックボックスを選択します。

4 [**Apply (適用)**] を選択します。

5 [**OK**] を選択します。

Citrix の構成

ドロップダウン メニューで [Citrix] を選択すると、[**Advanced (詳細設定)**] タブのオプション メニューが変更され、セクションの各項目にデフォルト設定が入力されます。

Citrix サーバ ファームを設定するには:

1 [**Port (ポート)**] フィールドには、Citrix サーバ ファームで使用するポート番号を入力します。(Citrix の既定は **1494** です)。

2 [**Single Sign-on (シングル サインオン)**] セクションで、エンド ユーザーのサインオン方法を選択します。

> **メモ：Advanced (詳細)** ページのシングル サインオン フィールドは、絶対値で埋めることができ、またはフィールドの右側の [**Variable (変数)**] ボタンをクリックして、表示されるリストから必要な変数を選択し、[**Insert (挿入)**] をクリックすることで埋めることができます。

- **なし (入力をユーザーに求める)** - エンド ユーザーにクレデンシャルの入力を求めるプロンプトを表示します。
- **Forward user's session credentials (ユーザーのセッション クレデンシャルを転送する)** - バックエンド RDP マシンにログインするのに、ユーザーのセッション クレデンシャル (ユーザー名/パスワード) を使用します。[**Domain (ドメイン)**] フィールドには、ログイン試行時にバックエンド RDP マシンに転送する必要のある Windows ドメインを指定します。
- [**Forward static credentials (静的クレデンシャルの転送)**] - ログオン要求時にバックエンド サーバに送信する静的クレデンシャルを (手動またはポリシー変数による設定のいずれかの方法で) 定義します。静的クレデンシャルを転送するには、使用する静的な**ユーザー名**、**パスワード**、および**ドメイン**を指定します。

3 公開されているアプリケーションに対するクレデンシャルの送信を許可する場合は、[**Enable SSO to Citrix applications (Citrix アプリケーションへの SSO を有効にする)**] チェックボックスを選択します。デフォルトではオフになっています。

4 [**Bring remote audio to local computer (リモート デバイスの音声をローカル コンピュータ上で再生する)**] チェックボックスを選択すると、ユーザーはセッション中にリモートの音声にアクセスできるようになります。デフォルトではオフになっています。

> **メモ**：音声のリダイレクションはネットワーク リソースを多く消費するため、パフォーマンスが低下する可能性があります。

5 [**Share clipboard between local and remote computers (ローカル コンピュータとリモート コンピュータでクリップボードを共有する)**] チェックボックスを選択すると、ユーザーは双方向でクリップボードの内容のコピーと貼り付けができるようになります。デフォルトでは、この機能が有効になっています。

6 [**Screen resolution (画面解像度)**] を変更するには、目的の画面解像度をドロップダウン メニューから選択する、または[**Custom (ユーザー定義)**] を選択してユーザー定義の解像度を入力します (既定は、**1024 x 768 ピクセル**)。管理者は、Workplace ユーザーに解像度を選択させることもできます。

7 表示の色深度を変更するには、[**Color Depth (色深度)**] ドロップダウン メニューから必要な色深度を選択します (既定は、**16-ビット**)。

8 設定を保存するには[**Finish (完了)**] **をクリックし、項目を削除するには [Cancel (キャンセル)] をクリックし、[General (一般)] タブに戻るには [Back (戻る)**] をクリックします。

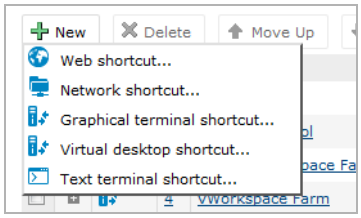
仮想デスクトップ ショートカットの追加

このページを使用して、WorkPlace に表示される仮想デスクトップ ショートカットを作成または編集します。これらのショートカットを使用して、ユーザーは VMware View リソースに簡単に接続できます。

仮想デスクトップ ショートカットを追加するには、

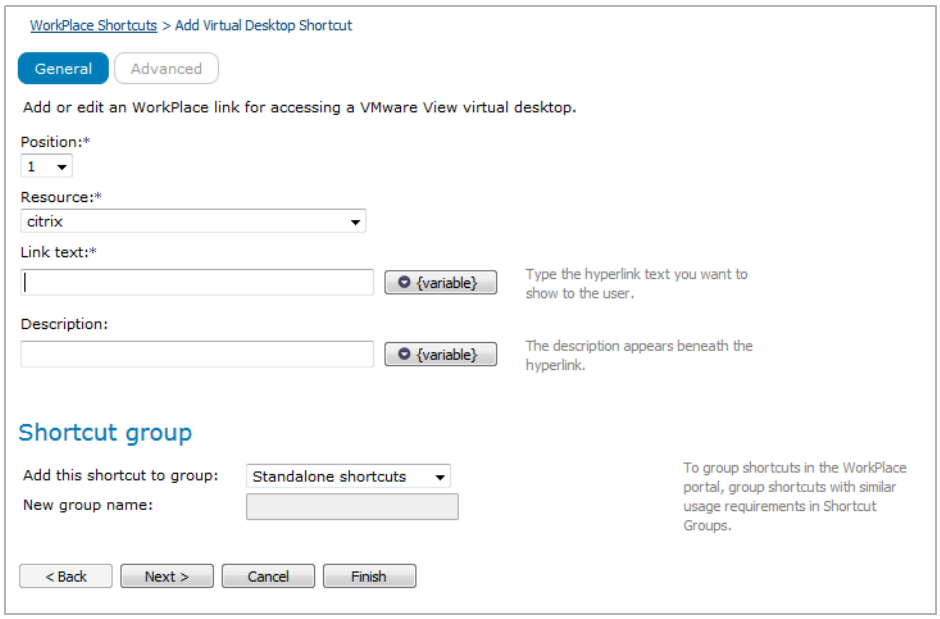
1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**Shortcuts (ショートカット)**] ページで、[**New (新規)**] をクリックします。ドロップダウン メニューが表示されます。



3 [**Virtual Desktop Shortcut (仮想デスクトップ ショートカット)**] を選択します。[**Add Virtual Desktop Shortcut (仮想デスクトップ ショートカットの追加)**] ページが表示されます。

4 [**General (一般)**] タブで、[**Resources (リソース)**] リストからリソースを選択します。



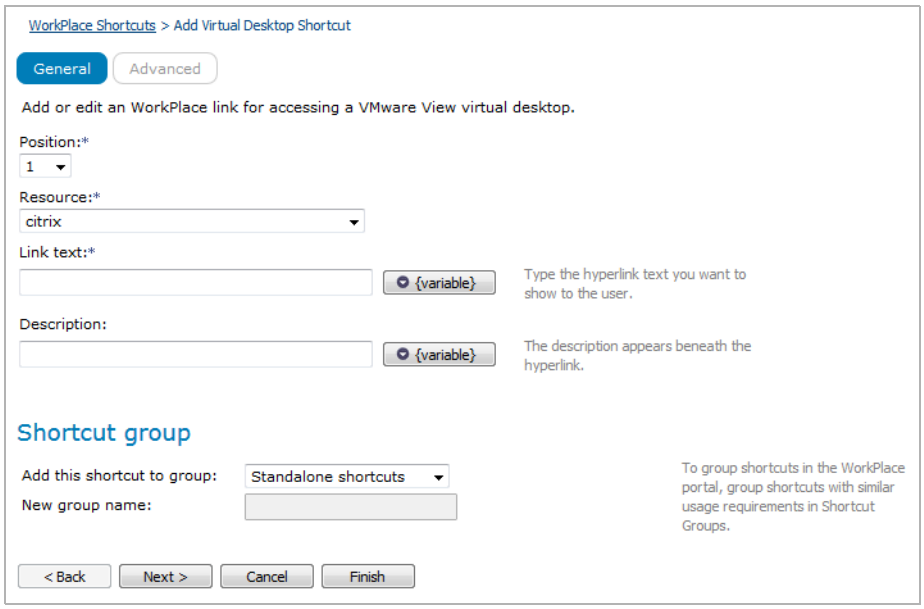
5 [**Link text (リンク テキスト)**] フィールドに、ハイパーリンク テキストを入力します。このハイパーリンク テキストは、VMware View ホストのショートカットとして表示されます。

6 ショートカットの説明を [**Description (説明)**] フィールドに入力します。

7 このショートカットをグループに含めない場合は、[**Add this shortcut to group (このショートカットをグループに追加する)**] ドロップダウン メニューで [**Standalone shortcuts (スタンドアロン ショートカット)**] を選択します。それ以外の場合は、リストから既存のグループを選択します。新しいグループを作成するには、[**New (新規)**] を選択します。

8 [**New (新規)**] を選択した場合は、[**New group name (新規グループ名)**] フィールドに新しいグループの名前を入力します。

9 「**次へ**」を選択します。[**Advanced (詳細)**] タブが表示されます。



10 セッションのタイプ (**Citrix XenDesktop** または **VMware View** など) を選択します。

11 [**Single sign-on (シングル サインオン)**] エリアで、どのようにホストへユーザー クレデンシャルを転送するかを指定します。

- [**None (なし)**] をクリックすると、シングル サインオンが無効化され、ユーザーにクレデンシャルの入力を求めるプロンプトが表示されるようになります。
- [**Forward user's session credentials (各ユーザーの個別のユーザー名とパスワードを転送)**] をクリックすると、WorkPlace での認証に使用したユーザー名とパスワードがホストにも送信されます。
- すべてのユーザーについて同じユーザー名とパスワードを転送するには、[**Forward static credentials (静的資格情報を転送)**] をクリックします。すべてのユーザーに転送するには、静的なユーザー名、パスワード、ドメインを [**Username (ユーザ名)**]、[**Password (パスワード)**]、[**Domain (ドメイン)**] に入力します。
- 横の [**{variable}**] ボタンをクリックすると変数のリストが表示され、これらの各フィールドに変数を挿入できます。

12 [**Resource redirection (リソースのリダイレクト)**] エリアで、仮想デスクトップとホストとの間でどのようにデータをやりとりするかを指定します。

a リモート デバイスの音声をローカル コンピュータ上で再生するには、[**Bring remote audio to local computer (リモート デバイスの音声をローカル コンピュータ上で再生する)**] チェック ボックスを選択します。

b コンピュータ間でクリップボードの内容をコピーするには、[**Share clipboard between local and remote computers (ローカル コンピュータとリモート コンピュータでクリップボードを共有する)**] チェック ボックスを選択します。

c リモート デバイス上のドライブやプリンタにアクセスするには、[**Drives (ドライバ)**] チェック ボックスや [**Printers (プリンタ)**] チェック ボックスを選択します。

13 [Display properties (表示プロパティ)] エリアで、仮想デスクトップの画面の外観を指定します。

a [**Screen resolution (画面解像度)**] ドロップダウン メニューを使用して、仮想デスクトップの画面の解像度を選択します。

b [**Color depth (色深度)**] (画面解像度)を使用して、仮想デスクトップの画面の色深度を選択します。

14 「**完了**」をクリックします。

テキスト ターミナル ショートカットの追加

このページを使用して、WorkPlace に表示されるテキスト ターミナル ショートカットを作成または編集します。これらのショートカットを使用して、ユーザーは SSH リソースや Telnet リソースに簡単に接続できます。

テキスト ターミナル ショートカットを追加するには、

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**Shortcuts (ショートカット)**] ページで、[**New (新規)**] をクリックします。ドロップダウン メニューが表示されます。

3 [**Text Terminal Shortcut (テキスト ターミナル ショートカットの追加)**] を選択します。[**Add Text Terminal Shortcut (テキスト ターミナル ショートカットの追加)**] ページが表示されます。

4 [**General (一般)**] タブで、[**Resources (リソース)**] ドロップダウン メニューからリソースを選択します。

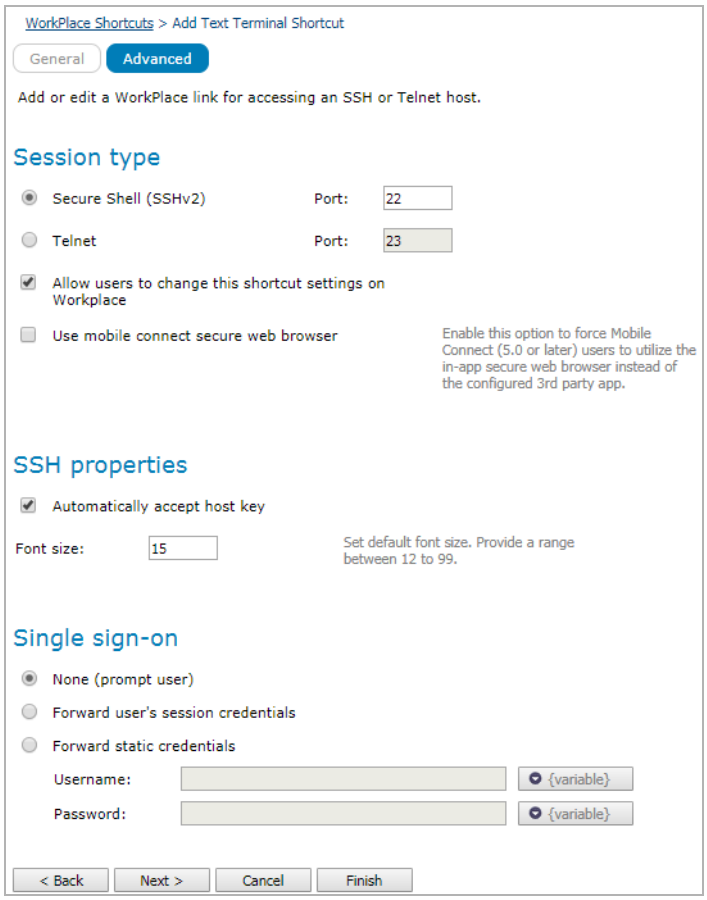
5 [**Link text (リンク テキスト)**] フィールドに、ハイパーリンク テキストを入力します。このハイパーリンク テキストは、SSH または Telnet ホストのショートカットとして表示されます。

6 ショートカットの説明を [**Description (説明)**] フィールドに入力します。

7 このショートカットをグループに含めない場合は、[**Add this shortcut to group (このショートカットをグループに追加する)**] ドロップダウン メニューで [**Standalone shortcuts (スタンドアロン ショートカット)**] を選択します。それ以外の場合は、リストから既存のグループを選択します。新しいグループを作成するには、[**New (新規)**] を選択します。

8 [**New (新規)**] を選択した場合は、[**New group name (新規グループ名)**] フィールドに新しいグループの名前を入力します。

9 「**次へ**」を選択します。[**Advanced (詳細)**] タブが表示されます。



SSHv2 の構成

[**Secure Shell (SSH)**] セッション タイプを選択すると、[**Advanced (詳細)**] タブのオプションのセクションが変更され、このセクションに適切なデフォルト設定が入力されます。

[**Port (ポート)**] には、FTP 通信に使用するポートを定義します既定: **22**

[**Advanced Session Options ([Advanced] タブのセッション関連オプション)**] エリアで以下のことを確認します。

- [**Automatically accept host key (自動的にホスト キーを受け入れる)**] を選択すると、管理者は、ホスト キーが一致しない場合に接続を受け入れるかどうかのプロンプトを、Workplace ユーザーに対して表示するかどうかを制御できます既定: **オン**
- [**Bypass username for SSHv2 only (SSHv2 の場合のみユーザー名をバイパスする)**] は、ログイン時にユーザー名フィールドを無視する/空白にする必要があるかどうかを制御します。Secure Mobile Access ファイアウォールに対してのみ有効です。既定: 非選択

[**General (一般)**] メニューに戻るには、[**Back (戻る)**] をクリックします。新しい設定を有効にするには、[**Finish (完了)**] をクリックします。

Telnet の構成

[**Telnet**] セッション タイプを選択すると、オプションのセクションが変更され、デフォルト設定が事前に入力されます。

[**Port (ポート)**] オプションには、Telnet 通信に使用するポートを定義します既定: **23**

[General (一般)] メニューに戻るには、[**Back (戻る)**] をクリックします。新しい設定を有効にするには、[**Finish (完了)**] をクリックします。

ショートカットの編集

リソースを定義する際に新しい WorkPlace ショートカットを作成できますが、ショートカットの編集や削除には [**Shortcuts (ショートカット)**] ページを使用する必要があります。

ショートカットを編集するには、

1 メイン ナビゲーション メニューから、[**WorkPlace**] をクリックします。

2 編集するショートカットの番号またはリンク テキストをクリックします。

3 必要な編集を加えてから、[**Save (保存)**] をクリックします。

ショートカットを削除すると、そのショートカットはユーザーの WorkPlace に表示されなくなります。ショートカットを削除するには、[**Shortcuts (ショートカット)**] ページを使用する必要があります。

ショートカットを削除するには、

1 メイン ナビゲーション メニューから、[**WorkPlace**] をクリックします。

2 削除するショートカットの左にあるチェック ボックスを選択し、[**Delete (削除)**] をクリックします。ショートカットを削除しても、そのショートカットが参照しているリソースは削除されません。

WorkPlace で表示されるショートカットのリストの順序は、[**Shortcuts (ショートカット)**] ページでの順序と同じです。一度に複数のショートカットを移動できます。ショートカット (およびショートカット グループ) の順序は、後で [**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページを使用して、WorkPlace サイト用に選択するレイアウト内で変更できます。

1 つ以上のショートカットを移動するには、

1 メイン ナビゲーション メニューから、[**WorkPlace**] をクリックします。

2 移動するショートカットの左にあるチェック ボックスを選択します。

3 [**Move Up (上に移動)**] または [**Move Down (下に移動)**] を適宜クリックします。ボタンをクリックするたびに、選択したショートカットがリストの 1 つ上または下に移動します。

個々の WorkPlace ショートカットの順序を変更する別の方法としては、ショートカットの番号またはリンク テキストをクリックして、リスト内での新たな順序を [**Position (位置)**] フィールドに入力します。

WorkPlace サイト

従業員、ビジネス パートナー、供給業者など、異なるユーザー向けに複数の WorkPlace サイトを作成できます。各サイトに一意の外部 URL と固有の外観を設定できるほか、WorkPlace ポータルを迂回してユーザーを別のスタート ページにリダイレクトすることもできます。

例えば、従業員向けとしてタイトルとロゴのカスタマイズされた WorkPlace サイト (URL は *http://employees.headquarters.com*) を作成し、パートナー向けとして *http://partners.subsidiary.com* に別のサイトを作成することができます。一意の外部 URL を持つ複数の WorkPlace サイトを作成する場合は、アプライアンスにワイルドカード証明書を 1 つインポートしてその証明書を複数の WorkPlace サイトのサーバー証明書として指定することができます。または、FQDN がアプライアンスのドメイン名と異なる各サイトごとに個別の SSL 証明書を取得することもできます。詳細については、証明書を参照してください。

メモ：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

オプションで、複数のレルムを構成している場合は、1 つの WorkPlace サイトを 1 つのレルムに関連付けることができます。これにより、ユーザーは、認証プロセスの一部 (通常であればログインするレルムを指定する部分) を迂回できます。WorkPlace サイトをレルムに関連付けている場合、ユーザーはログイン先として別のレルムを選択することはできません。指定したレルムに属していないユーザーは、そのレルムに関連付けられた WorkPlace サイトにはログインできません。

以下の WorkPlace コンポーネントをカスタマイズできます。

- 企業ロゴ
- WorkPlace のタイトル
- ページ上部のメッセージ テキスト
- 色スキーム
- ヘルプ ファイル
- フォント ファミリ

ユーザーのログインするレルムにおいて、変換 Web アクセス、カスタム ポート マッピング Web アクセス、またはカスタム FQDN マッピング Web アクセスが排他的に許可されている場合は、ユーザーに WorkPlace ポータルを経由せずに別のスタート ページへ直接アクセスさせることができます。詳細については、WorkPlace サイトの追加を参照してください。

また、カスタムのライセンス契約を設定し、ユーザーがこれを承認しなければ使用を開始できないようにすることもお勧めします。

WorkPlace へログインする際にユーザーが入力する URL の先頭に、`http://` というプロトコル識別子が追加されます。その後、Web セッションは、安全な HTTP (HTTPS) と `https://` プロトコル識別子を使用するサイトにリダイレクトされます。

メモ：

- カスタムの WorkPlace サイトを指定しない場合や、ユーザーがデフォルトの名前を使用してアプライアンスにアクセスする場合は、デフォルトの WorkPlace サイトが自動的に使用されます。
- 新しい WorkPlace サイトをゼロから作成するのではなく、既存のサイトをコピーして新しいサイト用に一部のパラメータを変更すると、時間を節約できます。WorkPlace サイトのコピーについては、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。
- 不要となった WorkPlace サイトは削除できます。ただし、デフォルトの WorkPlace サイトは削除できません。WorkPlace サイトの削除については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

トピック:

- WorkPlace サイトの追加
- WorkPlace の外観の変更
- WorkPlace と小型携帯端末

WorkPlace サイトの追加

AMC には、構成済みのデフォルト WorkPlace サイトが含まれています。必要に応じて、WorkPlace サイトを追加で作成できます。このセクションではその作成方法について説明します。

異なるスタイルとレイアウトを設定すると、コミュニティごとに WorkPlace の外観を変えることができます。詳細については、WorkPlace の外観の変更を参照してください。小型携帯端末向けに WorkPlace サイトを構成する方法については、WorkPlace と小型携帯端末を参照してください。

WorkPlace サイトの完全修飾ドメイン名 (FQDN) には、次のいずれかを含めることができます。

- SMA アプライアンスと同じドメイン名のホスト。このタイプのサイトには、オプションで、個別の SSL 証明書を構成できます。
- カスタム FQDN。このオプションでは、ワイルドカード SSL 証明書を使用できます (そのワイルドカード証明書を使用する他の WorkPlace サイトと IP アドレスが同一の場合)。または、サイト用に個別の SSL 証明書を使用することもできます。サイトを作成する前に、証明書を取得する必要があります。詳細については、証明書を参照してください。

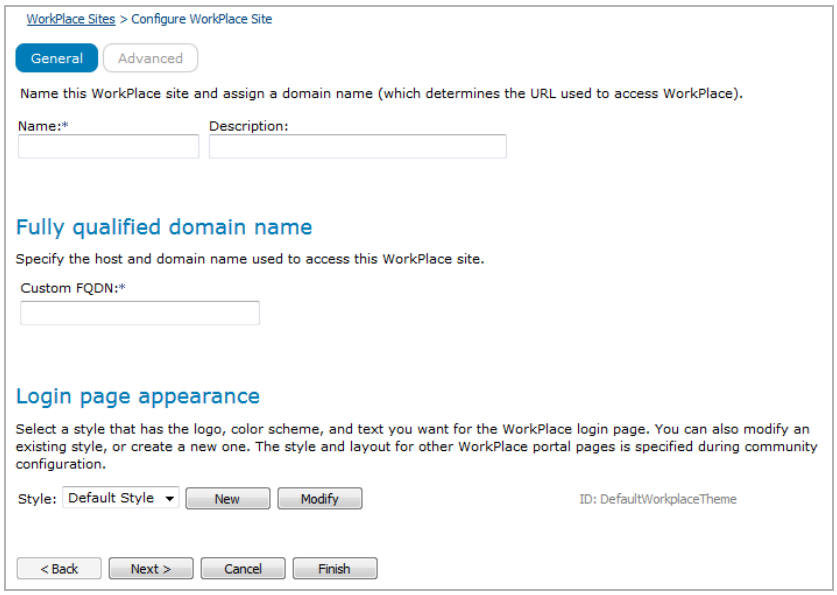
  メモ：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

いずれの場合でも、ユーザーが WorkPlace にアクセスできるよう、ユーザーに外部 FQDN を伝える必要があります。また、この FQDN をパブリック DNS に追加する必要があります。

WorkPlace サイトを追加するには、

1 [**User Access (ユーザー アクセス)**] の下のメインのナビゲーション メニューで [**WorkPlace**] をクリックし、次に [**WorkPlace Sites (WorkPlace サイト)**] タブをクリックします。

2 「**New (新規)**」をクリックします。[**Configure WorkPlace Site (WorkPlace サイトの設定)**] ページが開き、[**General (一般)**] 設定が表示されます。



3 [**Name (名前)**] フィールドに、WorkPlace サイトに付ける一意の名前を入力します。

4 (オプション) [**Description (説明)**] フィールドに、WorkPlace サイトについての分かりやすいコメントを入力します。

5 IPv4 または IPv6**ユーザ定義 FQDN** 名を入力します。デフォルトでは、AMC はすべてのサービスについてすべてのインターフェースを監視し、要求される FQDN に基づいて、要求を正しいサービスに接続します。

6 **(移行/インポートした構成のみ)** AMC に WorkPlace サイトの仮想 IP アドレスが構成されているか、AMC で CEM が使用されており、その AMC を以前のバージョンからアップグレードした場合は、追加の監視アドレスを指定できます。監視アドレスを追加するには、[**Listen on an additional IP address (追加の IP アドレスをリッスンする)**] チェック ボックスを選択して IP アドレスを入力します。

新規インストールの場合、[Listen on an additional IP address (追加の IP アドレスをリッスンする)] フィールドは表示されません。部分的インポートを行うと仮想 IP アドレスの情報は失われ、未解決の変更を適用すると、管理者は、別の IP アドレスを使用するよう構成した WorkPlace サイトや URL リソースを修正することが必要になります。その場合、[**Listen on an additional IP address (追加の IP アドレスをリッスンする)**] フィールドが、追加のアドレスの監視を有効化するチェック ボックスが選択された状態で表示されます。IP アドレスを入力するか、チェック ボックスの選択を解除します。

既存の仮想ホストを使用して移行/インポートされた構成の場合、UI セクションは表示されますが、管理者は、新しい仮想アドレスを作成できません。必要であれば、CEM を使用して、新規または移行/インポートされた構成に仮想ホスト アドレスを作成します。

部分的インポートを行うと仮想 IP アドレスの情報は失われ、未解決の変更を適用すると、管理者は、別の IP アドレスを使用するよう構成した WorkPlace サイトや URL リソースを修正することが必要になります。その場合、この UI は、追加のアドレスの監視を有効化するチェック ボックスが選択された状態で表示されます。アドレス フィールドには IP アドレスとして [(New)] が選択され、IP アドレスは未入力となっています。管理者は、IP アドレスを入力するか、チェックボックスの選択を解除できます。

証明書のホスト名または IP アドレスがこのサイトに指定した [**Custom FQDN (カスタム FQDN)**] または [**IP address (IP アドレス)**] と一致しないと、ユーザーがサイトにアクセスしたときにセキュリティ警告が表示されます。

7 WorkPlace ログイン ページ用のスタイル (ロゴ、色スキーム、およびテキストが含まれます) を選択します。他の WorkPlace ポータル ページのスタイルとレイアウトは、コミュニティの設定時に指定します。スタイルの変更や作成については、WorkPlace の外観の変更を参照してください。

8 [**Next (次へ)**] をクリックして [**Advanced (詳細)**] ページを開きます。

9 [**Realm (レルム)**] エリアで、次のいずれかのオプションを選択します。

- **このレルムを使用してログイン**: ユーザーにレルムの選択を求めるプロンプトは表示されません。指定されたレルムのメンバーのみがこの WorkPlace サイトにアクセスできます。
- **レルムの入力をユーザーに求める**: ユーザーにレルムのリストを表示し、選択するよう求めます。リストには、構成されているすべてのレルムを表示できます。また、[**All realms (すべてのレルム)**] の選択を解除して、リストに表示するレルムを選択することもできます。ログイン時にレルムを選択した後、認証済みのすべてのユーザーがこの WorkPlace サイトにアクセスできます。

10 認証後のユーザーにデフォルトの WorkPlace ホーム ページを表示させない場合は、[**Start page (開始ページ)**] エリアで [**Display this page after authentication (認証後にこのページを表示)**] を選択します。例えば、Web ベースのコンテンツ管理システム (CMS) を使用してコンテンツを投稿するユーザーがいる場合は、この設定を利用して、その投稿者にログイン後すぐに CMS のインターフェースを表示することができます。

この設定は、[**Realm (レルム)**] エリアで指定したレルムが、変換 Web アクセス、カスタム ポート マッピング Web アクセス、またはカスタム FQDN マッピング Web アクセスを排他的に提供している場合にのみ、利用できます。このテキスト ボックスに入力する URL には、自動的に `http://` という接頭辞が付けられます。安全なサイトの URL の場合は、`https://` プロトコル識別子を含める必要があります。

ユーザー向けに代替ページを指定し、ユーザーがデフォルトの WorkPlace ポータルを迂回する場合、ユーザーのセッションの有効期間は、ブラウザのウィンドウを開いている間か、セッションがタイムアウトになるまでの間となります。WorkPlace とは異なり、代替ページには [**Log out (ログアウト)**] オプションは表示されません。

11 [**Finish (完了)**] をクリックして、WorkPlace サイトの設定を保存します。

メモ：URL リソースを作成していれば、[**Start page (開始ページ)**] エリアに URL エイリアスを入力できます (ユーザーに WorkPlace で完全な URL を表示したくない場合)。例えば、URL リソースを *http://intranet.mycompany.com*、そのエイリアスを intranet と定義している場合は、ここで WorkPlace のスタート ページを intranet (または、より具体的なパス (intranet/some/path など) と指定できます。ユーザーは、認証時に `https://<appliance>/intranet` or `https://<appliance>/intranet/some/path` にリダイレクトされます。

WorkPlace の外観の変更

新しい WorkPlace サイトを作成する際に、ページのルック アンド フィールと、リソースのショートカットや他の要素 (イントラネットの参照やネットワーク エクスプローラなど) の配置を制御できます。WorkPlace の外観は、次のデザイン要素によって制御されます。これらは作成して再利用することができます。

- *WorkPlace スタイル*によって、WorkPlace で使用する色スキーム、フォント、および画像を指定します。スタイルは、ユーザー リソースを含んでいるページと、ログイン、エラー、および通知ページという、2 つのページ群に適用できます。

  WorkPlace のログイン、エラー、および通知ページにスタイルを割り当てるのは *WorkPlace サイト*の構成時ですが (詳細はWorkPlace サイトの追加を参照)、ポータル ページにスタイルを割り当てるのは*コミュニティ*の構成時 (詳細はコミュニティの作成と構成を参照) であることに注意してください。

- *WorkPlace レイアウト*は、WorkPlace のナビゲーションなどの要素、ページに表示する列の数、ユーザーに [**Intranet Address (イントラネット アドレス)**] ボックスを表示するかどうか、および表示するショートカットとその配置などを指定します。レイアウトは、WorkPlace リソース ページにのみ適用されます。

  サイトにおいて WorkPlace の外観を全面的に変える必要がある場合、管理者が Web コンテンツとスタイル シート (`.css`) の作成に習熟していれば、独自に作成したスタイルをアプライアンスにアップロードして、サイトの作成時にそのスタイルを選択して割り当てることができます。詳細については、WorkPlace ページの全面的なカスタマイズを参照してください。さらに詳細なカスタマイズ (ログイン プロセスに使用許諾契約書を挿入するなど) を行う方法については、カスタム WorkPlace テンプレートについてを参照してください。

メモ：WorkPlace のデフォルト スタイルとデフォルト レイアウトは削除できません。

トピック:

- WorkPlace スタイルの作成または編集
- WorkPlace レイアウトの作成または編集

WorkPlace スタイルの作成または編集

新しい WorkPlace スタイルを作成するには、

1. メイン ナビゲーション メニューの「**WorkPlace**」をクリックし、次に「**外観**」タブをクリックします。
2. [**Styles (スタイル)**] エリアで、新しいスタイルのベースにする既存のスタイルを選択 (チェックボックスを選択してから [**Copy (コピー)**] をクリック) するか、[**New (新規)**] をクリックします。
3. [**Name (名前)**] フィールドに、WorkPlace スタイルに付ける一意の名前を入力します。
4. (オプション) [**Description (説明)**] フィールドに、そのスタイルについての分かりやすいコメントを入力します。
5. [**Font family (フォント ファミリ)**] リストで、使用するフォントのタイプを選択します (**セリフ**または**サンセリフ**)。
6. [**Color scheme (色スキーム)**] ドロップダウン メニューで、使用する色スキームの名前をクリックします。[**Custom (ユーザ定義)**] を選択すると、WorkPlace の **Page background (ページ背景)**、**Subheadings (小見出し)**、および **Main heading (見出し)**にカスタムの色を設定できます。適切な RGB 値 (16 進数値) を入力するか、色見本をクリックして [**Please choose a color (色を選択してください)**] ダイアログで色を選択することによって、色の設定を指定します。
7. WorkPlace に表示される Secure Mobile Access ロゴを別のイメージで置き換えるには、[**Replace with (次に置き換え)**] フィールドからして、使用する `.gif` または `.jpg` ファイルを入力するか参照します。最適の結果を得るには、幅 200 ピクセル、高さ 50 ピクセル以内の画像を使用してください。

8 「**ロゴの背後にグラデーション背景を表示**」が選択されている場合、「**カラー スキーム**」のアクセント カラーが各 WorkPlace ページの一番上に、明暗のグラデーション (ページの最上部が暗い色) で表示されます。見出しは白で表示されます。

9 小型携帯端末では、デフォルトで、[**Images (画像)**] エリアで指定したロゴがサイズ変更されますが、最適の結果を得るには、40 x 100 ピクセル以内の代替画像を指定することをお勧めします。画像ファイルのパスを入力するか、[**Browse (参照)**] ボタンをクリックして使用する画像ファイルを選択します。WAP および i モード デバイスではロゴは自動的に省略されるため、この設定はこれらのデバイスでの表示には影響しません。

10 [**Title (タイトル)**] フィールドにタイトルのテキストを入力します。このテキストはページのタイトルとして表示され、またブラウザのタイトル バーに表示されます。タイトルは最長 25 文字です。

11 [**Greeting (あいさつ)**] フィールドに、紹介テキストを入力します。このテキストはタイトルの下に表示されます。このテキストは最長 250 文字です。ただし、特に小型携帯端末に表示する場合は、短いテキストにすることをお勧めします。

12 ユーザの支援をさらに進めるために、VPN で使用可能なリソースに関するより詳細な情報を提供するカスタム **ヘルプ ファイル**を指定したり、テクニカル サポートの受け方を説明したりすることもできます。[**Browse (参照)**] をクリックして、カスタムのヘルプ情報が含まれている適切な規格の HTML ファイルを指定します。カスタムのヘルプ コンテンツは、デフォルトの WorkPlace ヘルプ システムに統合されます。カスタムのヘルプ コンテンツに変更を加える場合は、ファイルをローカルで編集してから、アプライアンスに再度アップロードします。

13 [**Save (保存)**] をクリックして WorkPlace サイトの設定を保存します。[**Reset Defaults (デフォルトにリセット)**] をクリックすると工場出荷時のデフォルト設定にリセットされます。

WorkPlace レイアウトの作成または編集

新しい WorkPlace レイアウトを作成するには、

1 メイン ナビゲーション メニューの「**WorkPlace**」をクリックし、次に 「**外観**」タブをクリックします。

2 「**レイアウト**」エリアで、[**New (新規)**] をクリックします。

3 [**Name (名前)**] フィールドに、WorkPlace レイアウトにつける一意の名前を入力します。

4 (オプション) [**Description (説明)**] フィールドに、そのレイアウトについての分かりやすいコメントを入力します。

5 [**Initial content (初期コンテンツ)**] エリアで、現在の WorkPlace コンテンツのレイアウト (定義済みのショートカットおよびショートカット グループ) を選択します。または、コンテンツの初期構成の設定を選択して、後で WorkPlace リソースを追加します。ここで初期コンテンツのレイアウトを指定しても、後でページやページ コンテンツを追加、削除、再配置することによってレイアウトを変更できます。

6 「**ページ ナビゲーション**」エリアで、コンテンツで複数のページが必要になる場合に表示されるナビゲーション コントロールの種類を指定します。

7 このレイアウトが使用される際に [**Intranet Address (イントラネット アドレス)**] フィールドを表示するかどうかを指定します。ユーザーはこのボックスにリソース名 (UNC パス、URL、またはその両方) を入力して、リソースにアクセスできます。「**次へ**」を選択します。

8 [**Edit page properties (ページ プロパティの編集)**] リンクをクリックして、この WorkPlace ページの基本的なプロパティ (名前 (*ホーム*など) や簡単な説明) を変更します。

9 ページ、列、およびショートカットのコントロールを使用して、ページやコンテンツを追加したり、各ページの要素を再配置します。レイアウト内で項目を再配置したり、レイアウトから項目を削除しても、実際のリソースへの影響はありません。WorkPlace 内でのそれらの表示が変更されるだけです。

10 [**Next (次へ)**] をクリックして [**Device Preview (デバイス プレビュー)**] ページに移動します。このページを使用して、表示機能が異なる各種のデバイスでレイアウトがどのように表示されるかを確認できます。例えば、レイアウトで [**Intranet Address (イントラネット アドレス)**] フィールドを表示するよう構成していても、モバイル デバイスではこのボックスは表示できません。

WorkPlace と小型携帯端末

WorkPlace では、PDA、ポケット PC、スマートフォン、WAP 2.0 対応の携帯電話、および i モード携帯電話など、さまざまな小型携帯端末をサポートしています。このセクションでは、これらのデバイスをサポートするためのアプライアンスの構成方法について説明します。

トピック:

- WorkPlace と小型携帯端末について
- 小型携帯端末での表示用に WorkPlace を最適化する
- ブラウザ プロファイルについて
- ブラウザ プロファイルの追加
- ブラウザ プロファイルの移動

WorkPlace と小型携帯端末について

ユーザーが小型携帯端末から WorkPlace にログインすると、WorkPlace はデバイスのタイプを検出して、クライアント デバイスの機能に合わせて自動的に変換を行います。この変換により、ユーザー エクスペリエンスの一部に影響が及びます。

- **WorkPlace の機能:** 次に示す、一般的なデスクトップ ブラウザで利用可能な WorkPlace 機能の一部は、小型携帯端末では除外されます。
  - ネットワーク共有にアクセスするための**Network Explorer (ネットワーク エクスプローラ)** ページは利用できません。
  - URL や UNC パス名を入力する [**Intranet Address (イントラネット アドレス)**] ボックスは利用できません。
- WorkPlace の http および https のブックマークはサポートされます。
- SonicWall アクセス エージェント (OnDemand アクセス エージェント、EPC データ保護エージェント、およびターミナル サーバー エージェントなど) はサポートされません。
- カスタムのオンライン ヘルプ ファイルは利用できません。
- **WorkPlace のルック アンド フィール:** 標準の WorkPlace の外観 (管理者が加えたカスタマイズを含む) は、小型携帯端末での表示に最適化されるよう自動的に変更されます。

  メモ：小型携帯端末での WorkPlace の外観の構成については、小型携帯端末での表示用に WorkPlace を最適化するを参照してください。

- **利用できるリソース:** 小型携帯端末でどの WorkPlace ショートカットを表示するかを制御できます。これにより、特定のタイプのデバイスと互換性のない Web リソースを除外できます。

  例えば、Outlook Web Access のリンクは非表示にして、代わりに Outlook Mobile Access へのリンクを表示することをお勧めします。この設定は WorkPlace ショートカットの作成時に行います。詳細については、Web ショートカットの追加を参照してください。

- **End Point Control の分類:** デバイスの種類に基づいてアクセスを制限するために、特定の種類の Windows Mobile デバイス用に EPC ゾーンを作成し、アクセス制御ルールでそのゾーンを指定することができます。詳細については、ゾーンの定義を参照してください。

アプライアンスは、最も一般的な小型携帯端末を、複数のカテゴリのいずれかに分類するよう、事前に構成されています。ほとんどの導入環境ではデフォルト設定で問題ありませんが、必要に応じてこの構成を変更して、分類を変更したり、他のデバイスを認識させることができます。デバイスがどのように分類されるかについては、ブラウザ プロファイルについてを参照してください。

メモ：

- 一部の小型携帯端末ではエラー ページが表示されず、Web サーバーから、エラー内容を説明したテキストを伴わずにエラー コード (「500」エラーなど) が返されます。
- サポートされていないデバイスから WorkPlace へのログインを試行すると、エラー メッセージが表示されます。
- 小型携帯端末からアプライアンスに接続するユーザーがいる場合は、主要な CA (VeriSign など) の証明書を使用してアプライアンスを構成するか、ユーザーの使用する小型携帯端末のデバイスに CA 証明書をインポートする必要があります。多くのデバイスでは、不明な CA の証明書が提示されると接続に失敗し、いかなるエラー メッセージも表示されません。詳細については、CA 証明書を参照してください。

小型携帯端末での表示用に WorkPlace を最適化する

一般的な WorkPlace の外観 (管理者が加えたカスタマイズを含む) は、小型携帯端末での表示に最適化されるよう自動的に変更されます。変更結果はほとんどの導入環境で問題なく機能しますが、表示を改善するために、いくつかの設定を手動で変更することをお勧めします。ほとんどの設定は、WorkPlace *スタイル*の一部として構成されます。WorkPlace *レイアウト*を構成する際に、各モバイル デバイス上でページのナビゲーションや他の要素がどのように機能するかを確認できます。

小型携帯端末での表示用に WorkPlace サイトを最適化するには、

1. メイン ナビゲーション メニューの「**WorkPlace**」をクリックし、次に「**外観**」タブをクリックします。
2. [**Styles (スタイル)**] ドロップダウン メニューで、変更するスタイルを選択します。または、[**New (新規)**] をクリックしてゼロから作成します。
3. [**Images (画像)**] エリアで、WorkPlace のロゴを指定します。サイズの小さいデバイスでも表示が最適化されるよう、画像サイズは 100 x 40 ピクセル以内としてください。デフォルトでは、[**Standard logo image file**] ボックスに指定されたロゴが使用されます。別の画像を指定するには、[**Replace with (次に置き換え)**] フィールドに `.gif`、`.jpg`、または `.png` ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルを指定します。WAP および i モード デバイスでは、画像は自動的に省略されます。この設定は、これらのデバイスでの表示には影響しません。
4. 必要となる縦スクロールの量を減らすために、[**Text and Files (テキストとファイル)**] エリアの [**Display greeting on small form factor devices (あいさつを小型携帯端末に表示)**] チェック ボックスをオフにします。

5 [**Save (保存)**] または [**Finish (完了)**] をクリックして WorkPlace サイトの設定を保存します。[**Reset Defaults (デフォルトにリセット)**] をクリックすると、WorkPlace サイトの設定が工場出荷時のデフォルトにリセットされます。

メモ： UTF-8 をサポートしていないモバイル デバイス (SANYO W32SA 携帯電話など) を使用した場合、ローカライズされたコンテンツは表示の際に文字化けします。ユーザーがログインするためには、クレデンシャルを ASCII 形式で入力する必要があります。

小型携帯端末での WorkPlace のレイアウトをプレビューするには、

1 メイン ナビゲーション メニューの「**WorkPlace**」をクリックし、次に 「**外観**」タブをクリックします。

2 [**Layouts (レイアウト)**] ドロップダウン メニューで、使用する予定のレイアウトを選択するか、[**New (新規)**] をクリックして新しいレイアウトを構成します。

3 **全般**設定: レイアウトに複数のページが含まれている場合は、表示するナビゲーション コントロールの種類を指定できます。複数ページをサポートするのは、高機能のモバイル デバイス (JavaScript をサポートするブラウザを備えているデバイス) のみです。例えば、Windows Mobile Professional を搭載したポケット PC などが該当します。

4 **デバイスのプレビュー**: サイズの小さいデバイスでのコミュニティのレイアウトには、2 つの方法があります。

- アプライアンスに、サイズの小さいデバイスへ自動的に対応させることができます。例えば、[**Intranet Address (イントラネット アドレス)**] フィールド (レイアウトに含まれている場合) はモバイル デバイスでは自動的に非表示となり、指定されているロゴは縮小表示されます。
- この自動対応では不適切な結果となる場合は、モバイル デバイス専用の別のレイアウトを作成して、コミュニティの構成時にそのレイアウトを指定することができます。詳細については、WorkPlace の外観の構成を参照してください。

ブラウザ プロファイルについて

アプライアンスは、ほとんどの一般的なデスクトップ ブラウザと、多くの一般的な小型携帯端末を認識するよう、事前に構成されています。ユーザーが WorkPlace に接続すると、WorkPlace はこのプロファイル情報を使用して、デバイスを複数あるカテゴリのいずれかに分類します。これにより、WorkPlace の外観、デバイス上に表示されるショートカット、および、EPC で使用するデバイスの分類が決まります。

ブラウザ プロファイルは、Web ブラウザのユーザーエージェント文字列や HTTP ヘッダなどの、クライアントから送信されるさまざまな情報を調べることにより判別されます。分類の詳細はブラウザ プロファイルの分類の詳細のとおりです。

ブラウザ プロファイルの分類の詳細

クライアント デバイスの例	WorkPlace での分類
• Windows、Mac、または Linux	*デスクトップ (JavaScript 有効)*
• Apple iPhone	*デスクトップ (JavaScript 無効)* JavaScript が無効化されているため、アプライアンスは、どの EPC ゾーンに所属するかを判別するための情報を iPhone から取得できません。

ブラウザ プロファイルの分類の詳細

クライアント デバイスの例	WorkPlace での分類
• Windows ポケット PC • Windows Smartphone Professional • 多くの Windows CE デバイス • 多くの Palm OS デバイス	*高機能端末 (タッチ スクリーンおよび JavaScript が有効)*
• Windows Smartphone Standard	*一般的なモバイル端末 (JavaScript 有効)*
• JavaScript 非対応のスマートフォン • 一部の Palm OS デバイス	*一般的なモバイル端末 (JavaScript なし)*
• WAP 2.0 対応携帯電話 (多くの Symbian ベースの携帯電話を含む)	*WAP Phone v2.0*
• cHTML を使用する携帯電話ブラウザ (Cookie 非サポート)	*i モード携帯電話 (cHTML)*

携帯電話およびハンドヘルド デバイスの市場は急速に発展しているため、アプライアンスのデフォルト設定の変更が必要となる場合があります。例えば、自社のセールス組織に導入された新型のスマートフォンをサポートするために、アプライアンスを構成することが必要となる場合があります。また、PDA のベンダーがユーザーエージェント文字列を変更した場合には、それに対応するためにアプライアンスのデフォルト プロファイルを上書きする必要となります。ブラウザ プロファイルを定義すると、そのプロファイルが、アプライアンスに構成されている組み込みのプロファイルよりも優先されます。

AMC のブラウザ プロファイルを使用して、最新の小型携帯端末をサポートするようアプライアンスを構成できます。ブラウザ プロファイルは、特定のユーザーエージェント文字列をデバイスの種類にマップします。WorkPlace と小型携帯端末についてに記載のとおり、プロファイルはブラウザ プロファイルの機能に示す 3 つの判別に使用されます。

ブラウザ プロファイルの機能

ブラウザ プロファイルに指定されている機能	詳細情報
デバイスで WorkPlace がどのように表示されるか	WorkPlace と小型携帯端末についてを参照してください。
WorkPlace にどのリンクが表示されるか	Web ショートカットの追加を参照してください。
デバイスがどのように End Point Control ゾーンに分類されるか	アプライアンスが End Point Control でゾーンとデバイス プロファイルを使用する方法を参照してください。

アプライアンスは、一致するものが見つかるまで、リストされている順にブラウザ プロファイルを評価します。定義されているユーザーエージェント文字列に一致するものがない場合、アプライアンスは組み込みのプロファイルのリストをチェックします。どちらのリストにも一致するものがない場合、デバイスは *デスクトップ (JavaScript 有効)* と分類され、すべてのブラウザ機能が含まれます。

ブラウザ プロファイルの追加

アプライアンスは、多くの一般的な小型携帯端末を認識するよう、事前に構成されています。この情報を上書きしたり、情報を補足する目的で、WorkPlace の変換方法を指定したブラウザ プロファイルを作成できます。プロファイルは、ブラウザから送信されるユーザーエージェント文字列と、AMC に定義されているいずれかのデバイス タイプとの間のマッピングです。プロファイルを定義すると、そのプロファイルが、アプライアンスに構成されている組み込みのプロファイルよりも優先されます。

ブラウザ プロファイルを追加するには、

1 メイン ナビゲーション メニューで [**Agent Configuration (エージェント設定)**] をクリックします。

2 [**Other Agents (その他エージェント)**] エリアで、[**Web browser profiles (Web ブラウザ プロファイ)**] の下にある [**Edit (編集)**] をクリックします。[**Browser Profiles (ブラウザ プロファイ)**] ページが表示されます。

3 [**New (新規)**] をクリックし、[**User-agent string (ユーザーエージェント文字列)**] フィールドに、デバイスで使用されているユーザーエージェント文字列内の特徴的な部分を入力します。ユーザーエージェント文字列を定義する際は、一般的なワイルドカード文字の「*」および「?」を使用できます。例えば、*do** というユーザーエージェント文字列は *DoCoMo* と一致し、*MSI?* という文字列は *MSIE* のいずれかと一致します。

メモ：クライアント オペレーティング システムの制限により、Mobile Connect は、ワイルドカードを含むホスト名、URL、またはドメイン タイプのリソースを IP アドレスに変換できないため、アプライアンスにリダイレクトできません。

4 [**Device type (デバイス種別)**] ドロップダウン メニューで、ユーザーエージェント文字列で識別されたデバイスのクライアント情報に最もよく一致するエントリを選択します。デバイスの分類については、ブラウザ プロファイルについてを参照してください。

5 (オプション) [**Description (説明)**] フィールドに、そのブラウザ プロファイルについての分かりやすいコメントを入力します。

6 [**OK**] を選択します。新しいプロファイルがリストの末尾に追加されます。

7 「**Save (保存)**」を選択します。

メモ：アプライアンスは、一致するものが見つかるまで、リストされている順にブラウザ プロファイルを評価します。詳細については、ブラウザ プロファイルの移動を参照してください。

ブラウザ プロファイルの移動

ブラウザ プロファイルは、リストされている順に照合されます。アプライアンスは、一致するプロファイルを検出すると、リストの評価をストップします。必要に応じて、リスト内で 1 つまたは複数のプロファイルの順序を変更することで、特定の小型携帯端末を正しく認識させることができます。

ブラウザ プロファイルを移動するには、

1 メイン ナビゲーション メニューで [**Agent Configuration (エージェント設定)**] をクリックします。

2 [**Other Agents (その他エージェント)**] エリアで、[**Web browser profiles (Web ブラウザ プロファイ)**] の下にある [**Edit (編集)**] をクリックします。[**Browser Profiles (ブラウザ プロファイ)**] ページが表示されます。

3 移動するプロファイルのチェックボックスを選択します。

4 必要に応じて [**Move Up (上に移動)**] または [**Move Down (下に移動)**] をクリックします。ボタンをクリックするたびに、選択したプロファイルがリストの 1 つ上または下に移動します。

5 「**Save (保存)**」を選択します。

WorkPlace ページの全面的なカスタマイズ

AMC で実行できる WorkPlace のカスタマイズ (WorkPlace の一般設定の構成を参照) は WorkPlace の全般的なルック アンド フィールを変更するうえで便利ですが、一部の導入環境では十分な制御を行えないことがあります。

このセクションでは、次の 2 つのレベルのカスタマイズについて説明します。

- WorkPlace のスタイルとレイアウトは AMC で構成できます (WorkPlace の外観の変更を参照)。このカスタマイズをさらに進めて、例えば、WorkPlace ページに背景画像を使用したり、見出し部分のサイズを変更するには、既存のスタイルをダウンロードし、ローカルで編集してから、アプライアンスへ再度アップロードします。詳細については、WorkPlace スタイルのカスタマイズ: 手動での編集を参照してください。
- ログイン処理への使用契約書やエンド ユーザー ライセンス契約の追加など、さらに高度なカスタマイズが必要な場合は、WorkPlace 内の特定のページ (認証ページ、エラー ページ、通知ページなど) をカスタマイズできます。詳細については、カスタム WorkPlace テンプレートについてを参照してください。

トピック:

- WorkPlace スタイルのカスタマイズ: 手動での編集
- カスタム WorkPlace テンプレートについて
- テンプレート ファイルはどのように選択されるか
- WorkPlace テンプレートのカスタマイズ

WorkPlace スタイルのカスタマイズ: 手動での編集

WorkPlace のスタイルとレイアウトは AMC で構成できます (WorkPlace の外観の変更を参照)。Web コンテンツとスタイル シート (`.css`) の作成に習熟している場合は、このカスタマイズのレベルをさらに進めて、例えば、ログインとログオフのページを企業の標準に合わせて視覚的な一貫性を持たせたり、エラー ページ (リソースが利用不可の場合やユーザーが無効なクレデンシャルを入力した場合などに表示される) を変更してサポートやトラブルシューティングの詳細情報を加えることができます。

新しいスタイルを作成する際は、既存のスタイルをダウンロードし、ローカルで編集してから、アプライアンスに再度アップロードするという方法が最も効率的です。

WorkPlace スタイルを全面的にカスタマイズするには、

1. メイン ナビゲーション ページから、[**WorkPlace**] をクリックします。
2. [**Appearance (外観)**] ページの [**Styles (スタイル)**] ドロップダウン メニューで、ベースとして使用するスタイルを選択して、[**Download (ダウンロード)**] をクリックします。(スタイルは 1 度に 1 つのみダウンロードできます。)
3. スタイルは圧縮 (`.zip`) ファイルとしてダウンロードされます。ファイル名は、`WorkPlace_Style` の後に現在のスタイル名が続く形式となっています。
   - 新しいスタイルを作成する場合は、保存時にこの `.zip` ファイルの名前を変更してください。
   - 既存のスタイルに変更内容を上書きする場合は、現在のファイル名のままにします。

4 カスケード スタイル シート (デスクトップ デバイス用とモバイル デバイス用に 1 つずつ) と画像に編集を加えます。サンプルの WorkPlace ページとログイン HTML ページを使用して、ページ要素がどのように分類されるかを確認できます。

5 編集したファイルを `WorkPlace_Style_<スタイル名>.zip` という名前の単一の `.zip` ファイルにまとめ、WorkPlace の [**Appearance (外観)**] ページで [**Upload (アップロード)**] をクリックします。

6 [**Upload Style (スタイルのアップロード)**] ページで、変更内容を既存のスタイルにアップロードするのか、新しい WorkPlace スタイルを追加するのかを選択します。`.zip` ファイル形式でスタイルをアップロードすると、すべてのスタイル ファイルが上書きされます。

7 新しい WorkPlace スタイルをアップロードする場合は、スタイルに名前をつけます (例: *Corporate Branding*)。

8 [**Style zip file (スタイル zip ファイル)**] フィールドに、編集または作成した `.zip` ファイルの名前を入力します。例えば、新しいスタイルの名前が *Corporate Branding* の場合、対応するファイルの名前は *WorkPlace_Style_Corporate_Branding.zip* とする必要があります。

9 [**Upload (アップロード)**] をクリックして、スタイル関連のファイルをアプライアンスに転送します。

カスタム WorkPlace テンプレートについて

WorkPlace の外観やログイン処理に含まれるステップの全面的なカスタマイズが必要となる場合もあります。例えば、

- WorkPlace の代わりに既存の企業ポータル (そのポータル アプリケーションをリソースとして定義済み) を使用する必要がある場合。この場合は、ログイン、ログオフ、通知、およびエラーの各ページを、既存のポータルのルック アンド フィールに合わせてカスタマイズします。
- ビジネス パートナーに特定のアプリケーション (リソースとして定義済み) へのアクセスを提供する必要がある場合。この場合は、ログイン、ログオフ、通知、およびエラーの各ページを、アプリケーションのルック アンド フィールに合わせてカスタマイズします。

カスタマイズ可能なテンプレートは、3 つのカテゴリに分かれます。カスタム WorkPlace テンプレートの種別を参照してください。ある 1 つのカテゴリのテンプレートを変更する場合、一貫性を保つためには、他のカテゴリのテンプレートも変更することが必要となります。

カスタム WorkPlace テンプレートの種別

テンプレートのタイプ	説明
認証	ユーザーのクレデンシャルの収集 (レルムの選択や、ユーザー名、パスワード、またはパスコードの入力など) に使用されるページです。 これらのテンプレートを使用して、ユーザーに、ネットワークへのログイン方法についての情報を画面上で提供します。
エラー	エラーの発生時 (無効なユーザー入力 (認証拒否メッセージやログインの失敗)、またはアプライアンス内でのエラーなど) に表示されるページです。 これらのテンプレートを使用して、ユーザーにサポート情報 (管理者の連絡先やユーザー ガイドの場所など) を提供できます。
通知	システムを利用するうえで必要な基本情報 (ログアウト ページ (正常にログアウトしたことを示す) を含む) をユーザーに提供するページや、認証モジュールからのメッセージ (パスワードの期限切れの警告など) が表示されるページです。

これらのページでレイアウトのデザインを変更したり、画像やテキストを追加することは可能ですが、既存の要素を変更または削除することはできません。例えば、認証ページで [**Login (ログイン)**] ボタンの名前を変更することはできません。これらの要素は WorkPlace によって動的に生成されます。

ログイン後にユーザーに表示される WorkPlace ページは、手動ではカスタマイズできません。これらのページは AMC から制御されます。

テンプレート ファイルはどのように選択されるか

テンプレートのカスタマイズは、全体的に行うことも、また、WorkPlace サイトごとに行うこともできます。例えば、単一のデザインを使用するようグローバル テンプレートをカスタマイズし、そのうえで、サイトごとにテンプレートを変更することによって、サイト ベースでデザインを上書きできます。

ユーザーが WorkPlace サイトに接続すると、アプライアンスはまず、最も限定的なテンプレートを探します。該当するものが見つからない場合、アプライアンスはそのカテゴリ (認証、エラー、または通知) 向けの汎用テンプレートをチェックします。どちらも見つからない場合は、デフォルトの WorkPlace テンプレート (AMC の制御下にあるもの) が使用されます。

以下の表に、フルスクリーンのデバイス (デスクトップおよびラップトップ) で利用可能なテンプレートと、対応するファイル名を示します。小型携帯端末向けのファイルには、次のようにファイル名に接頭辞が付きます。

- スマートフォンおよび PDA デバイスの場合は、ファイル名に `compact-` という接頭辞が付きます。
- WAP デバイスの場合は、ファイル名に `micro-` という接頭辞が付きます。

例えば、レルムの選択時にユーザーに表示されるページをカスタマイズするには、`realm-select.tmpl` を編集します。サイズの小さなデバイス向けのこれに相当するページは `compact-realm-select.tmpl` (スマートフォンおよび PDA 向け) および `micro-realm-select.tmpl` (WAP デバイス向け) になります。

認証

テンプレート ファイル: 認証

説明	ファイル名
ユーザーがレルムを選択	*realm-select.tmpl*
ユーザーがログイン クレデンシャルを入力	*authentication-request.tmpl*

エラー

テンプレート ファイル: エラー

説明	ファイル名
レルムの選択に失敗	*realm-error.tmpl*
入力されたクレデンシャルが無効	*authentication-error.tmpl*
リソースへのアクセスが拒否された	*authorization-error.tmpl*
アプライアンスのライセンス許容数を超過	*licensing-error.tmpl*
EPC エラー	*epc-error.tmpl*

状況

テンプレート ファイル: 状況

説明	ファイル名
認証の通知 (パスワードの期限切れなど)	*authentication-status.tmpl*
ログオフ完了ページ	*logoff-status.tmpl*
EPC のログオフ完了ページ	*epc-logoff.tmpl*

汎用

テンプレート ファイル: 汎用

説明	ファイル名
EPC ダウンロード ページ	*epc-launch.tmpl*
ユーザーがログイン クレデンシャルを入力	*authentication.tmpl*
一般的なエラー	*error.tmpl*
一般的なステータス	*status.tmpl*
一般的なページ (他の特定のテンプレートが見つからなかった場合に適用)	*custom.tmpl*

メモ：デフォルトの WorkPlace テンプレート ファイル (`extraweb.tmpl`、`compact-extraweb.tmpl`、および `micro-extraweb.tmpl`) は、編集しないでください。変更した内容は、次回 AMC で WorkPlace をカスタマイズする際に上書きされます。

WorkPlace テンプレートのカスタマイズ

WorkPlace の外観は、複数のテンプレートを使用して制御されます。テンプレートをカスタマイズするには、一般的な Web デザイン ツールやテキスト エディタを使用して HTML ファイル (小型携帯端末の場合は `XHTML` や `cHTML` ファイル) を作成します。

カスタマイズに画像が含まれる場合は、画像を次のフォルダにアップロードします。

```
/usr/local/extranet/htdocs/__extraweb__/images
```

`images` ディレクトリがまだない場合は、次のコマンドを実行することで作成できます。

```
mkdir -p /usr/local/extranet/htdocs/__extraweb__/images
```

使用する必要のあるファイル名については、テンプレート ファイルはどのように選択されるかを参照してください。小型携帯端末の場合は、次のように接頭辞が追加されます。

- スマートフォンおよび PDA デバイスの場合は、ファイル名に `compact-` という接頭辞が付きます。
- WAP デバイスの場合は、ファイル名に `micro-` という接頭辞が付きます。

デスクトップ デバイス向けの WorkPlace テンプレートをカスタマイズするには、

1 必要なレイアウトを含んだ HTML ファイルを作成し、WorkPlace 固有のタグを次のように追加します。

- BODY タグ内に、次のような「EXTRAWEB」という語を含んだ HTML コメント タグを追加します。

  ```
  <!-- EXTRAWEB -->
  ```

  このタグは必須です。このタグにより、アプライアンスによって動的に生成されるコンテンツの配置場所が決定されます。このタグがないと、ユーザーは WorkPlace にログインしようとしても、認証プロセスの最初へと繰り返し戻されます。
- 次のように、外部 JavaScript ファイルへの参照を追加します。

  ```
  <script language="javascript"
  src="/__extraweb__/template.js"></script>
  ```
- テンプレートに WorkPlace のコンテンツ (AMC で構成したカスタムのロゴや .css ファイルを含む) を表示するために、HTML のコードを変更してパス /__extraweb__/images/ への参照を追加します。例えば、

  ```
  <img src="/__extraweb__/images/mylogo.gif">
  ```

2 適切なファイル名を付け、ファイル拡張子に .tmpl を使用してファイルを保存します。

小型携帯端末向けの WorkPlace テンプレートをカスタマイズするには、

1 必要なレイアウトを含んだファイルを XHTML (スマートフォンまたは PDA 向け) または cHTML (WAP デバイス向け) 形式で作成し、WorkPlace 固有のタグを追加します。

- BODY タグ内に、次のような「EXTRAWEB」 という語を含んだコメント タグを追加します。

  ```
  <!-- EXTRAWEB -->
  ```

  このタグは必須です。このタグにより、アプライアンスによって動的に生成されるコンテンツの配置場所が決定されます。このタグがないと、ユーザーは WorkPlace にログインしようとしても、認証プロセスの最初へと繰り返し戻されます。
- テンプレートに WorkPlace のコンテンツ (AMC で構成したカスタムのロゴや .css ファイルを含む) を表示するために、コードを変更してパス /__extraweb__/images/ への参照を追加します。例えば、

  ```
  <img src="/__extraweb__/images/mylogo.gif">
  ```

2 適切なファイル名を付け、ファイル拡張子に .tmpl を使用してファイルを保存します。

ユーザーに WorkPlace へのアクセスを提供する

WorkPlace は Web アプリケーションであるため、ユーザーは一般的な Web ブラウザを使用してアクセスできます。自社のネットワーク上でホストされている Web ページやポータルに WorkPlace のリンクを含めることもできます。

WorkPlace へのアクセスに使用する URL を、ユーザーに伝える必要があります。ユーザーには、デフォルトの WorkPlace URL のほか、カスタマイズした WorkPlace サイトの URL を伝えることもできます。WorkPlace サイトのタイプを参照してください。

WorkPlace サイトのタイプ

WorkPlace サイトのタイプ	URL	説明
デフォルトの WorkPlace サイト	`https://<server_name>`	*<server_name>* は、アプライアンスの SSL 証明書に含まれている完全修飾ドメイン名 (FQDN) です。詳細については、証明書を参照してください。
カスタム WorkPlace サイト	`http://<custom_fqdn>`	*<custom_fqdn>* は、WorkPlace サイトに関連付けられている外部 FQDN です。詳細については、WorkPlace サイトを参照してください。

自社のネットワーク上でホストされている Web ページやポータルからユーザーが WorkPlace にアクセスする場合は、ユーザー アカウントのセキュリティ保護のために、[**Log out (ログアウト)**] ボタンを用意することをお勧めします。これを行うには、ユーザーに次の WorkPlace サイトの URL を提供します。

```
https://<server_name>/__extraweb__logoff
```

<server_name> はアプライアンスの SSL 証明書に含まれている実際の FQDN です。

End Point Control とユーザー エクスペリエンス

Secure Mobile Access End Point Control コンポーネントが有効化されている場合、WorkPlace のログイン処理にいくつかのステップが追加されます。追加されるステップは、Cache Cleaner が使用されているかどうかに応じて変わります。詳細については、End Point Control についてを参照してください。

Cache Cleaner の仕組み

Cache Cleaner を使用している場合、一般的な WorkPlace セッションは次のようになります。

1. Web ブラウザで、ユーザーが適切な WorkPlace の URL を入力します。
2. ユーザーが WorkPlace にログインします。
3. ユーザーは、表示される Secure Mobile Access セキュリティ警告を受け入れる必要があります。Cache Cleaner アイコンがタスクバー通知エリアに表示されます。
4. 必要に応じて、ユーザーがネットワーク リソースにアクセスします。
5. ユーザーが Cache Cleaner セッションを終了する際、Cache Cleaner によって、セッションに関連付けられているすべてのデータが削除されます。ログアウト時に、すべてのブラウザ ウィンドウが Cache Cleaner によって閉じられます。ログアウト時に、すべてのブラウザ ウィンドウが閉じられることを警告するダイアログが表示されます。

メモ：Cache Cleaner によってログアウト時にすべてのブラウザ ウィンドウが閉じられるほか、Cache Cleaner の起動時に他のブラウザ ウィンドウを閉じるよう構成している場合には、ユーザーに対して注意を促しておく必要があります。例えば、ユーザーがフォームを入力中の場合、ブラウザ ウィンドウが閉じられた時点で未送信の内容はすべて失われます。

10

ユーザー アクセス コンポーネントおよびサービス

ユーザー アクセス コンポーネントおよびサービスについて

SMA アプライアンスには、ネットワーク上のリソースに対するユーザー アクセスを可能にするコンポーネントが含まれています。このセクションでは、各ユーザー アクセス コンポーネントと、それらを制御するサービスについて説明します。

ユーザー アクセス コンポーネントの多くは、WorkPlace ポータルからプロビジョニングまたはアクティブ化が行われます。WorkPlace の詳細については、WorkPlace ポータルを参照してください。

ユーザー アクセス エージェント

ユーザー アクセス エージェントは、ユーザーの所属するコミュニティに基づいてクライアント デバイスに展開されます。ほとんどのエージェントは、ユーザーがブラウザを使用して WorkPlace ポータルにログインする際に自動的に展開されます。また、これらの 2 つのアクセス エージェントのインストール パッケージは、ネットワーク上のファイル共有からダウンロードできるように用意することも、Microsoft Systems Management Server (SMS) や IBM Tivoli などのアプリケーションを介して展開することもできます。詳細については、コミュニティに対するアクセス方式の選択を参照してください。

ユーザーがブラウザを使用してログインする際にアクセス エージェントを自動的に展開する場合、アクセス エージェントの展開とアクティブ化はいずれも初回アクセス時に実行されます。この方式では通常、ユーザーが Secure Endpoint Manager (SEM) のダウンロードを受け入れる必要があります。SEM によって、アクセス エージェントのインストールやその後のアクセス エージェントの更新が管理されます。2 回目以降の WorkPlace ポータルへのアクセスで、同じクライアント デバイスから同じブラウザを使用すると、アクセス エージェントはユーザーの操作なしで自動的にアクティブ化され

ます。詳細については、クライアントおよびエージェント プロビジョニング (Windows)を参照してください。

アクセス エージェントの比較では、アクセス エージェントの機能を比較し、その要件を示しています。他のシステム要件については、クライアント コンポーネントを参照してください。

アクセス エージェントの比較

	ネットワーク トンネル アクセス (IP プロトコル)		プロキシ アクセス (TCP プロトコル)	Web アクセス (HTTP プロトコル)	
	OnDemand Tunnel エージェント	Connect Tunnel クライアント	OnDemand マップ モード	Web プロキシ エージェント	変換、カスタム ポート マッピング、カスタム FQDN マッピング
アプリケーション サポート					
TCP ベースのクライアント/サーバー アプリケーション	x	x	x		
TCP または UDP ベースのクライアント/サーバー アプリケーション	x	x			
URL および Web アプリケーション	x	x	x	x	x
Windows ネットワーク					
Web ベースのファイル アクセス	x			x	x
ネイティブ Windows ファイル アクセス ([ネットワーク コンピュータ])	x	x			
マッピングされたネットワーク ドライブ	x	x			
Windows ドメイン ログオン		x			
接続タイプ					
順方向接続	x	x	x	x	x
逆方向接続 (FTP や SMS など)	x	x			
相互接続 (VoIP など)	x	x			
オペレーティング システム					
Windows	x	x	x	x	x
Linux または Macintosh	x	x	x		x
Windows Mobile					x
クライアント/エージェントのインストールで必要な管理者権限	x	x			
配備					
WorkPlace からの自動起動	x		x	x	x

アクセス エージェントの比較

	ネットワーク トンネル アクセス (IP プロトコル)		プロキシ アクセス (TCP プロトコル)	Web アクセス (HTTP プロトコル)	
	OnDemand Tunnel エージェント	Connect Tunnel クライアント	OnDemand マップ モード	Web プロキシ エージェント	変換、カスタム ポート マッピング、カスタム FQDN マッピング
WorkPlace からのプロビジョニング	x	x	1	x	
WorkPlace 以外からのプロビジョニング		x			

1. ポート マップ モードでは ActiveX または Java が必要です。管理者権限がなく ActiveX を実行できないユーザーの場合は、Java Runtime Environment (JRE) が使用されます。

トピック:

- クライアントおよびエージェント プロビジョニング (Windows)
- WorkPlace
- Tunnel クライアント
- Web アクセス

クライアントおよびエージェント プロビジョニング (Windows)

Secure Endpoint Manager は、Windows ユーザーが WorkPlace にログインするとき、信頼できる方法で、EPC とアクセス エージェントをプロビジョニングできるようにするコンポーネントです。このコンポーネントでは、エージェントを必要とするアプリケーションの互換性が向上する上、EPC の信頼性が向上し、ほとんどのクライアント アップデートで管理者権限が不要になります。プロビジョニングの際に問題が発生した場合は、AMC で表示できるクライアント インストール ログ (ユーザー名で識別) にエラーが自動的に記録されます。

Secure Endpoint Manager のインストールは 1 段階の手順で行います。その際、ユーザーに管理者権限は不要です。インストール時を除くと、ユーザーが Access Manager を (一時的に) 意識するのは、アクセス エージェントまたは Access Manager 自体を更新する必要がある場合に限られます。Secure Endpoint Manager のインストールは必須ではありませんが、Secure Endpoint Manager をインストールしていないユーザーは WorkPlace でリソースにアクセスする際 Web アクセスのみが認められ、コミュニティの構成方法によってはログアウトを強要されることもあります。

トピック:

- Secure Endpoint Manager
- Secure Endpoint Manager のインストール

- Secure Endpoint Manager ソフトウェアの更新ポリシーの有効化
- プロビジョニングとパーソナル ファイアウォール
- クライアント インストール ログ

Secure Endpoint Manager

Secure Endpoint Manager (SEM) は、クライアント デバイスにインストールされるソフトウェア コンポーネントです。Webブラウザから SMA 製品にアクセスするとインストールされます。SEM を使用すると、クライアント デバイス上のユーザーは SMA アプライアンスにログインし、Web ブラウザを使用してタスクを実行できます。

SEM は、OnDemand Tunnel、End Point Control、OnDemand マップ モード、Native Access Module など、いくつかのクライアント コンポーネントのインストールとアクティブ化を提供します。

SMA は、Secure Endpoint Manager (SEM)、および Native Access Module、End Point Control、OnDemand Tunnel、Web プロキシ、OnDemand マップ モードなどの関連サブコンポーネントの更新ポリシーを提供します。

SEM のインストールおよびソフトウェア更新ポリシーは、Windows、Mac OSX、および Linux クライアント オペレーティング システムでサポートされています。

サーバー側ファームウェアが更新された後、SMA 管理者は特定のユーザー グループとコミュニティを個別に制御および更新できます。何千ものクライアント デバイスを同時に更新する必要はありません。

SEM ソフトウェアの更新は、Web アクセスまたはトンネル アクセス方法を使用するか、または両方の方法を使用してトリガーできます。

Secure Endpoint Manager のインストール

ユーザーが WorkPlace にログインするとき、ネットワーク リソースに対するアクセスを許可する前に、Secure Mobile Access エージェントまたはクライアントをインストールするようユーザーに要求できます。これは推奨設定です。このように設定すると、エージェントを必要とするアプリケーションとの互換性が向上するため、ユーザーが広範囲にアクセスできるようになり、ヘルプ デスクで呼び出される回数も減ります

この設定が有効になっている場合、ユーザーが WorkPlace にログインする際に、次のような選択項目が表示されるようになります。

- **インストール:** Secure Endpoint Manager がユーザーのコンピュータにインストールされます。ユーザーはこれを 1 回だけ行う必要があります。
- **ログアウト**: ユーザーのセッションが終了します。

エージェントまたはクライアントが*必要ない*コミュニティを構成する場合、ユーザーがログインするとき、次のような選択項目が表示されます。

インストール: Secure Endpoint Manager がユーザーのコンピュータにインストールされます。ユーザーはこれを 1 回だけ行う必要があります。

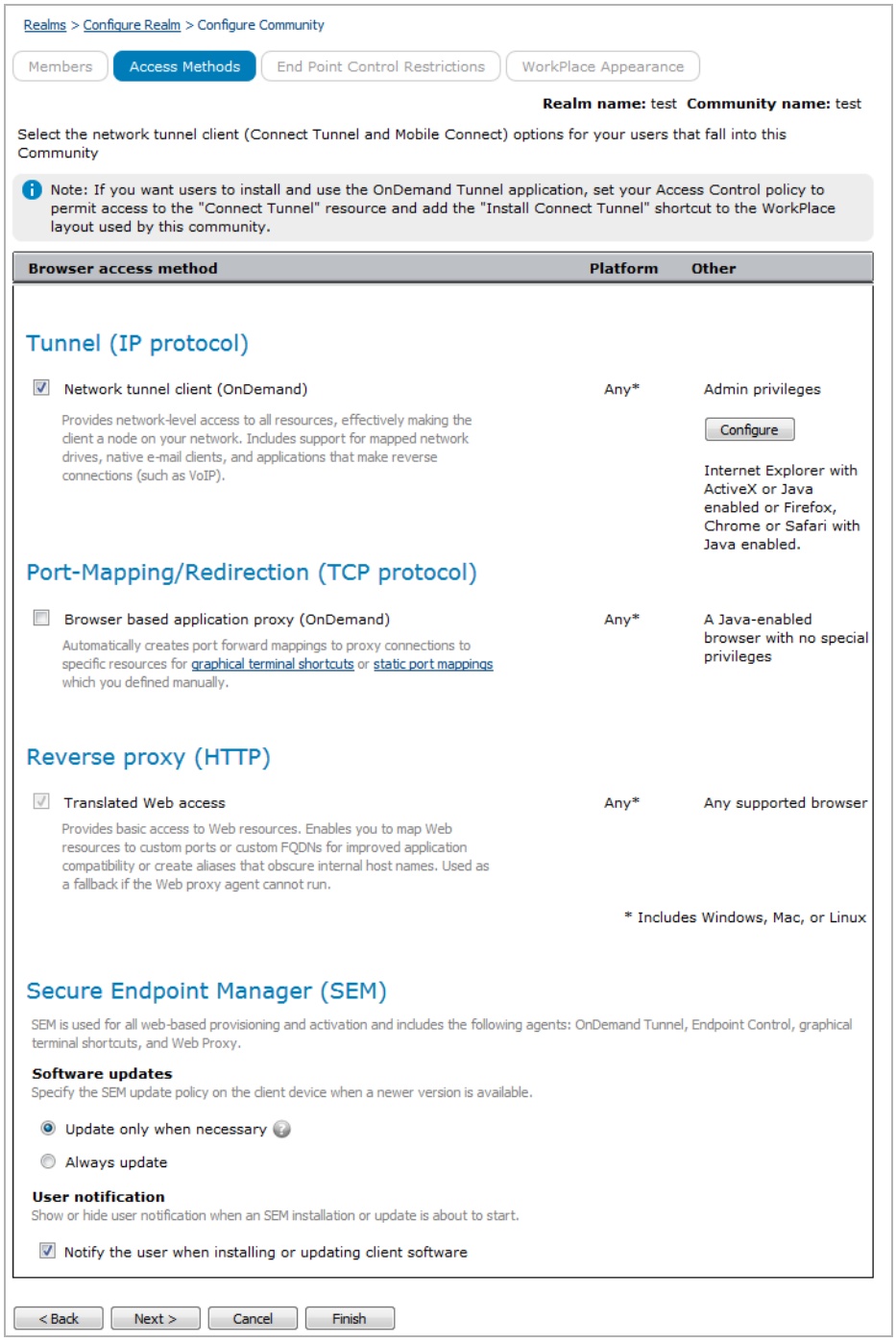
> △ **注意：このシナリオ (EPC が有効であることが前提) では、ユーザーは、コミュニティがどのように構成されているかによって、デフォルト ゾーンまたは隔離ゾーンに入れられます。隔離ゾーンは、場合によっては制約が多すぎ、デフォルト ゾーンは他の多くのタイプのユーザーに対応する必要があります。エージェントを必要としないユーザー向けに、固有の Web 専用ゾーンを作成することもできます。この種のゾーンを設定する方法については、シナリオ 3: キオスク端末から従業員が接続する場合を参照してください。**

Vista を実行するコンピュータでの Secure Endpoint Manager のインストール

ユーザーが Microsoft Vista オペレーティング システムを実行するコンピュータ上で初めて Secure Endpoint Manager をインストールする場合は、古いバージョンの Windows のユーザーには表示されない追加の同意を求めるダイアログが表示されます。ユーザーは画面の指示に従って、[**Do not show me the warning for this program again (このプログラムでは警告を再度表示しない)**] を選択し、[**Allow (許可)**] をクリックしなければなりません。

Secure Endpoint Manager ソフトウェアの更新ポリシーの有効化

Secure Endpoint Manager (SEM) のソフトウェア更新ポリシーは、コミュニティ レベルで有効になっています。



450

Secure Endpoint Manager の自動ソフトウェア更新ポリシーを有効にするには

1 AMC にログインします。

2 [**Realms (レルム)**] > [*{お使いのレルム}*] > [**Communities (コミュニティ)**] > [*{お使いのコミュニティ}*] > [**Access Methods (アクセス方法)**] ページ**にアクセスします。**Secure Endpoint Manager (SEM) パネルがページの下部にあります。

SEM ソフトウェア更新ポリシーには、次の 3 つのオプションを設定できます。

- **Update only when necessary (必要な場合にのみ更新)** - クライアント デバイス上で、SEM が必要かどうかに応じて以下の基準に基づいて SEM を更新する場合は、このオプションを選択します。次の基準によって更新がトリガーされます。
  - 11.4 以前のクライアント バージョンで個人機器認証が有効になっていない場合バージョン 12.X.X を実行しているクライアントには、更新を求めるプロンプトは表示されません。
  - 11.4 以前のクライアント バージョンで個人機器認証が有効になっている場合

  [**Update only when necessary (必要な場合にのみ更新)**] オプションを選択すると、**システム**が更新を**要求**するとき、または管理者が更新を要求するときはいつでも更新とインストールが実行されます。
- **Always update (常に更新)** - クライアント デバイス上で SEM を常に最新の状態に保つには、このオプションを選択します。これには、修正プログラム、メンテナンス、およびメジャー リリースの相違点 (更新をトリガーするすべての相違点) が含まれます。

  [**Always Update (常に更新)**] オプションが選択されている場合、ユーザーがログインすると、SEM を更新するかログアウトするかを選択するよう求められます。
- **Notify user (ユーザーに通知)** - インストールまたは更新中に SEM に関する通知をユーザーに送信する場合は、[**Notify the user when installing or updating client software (クライアント ソフトウェアのインストールまたは更新時にユーザーに通知)**] オプションを選択します。これは AMC 管理者によって制御され、SEM のインストールと更新の両方に適用されます。

  WorkPlace にアクセスできないユーザーが通知を受け取らないのは、AMC 管理者が通知を有効にしても、ユーザーが [**Logout (ログアウト)**] をクリックしてオプトアウトした場合のみです。

  SEM が必要な場合は、アクセス エージェントまたは EPC のいずれかをプロビジョニングする必要があります。そうしないと、SEM のインストールまたは更新が失敗します。

SEM コンポーネントの自動インストール

SEM およびそのサブコンポーネントがデバイスに存在しない場合は、SEM ソフトウェア更新ポリシーで選択されているオプションに関係なく、更新プロセス中にインストールされます。SEM およびそのサブコンポーネントが適切にインストールされていなければ、WorkPlace リソースへのアクセスは保証されません。

- SEM が**インストールされていない**場合、SEM コンポーネントの**インストールの受け入れ**を求められます。
  - [**Yes (はい)**] を選択すると、SEM がインストールされます。
    - SEM のインストールが**成功**した場合は、[**Land on WorkPlace (WorkPlace にアクセス)**] に進むことができます。
    - SEM のインストールが**失敗**した場合は、**ログアウト**されます。
  - [**No (いいえ)**] を選択すると、**ログアウト**されます。

プロビジョニングとパーソナル ファイアウォール

サードパーティ製のファイアウォール製品には、(ポートやプロトコルに加え) プロセスによってアウトバンド接続を制限するものがあります。これらのファイアウォールでは、エージェントや EPC コンポーネントのプロビジョニングの際に、Secure Endpoint Manager についてのセキュリティ警告ダイアログが表示されることがあります。ほとんどの場合、ユーザーはアウトバンド接続を「ブロックしない」または「許可」するよう求められます。

また、Trend Micro 製品のように、権利に制約があるユーザーが、ファイアウォール設定を上書きするのを認めないファイアウォールもあります。ユーザーに限定されたアクセス権限しか与えていない企業システムの場合、ユーザーがこのようなセキュリティ ダイアログ プロンプトに応答しなくていいようにするため、Secure Mobile Access VPN を展開する前にファイアウォール設定を更新することもできます。詳細については、エージェントでのパーソナル ファイアウォールの使用を参照してください。

クライアント インストール ログ

Windows 搭載のコンピュータへクライアントまたはエージェントをインストールしているときに問題が起こった場合、ユーザーのローカル コンピュータのクライアント インストール ログにエラーが記録されます。これらのログは、アプライアンスに自動的にアップロードされ、ユーザーに Secure Endpoint Manager がインストールされている場合は、AMC に表示されます。詳細については、クライアント インストール ログ (Windows) を参照してください。

WorkPlace

WorkPlace は、Web ベースのポータルで、Web プロキシ サービスで保護された Web リソースに対するアクセスを、動的にパーソナライズできます。ユーザーが WorkPlace にログインするとホーム ページが現れ、管理者が定義したショートカットのリストが表示されます。これらのショートカットは、ユーザーがアクセス権限を持つ、Web ベースのファイル共有、Windows ベースのアプリケーション、ターミナル サーバー リソースなどにリンクしています。

すべての Secure Mobile Access ユーザー アクセス コンポーネントは、WorkPlace ポータルを介してプロビジョニングまたはアクティブ化が行われます。WorkPlace には、あらゆる一般的な Web ブラウザからアクセスできます。詳細については、WorkPlace ポータルを参照してください。

ネットワーク エクスプローラ

ネットワーク エクスプローラは、WorkPlace で使用する Web ベースのユーザー インターフェースです。ユーザーにアクセス権限がある場合、これを使用することで、(Windows を搭載していないコンピュータからでも) 共有されている Windows ファイル システム リソースにアクセスできます。これらのリソースには、ドメイン、サーバー、コンピュータ、ワークグループ、フォルダ、ファイルなどが含まれます。

ネットワーク エクスプローラは、オプションのコンポーネントであり、ポリシーで制御できるほか、完全に無効にすることもできます。WorkPlace がサポートする任意のブラウザがサポートされています。詳細については、WorkPlace ポータルを参照してください。

Tunnel クライアント

Secure Mobile Access トンネル クライアントは、TCP および UDP トラフィック、双方向トラフィック (リモート ヘルプ デスク アプリケーションなど)、相互接続 (VoIP アプリケーションなど)、逆方向接続 (SMS など) についてセキュアなアクセスを提供します。トンネル クライアントはいずれも、あらゆるリソースに対してネットワーク レベルのアクセスを提供することで、ユーザーのコンピュータを効率的にネットワーク上のノードにします。

- OnDemand Tunnel エージェントは、Web 起動されるブラウザベースのエージェントです。
- Connect Tunnel クライアントは、Web インストール型クライアントです。トンネル クライアントは、AMC からネットワーク トンネル サービスを使用して管理されます。ネットワーク トンネル クライアントから TCP/IP 接続を管理するよう、このサービスを構成する場合、クライアントに IP アドレスを割り当てるための IP アドレス プールを設定する必要があります。

トピック:

- OnDemand Tunnel エージェント
- Connect Tunnel クライアント

OnDemand Tunnel エージェント

OnDemand Tunnel エージェントを使用すると、Web ブラウザを使用して、ネットワーク トンネル サービスで保護されたリソースに対し、完全なネットワークおよびアプリケーション アクセスが可能になります。OnDemand Tunnel エージェントは、Connect Tunnel クライアントと同様、広範なアプリケーションおよびプロトコル アクセスを提供する軽量なエージェントですが、WorkPlace ポータルに統合されており、ユーザーが WorkPlace にログインするたびに自動的に起動します。

OnDemand Tunnel エージェントは Windows、Linux、Macintosh でサポートされており、ActiveX または Java を有効にした Internet Explorer か、Java Runtime Environment (JRE) がインストールされた Mozilla Firefox または Safari が必要になります。

Connect Tunnel クライアント

Connect Tunnel クライアントは、ネットワーク トンネル サービスで保護されたリソースに対して、フル アクセスできるようにします。また、TCP を使用するアプリケーションや、VoIP や ICMP といった非 TCP プロトコルを使用するアプリケーションなど、あらゆる種類のアプリケーションにもアクセスできるようになります。また、Connect Tunnel は、トンネル分割制御、細かいアクセス制御、プロキシ検出、認証などの機能も備えています。

Connect Tunnel クライアントは、さまざまな方法で展開できます (詳細については、クライアント インストール パッケージを参照してください)。

- WorkPlace 内で、ユーザーにクライアントをダウンロードしてインストールするためのショートカットを提供します。このリンクは *Connect Tunnel* リソースをポイントします (組み込みリソースを参照)。
- ユーザーが WorkPlace にログインするのを望まない場合、ユーザーにネットワーク上 (Web サーバー、FTP サーバー、ファイル サーバーなど) から Connect Tunnel クライアント コンポーネントをダウンロードしてインストールできるようにすることもできます。
- SMS や Tivoli などのアプリケーションを使用して、インストール パッケージを配布することもできます。

- サード パーティ製のディスク イメージ コピー ユーティリティ (Norton Ghost など) を使用して、Connect Tunnel インストールのマスター イメージを作成し、それをユーザーのシステムにコピーするという方法もあります。

Connect Tunnel クライアントは、Windows、Linux、Macintosh オペレーティング システムでサポートされていますが、Connect Tunnel クライアントをインストールするにはユーザーに管理者権限が必要です。Connect Tunnel のすべての構成と管理は AMC で実行します。

Connect Tunnel クライアントでは「`ngdial`」などのコマンドライン ユーティリティをサポートしており、標準のグラフィカル ユーザー インターフェースを使用せずに、クライアントの通常実行時の動作を変更できるほか、トラブルシューティングおよび診断タスクを実行できます。詳細については、Connect Tunnel へのコマンドラインでのアクセス (NGDIAL を使用) を参照してください。

Connect Tunnel がアクティブになっていると、システムのタスクバーに **Connect Tunnel** アイコンが表示されます。

Windows バージョンの Connect Tunnel クライアント ソフトウェアでは、新バージョンが利用可能となった場合にユーザーのコンピュータで自動的に更新されるよう構成することもできます。詳細については、Windows Tunnel クライアントの自動クライアント更新を参照してください。

メモ： Windows Vista オペレーティング システムを搭載したコンピュータにゲストとしてログインした場合、Connect Tunnel を実行できません。ゲスト アカウントは、そのコンピュータまたはドメインに永続的なアカウントを持たないユーザー用であり、個人ファイルへのアクセスを認めないままコンピュータを使用できるようにするためのものです。

Quest Desktop Workspace のサポート

Moka5 Suite は、Type-2 ハイパーバイザーでゲストとして実行される LivePC というレイヤード仮想デスクトップ イメージの作成と管理に使用される、エンタープライズ デスクトップ管理プラットフォームです。

SonicWall は、Moka5 Creator を使用して作成された仮想 Windows OS イメージにあらかじめインストールされた SMA VPN クライアント (Windows) を提供します。

Windows SMA Connect Tunnel クライアントは、Moka5 統合ガイドで指定されている SMA Connect Tunnel クライアント (Windows) に変更を加えることで、Moka5 Creator と統合できます。

SMA Connect Tunnel クライアントは、Quest KACE K1000 管理アプライアンスで機能します。

Web アクセス

このセクションでは、Web プロキシ エージェントの概要と、クライアントを使用しない Web アクセス方法 (変換 Web アクセス、カスタム ポート マッピング Web アクセス、およびカスタム FQDN マッピング Web アクセス) の概要を説明します。また、Exchange ActiveSync Web アクセスについて説明するセクションも含まれています。

トピック:

- Web プロキシ エージェント
- 変換 ActiveSync Web アクセス
- カスタム ポート マッピング Web アクセス
- カスタム FQDN マッピング Web アクセス
- カスタム ポート マッピングまたはカスタム FQDN マッピング Web アクセスに関する注意事項

- SharePoint でのシームレスな編集
- Exchange ActiveSync Web アクセス
- SAN 証明書による ActiveSync リソース設定
- Outlook Anywhere Web アクセス

Web プロキシ エージェント

Web プロキシ エージェントを使用すると、WorkPlace ポータルから、Windows ネットワーク共有へのアクセスだけでなく、Web ベースのアプリケーション、Web ポータル、Web サーバーなど、あらゆる Web リソースにもアクセスできるようになります。Web プロキシ エージェントでは、変換 Web アクセスが間に入ることで互換性は向上しますが、Web プロキシ エージェントをプロビジョニングすると、場合によっては、ユーザーが WorkPlace に最初にログインするときに若干余分の時間がかかるようになります。Web プロキシ エージェントを使用するには、ActiveX が有効になっている Internet Explorer が必要です。

メモ：Web プロキシ エージェントは廃止される予定です。

Web プロキシ エージェントがない場合、管理者は特定のユーザー コミュニティに対して、[**User Access (ユーザー アクセス)**] > [**Realms (レルム)**] > [**Configure Community (コミュニティの設定)**] > [**Access Methods (アクセス方法)**] > [**Tunnel IP Protocol (トンネル IP プロトコル)**] ページの [**Network tunnel client (ネットワーク トンネル クライアント)**] オプションを選択する必要があります。Web ベースのリソースにのみアクセスできる Web プロキシ エージェントとは異なり、**ネットワーク トンネル クライアント**は、あらゆる種類のリソースへのアクセスを提供します。

メモ：ネットワーク トンネル クライアント オプションをインストールするには、管理者権限が必要です。Tunnel クライアントを参照してください。

変換 ActiveSync Web アクセス

デフォルトでは、アプライアンスは Internet Explorer が動作する Microsoft Windows システムに対して、Microsoft ActiveX コントロール (Web プロキシ エージェント) を展開するように構成されています。ただし Web プロキシ エージェントが動作不可能な場合は、代替システムとして変換 Web アクセスが使用されます。変換 Web アクセスでは、Web リソースに対する基本アクセスが可能になると同時に、内部ホスト名を隠すエイリアスも作成できるようになります。変換 Web アクセスは、Web コンテンツをアプライアンスから直接プロキシします。これを使用すると、Windows ネットワーク共有へのアクセスだけでなく、WorkPlace で実行するよう個別に構成されている任意の Web リソースにもアクセスできるようになります。変換 Web アクセスは、SSL をサポートし JavaScript が有効化されたあらゆる Web ブラウザで機能します。URL リライトを使用するため、一部の Web アプリケーション (AJAX など) は制限される場合があります。カスタム ポート マッピングまたはカスタム FQDN マッピングを、URL 変換の代替として使用できます。

カスタム ポート マッピング Web アクセス

カスタム ポート マッピングでは、バックエンドのリソースまたはサーバーと、EX Series アプライアンスのポート番号とのマッピングが行われます。Apache がこのポートをリッスンし、このポートで受信したすべての HTTP トラフィックはアプライアンスで切断されます。マッピングされたバックエンド リソースを取得するための新しい HTTP 要求が作成されます。絶対 URL の変換を容易にするために、HTTP 応答はプレーン テキストを使用して送信されます。URL リライトは使用されません。カス

タム ポート マッピングを使用する際は、ネットワーク内のすべてのファイアウォールにおいて、特定のポートを開けておくよう構成する必要があります。カスタム ポート マッピングではクライアント エージェントのインストールは不要であり、あらゆる Web ブラウザで機能します。

カスタム FQDN マッピング Web アクセス

カスタム FQDN マッピングでは、バックエンドのリソースまたはサーバーが外部の完全修飾ドメイン名 (ホストおよびドメイン) にマッピングされます。リソースには、IP アドレスではなく、この FQDN 名を使用してアクセスする必要があります。FQDN 名は、パブリック ドメイン内の IP アドレスに解決できる必要があります。Apache はこの IP アドレスでポート 443 をリッスンします。すべての HTTPS トラフィックはこのソケットで切断されます。マッピングされたバックエンド リソースを取得するための新しい HTTP 要求が作成されます。絶対 URL の変換を容易にするために、HTTP 応答はプレーン テキストを使用して送信されます。URL リライトは使用されません。

カスタム ポート マッピングまたはカスタム FQDN マッピング Web アクセスに関する注意事項

これらのアクセス方法は、相対 URL を主に使用し、問題なく機能するすべてのアプリケーションに最適です。Ajax および Flash アプリケーションは、変換 Web アクセスよりもこれらのアクセス方法でうまく動作する場合もあります。

変換 Web アクセスでカスタム ポート マッピングまたはカスタム FQDN マッピング Web アクセスを使用する場合は、次のアプリケーションをお勧めします。

- SharePoint 2010、SharePoint 2013
- Outlook Web Access 2013
- Domino Web Access
- 複雑な Web アプリケーション (Java アプレット/AJAX/Flash/その他の高度な Web テクノロジー)

トピック:

- 設定要件
- 既知の動作

設定要件

- それぞれのリソースは、いずれか 1 つのアクセス方法のみを使用して構成する必要があります。変換モード、カスタム ポート マッピング モード、カスタム FQDN マッピング モードを混在させないでください。
- URL にパスを含めないでください。例えば、次のような URL は使用しないでください。

  ```
  http(s)://backend_hostname(:portNumber)
  ```

  WorkPlace で完全なパスを設定するには、Web ショートカットの追加の説明に従って、[Edit WorkPlace Shortcuts (WorkPlace ショートカットの編集)] > [Advanced (詳細)] ページで開始ページを指定します。
- 有効な証明書の使用を強くお勧めします。
  - 無効な証明書を持つカスタム FQDN マッピングのリソースに WorkPlace からアクセスした場合、Internet Explorer ではアプライアンスのシングル サインオンが機能しないことがあ

ります。例えば、ユーザーが WorkPlace にログインしてカスタム FQDN マッピングのリソースをクリックした際に、そのリソースが自己署名証明書を使用しているか、またはアプライアンス上で有効な証明書を持っていないと、このようなケースが発生することがあります。JavaScript による証明書の警告が、Internet Explorer のユーザーにポップアップで表示されます。ユーザーが証明書を受け入れた後、Internet Explorer は初期ページに「referrer」HTTP ヘッダーを送信しません。シングル サインオン機能ではこの referrer の値が必要です。この問題は、Internet Explorer 以外のブラウザを使用している場合や、証明書に関する警告がない場合、ワイルドカードまたは SAN 証明書が使用されている場合には、発生しません。

この Internet Explorer の問題は、以下のページで説明されています。

http://connect.microsoft.com/IE/feedback/ViewFeedback.aspx?FeedbackID=379975

- Internet Explorer でアクセスする際に証明書の警告が発生した場合、カスタム ポート マッピングされたリソースが Workplace ポータルにリダイレクトされることがあります。

- このリソースの構成およびアクセスには、IP アドレスではなく、ホスト名とドメイン名のみを使用する必要があります。

既知の動作

Internet Explorer ブラウザで OWA、DWA、SharePoint などのアプリケーションからログアウトすると、WorkPlace からもログアウトする場合があります。

メモ：ログアウトしても、他のアクティブな WorkPlace ショートカット セッションには影響しません。バックエンド アプリケーションがログオフ時にすべての Cookie (アプライアンス固有の Cookie を含む) を消去するので、ブラウザのみがログオフされます。

SharePoint でのシームレスな編集

SonicWall Secure Mobile Access (SMA) プラットフォームは、リバース プロキシを使用した Microsoft SharePoint アクセスと、SharePoint での Office ドキュメントのシームレスな編集をサポートしています。SMA は、永続 Cookie 情報を適切なゾーンに保存できるようにすることでこれを実現します。管理者は、ユーザーのシステム上で永続 Cookie 情報を有効または無効にすることができます。

メモ：永続的なセッション ストレージを可能にするゾーンからの SharePoint ドキュメントの編集には、Microsoft Internet Explorer (IE) のみが使用できます。

メモ：永続 Cookie を保存する前に法的規制によりユーザーの同意が必要な場合、管理者は規約の承諾 (AUP) を作成することができます。

メモ：ユーザーが安全でないゾーン (キオスク モード ゾーンなど) に移動できるゾーンがある場合、そのゾーンに対して永続 Cookie を有効にしないでください。

SharePoint でのシームレスな編集の設定は、次の 3 つの部分で行います。

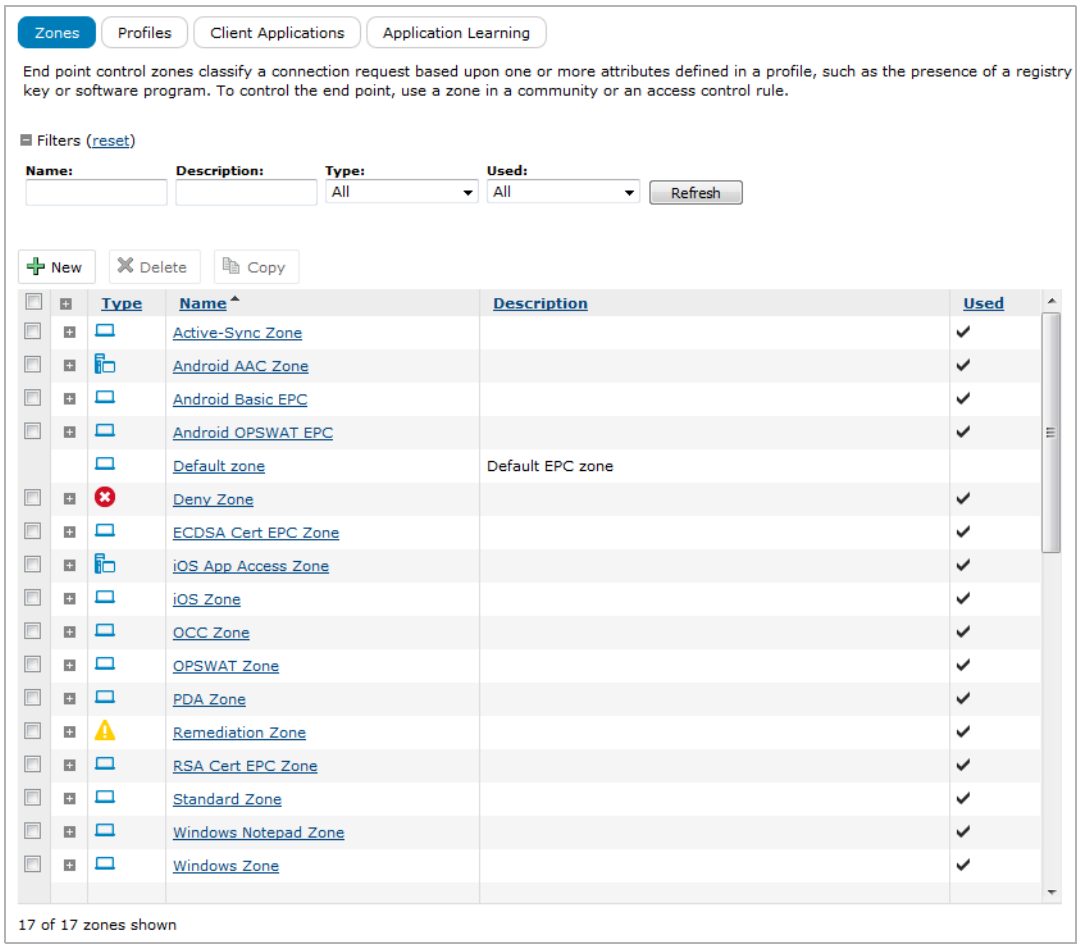
- 永続セッション情報の保存を有効にする
- リソースを SharePoint Web サービスとして構成する
- 永続セッション情報を保存できるようにゾーンを変更する

永続セッション情報の保存を有効にする

ユーザーのシステムで永続 Cookie 情報を有効にするには

1 [**User Access (ユーザー アクセス)**] > [**End Point Control**] ページに移動します。

2 [**Zones and Profiles (ゾーンとプロファイル)**] パネルで、[**Zones (ゾーン)**] の [**Edit (編集)**] をクリックします。[**Zones (ゾーン)**] ページが表示されます。

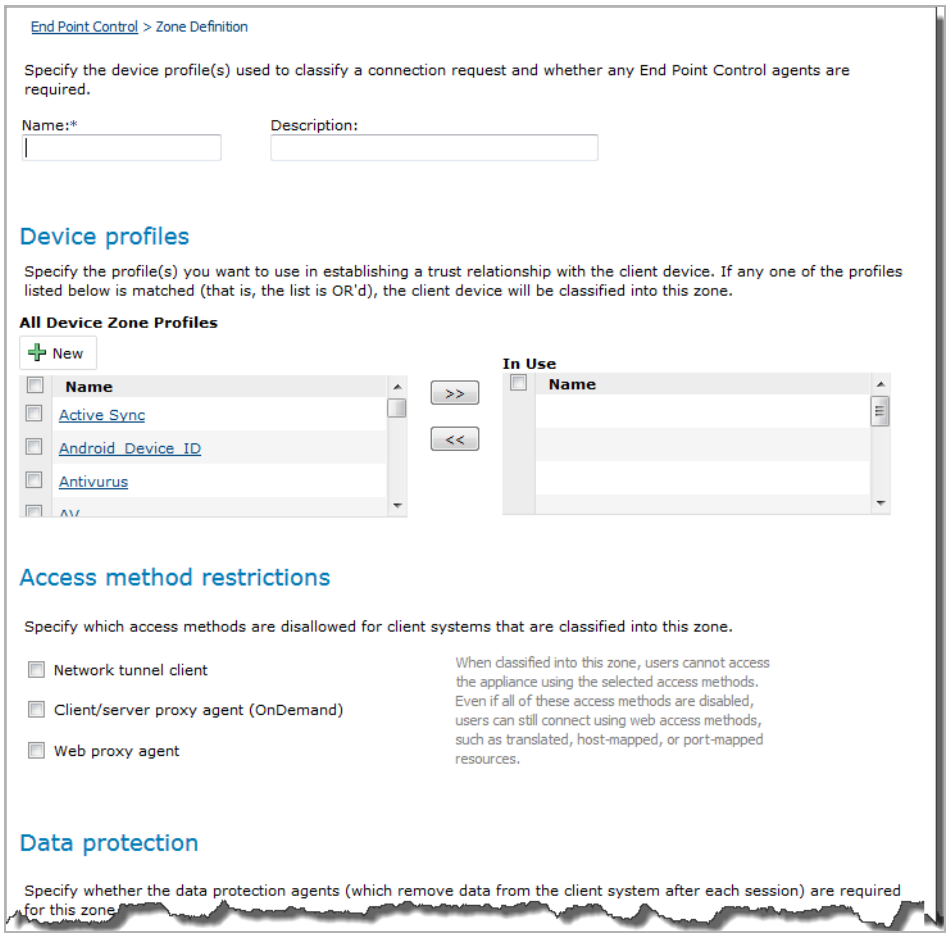


3 ゾーンを選択するか、次のように新しいゾーンを作成します。

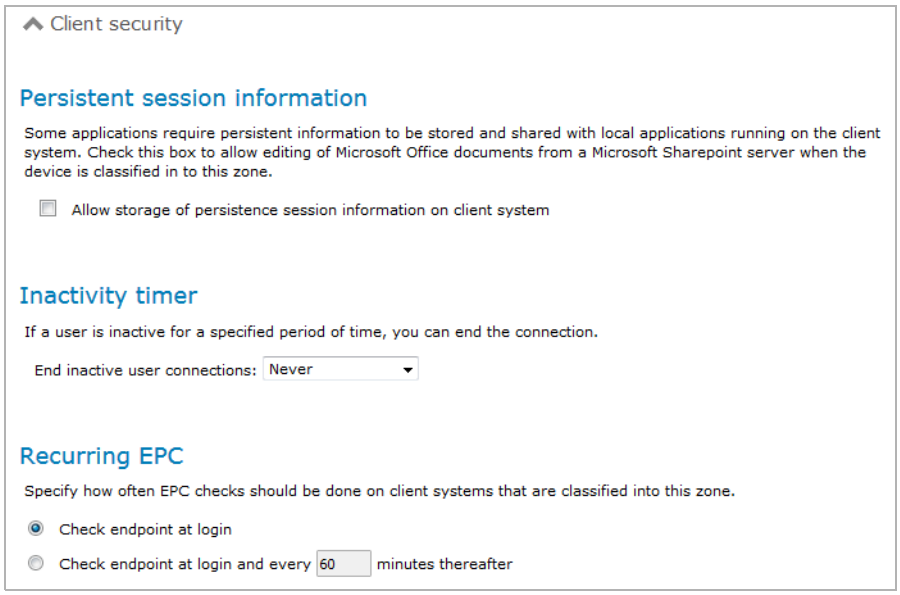
a 新しいゾーンが必要な場合は、デバイス ゾーンの作成を参照してください。

b 既存のゾーンの 1 つを変更する場合は、表のそのゾーンをクリックします。

[Zone Definition - Device Zone (ゾーン定義 - 機器ゾーン)] ページが表示されます。



4 [Client Security (クライアント セキュリティ)] パネルまでスクロールダウンして開きます。

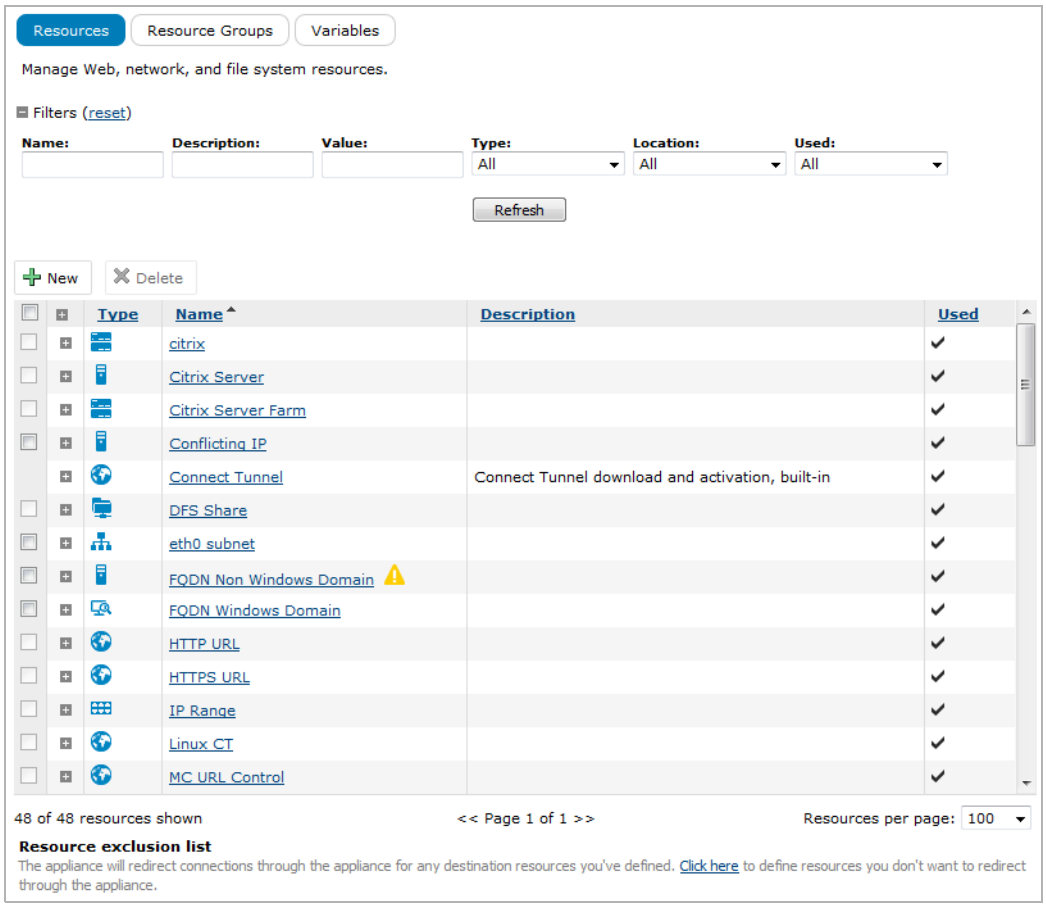


5 [Persistent session information (永続セッション情報)] で、[Allow storage of persistence session information on client system (クライアント システムへの永続セッション情報の保存を許可する)] チェックボックスを選択します。

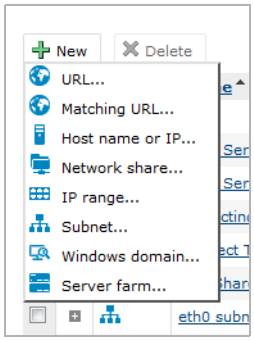
リソースを SharePoint Web サービスとして構成する

リソースを SharePoint Web サービスとして構成するには

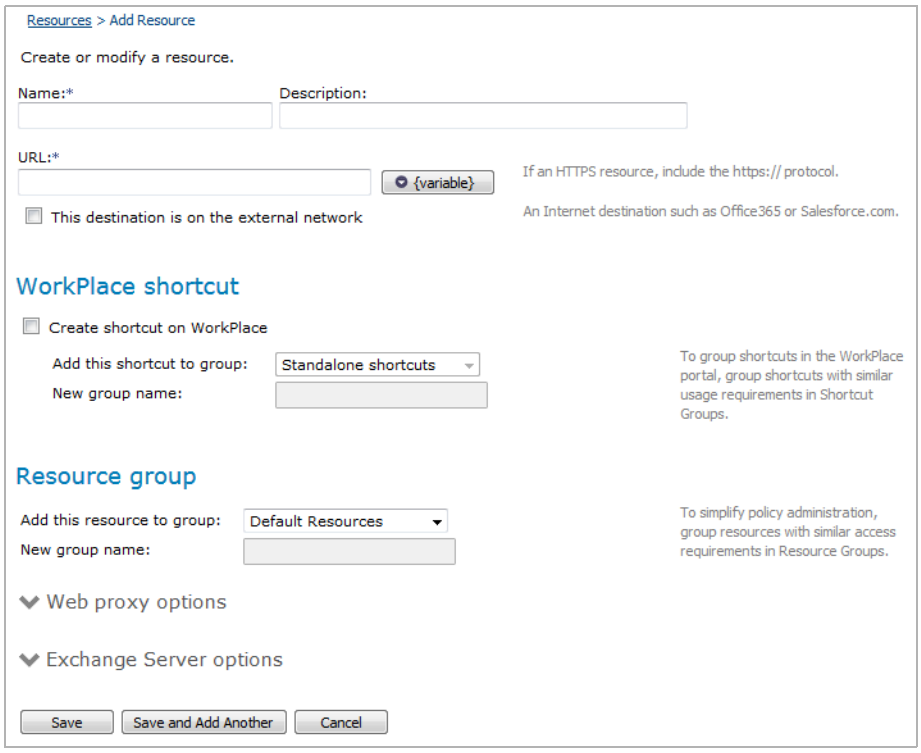
1 [Security Administration (セキュリティ管理)] > [Resources (リソース)] ページに移動します。



2 [New (新規)] をクリックし、ドロップダウン メニューから [URL] を選択します。



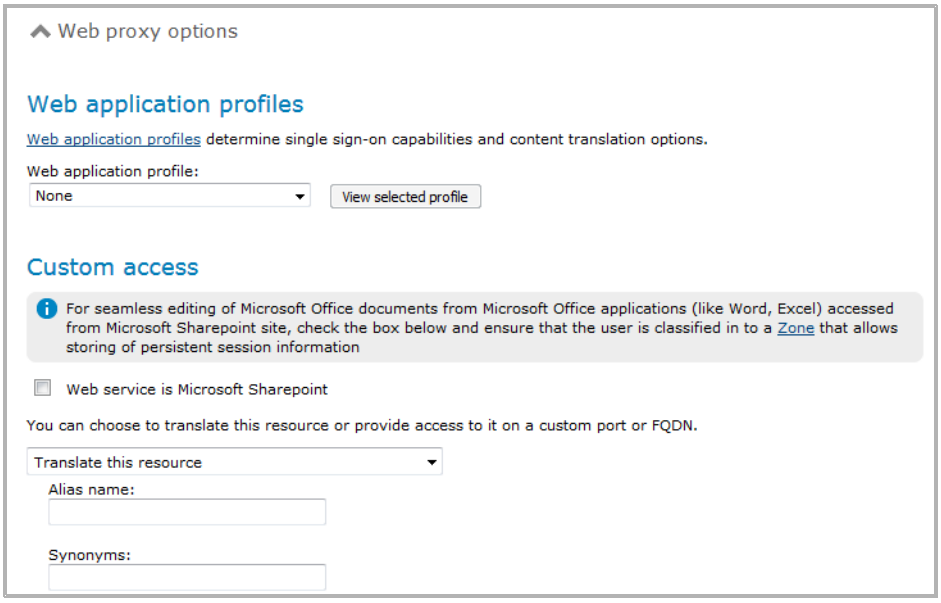
[**Add Resource URL (リソース URL の追加)**] ページが表示されます。



3 このリソースの**名前**と **URL** を入力します。

4 このリソースが外部ネットワーク上にある場合は、[**This destination is on the external network (この宛先は外部ネットワーク)**] チェックボックスを選択します。

5 [**Web proxy options (Web プロキシ オプション)**] パネルまでスクロールダウンして開きます。



6 [**Web application profile (Web アプリケーション プロファイル)**] ドロップダウン メニューから [**SharePoint**] を選択します。

7 [**Web service is Microsoft SharePoint (Web サービスは Microsoft Sharepoint)**] チェックボックスを選択します。

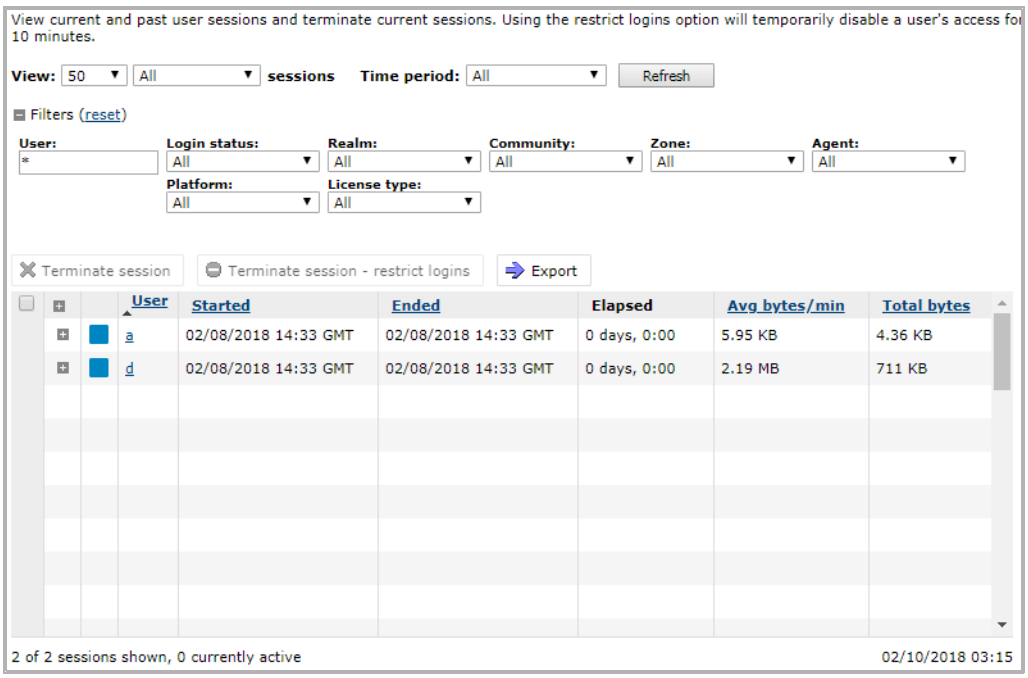
8 [**Access this from resource using a custom FQDN (カスタム FQDN を使用してリソースからアクセス)**] を選択します。

9 [**Custom FQDN (カスタム FQDN)**] フィールドに、FQDN を入力します。

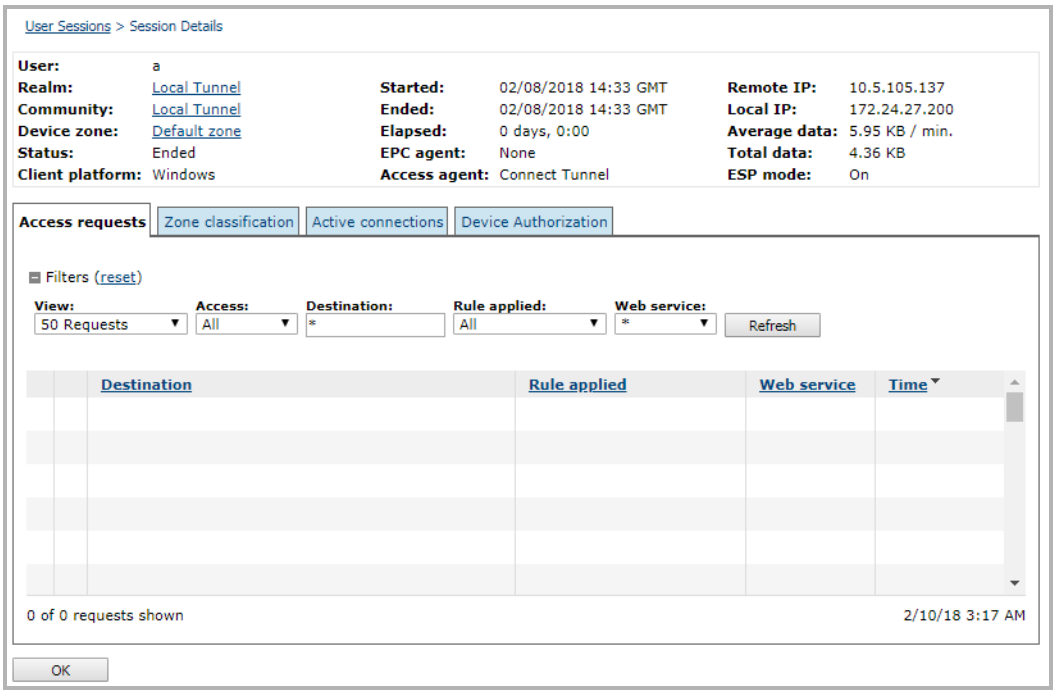
永続セッション情報を保存できるようにゾーンを変更する

クライアント システムに永続セッション情報を保存できるようにゾーンを変更するには

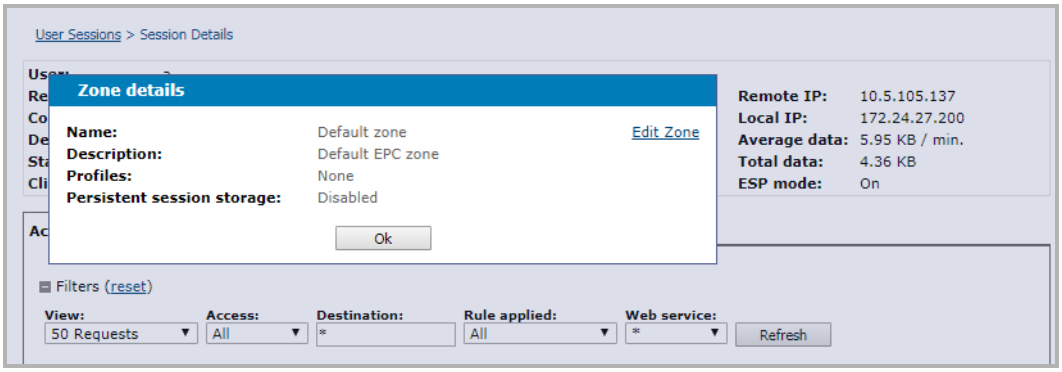
1 **Monitoring (監視) > User Sessions (ユーザー セッション)** ページに移動します。



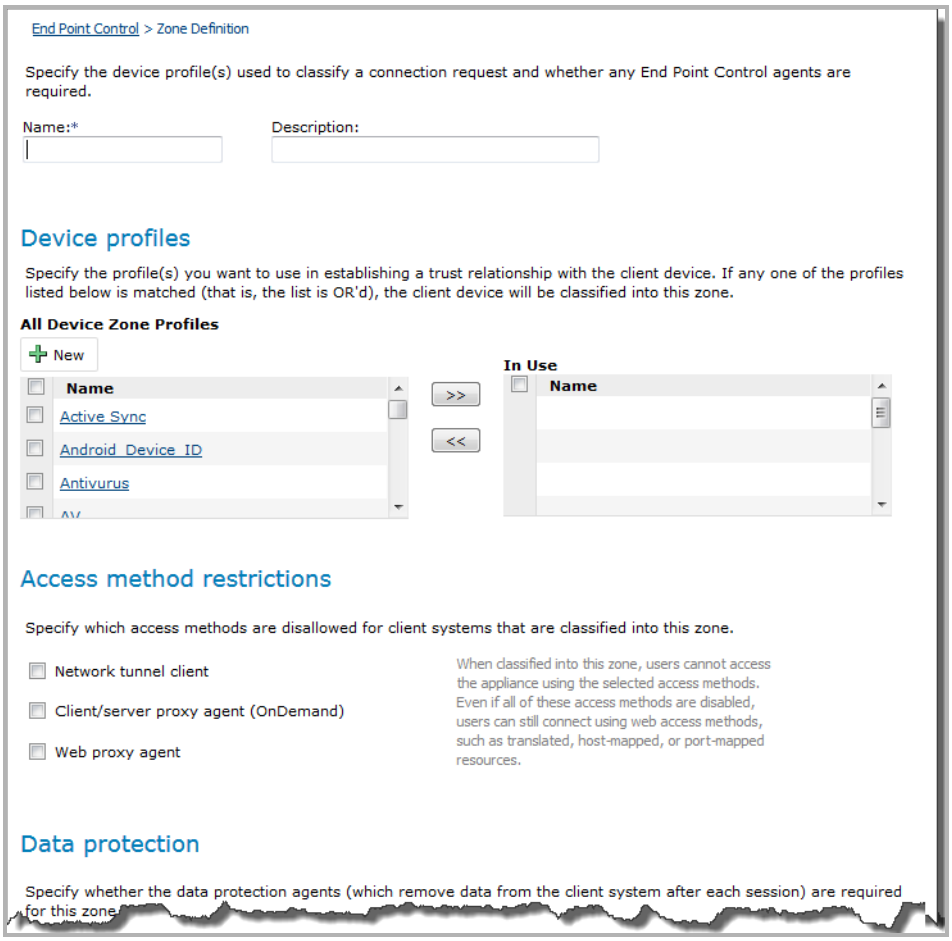
2 必要なユーザー セッションをクリックします。[**Session Details (セッションの詳細)**] ページが表示されます。



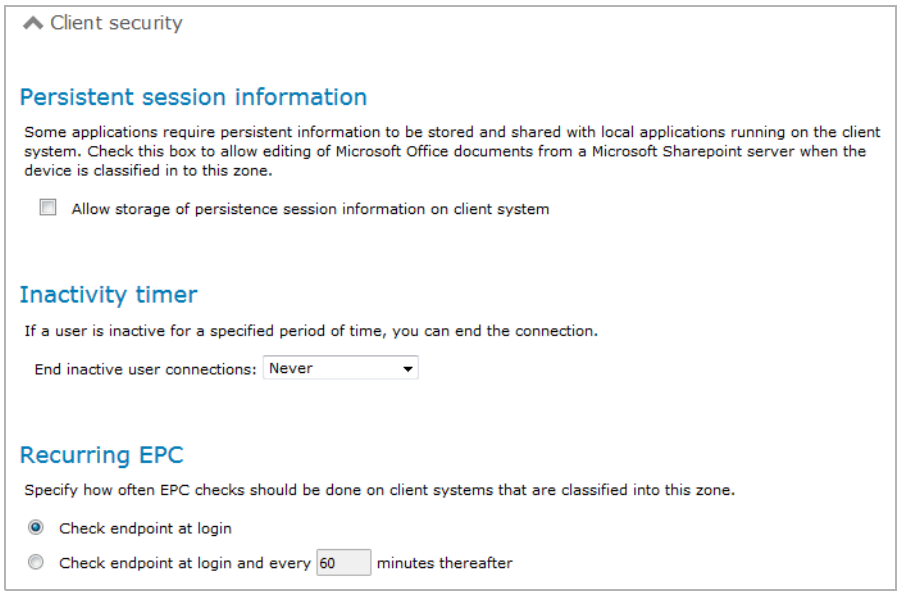
3 必要なゾーンをクリックします。[**Zone Details (ゾーンの詳細)**] ページが表示されます。



4 [**Edit Zone (ゾーンの編集)**] をクリックします。[**Zone Definition - Device Zone (ゾーン定義 - 機器ゾーン)**] ページが表示されます。



5 [**Client Security (クライアント セキュリティ)**] パネルまでスクロールダウンして開きます。



6 [**Persistent session information (永続セッション情報)**] で、[**Allow storage of persistence session information on client system (クライアント システムへの永続セッション情報の保存を許可する)**] チェックボックスを選択します。

Exchange ActiveSync Web アクセス

Secure Mobile Access では、Apple iPhone/iPad、および Android 2.1/2.2/2.3 以降または Symbian 9.x オペレーティング システム搭載のスマートフォンやタブレットでの Exchange ActiveSync をサポートします。

Symbian は、数多くのデバイスのホストとして利用されているオープン OS です。最新バージョンの Symbian OS を搭載し、Exchange ActiveSync (Nokia デバイスでのブランドは「Mail for Exchange」) をサポートしている一般的なデバイスの例は次のとおりです。

- Symbian OS 9.1 : Nokia E65、N71
- Symbian OS 9.3 : Nokia E72
- Symbian OS 9.4 : Nokia X6、Samsung Omnia HD

管理者が SMA アプライアンスを構成したら、サポートされているスマートフォンまたはタブレットを持つユーザーは、Exchange ActiveSync を使用して電子メールにアクセスするようにデバイスを設定できます。

これを行う場合、ユーザーは電子メールのアカウント名、サーバー、ドメイン、ユーザー名、パスワードを入力します。ユーザーはこのアカウントについて ActiveSync をオンにします。その結果、新しい電子メール アカウントとしてデバイス上に保存されます。

ActiveSync がオンになっている場合、新着メールがあるとデバイスはユーザーに通知します。

ユーザーが、iPhone または Symbian デバイスを、SMA アプライアンス経由で Exchange サーバーに接続されているコンピュータと同期すると、メール、アドレス帳、およびカレンダーが更新されます。Symbian では、[Tasks] および [Out Of Office] の設定もサポートされます。

トピック:

- アプライアンスでの Exchange ActiveSync アクセスの有効化
- Exchange ActiveSync セッション
- Exchange ActiveSync のデバイス プロファイルについての注意事項

アプライアンスでの Exchange ActiveSync アクセスの有効化

管理者は、iPhone または Symbian デバイスのユーザーのコミュニティに対して Exchange ActiveSync のアクセスを有効化できます。これには、次のタスクが含まれます。

- Active Directory 認証サーバーを使用するレルムを作成します。連鎖式認証を使用するレルムは、Exchange ActiveSync ではサポートされません。
- URL リソースの [**Resources Add/Edit (リソースの追加/編集)**] ページの [**Exchange Server Options (Exchange サーバー オプション)**] セクションを使用して、Exchange ActiveSync 用リソースを作成します。

  管理者は [**Exchange Server Options (Exchange Server オプション)**] セクションを使用して、Exchange ActiveSync のアクセスの提供に使用するカスタム FQDN、IP アドレス、SSL 証明書、レルムを指定できます。

カスタム FQDN、IP アドレス、SSL 証明書の各オプションは、これらのオプションを使用する WorkPlace サイトの場合と同じように機能します。カスタム FQDN で提供されるホスト/ドメイン名を使用して、ActiveSync の接続またはセッションを確立できます。

IP アドレスはアプライアンスによってホストされる仮想 IP アドレスです。このアドレスは、SMA アプライアンスの公開インターフェースを介してアクセスできるよう、アプライアンスの外部インターフェース (シングルホーム構成の場合は内部インターフェース) と同じサブネット上である必要があります。

SSL 証明書にはワイルドカード証明書を使用できるほか、ホスト名と一致するサーバー証明書を構成することもできます。

[Realm (レルム)] ドロップダウン メニューには、Active Directory 認証サーバーを使用するレルムのみが表示されます。連鎖式認証を使用するレルムは、メニューに表示されません。Exchange ActiveSync に使用するレルムは、連鎖式認証を提供するよう変更したり、Active Directory 以外の認証サーバーを使用するよう変更することはできません。

- AMC の [**EPC**] ページで、Exchange ActiveSync デバイスの終点制御用のデバイス プロファイルを定義します。デバイス プロファイルのタイプとして Exchange ActiveSync を選択できます。

  このデバイス プロファイルで構成可能な属性は、「**機器 ID**」のみです。デバイスのシリアル番号が識別子として使用されます。「機器 ID」 の取得には、ベースとなるオペレーティング システムのハード ディスク ドライバが使用されます。「機器 ID」の取得が確実に機能するよう、ドライバの更新をすべて適用しておく必要があります。

  Exchange ActiveSync のデバイス プロファイルは、評価用にあらゆるゾーンに含めることができます。

  メモ：ActiveSync クライアントは、デバイスの承認が有効なゾーンでは接続できません。

- [**Network Settings (ネットワーク設定)**] ページを参照して、仮想ホスティングに使用するすべてのカスタム IP アドレス、これらのアドレスで監視する FQDN、および関連する [Resources] または [WorkPlace Sites] を確認します。

  簡単に移動して編集できるよう、[**Resources (リソース)**] および [**WorkPlace Site (WorkPlace サイト)**] の項目は構成ページにリンクされています。

- [**User Sessions (ユーザ セッション)**] ページを参照します。[Exchange ActiveSync] アクセス エージェントに属している Exchange ActiveSync セッションが表示されます。[**Exchange ActiveSync**] は、[**Filters (フィルタ)**] の下にある [**Agent (エージェント)**] リストのオプションです。

Exchange ActiveSync セッション

ActiveSync Exchange サーバーの FQDN 名に初めて接続すると、アプライアンスによって、ユーザー名とパスワードの入力が求められます。

ユーザーの認証が成功すると、それ以上のユーザーの操作なしで Exchange サーバーとの ActiveSync セッションが確立されます。

ユーザーが Exchange 2007 に接続する場合、セッションの初期化時に、デバイスの IMEI シリアル番号が ActiveSync ストリーム外で解析されます。Exchange システムの管理者は、デバイス識別子を送信するように構成の変更が必要となる場合があります。

アプライアンスから Exchange サーバーに対する認証の方式には、ベーシック認証が使用されます。

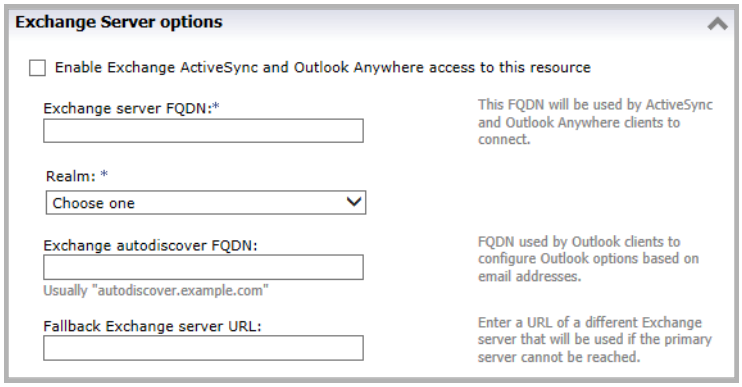
Exchange ActiveSync のデバイス プロファイルについての注意事項

- ActiveSync クライアントでは、デバイスの承認はサポートされていません。ActiveSync クライアントは、デバイスの承認が有効なゾーンでは接続できません。
- このプロファイルは、ActiveSync ストリームでのみ機能します (デバイスの値を取得する唯一の方法であるため)。
- このプロファイルは、Exchange 2007 サーバーと通信する ActiveSync ストリームでのみ機能します。
- このリリースでは、Exchange の ActiveSync のみがサポートされています。

SAN 証明書による ActiveSync リソース設定

SAN 証明書は、同じ IP アドレス上の異なるホスト名に使用できます。ただし、SAN 証明書を使用せず、以前のバージョンのように ActiveSync リソースの設定を続行したい場合は、`MGMT_ALLOW_LEGACY_VIRTUAL_HOSTS` という CEM 変数を「`TRUE`」に設定しても同じことができます。

SAN 証明書を使用するには、[**Exchange Server Options (Exchange サーバー オプション)**] ページで IP アドレスを設定します。



Outlook Anywhere Web アクセス

SMA は、Windows 上の Microsoft Outlook クライアントで Outlook Anywhere をサポートします。管理者が SMA アプライアンスを構成したら、Outlook Anywhere を使用して電子メールにアクセスするように Microsoft Outlook クライアントを設定し、不在サービスも使用できます。

アプライアンスでの Outlook Anywhere の設定

Microsoft Outlook クライアント ユーザーに対して Outlook Anywhere アクセスを有効にすることができます。これには、次のタスクが含まれます。

- Active Directory 認証サーバーを使用するレルムを作成します。連鎖式認証を使用するレルムは、Outlook Anywhere ではサポートされません。
- URL リソースの [Resources Add/Edit (リソースの追加/編集)] ページの [Exchange Server Options (Exchange サーバー オプション)] セクションを使用して、Outlook Anywhere 用リソースを作成します。

  管理者は [Exchange Server Options (Exchange サーバー オプション)] セクションを使用して、Exchange のアクセスの提供に使用する Exchange サーバーの FQDN とレルムを指定できます。Exchange サーバーの FQDN は、Outlook Anywhere RPC over HTTP または MAPI over HTTP の Exchange

サーバーで構成されたものと同じで、SMA アプライアンスのパブリック IP に解決する必要があります。

[Realm (レルム)] ドロップダウン リストには、Active Directory 認証サーバーを使用するレルムが表示されます。連鎖式認証を使用するレルムは、リストに表示されません。Outlook Anywhere に使用するレルムは、連鎖式認証を提供するよう変更したり、Active Directory 以外の認証サーバーを使用するよう変更することはできません。

Microsoft Outlook は、電子メール アカウントを設定するときに、Exchange Autodiscover FQDN に接続しようとします。例えば、電子メール アドレス user@example.com の Autodiscover FQDN は autodiscover.example.com になります。autodiscover.example.com という名前は、アプライアンスのパブリック IP アドレスを持つパブリック DNS サーバーで設定する必要があります。

[**User Sessions (ユーザー セッション)**] ページには、Exchange セッションが Outlook Anywhere アクセス エージェントに属するものとして表示されます。

Outlook Anywhere セッション

Outlook Anywhere に接続する場合、ユーザーはユーザー名/パスワードの資格情報をアプライアンスに送信する必要があります。ユーザーの認証が成功すると、Exchange サーバーとの QA セッションが確立されます。

ユーザー名/パスワードは、クライアントからの基本認証ヘッダーから抽出され、Active Directory サーバーで認証され、アプライアンスへのセッションを確立します。すると、認証が成功した後に Exchange サーバーへの接続が確立されます。

非基本認証ヘッダーが最初の要求に含まれる場合、クライアントは基本ヘッダーの入力を再度求められます。次に、ユーザー名/パスワードが抽出され、Active Directory サーバーに対して認証されます。認証が成功すると、Exchange サーバーとのセッションが確立されます。

Autodiscover が有効になっている場合、Outlook Anywhere クライアントは電子メール ID を使用してサーバー情報を自動的に更新します。この処理には、サーバーの更新中は時間がかかることがあります。

Microsoft Outlook クライアントの構成

トピック:

- 新しい Microsoft Outlook クライアント アカウントを設定する
- 既存の Microsoft Outlook クライアント アカウントを設定する
- Outlook Anywhere アクセス エージェントの Outlook Anywhere セッションを表示する

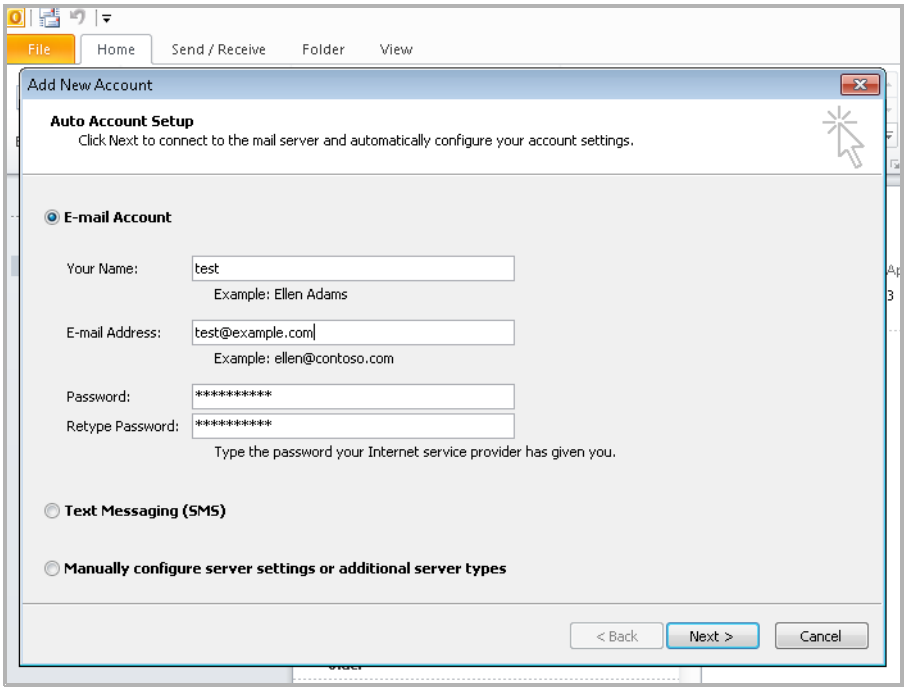
新しい Microsoft Outlook クライアント アカウントを設定する

新しい Microsoft Outlook クライアント アカウントを設定するには

1 Microsoft Outlook を起動します。

2 [**File (ファイル)**] > [**Info (情報)**] ページにアクセスします。

3 [**Add Account (アカウントの追加)**] ボタンをクリックします。[**Add New account (新規アカウントの追加)**] ページが表示されます。



4 **自分の名前、電子メール アドレス**、および**パスワード**を入力します。

クライアントは Autodiscover を使用してサーバー情報を自動的に取得し、アカウントを設定します。AMC および Exchange サーバーの Autodiscover URL が正しく構成されていることを確認してください。

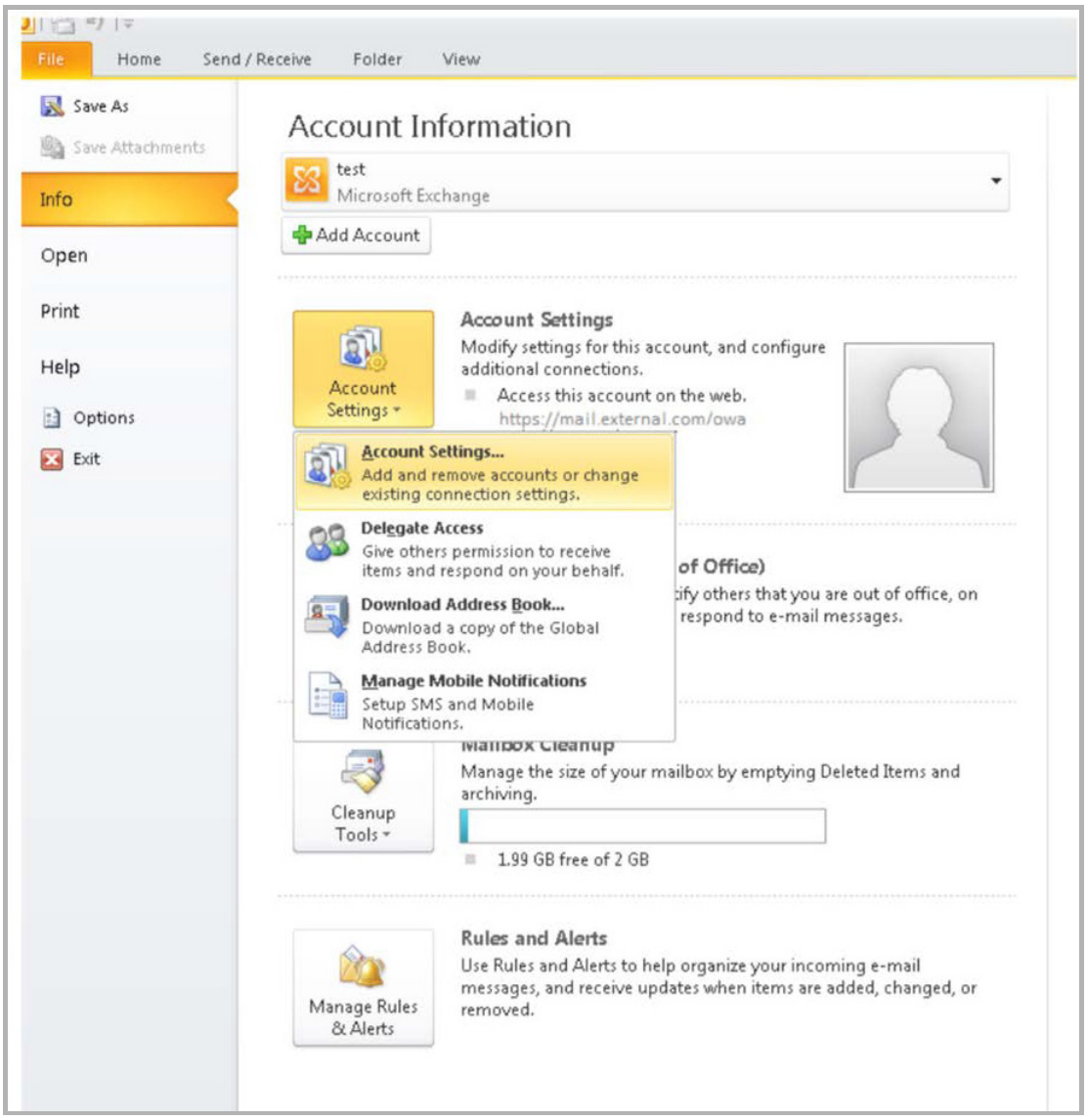
RPC/HTTP の場合は Microsoft Outlook クライアントで Outlook Anywhere 設定を手動で指定できますが、Autodiscover が有効になっている場合はサーバー情報を自動的に更新します。

既存の Microsoft Outlook クライアント アカウントを設定する

既存の Microsoft Outlook クライアント アカウントを設定するには

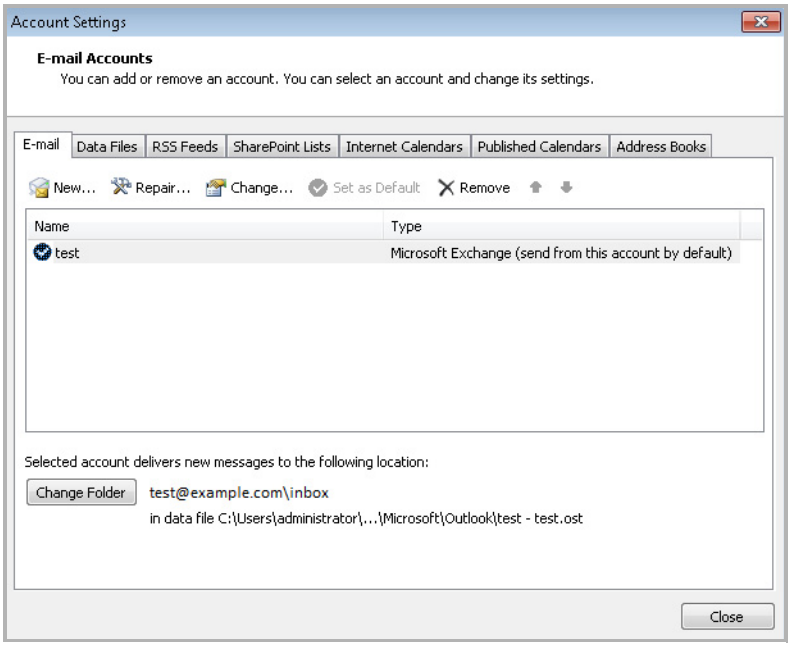
1 Microsoft Outlook を起動します。

2 [**File (ファイル)**] > [**Info (情報)**] ページをクリックします。

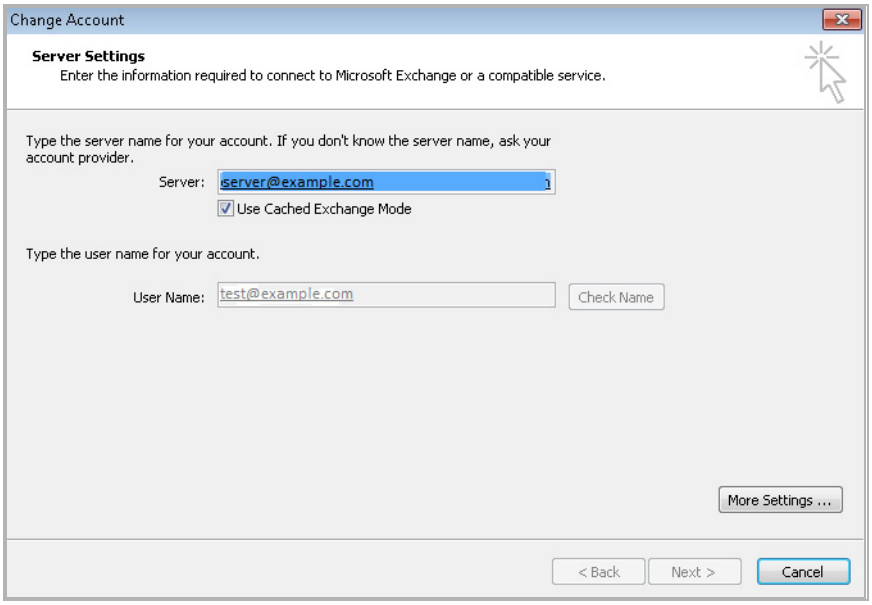


3 [**Account Settings (アカウント設定)**] をクリックします。

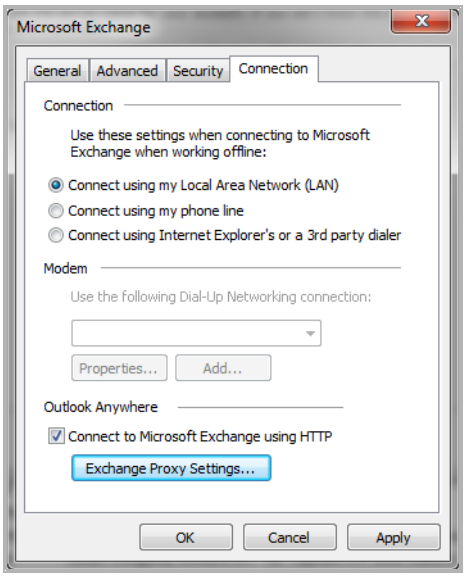
[**Account Settings (アカウント設定)**] ダイアログが表示されます。



4 **Change... (変更...)** をクリックします。[**Change Account (アカウントの変更)**] ダイアログが表示されます。



5 [**More Settings... (詳細設定)**] ボタンをクリックします。[**Microsoft Exchange**] ダイアログが表示されます。

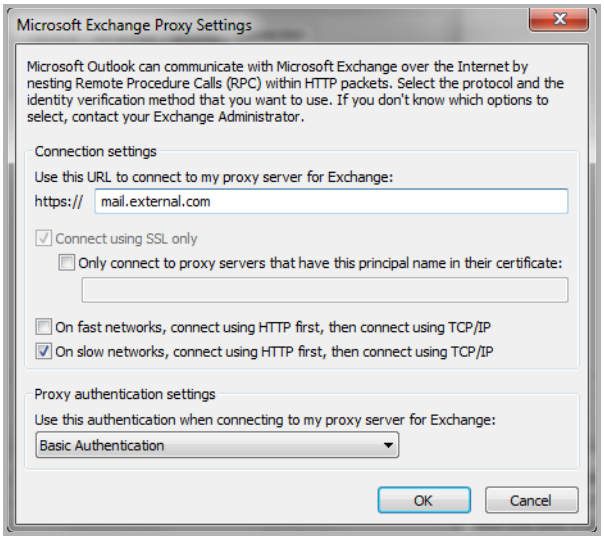


6 [**Connection (接続)**] タブを選択します。

ⓘ **メモ**：[**Connection (接続)**] タブは、MAPI/HTTP では使用できません。サーバー情報を自動的に取得します。

7 [**Outlook Anywhere**] で、[**Connect to Microsoft Exchange using HTTP (HTTP を使用して Microsoft Exchange に接続する)**] を選択します。

8 [**Exchange Proxy Settings (Exchange のプロキシ設定)**] ボタンをクリックします。[**Microsoft Exchange Proxy Settings (Microsoft Exchange のプロキシ設定)**] ダイアログが表示されます。



9 [**Use this URL to connect to my proxy server for Exchange (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 の FQDN を入力します。

10 [**Proxy authentication settings (プロキシ認証設定)**] で、ドロップダウン メニューから [**Basic Authentication (基本認証)**] を選択します。

> **メモ**：基本認証は SMA の RPC/HTTP に対してのみサポートされているため、Exchange サーバーの Outlook Anywhere RPC/HTTP に対して基本認証が構成されていることを確認する必要があります。

11 [**OK**] を選択して設定を保存します。

12 Microsoft Outlook を終了します。

13 Microsoft Outlook を起動して新しいセッションを開始します。

Outlook Anywhere アクセス エージェントの Outlook Anywhere セッションを表示する

Outlook Anywhere アクセス エージェントに属する Outlook Anywhere セッションを表示するには

1 [**Monitor (監視)**] > [**Users Session (ユーザー セッション)**] ページに移動します。

2 [**Filters (フィルタ)**] の [**Agent (エージェント)**] リストで、[**Exchange**] オプションを選択します。

クライアント インストール パッケージ

Connect Tunnel クライアント コンポーネントを、WorkPlace にログインしなくても、ユーザーが別のネットワークの場所 (Web サーバー、FTP サーバー、またはファイル サーバー) からダウンロードおよびインストールできるようにすることもできます。また、Tivoli や SMS などのアプリケーションを使用してユーザーに Connect Tunnel クライアント インストール パッケージを送信することも、サードパーティ製のディスク イメージ コピー ユーティリティを使用して、クライアント インストールのマスター イメージを作成してユーザーのシステムにコピーすることもできます。

クライアントのセットアップ パッケージは、AMC からダウンロードできます。また、Windows ベースのパッケージ (Connect Tunnel for Windows) では、クライアントをユーザーに配布する前に、`.ini` 構成ファイルでさまざまなクライアントの設定を指定することもできます。

> **メモ**：ユーザーに確実に最新バージョンを実行させるためには、クライアントを自動更新にすることが最も簡単な方法です。詳細については、Windows Tunnel クライアントの自動クライアント更新を参照してください。

トピック:

- Secure Mobile Access クライアント インストール パッケージのダウンロード
- Connect Tunnel クライアント用構成のカスタマイズ
- Connect Tunnel へのコマンドラインでのアクセス (NGDIAL を使用)
- コマンド構文
- Connect をサービスとして実行する

Secure Mobile Access クライアント インストール パッケージのダウンロード

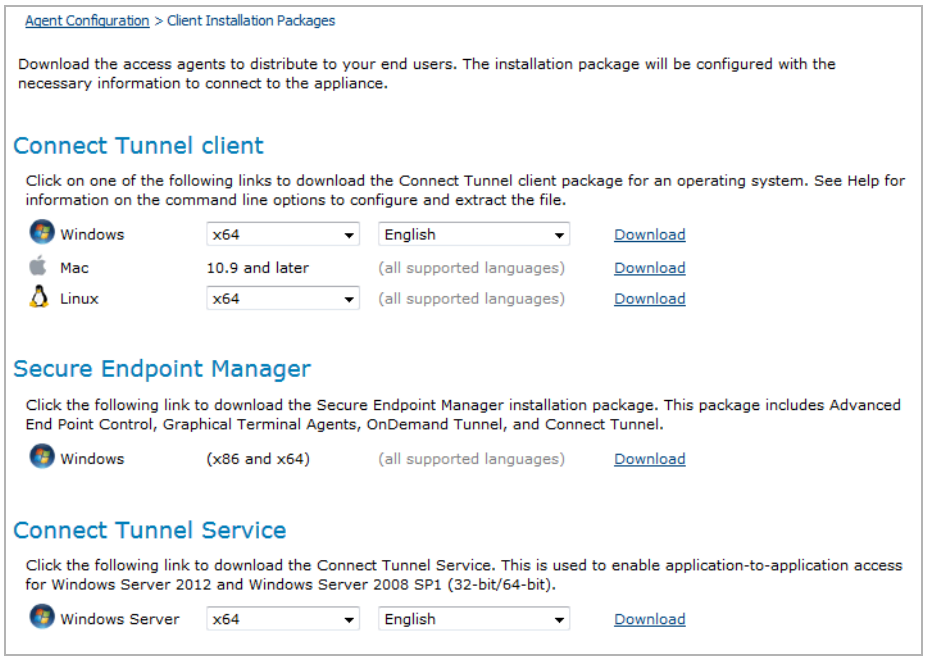
このセクションでは、Connect Tunnel クライアントのインストール パッケージを、ローカルのワークステーションへダウンロードする方法について説明します。

クライアント インストール パッケージをダウンロードするには

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**Agent Configuration (エージェント設定)**] をクリックします。

2 [**Secure Mobile Access access agents (Secure Mobile Access アクセス エージェント)**] エリアの [**Client installation packages (クライアント インストール パッケージ)**] で、[**Download (ダウンロード)**] をクリックします。[**Client Installation Packages (クライアント インストール パッケージ)**] ページが表示されます。

3 インストール パッケージの言語を選択します。各パッケージには、翻訳されたユーザー インターフェース要素とオンライン ヘルプが含まれています。



4 サポートするプラットフォームに対するクライアント インストール ファイルをダウンロードします (*<xx>* には選択した言語が示されます)。

ダウンロードのリンク

ダウンロードのリンク	インストール パッケージ
Windows	*ngsetup_<xx>.exe*
Linux x86	*SMA1000Connect-Linux.tar*
Mac OS X 10.5.x	*SMA1000Connect-OSX.dmg*
Windows Mobile	*cmsetup.exe*
Windows サービス (Connect Tunnel Service)	*ctssetup_<xx>.exe*

5 [**Download Client Package (クライアント パッケージをダウンロード)**] ページが表示されます。[**File Download (ファイルのダウンロード)**] ダイアログで、ローカル コンピュータにファイルを保存するよう求められます。

6 [**Save (保存)**] をクリックし、適切なディレクトリを参照して選択してから、再度 [**Save (保存)**] をクリックします。

7 [**Download Client Package (クライアント パッケージをダウンロード)**] ページで [**OK**] をクリックします。[**Client Installation Packages (クライアント インストール パッケージ)**] ページに戻ります。

Connect Tunnel クライアント用構成のカスタマイズ

アプライアンスからダウンロードした Connect Tunnel クライアント セットアップ パッケージは、そのままではまだ構成されていません。セットアップ パッケージをユーザーに展開する前に、Connect Tunnel 構成ファイル (`.ini` ファイル) をカスタマイズできます。こうすることで、それぞれのクライアントについて、アプライアンスのホスト名や IP アドレス、ログイン時に使用するレルム名などのクライアント オプションをあらかじめ構成することにより、作業を迅速に行えるようになります。この手順をスキップすると、パッケージではデフォルトのアプライアンス設定が使用されます。

Connect Tunnel の構成ファイルをカスタマイズするには

1 Connect Tunnel インストール ファイルを Windows コンピュータにダウンロードします (Secure Mobile Access クライアント インストール パッケージのダウンロード を参照)。

2 **Start (スタート) > Run (ファイル名を指定して実行)** で「`cmd`」と入力して、Windows のコマンド プロンプトを開きます。

3 `ngsetup_<xx>.exe` を保存したディレクトリまで移動し、以下のコマンドを実行してインストール ファイルを解凍します。ファイルの解凍先は現在の作業ディレクトリになります (`expand`) パラメータで「*<path>*」を指定した場合を除く。

```
ngsetup_<xx>.exe -expand=<path>
```

4 テキスト エディタで `ngsetup.ini` ファイルを開き、適切な構成設定を指定します。

5 変更した `ngsetup.ini` ファイルを保存して閉じます。*ngsetup_<xx>.exe* の保存先と同じディレクトリにこのファイルをコピーすると、`.ini` に対して行ったカスタマイズはセットアップ時に取り込まれます。`.ini` ファイルに別の場所を指定するには、次のコマンドを使用します。

```
ngsetup_<xx>.exe -f=<path>\<configuration file name>
```

また、インストールのデータは、`%ALLUSERSPROFILE%\Documents および Settings\All Users\Application Data\SMA1000` フォルダの *ngmsi.log* というファイルに記録できます。指定可能なパラメータの全リストを表示するには、次のコマンドを実行してください。

```
ngsetup_<xx>.exe -?
```

6 構成オプションでは、構成オプションを示しており、それに続いてサンプル `.ini` ファイルを紹介しています。これらのオプションの一部は、WorkPlace から Connect Tunnel がインストールされた場合に限って使用できます。指定しないオプション コンポーネントについては、デフォルト値が使用されます。

構成オプション

オプション	説明
[Connectoid *number*] セクション	(必須) アプライアンスにアクセスするための基本設定を制御します。ユーザーが複数のアプライアンスにアクセスできるようにするには、この構成ブロックをコピーして、([Connectoid 1]、[Connectoid 2] のように) *number* の値を 1 ずつ増やしていきます。
ConnectionName=name	(オプション) クライアントのユーザー インターフェースに表示される接続の名前。値を指定しない場合は、デフォルトの接続名 (**SMA1000 VPN Connection**) が使用されます。
VpnServer=host name | IP address	(オプション) アプライアンスのホスト名または IP アドレス。値を指定しない場合は、アプライアンスのホスト名や IP アドレスをユーザーが手動で入力する必要があります。
StartMenuIcon=[0 | 1]	(オプション) [**Secure Mobile Access**] スタート メニュー フォルダに、[**Secure Mobile Access VPN Connection**] という名前のショートカットを追加するかどうかを指定します。デフォルト値は **1** (ショートカットを追加する) です。
DesktopIcon=[0 | 1]	(オプション) デスクトップにショートカットを追加するかどうかを指定します。デフォルト値は **1** (ショートカットを追加する) です。
UserRealm=name	(オプション) ユーザーがログインするデフォルトのレルムを指定します。レルム名は、AMC で表示されているのと同じものを正確に指定します。
DefaultAuthType= [ADUNPW | LDAPUNPW | RADIUSUNPW | RADIUSCRAM | UNIX]	(廃止) この設定は、実行するユーザー認証のタイプを指定します。v8.7.0 より前の E-Class SMA アプライアンスにアクセスする場合にのみ適用されます。
StatusDlg=[0 | 1]	(オプション) アプライアンスへの接続時にステータス ダイアログ ボックスを表示するかどうかを指定します。デフォルト値は **1** (ステータス表示が有効) です。
Taskbar=[0 | 1]	(オプション) アプライアンスに接続するとき、タスクバー通知エリアにアイコンを表示するかどうか指定します。デフォルト値は **1** (アイコンの表示が有効) です。
RunAtStartup=[0 | 1]	(オプション) Windows の起動時に接続を自動的に開始するかどうかを指定します。デフォルト値は **1** (自動起動が有効) です。
[インストール設定] セクション	(オプション) このセクションでは、実行する MSI インストールのタイプについての情報を指定します。各 .ini ファイルには [インストール設定] セクションを 1 つのみ含めることができます。
UILevel=[FULL | REDUCED | BASIC | NONE]	(オプション) インストール時に含めるユーザー インターフェースのレベルを指定します。デフォルト値は **NONE** です。
ProductCode=key PackageCode=key FileSize=bytecount ProductVersion=x.yy.zzz	これらは事前に指定されている必須の設定です。変更しないでください。

サンプル ngsetup.ini ファイル

```
インストール設定
UILevel=FULL
ProductCode={A814B50B-B392-458A-8C31-51697E1EBB7A}
PackageCode={A77CB50B-0384-5D8A-DE3D-61099E9EB37C}

Branding=C:\Users\Admin\AppData\Roaming\SMA1000\CustomBranding.zip
BrandingMD5=1fc1a7b361c3b7e81e29842372f5e875
```

メモ：Branding の値は、カスタム ブランディング ファイルの絶対パスを指定する必要があります。Branding MD5 の値は、任意の MD5 ツールを使用して取得することができます。

```
[Connectoid 1]
ConnectionName="XYZ Company Network"
VpnServer=64.94.142.134

[Connectoid 2]
ConnectionName="Test Network"
VpnServer=64.94.142.134
StartMenuIcon=1
DesktopIcon=1
UserRealm="employees"
StatusDlg=1
Taskbar=1
RunAtStartup=1
```

メモ：Windows オペレーティング システム搭載のコンピュータには、プログラムを 1 回だけ起動させるレジストリ キーがあります。プログラムが 1 回起動した後は、そのリファレンスが削除され、そのプログラムが動作しなくなります。Connect Tunnel のインストール後、

```
HKEY_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

にあるすべてのプログラムが実行されます。

メモ：このファイルには、VPN アプライアンスとの接続が確立されるまで、(認証のタイプやカスタム プロンプトなど) 特定の項目を含めることはできません。つまり、ユーザーの初回アクセス時には認証プロンプトがグレーで表示されます。これを回避するための方法には、次のようなものがあります。

- ユーザーに WorkPlace からインストールさせる。
- ユーザーに [Connect] ダイアログ ボックスの [**Properties (属性)**] をクリックさせ、レルムを選択させる。
- WorkPlace のインストールから完全な構成ファイルを取得し、これをユーザーに合わせて変更します。方法については、「*Connect Tunnel の初期化ファイルのカスタマイズと WorkPlace からのインストール* (SW2831)」を参照してください。

Connect Tunnel へのコマンドラインでのアクセス (NGDIAL を使用)

NGDIAL コマンドライン ユーティリティは、Connect Tunnel を使用してリモート ネットワークへの接続を確立します (Windows RASDIAL が他のネットワーク接続で行う方法と非常に似ています)。

また、NGDIAL コマンドライン ユーティリティを使用して、ネットワーク接続の電話帳のエントリを作成、削除、変更できます。NGDIAL コマンドをパラメータなしで実行すると、すべての RAS 接続がリストされます。

Linux および Macintosh の構成で Connect Tunnel と Connect Tunnel Extensibility Toolkit がサポートされるようになりました。

コマンド構文

コマンド構文

オプション	説明
<*connection name*>	ネットワーク接続の名前。名前にスペースが含まれる場合は、引用符で囲みます。
<*public*>	ユーザーの認証用パブリック クレデンシャル (ユーザー名)。名前にスペースが含まれる場合は、引用符で囲みます。例えば、 `ngdial report_server "Jen Bates"` クレデンシャルの public および <*private*> の部分は、E-Class SMA アプライアンス上の認証レルムで指定されている認証タイプと正しく対応する必要があります。
[<*private*>|* [<*auth type*>]]	ユーザー認証時に使用するプライベート クレデンシャル (パスワード) と認証タイプ (<auth type> パラメータは、v8.7.0 より前のアプライアンスにログインする場合のみ必須です)。 クレデンシャルの <private> の部分が指定されていないか、またはアスタリスク (*) が指定されている場合は、NGDIAL コマンドからユーザーにパスワードの入力を求めるプロンプトが表示されます。 v8.7.0 より前のアプライアンスへログインする際に <auth type> を指定していない場合は、レルムのデフォルトの認証タイプが使用されます。<auth type> の値は次のとおりです。 • NULL: 認証は不要です • LDAPUNPW: LDAP ユーザー名/パスワード クレデンシャル • LDAPCERTIFICATE: LDAP 証明書クレデンシャル • RADIUSCRAM: RADIUS トークン/SecurID クレデンシャル • RADIUSUNPW: RADIUS ユーザー名/パスワード クレデンシャル • UNIX: UNIX ユーザー名/パスワード クレデンシャル • チーム: SMA TEAM クレデンシャル • ADUNPW: Active Directory ユーザー名/パスワード クレデンシャル
-create	コマンドラインで指定した情報を使用して、新しいネットワーク接続を生成するか、または既存のネットワーク接続を更新します。
-delete	指定したネットワーク接続エントリを、指定した電話帳から削除します。この操作を実行するにはシステム管理者権限が必要です。
[-connection=<connection name> | <*connection list friendly name*>]	ダイヤルする接続エントリを接続リストから読み込みます。
-disconnect | -d	VPN を <connection name> リモート ネットワークから切断します。
[-gui]	VPN ネットワーク接続を確立するために追加の情報が必要な場合は、このパラメータを使用して、RAS でグラフィカル ユーザー インターフェース (GUI) のプロンプトをユーザーに表示できます。 例えば、これを使用して、証明書に問題がある場合にアプライアンスのサーバー証明書を受け入れるよう求めるプロンプトをユーザーに表示できるほか、ユーザーにパスワードの期限切れや変更要求を通知することが必要な場合に対応できます。このような場合に -gui オプションが指定されていないと、NGDIAL ユーティリティは失敗し、呼び出し元にエラー コードを返します。

コマンド構文

オプション	説明
-help | -?	NGDIAL コマンドのコマンドライン構文を表示します。-gui オプションと一緒に使用した場合、オンライン ヘルプを表示します。
[-icon[=enable|disable]]	タスクバー通知エリアへのアイコンの表示を制御します。ユーザーはこのアイコンを使用して、VPN ネットワーク接続を管理したり、接続に関する通知を受け取ることができます。注意事項を参照してください。
[-login=<login group>]	ユーザーの認証に使用するログイン グループ (認証レルム) の名前。(v8.7.0 より前のアプライアンスに接続する際に) クレデンシャルの <auth type> なしでログインが指定された場合、NGDIAL では <auth type> に ADUNPW を使用します。
[-phonebook=<phonebook>]	<connection name> が定義されている電話帳のファイル名を指定します。ファイル名には、電話帳ファイルの完全修飾パスを含める必要があります。パスが指定されていない場合、NGDIAL はシステムの電話帳 (rasphone.pbk) が含まれているディレクトリで、指定された電話帳ファイルを検索します。
[-list=<connection name>]	引数なしで使用した場合は、リスト内のすべての接続を表示します。引数を指定して使用した場合は、接続リストを詳細表示します。
-prompt	NGDIAL コマンドがユーザーに、<connection name> リモート ネットワークへの接続のプロンプトを表示します。
[-proxycredential=<username>[,<password>|*]]	アプライアンスへのアクセスにプロキシ サーバーが必要な場合、このオプションを使用してプロキシ サーバー用のユーザー名とパスワードのクレデンシャルを指定します。 パスワードが指定されていないか、アスタリスク (*) が入力された場合、NGDIAL コマンドからユーザーにプロキシのパスワードの入力を求めるプロンプトが表示されます。
[-server=<server name>|<server IP>]	アプライアンス名または IP アドレスを指定します。サーバーを指定し、そのサーバーが電話帳のエントリに定義されているサーバーと異なる場合、サーバーとログイン グループ (指定されている場合) が電話帳のエントリに保存されます。
[-editserver=<server name>]	カスタム接続リストのサーバー名を編集します。
[-editrealm=<realm name>]	カスタム接続リストのレルム名を編集します。
[-status[=enable|disable]]	VPN ネットワークへの接続に 2 秒以上を要している場合に、接続ステータス ダイアログ ボックスを表示するかどうかを制御します。
[-nocerterrors]	サーバー証明書のエラーを抑制します。

```
ngdial <connection name> <public> [<private>|* [<auth type>]]
        [-phonebook=<phonebook>]
        [-server=<server name>|<server IP>]
        [-login=<login group>]
        [-proxycredential=<username>[,<password>|*]]
        [-status[=enable|disable]] [-icon[=enable|disable]] [-gui]
ngdial <connection name> <public> [<private>|* [<auth type>]]
```

```
          [-phonebook=<phonebook>]
          [-connection=<connection name>|<Connection list friendly name>]
          [-proxycredential=<username>[,<password>|*]]
          [-status[=enable|disable]] [-icon[=enable|disable]] [-gui]
          [-nocerterrors]
ngdial <connection name> -disconnect|-d
ngdial <connection name> -prompt
          [-phonebook=<phonebook>]
ngdial <connection name> [-list= <connection name>]
ngdial <connection name> [-editserver= <server name>]
ngdial <connection name> [-editrealm= <realm name>]
ngdial <connection name> -create
          [-phonebook=<phonebook>]
          [-server=<server name>|<server IP>]
          [-login=<login group>]
          [-status[=enable|disable]] [-icon[=enable|disable]]
ngdial -help | -?
```

例

```
NGDIAL "ACME Corp" -create -server=remote.acme.com -icon -status
NGDIAL "ACME Corp" "Jen Bates" * -login="Business Partners" -icon -gui
NGDIAL "ACME Corp" jdoe password
NGDIAL "ACME Corp" -disconnect
```

メモ：`ngdial -help` で表示される使用方法では、`-icon=disable` フラグは `-create` フラグ不要のオプションと記載されていますが、一部のケースでは、アイコンを無効化するために `-create` フラグが必要になります。

アイコンを無効化してタスクバーに表示されないようにするには、次のいずれかの方法を使用できます。

- `ngsetup.ini` ファイルに `taskbar=0` を設定してから、次のようなコマンドを実行します。

  ```
  ngdial "SMA VPN Connection" -server=<server IP address> -login="Realm name"
  username password -icon=disable -gui
  ```

- -icon=disable オプションとともに -create オプションを用いたコマンドを実行して icon パラメータを保存してから、次のようなコマンドを実行して接続します。

  ```
  ngdial "SMA VPN Connection" -create -server=<server IP address>
  -icon=disable -gui

  ngdial "SMA VPN Connection" -server=<server IP address> -login="Realm name"
  username password -icon=disable -gui
  ```

Connect をサービスとして実行する

Connect Tunnel クライアントは、Secure Mobile Access の VPN ソリューションの Windows クライアント コンポーネントで、Web ベースとクライアント/サーバー アプリケーション、さらに Windows ファイル共有に対して、安全かつ認証済みアクセスが可能になります。

サーバー環境では、アドオン コンポーネントの「Connect Tunnel サービス」をインストールして構成し、ユーザーの操作なしで VPN 接続を自動的に開始できます。ユーザーのログインは必要なく、ユーザー インターフェースやアイコンも表示されません。例えば、現場のリモート システムと本社の VPN で保護されたファイル サーバーを同期する必要があるとします。リモート システム (Windows Server プラットフォームを実行) で、Connect Tunnel サービスを特定の時刻に実行し、会社のファイル サーバーに接続して、リモートのデータベースを本社のマスター データベースと同期するように構成できます。

メモ：Connect Tunnel は、SMA アプライアンスに接続する前にダイヤルアップ接続を確立する機能を備えています。一方、Connect Tunnel サービスではこのオプションをサポートしていません。常時接続の非ダイヤルアップ ネットワーク接続が必要になります。

トピック:

- Connect Tunnel Service のインストール
- Windows サービスとスクリプトのオプション
- Windows サービスを使って Connect Tunnel サービスを構成および実行するには
- コマンドまたはスクリプトを使って Connect Tunnel Service を実行する
- トラブルシューティング
- Connect Tunnel のクライアント インストール パッケージの展開

Connect Tunnel Service のインストール

Connect Tunnel サービスを使用する場合は、Connect Tunnel と Connect Tunnel サービスの両方をインストールします。

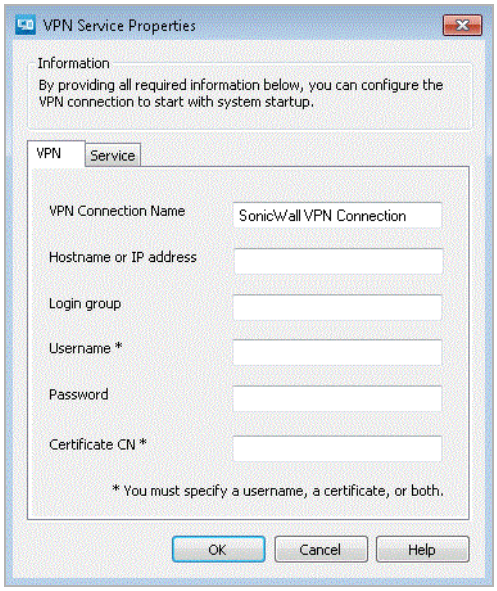
Connect Tunnel Service をインストールして設定するには:

1 AMC の [**Client Installation Packages (クライアント インストール パッケージ)**] ページ ([**Agent Configuration (エージェント設定)**] > [**Download (ダウンロード)**]) で、言語を選択してから Connect Tunnel (`ngsetup_<xx>.exe`) と Connect Tunnel サービス (`ctssetup_<xx>.exe`) の両方のインストール パッケージをダウンロードします。

2 最初に Connect Tunnel (`ngsetup_<xx>.exe`) をインストールします。「*Secure Mobile Access VPN 接続*」という名前のショートカットがデスクトップに作成されます。

3 Connect Tunnel Service (`ctssetup_<xx>.exe`) をインストールします。「*Secure Mobile Access VPN サービス オプション*」という名前のショートカットがデスクトップに作成されます。

4 デスクトップで、「**Secure Mobile Access VPN Service Options**」ショートカットをダブルクリックします。または、コントロール パネルの「**VPN Service Options (サービス オプション)**」をダブルクリックします。「**VPN Service Properties (VPN サービス プロパティ)**」ダイアログが表示されます。



5 [**VPN**] タブで、これらの設定を行います。

VPN タブの設定

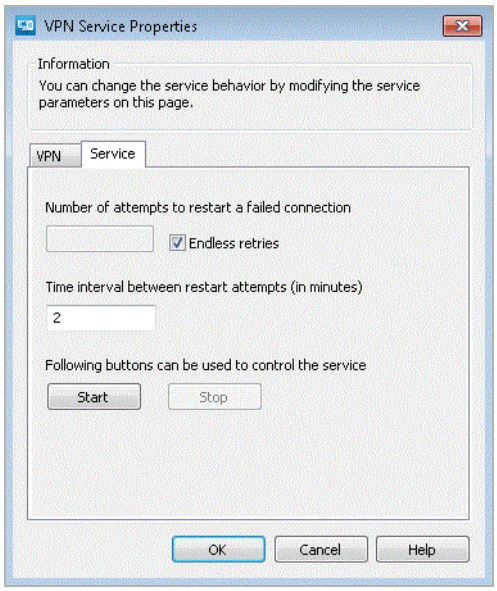
設定	説明
VPN 接続名	Connect クライアント接続オブジェクトの名前を Windows の [**Network Connections (ネットワーク接続)**] ウィンドウ ([**Start (スタート)**]|[**Connect To (接続)**]|[**Show All Connections (すべての接続の表示)**]) に表示されるとおりに入力します。デフォルトでは、「**VPN Connection (VPN 接続)**」です。
ホスト名または IP アドレス	ログインする E-Class SMA アプライアンスのホスト名または IP アドレスを入力します。
ログイン グループ	ログインするレルムの名前を入力します。
[ユーザー名とパスワード]	この**ログイン グループ** (レルム) にユーザーのクレデンシャルを入力します。

6 [**Service (サービス)**] タブで、次の設定を行います。

[Service (サービス)] タブの設定

設定	説明
失敗した接続を再開するときの試行回数	最初の接続に失敗した場合に再起動を試行する回数を指定します。
再試行する間隔	再起動を試行する間隔を分単位で指定します。

7 サービスを制御するには、[**起動**] および [**停止**] ボタンをクリックします。



8 Connect Tunnel が起動しているかどうかを確認するには、デスクトップの 「**VPN Connection (VPN 接続)**」ショートカットを開きます。確立されている接続が表示されます。または、コマンドラインで `ipconfig` コマンドを実行して、VPN 接続の仮想 IP アドレスを取得しているか確認できます。

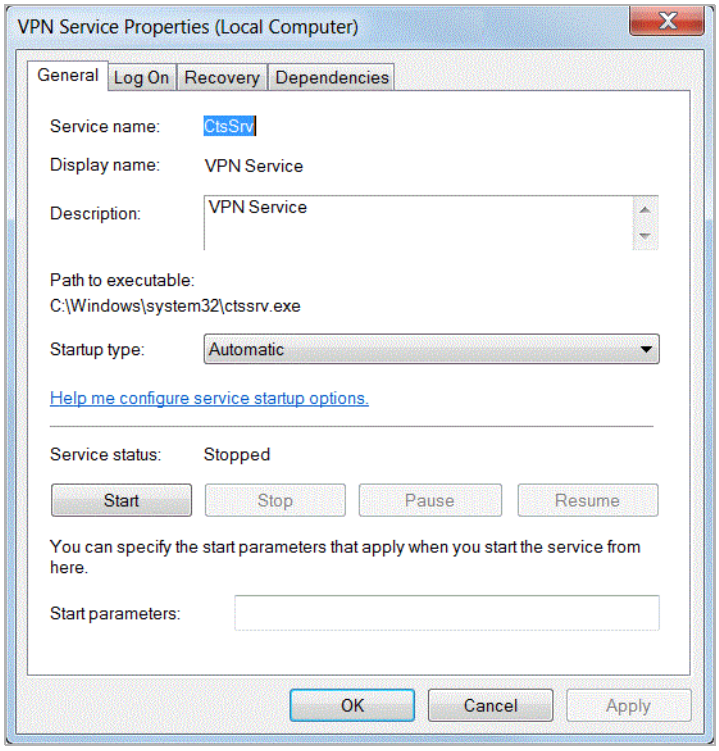
Windows サービスとスクリプトのオプション

Windows サービスを使用して、ローカルまたはリモートのコンピュータで Connect Tunnel サービスを管理できます。

Windows サービスを使って Connect Tunnel サービスを構成および実行するには

Windows サービスを使って Connect Tunnel Service を構成および実行するには

1 Windows Server プラットフォームと Connect Tunnel Service を実行しているコンピュータで、Windows サービスを実行し、[**VPN Service Properties (VPN サービスのプロパティ)**] ダイアログを開きます ([**Control Panel (コントロール パネル)**] > [**Administrative Tools (管理ツール)**] > [**Services (サービス)**] > [**VPN Service (VPN サービス)**])。



2 これらの設定を使用して、サービスを制御 (開始、停止、一時停止、再開、無効化) したり、サービスで障害が発生した場合の修復作業を設定したり、ハードウェア プロファイルのサービスを無効化します。

コマンドまたはスクリプトを使って Connect Tunnel Service を実行する

Windows の *sc.exe* ユーティリティを使用すると、コマンド プロンプトまたはバッチ ファイルでサービス コントローラ (*services.exe*) と通信できます。これにより、例えば、VPN サービスの起動とシャットダウンを自動化できます。また、ユーザーがショートカットをクリックして (クレデンシャルを意識しないで) VPN 接続を開始できるように、コマンドまたはバッチ ファイルを起動するショートカットをデスクトップに作成できます。

例えば、次のコマンドは、リモート コンピュータのサービスを起動または停止します。

```
sc \\SERVERNAME start ctssrv
sc \\SERVERNAME stop ctssrv
```

コマンドラインまたはサードパーティ製のアプリケーションから Connect Tunnel Service を起動または停止するには、次のコマンドを使用します。

```
%windir%\system32\sc.exe start ctssrv
%windir%\system32\sc.exe stop ctssrv
```

トラブルシューティング

Connect Tunnel サービスの実行に関連する情報、警告、エラー メッセージを表示するには、Windows イベント ビューア (**Control Panel (コントロール パネル) > Administrative Tools (管理ツール) > Event**

Viewer (イベントビューア) > Application (アプリケーション) > CTS) を使用します。詳細なメッセージは、サービスのログで確認します。このログのデフォルトの場所は次のとおりです。

```
%ALLUSERSPROFILE%\Application Data\SMA1000
```

メモ：アウトバンド HTTP プロキシを使ってインターネットにアクセスする環境では、認証を必要としないプロキシを使用する必要があります。そうしないと、Connect Tunnel Service のログ ファイル (ctssrv.log) に、次のエラー メッセージが表示されます。インターネットに直接アクセスできません。また、管理者権限を持つ Windows ユーザー アカウントで実行されるように Connect Tunnel Service を設定する必要があります。Secure Mobile Access クライアント セットアップ パッケージの配布

ユーザーに WorkPlace へのログインを求めることなく、Connect Tunnel クライアントのセットアップ パッケージをネットワーク上 (Web サーバー、FTP サーバー、ファイル サーバーなど) からユーザーに展開できます。

また、Connect Tunnel クライアントは、Microsoft Systems Management Server (SMS) や IBM Tivoli Configuration Manager などの構成管理アプリケーションを介してユーザーにインストール パッケージを送信できるほか、事前設定済みの Connect Tunnel のインストールが含まれているディスク イメージを配布することもできます。

クライアントの `.ini` ファイルを構成した場合は、ファイルをセットアップ プログラムとともに配布する必要があります (セットアップ プログラムのみを配布した場合、クライアントではデフォルトの設定が使用されます)。

Connect Tunnel のクライアント インストール パッケージの展開

Connect Tunnel クライアントは、`.exe` ファイルとしてインストールできるほか、Microsoft Installer (`.msi`) ファイルとしての配布や、ディスク イメージの一部としての配布が可能です。

トピック:

- .exe ファイルとして展開する
- .msi ファイルを使用して展開する
- マシンごとのインストールを指定して MSI の更新がサポートされるようにする
- ディスク イメージとして展開する

.exe ファイルとして展開する

Connect Tunnel クライアントを .exe ファイルとして展開するには

ngsetup_<xx>.exe ファイルをユーザーに配布します (*<xx>* は選択した言語を表します)。`ngsetup.ini` ファイル (Connect Tunnel クライアント用構成のカスタマイズの説明を参照) を変更した場合は、このファイルも一緒に配布します。この `.ini` ファイルを読み込むには、次のコマンドを実行して、コマンドライン パラメータとしてセットアップ プログラムに渡します。

```
ngsetup_<xx>.exe -f=<path>\<configuration file name>
```

ユーザー側の手順を簡略化するために、このパラメータを指定してセットアップ プログラムを呼び出すバッチ ファイルを作成することもできます。

.msi ファイルを使用して展開する

Connect Tunnel クライアントをこの方法でインストールする (つまり、*ngsetup_<xx>.exe* を実行しない) 場合は、インストールをユーザーごとではなくマシンごとに実行するよう Windows Installer を設定する必要があります。マシンごとのインストールを指定して MSI の更新がサポートされるようにするを参照してください(ユーザーごとのインストールでは、後に更新で必要となるレジストリ エントリが作成されません)。

.msi ファイルを使用して Connect Tunnel クライアントを展開するには

1 `.msi` インストール パッケージと変更した `ngsetup.ini` ファイル (このファイルを作成した場合) を展開するよう、構成管理ソフトウェア プログラム (Microsoft SMS や IBM Tivoli など) を設定します。

マシンごとのインストールを指定して MSI の更新がサポートされるようにする

マシンごとのインストールを指定して、インストール後の MSI の更新がサポートされるようにするには

1 AMC の [*Client Installation Packages (クライアント インストール パッケージ)*] ページから **ngsetup_<xx>.exe** をダウンロードし、次のコマンドを実行してインストール ファイルを解凍します。ファイルの解凍先は現在の作業ディレクトリになります (`expand`) パラメータで「`<path>`」を指定した場合を除く。

```
ngsetup_<xx>.exe -expand=<path>
```

2 必要に応じて `ngsetup.ini` ファイルを変更します (Connect Tunnel クライアント用構成のカスタマイズを参照)。

3 Windows Installer を実行するために、以下のコマンドを入力します。

```
msiexec.exe /i ngvpn.msi ALLUSERS=1 NGSETUP=1 CONFIGURATIONFILE=<path>\
<.ini file name>
```

ディスク イメージとして展開する

ディスクのクローンは、Windows オペレーティング システムとアプリケーションを配布するための一般的な方法です。この方法で Connect Tunnel を配布する場合は、Windows System Preparation Tool (`Sysprep.exe`) を実行して複製用のディスク イメージを作成する必要があります。Sysprep を使用しないと、コンピュータのセキュリティ ID (SID) が変更されず、Connect Tunnel の固有 ID が複製されるため、IP アドレスが競合します。ディスク イメージを作成して配布する方法の概要を以下に示します。

Connect Tunnel クライアントをディスク イメージとして展開するには

1 参照元となるシステムに Connect Tunnel for Windows をインストールし、必要に応じた構成を行います。

2 Windows System Preparation Tool を実行し、コンピュータをシャットダウンします。

3 サード パーティ製のアプリケーションまたはディスク複製ツールを使用して、マスター ディスクを複製します。

4 このディスクを配布先のコンピュータに挿入すると、ミニ セットアップによって、ユーザーに情報 (コンピュータ名など) の入力を求めるプロンプトが表示されます。この手順は「応答ファイル」(`sysprep.inf`) を作成することで自動化できます。System Preparation Tool の使用につ

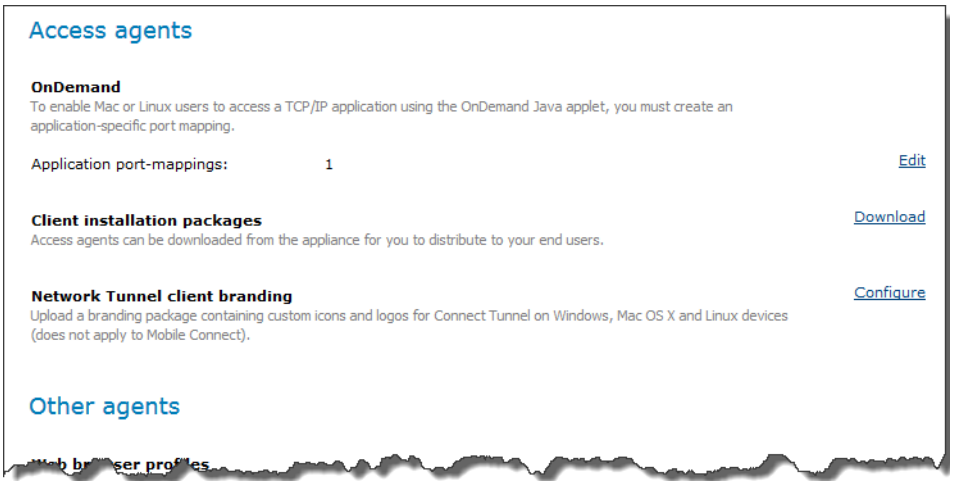
いては、以下の Microsoft の Web サイトを参照してください。
http://support.microsoft.com/kb/302577

ネットワーク トンネル クライアントのブランド

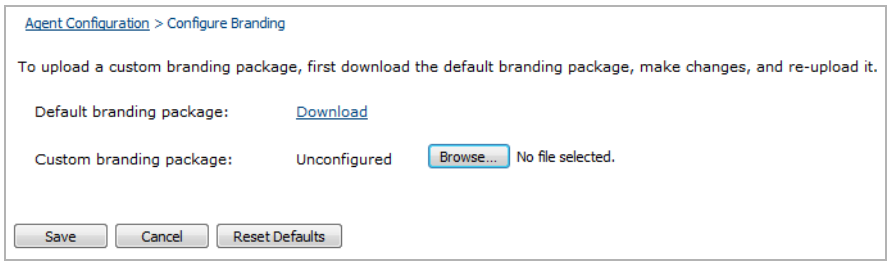
Connect Tunnel のユーザー インターフェースでは、カスタム ブランドを利用できます。この機能を利用して、企業は Connect Tunnel のウィンドウに表示される SonicWall のブランドを、独自の企業名とロゴに変更できます。Connect Tunnel のブランドは、Windows、Mac OS X、および Linux プラットフォーム上で利用でき、アプライアンスごとに設定できます。

カスタマイズしたブランド用画像とガイドラインをアップロードするには

1 メインのナビゲーション メニューの [**User Access (ユーザー アクセス)**] で [**Agent Configuration (エージェント設定)**] を選択し、[**Network Tunnel client branding (ネットワーク トンネル クライアントのブランド)**] の横にある [**Configure (設定)**] をクリックします。



2 [**Default branding package (デフォルト ブランディング パッケージ)**] の横にある [**Download (ダウンロード)**] をクリックし、ダウンロード先を選択します。



3 [**OK**] をクリックして [**Configure custom branding package (カスタム ブランディング パッケージの設定)**] ページに戻ります。

4 ダウンロードしたファイルを解凍します。このファイルには、各プラットフォーム (Windows、Linux、および Mac) 用のブランド ファイルのフォルダが含まれています。`README.txt` を参照してデフォルトのファイルをカスタムのブランド ファイルで置き換えてから、ファイルを ZIP 形式で圧縮します。

5 [**Configure custom branding package (カスタム ブランディング パッケージの設定)**] ページで、[**Browse (参照)**] ボタンをクリックしてカスタムのブランド ファイルが含まれている ZIP ファイルを選択します。

6 ファイルを保存した後で、[**Save (保存)**] をクリックします。すべての Connect Tunnel ウィンドウとアイコンが、カスタムのブランドに更新されます。

OnDemand プロキシ エージェント

OnDemand プロキシ エージェントは、TCP/IP リソースへのアクセスを提供する、安全で軽量なエージェントです。ローカルのループバック プロキシを使用し、AMC に定義されたルーティング ディレクティブに従って、保護されたネットワーク リソースに通信をリダイレクトします (UDP アプリケーションはサポートされていません)。

OnDemand プロキシ エージェントは、OnDemand Tunnel エージェントほど効果的にはスケールしないことに注意してください。OnDemand プロキシ エージェントを広範な VPN エージェントとして使用することはお勧めしません。そのため WorkPlace 経由での特定のアプリケーションへのアクセス用としてください。WorkPlace ポータル経由でアプリケーションへの広範なアクセス (同時接続ユーザー数 500 超) を提供するようなケースでは、OnDemand Tunnel エージェントを展開することをお勧めします。OnDemand Tunnel をインストールできない場合 (管理者権限関連の問題が原因の場合など) は、OnDemand プロキシを OnDemand Tunnel の代替として使用できます。そのようなシナリオでは、単一のコミュニティに OnDemand Tunnel と OnDemand プロキシの両方を構成します。

このセクションでは、OnDemand の概要とその構成および展開方法について説明します。

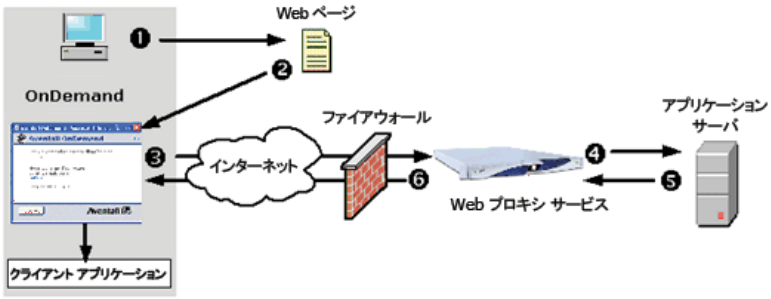
トピック:

- OnDemand プロキシについて
- OnDemand によるネットワーク トラフィックのリダイレクトの仕組み
- 特定のアプリケーションにアクセスするよう OnDemand を構成する
- OnDemand の詳細オプションの構成
- クライアントの構成

OnDemand プロキシについて

OnDemand プロキシはループバック ベースのプロキシ ソリューションで、クライアント アプリケーションとアプリケーション サーバーとの間の通信を保護します。OnDemand プロキシ接続シーケンスに接続シーケンスを示します。

OnDemand プロキシ接続シーケンス



1 ユーザーが WorkPlace にログインすると自動的に OnDemand が起動。

2 OnDemand は WorkPlace ウィンドウ内で実行。

3 OnDemand がローカルのループバック アドレス (127.0.0.1) でアプリケーションの要求を待機し、トラフィックを Web プロキシ サービスにリダイレクト。

4 Web プロキシ サービスが、アプリケーションの求めるポートを使用して、アプリケーション サーバーへのトラフィックをプロキシ。

5 アプリケーション サーバーがアプリケーションのトラフィックを Web プロキシ サービスに送信。

6 Web プロキシ サービスがアプリケーションのトラフィックを OnDemand に送信。OnDemand はこのトラフィックをクライアント アプリケーションに渡す。

OnDemand では、動的にポートを定義するアプリケーションを含め、1 つまたは複数のポートを使用する TCP アプリケーションをサポートしています (UDP ベースのアプリケーションはサポートしていません)。OnDemand を使用して一般的にアクセスされるアプリケーションをOnDemand を使用してアクセスされるアプリケーションに示します。

OnDemand を使用してアクセスされるアプリケーション

アプリケーション	例
常駐クライアント/サーバー 通常、これらのクライアント アプリケーションはローカルのクライアント コンピュータ上にインストールされます。	インターネット メール アプリケーション: • Microsoft Outlook • Outlook Express • Lotus Notes • Netscape Mail • Eudora ターミナル エミュレーション アプリケーション: • WRQ Reflection • NetManage RUMBA PC-to-Host リモート オフィス接続アプリケーション: • Citrix ICA/XenApp • Microsoft Windows Terminal Services

デフォルトでは、OnDemand はユーザーが WorkPlace へ接続すると自動的に起動するよう構成されています。パフォーマンスを最適化するために、OnDemand は初回アクセス時にユーザーのコンピュータにインストールされます。これにより、ユーザーが繰り返し使用する場合でもダウンロードを最小限に抑えられます。

トピック:

- OnDemand マップ モード
- OnDemand のアクティブ化

OnDemand マップ モード

デフォルトでは、OnDemand はユーザーが WorkPlace にログインすると自動的に起動します。マップ モードを使用すると、ユーザーは特定のアプリケーション用に構成されたショートカットをクリックできます。オプションで、ユーザーがショートカットをクリックした際に特定の Web URL を自動的に開くよう、OnDemand を構成できます。これは、OnDemand の実行時にアプリケーション (シン クライアント アプリケーションなど) を起動する場合に便利です。特定のアプリケーションへのショートカットは手動で作成する必要があります。マップ モードは、Windows、Macintosh、および Linux プラットフォームでサポートされています。

Windows PC では、ユーザーが初めて WorkPlace にログインすると、WorkPlace が自動的にそのユーザーのコンピュータに OnDemand をダウンロードしてインストールし、起動します (ユーザーの属するコミュニティがそのように処理を行うよう構成されていることが前提となります)。WorkPlace へのそれ以降のログイン時には、WorkPlace が自動的に OnDemand を起動します。

OnDemand のアクティブ化

デフォルトでは、OnDemand が有効になっている場合、OnDemand はユーザーが WorkPlace にログインすると自動的に起動し、WorkPlace ウィンドウ内で稼働します。この組み込みモードで OnDemand を使用している間、ユーザーは WorkPlace ウィンドウを開いたままにしておく必要があります。

メモ:

- ユーザーは OnDemand ウィンドウからアプリケーションを起動することはできません。ユーザーの OnDemand 起動時に自動的に開く URL が構成されている場合を除き、ユーザーは通常と同じようにアプリケーションを手動で起動する必要があります。
- ユーザーは、パーソナル ファイアウォールを構成して OnDemand のトラフィックを許可することが必要となる場合があります。

OnDemand によるネットワーク トラフィックのリダイレクトの仕組み

OnDemand ではローカルのループバック アドレスを使用して、アプライアンス経由でトラフィックをリダイレクトして保護します。このセクションでは、ループバック プロキシの概要とさまざまなリダイレクト方法について説明します。

トピック:

- 概要: ループバック プロキシ
- hosts ファイルによるリダイレクト

概要: ループバック プロキシ

OnDemand ではローカルのループバック プロキシを使用して、Web プロキシ サービス経由でアプリケーションのトラフィックを安全に送信します。例えば、アプライアンスに接続して Citrix アプリケーションを実行したい Windows ユーザーがいるとします。

1 ユーザーが WorkPlace にログインし、自動的に OnDemand が起動します。

2 OnDemand がローカルのループバック アドレスを Citrix サーバーのホスト名に動的にマップします。

3 ユーザーが Citrix アプリケーションを起動します。このアプリケーションは *citrix.example.com* への接続を試行します。OnDemand が Citrix のホスト名を `127.0.0.1` に解決し、トラフィックを Web プロキシ サービスにルーティングします。

4 OnDemand が SSL を使用して Citrix のトラフィックを暗号化し、SMA アプライアンスへ安全にルーティングします。トラフィックはこのアプライアンスによって Citrix サーバーに転送されます。

5 Citrix サーバーが応答し、SMA アプライアンス経由でデータを戻します。

6 アプライアンスが応答を OnDemand に転送します (SSL を使用)。

7 OnDemand が情報を Citrix アプリケーションに転送します。

hosts ファイルによるリダイレクト

トラフィックを送信先のサーバーにリダイレクトするには、ユーザーのコンピュータ上の hosts ファイルを変更します。このリダイレクト方法は、Windows、Macintosh、および Linux プラットフォームでサポートされます (ユーザーがローカル コンピュータの管理者権限を有している場合)。

ユーザーのシステム上の hosts ファイルを変更して、送信先のサーバーをローカルのループバック アドレスにマップします。アプリケーションがホスト名の解決を試行すると、トラフィックは OnDemand が監視しているループバック アドレスにリダイレクトされます。

Hosts ファイルに、一般的な hosts ファイル (ホスト名が IP アドレスにマップされている) と、OnDemand 用に変更された hosts ファイルの例を示します。

Hosts ファイル

一般的な Hosts ファイル

```
192.168.1.135 telnet.example.com telnet
192.168.1.140 mailhost.example.com mail
192.168.1.143 citrix.example.com citrix
```

OnDemand 用の Hosts ファイル

```
127.0.0.1 telnet.example.com telnet
127.0.0.1 mailhost.example.com mail
127.0.0.1 citrix.example.com citrix
```

メモ：OnDemand 用の hosts ファイルでは、ホスト名が、ホストの IP アドレスではなく、ローカルのループバック アドレスにマップされます。アプリケーション固有の構成では、これらのループバック アドレスを、AMC での OnDemand の構成時に指定したアドレスに対応付けます。詳細については、特定のアプリケーションにアクセスするよう OnDemand を構成するを参照してください。

特定のアプリケーションにアクセスするよう OnDemand を構成する

Windows 以外のプラットフォームのユーザーに OnDemand を展開する場合や、ユーザーが OnDemand を立ち上げた際に自動的に URL 起動機能を使用してシン クライアント アプリケーションを起動させたい場合には、AMC でアプリケーション固有の構成を定義する必要があります。この作業には、「ポート マッピング」と呼ばれる、クライアントとサーバーのポート番号のマッピングが含まれます。

トピック:

- ポート マッピングについて
- OnDemand で使用するアプリケーションの構成

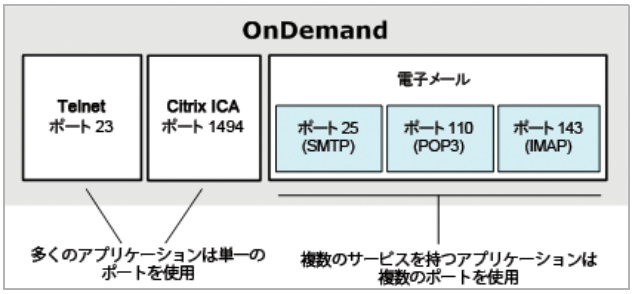
ポート マッピングについて

特定のアプリケーションのトラフィックをリダイレクトするよう OnDemand を構成するには、そのアプリケーションがクライアントとサーバーで使用しているポート番号を調べて、AMC でそれらのポートをマッピングする必要があります。OnDemand はクライアント上で特定のポートの要求の受信を監視してそれらをアプライアンスにプロキシし、このアプライアンスが情報をアプリケーション サーバーの IP アドレスとポートに転送します。

例えば、クライアントの IP アドレスとポート (*127.0.1.1:23* など) を、送信先サーバーのホストまたは IP アドレスとポート (*telneta.example.com:23*) に対して構成します。

一部のアプリケーション (電子メールなど) では、異なる複数のプロトコル用に複数のポートを使用します。この場合は、該当する複数のポートを監視するよう OnDemand を構成する必要があります。この構成は、異なる複数のアプリケーションを使用するよう OnDemand を構成する場合にも便利です。例: OnDemand の構成では、異なる 5 個のポートを使用する 3 つのアプリケーションが構成された OnDemand を示しています。

例: OnDemand の構成



この例では、OnDemand はポート 23 で telnet を監視し、ポート 1494 で Citrix を監視するよう構成されています。電子メールについては、ポート 25 (SMTP)、ポート 110 (POP3)、およびポート 143 (IMAP) で要求を監視しています。

OnDemand で使用するアプリケーションの構成

アプリケーションを構成するには、そのアプリケーションがそれぞれのサービスごとに使用しているプロトコルを調べて、クライアントのソース アドレスとポートを、送信先ホストのアドレスとポー

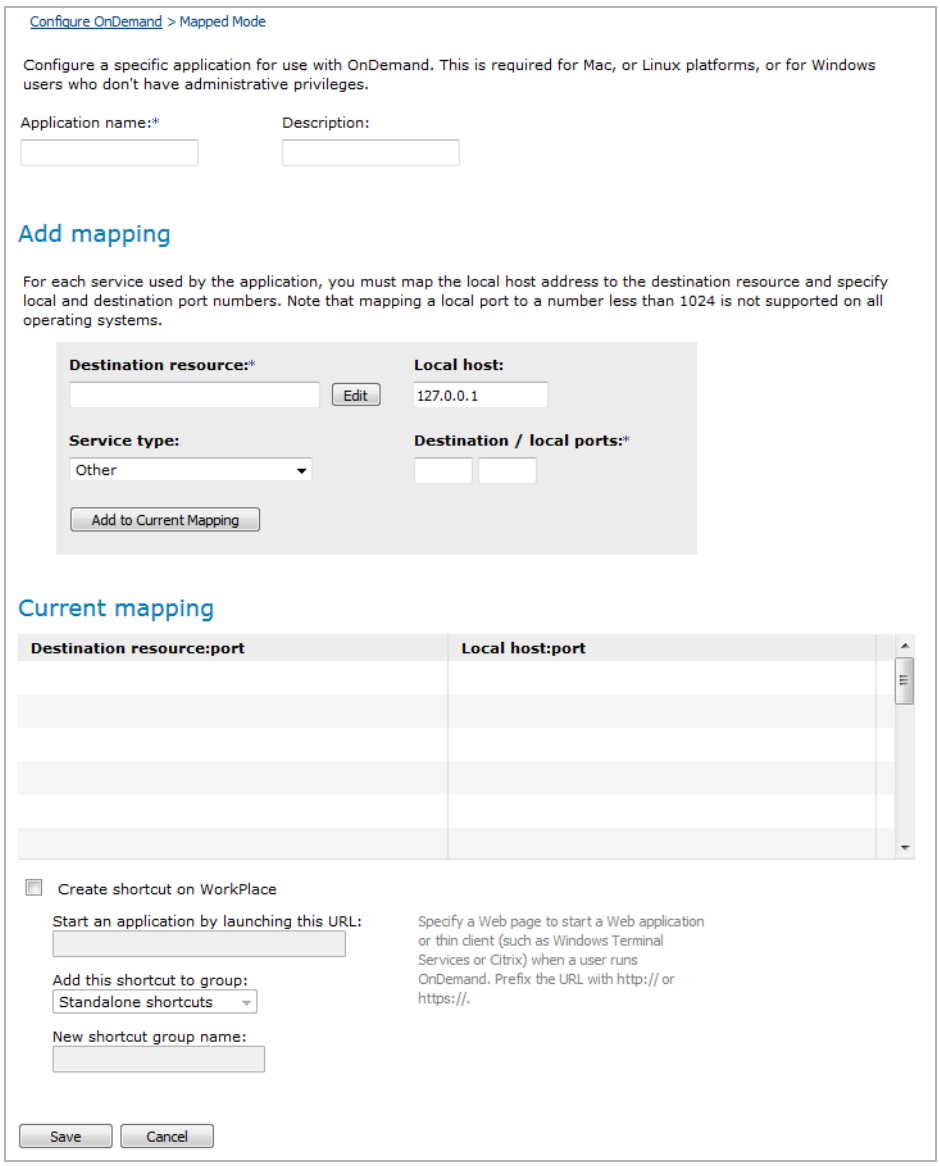
トにマッピングする必要があります。また、URL を指定して Web ページを開くこともできます。これは、ユーザーが OnDemand を起動した際に自動的にアプリケーションを起動させる場合に便利です。

OnDemand で使用するアプリケーションを構成するには

1 AMC のメイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**Agent Configuration (エージェント設定)**] をクリックします。

2 [**OnDemand**] エリアの [**Access agents (アクセス エージェント)**] で、[**Edit (編集)**] をクリックします。[**Configure OnDemand (OnDemand の設定)**] ページが表示されます。

3 [**Mapped mode (マップ モード)**] エリアで、[**New (新規)**] をクリックします。



4 [**Application name (アプリケーション名)**] フィールドに、アプリケーションに用いる名前を入力します。この名前は WorkPlace でユーザーに表示されます。短く分かりやすい名前を使用してください。

5 [**Description (説明)**] フィールドに、アプリケーションについての分かりやすいコメントを入力します。

6 [**Add mapping (マッピングの追加)**] エリアで、アプリケーションで使用する各サービスを構成します。

a [**Destination resource (送信先リソース)**] フィールドの横の [**Edit (編集)**] ボタンをクリックし、構成するネットワーク リソースを選択してから、[**Save (保存)**] をクリックします。または、[**Resources (リソース)**] ダイアログの [**New Resource (新規リソース)**] ボタンをクリックして、新しいネットワーク リソースを作成することもできます。

b IP アドレス/ポートの組み合わせが他のサービスと競合する場合は、[**Local host (ローカル ホスト)**] フィールドに表示されている IP アドレスを変更するか、後出の説明に従ってポートをマップすることができます。[**Local host (ローカル ホスト)**] の値は、アドレス空間 `127.x.y.z` 内の任意の IP アドレスに変更できます。

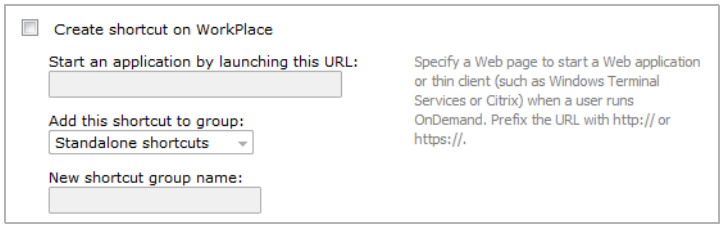
> **メモ：** MacOS では、**OnDemand**は、ローカル ホストに対して `127.0.0.1` という IP アドレスを使用している場合にのみ機能します。

c [**Service type (サービス種別)**] ドロップダウン メニューで、アプリケーションが使用するサービスのタイプを選択します。これにより、[**Destination/local ports (送信先/ローカル ポート)**] フィールドに、そのサービス用の一般的なポートが自動的に入力されます。サービスの使用するポートが送信先とローカルとで異なる場合は、必要に応じて [**Destination/local ports (送信先/ローカル ポート)**] ボックスの情報を編集してポートを互いにマッピングします。

d [**Add to Current Mapping (現在の属性に追加)**] をクリックします。[**Current mapping (現在のマッピング)**] リストにマッピングが追加されます。

7 アプリケーションが複数のサービスを使用する場合は、ステップ 6 を繰り返して各サービスを構成します。ほとんどのアプリケーションでは使用するサービスは 1 つのみですが、一部のアプリケーション (電子メールなど) では複数のプロトコルを使用するため、複数のサービスを必要とします。

8 [**Create shortcut on WorkPlace (WorkPlace 上にショートカットを作成)**] チェックボックスを選択します。



- OnDemand で Web ページを自動的に開く (シン クライアント アプリケーションを自動的に起動する場合に便利です) 場合は、そのページの URL を [**Start an application by launching this URL (開いてアプリケーションを起動する URL)**] フィールドに入力します。`http://` または `https://` のいずれかのプロトコル識別子を指定する必要があります。指定した URL は、OnDemand が読み込まれた後に新しいブラウザ ウィンドウで自動的に開きます。
- WorkPlace において、グループを設定してユーザー向けのリソースをまとめることができるほか、各ショートカットを個別に表示することもできます。[**Add this shortcut to group (このショートカットをグループに追加)**] ドロップダウン メニューで、ショートカットの追加先にする新規または既存のグループを選択します。ショートカットを個別に表示する場合は、[**Standalone shortcuts (スタンドアロンのショートカット)**] を選択します(ショートカットの表示順序は [**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページ

で変更できます。詳細については、WorkPlace レイアウトの作成または編集を参照してください)。

メモ：[Create shortcut on WorkPlace] オプションは、最初の構成時以降は [Mapped Mode] ページでのみ表示できます。このページでオプションを編集することはできません。この設定を最初に構成した後、ショートカットは AMC の [Shortcuts] ページで管理します。詳細については、WorkPlace ショートカットについての作業を参照してください。

OnDemand の詳細オプションの構成

このセクションでは、アプライアンスの外部 IP アドレスを使用してアプライアンスにアクセスする方法、および OnDemand ログにデバッグ メッセージを追加する方法について説明します。

トピック:

- アプライアンスの外部 IP アドレスを使用してアプライアンスにアクセスする
- OnDemand ログへのデバッグ メッセージの追加

アプライアンスの外部 IP アドレスを使用してアプライアンスにアクセスする

デフォルトでは、OnDemand はアプライアンスの SSL 証明書に含まれている FQDN を使用してアプライアンスにアクセスします。これは実稼働環境 (FQDN がパブリック DNS に追加される) では機能しますが、テスト環境では次のような理由から問題が生じる可能性があります。

- アプライアンスの FQDN が DNS に追加されていない。
- 環境でネットワーク アドレス変換 (NAT) を使用しているため、外部 IP アドレスがアプライアンス上の外部ネットワーク アドレスと一致しない。

いずれの場合も、外部ネットワーク インターフェースの IP アドレスを使用するよう OnDemand を構成する必要があります。

アプライアンスの外部 IP アドレスを使用するよう OnDemand を構成するには

1. AMC のメイン ナビゲーション メニューで [**Agent Configuration (エージェント設定)**] をクリックします。
2. [**Access agents (アクセスエージェント)**] エリアで、[**OnDemand**] の右側にある [**Edit (編集)**] をクリックします。[**Configure OnDemand (OnDemand の設定)**] ページが表示されます。
3. [**Advanced (詳細)**] エリアをクリックして展開し、[**Appliance FQDN or IP address (アプライアンスの FQDN または IP アドレス)**] フィールドに、外部ネットワーク インターフェースの IP アドレスを入力します。

アプライアンスを実稼働へ移行する前に、この値にアプライアンスの SSL 証明書の FQDN が含まれていることを確認します。アプライアンスの SSL 証明書を更新するたびに、AMC によってこのフィールドに FQDN が自動的に挿入されます (以前に指定された値はすべて上書きされます)。

ユーザーが初めて OnDemand を起動すると、OnDemand の実行許可を求めるセキュリティ警告が Web ブラウザに表示されます。ブラウザの構成については、Java セキュリティ警告の抑制を参照してください。

OnDemand ログへのデバッグ メッセージの追加

通常、OnDemand のログには、情報メッセージと警告メッセージのみが記録されます。デバッグ メッセージもログに記録できます。ただし、デバッグ メッセージの記録はトラブルシューティング時のみとしてください (そのようにしない場合、ログ ファイルのサイズが非常に大きくなります)。

OnDemand ログにデバッグ メッセージを追加するには

1 AMC のメイン ナビゲーション メニューで [**Agent Configuration (エージェント設定)**] をクリックします。

2 [**Access agents (アクセスエージェント)**] エリアで、[**OnDemand**] の右側にある [**Edit (編集)**] をクリックします。[**Configure OnDemand (OnDemand の設定)**] ページが表示されます。

3 [**Advanced (詳細)**] エリアをクリックして展開し、[**Enable debug OnDemand log messages (デバッグ OnDemand ログ メッセージを有効にする)**] チェック ボックスを選択します。

クライアントの構成

このセクションでは、OnDemand の利用において役立つクライアント側の構成について説明します。

トピック:

- Java セキュリティ警告の抑制
- Web ブラウザでのプロキシ サーバーの構成

Java セキュリティ警告の抑制

OnDemand の起動時に、OnDemand の実行許可を求めるセキュリティ警告が Web ブラウザに表示されます。オペレーティング システムとブラウザに応じて、さまざまな警告が表示されます。ユーザーは、OnDemand を起動するにはこの証明書を受け入れる必要があります。

OnDemand には、アプレットの有効性を保証する Java コード サイニング証明書が含まれています。Windows および Mac OS X の場合、この証明書には Thawte の Class 3 Digital ID が含まれています。

この ID は商用ソフトウェアの発行者により広く利用されています。OnDemand の起動時に毎回セキュリティのプロンプトが表示されないようにするために、ユーザーは自身のシステムで Secure Mobile Access の証明書を信頼するよう構成できます。この構成を行った後、ブラウザはそれ以降 Secure Mobile Access からダウンロードされるすべてのソフトウェアを信頼します。

Web ブラウザでのプロキシ サーバーの構成

プロキシ サーバーを介してアウトバンド接続を渡す際、OnDemand では Web ブラウザの設定を使用してプロキシ サーバーのアドレスとポートを判別します。この構成を行うには、アウトバンド プロキシ サーバーのアドレスとポートを指定するか、プロキシの自動検出を有効にするかのいずれかの方法で、ユーザーが自身の Web ブラウザを構成する必要があります。

ユーザーが自動プロキシ検出と手動でのプロキシ識別の両方を有効にしている場合、OnDemand は次の順序でプロキシ サーバーの設定をチェックします。

1 [**Automatically detect settings (設定を自動的に検出する)**] オプションが有効になっている場合、OnDemand はプロキシ サーバーの設定の自動検出を試行します。

2 プロキシ サーバーの設定を自動検出できない場合、OnDemand は[**Use automatic configuration script (自動構成スクリプトを使用する)**] オプションが有効になっているかどうかをチェックします。

3 構成スクリプトによるプロキシ サーバーの設定を検出できない場合、OnDemand はユーザーが手動で指定したプロキシ サーバーの設定を使用します。

Windows 版 Internet Explorer でプロキシの自動検出を構成するには

1 [**Tools (ツール)**] メニューの [**Internet Options (インターネット オプション)**] をクリックします。

2 [**Connections (接続)**] タブで [**LAN Settings (LAN の設定)**] をクリックします。

3 [**Automatic Configuration (自動構成)**] 内で、次のいずれかまたは両方のオプションを有効にします。

- プロキシ サーバーの設定を自動検出するには、[**Automatically detect settings (設定を自動的に検出する)**] チェックボックスを選択します(このオプションは、Microsoft Virtual Machine が含まれた Internet Explorer を実行しているユーザーでのみサポートされます)。
- 構成ファイルに含まれている構成情報を使用するには、[**Use automatic configuration script (自動構成スクリプトを使用する)**] チェックボックスを選択し、[**Address (アドレス)**] フィールドに構成ファイルの URL またはパスを入力します。

Windows 版 Internet Explorer でプロキシ サーバーの設定を手動で指定するには

1 [**Tools (ツール)**] メニューの [**Internet Options (インターネット オプション)**] をクリックします。

2 [**Connections (接続)**] タブで [**LAN Settings (LAN の設定)**] をクリックします。

3 [**Proxy Server (プロキシ サーバー)**] 内で、[**Use a proxy server (プロキシ サーバーを使用する)**] チェックボックスを選択して、IP アドレスとポートを指定します。

プロトコルごとに異なるプロキシ サーバーを使用する場合は、[**Advanced (詳細設定)**] をクリックして必要な情報を指定します。必ず、[**HTTP**] と [**Secure (保護)**] の両方にプロキシ サーバーを指定してください。

△ **注意：[ローカル エリア ネットワーク (LAN) の設定] ダイアログ ボックスで、自動設定のいずれか ([設定を自動的に検出する] または [自動構成スクリプトを使用する]) を有効にすると、プロキシ サーバーの設定が上書きされる可能性があります。これら 2 つのチェック ボックスをオフにして、プロキシの検出が正常に機能するようにしてください。**

アクセス サービスの管理

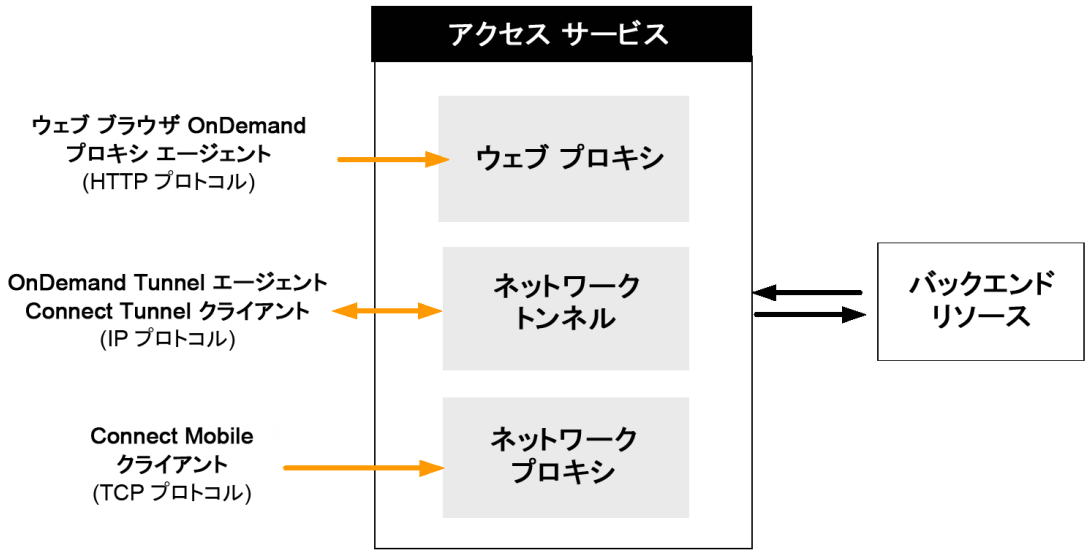
このセクションでは、アクセス サービスの概要と、サービスの開始、停止、および構成方法について説明します。

トピック:

- アクセス サービスについて
- Secure Mobile Access サービスの停止と開始
- ネットワーク トンネル サービスの構成
- IP アドレス プールの構成
- Web リソースのフィルタリングの構成
- カスタム接続の構成

- 代替サーバーの構成
- Web プロキシ サービスの構成
- Android アプリケーションのアクセス制御 - 任意のバージョンを許可する

アクセス サービスについて



ユーザーは、SMA アプライアンスによって保護されている VPN リソースに、3 つの主な方法 (アクセス サービス) を使用してアクセスできます。このセクションでは、各アクセス サービスと、それらがアクセスを提供するリソースのタイプについて説明します。

- **ネットワーク トンネル サービス**はネットワーク ルーティング技術の 1 つで、非 TCP プロトコル (VoIP や ICMP、逆方向接続プロトコル、双方向プロトコル (例: リモート ヘルプ デスク アプリケーションで使用) など) を使用するアプリケーションなどの、広範なクライアント/サーバー アプリケーションに安全なネットワーク トンネル アクセスを提供します。このサービスは、Connect Tunnel クライアントや OnDemand Tunnel エージェントと連動して、アクセスの認証と暗号化を提供します。ネットワーク トンネル サービスでは、ファイアウォールや NAT デバイスの他、従来型の VPN デバイスと干渉する可能性があるプロキシ サーバーもトラバースできます。

  ネットワーク トンネル サービスで Web リソースのフィルタリングが有効になっている場合、トンネル セッションのポリシーでは、IP ベースのルールに加えて URL ベースのルールを使用できます。

- **WorkPlace サービス**は、Web ブラウザからのネットワーク ファイル共有へのアクセスを制御します。WorkPlace サービスは、Server Message Block (SMB) ファイル共有プロトコルを使用して、Windows ファイル サーバーおよびネットワーク共有 (Microsoft 分散ファイル システム (DFS) リソースを含む) と通信します。WorkPlace サービスの構成については、WorkPlace の一般設定の構成を参照してください。

SMA アクセス サービスとユーザー アクセス コンポーネントの関係に、Secure Mobile Access アクセス サービスと、各サービスにより制御されるユーザー アクセス コンポーネントとの関係を示します。

SMA アクセス サービスとユーザー アクセス コンポーネントの関係

サービス	ユーザー アクセス コンポーネント	説明
ネットワーク トンネル サービス	• OnDemand Tunnel エージェント • Connect Tunnel クライアント	• ネットワーク トンネル クライアントからの TCP/IP および非 TCP (VoIP や ICMP など) 接続を管理します。 • あらゆるリソースへのネットワーク レベルのアクセスを提供することで、事実上、ユーザーのコンピュータをネットワーク上のノードにします。 • マッピングされたネットワーク ドライブ、ネイティブの電子メール クライアント、および逆方向接続 (VoIP など) を行うアプリケーションのサポートを含みます。
Web プロキシ サービス	• Web プロキシ エージェント • 変換 Web アクセス • カスタム ポート マッピング Web アクセス • カスタム FQDN マッピング Web アクセス	• Web ブラウザからの HTTP および TCP/IP 接続を管理します。
WorkPlace サービス	• WorkPlace ポータル	• あらゆる Web ブラウザから利用できる Web ベースのポータルを提供します。 • ファイル システム リソースへのアクセスを提供します。 • あらゆるユーザー アクセス コンポーネントをインストールおよび展開します。

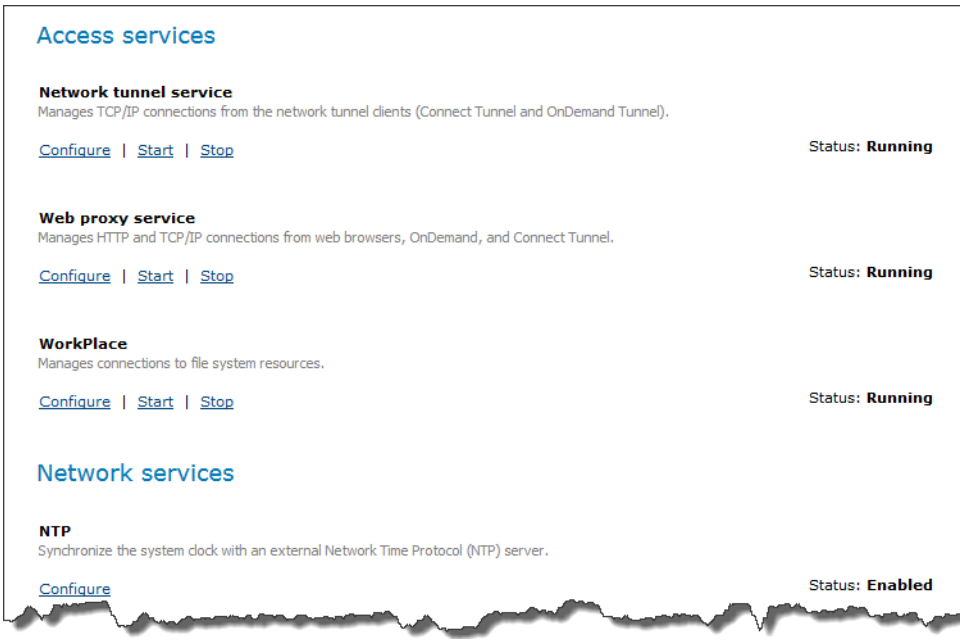
Secure Mobile Access サービスの停止と開始

Secure Mobile Access サービスのいずれかを一時的に停止することが必要となる場合があります。

△ **注意：SonicWall のサービスの停止は、計画的な保守期間中またはオフ ピーク時にのみ行うようお勧めします。また、ユーザーに対して、サービスの停止を事前に警告する必要があります。**

サービスを起動または停止するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。



2 [**Access Services (アクセス サービス)**] の下で、該当するリンクをクリックします。

- [**Stop (停止)**] をクリックするとサービスを停止します。既存のユーザー接続はすべて切断されます。
- [**Start (起動)**] をクリックするとサービスを起動します。

ネットワーク トンネル サービスの構成

ネットワーク トンネル サービスは、Connect Tunnel クライアントおよび OnDemand Tunnel エージェントからのアクセスを制御します。ネットワーク トンネル クライアントをユーザーに展開するには、まず、コミュニティに対して 1 つ以上の IP アドレス プールを用意する必要があります。ネットワーク トンネル サービスの構成には、クライアントへの IP アドレスの割り当てに使用する IP アドレス プールのセットアップが必要です。これらの IP アドレスは VPN 接続でのクライアントのエンド ポイントとなります。

また、ネットワーク トンネル サービスの構成では、Web リソースのフィルタリングを有効にして、管理者が ExtraWeb に定義したものと同じ URL ベースのルールをトンネル セッションに適用することもできます。Web リソースのフィルタリングを使用して、Web アプリケーションのアクセス時にシングル サインオン機能を利用することもできます。

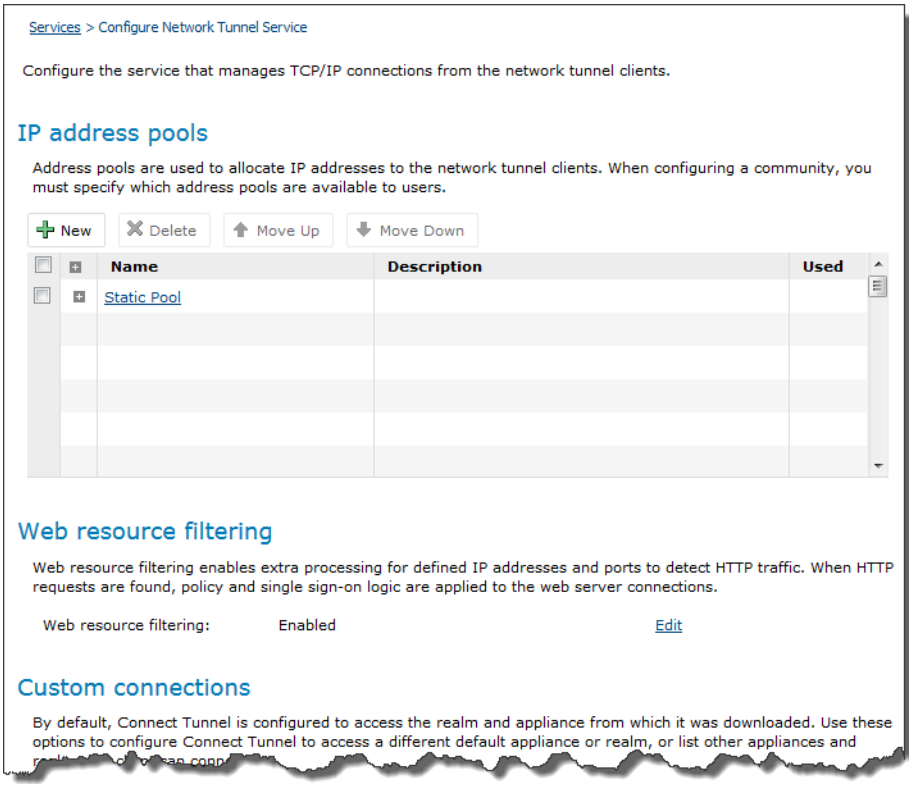
カスタム接続を追加して、別のデフォルト アプライアンスまたはレルムにアクセスするよう Connect Tunnel を構成したり、当該クライアントから接続可能な他のアプライアンスやレルムのリストを表示するよう Connect Tunnel を構成することができます。デフォルトでは、Connect Tunnel は、自身のダウンロード元のレルムとアプライアンスにアクセスするよう構成されます。

また、代替サーバーを設定しておき、接続障害時に接続するサーバーのリストをネットワーク トンネル クライアントに提示できます。

ネットワーク トンネル サービスを構成するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] の [**Network tunnel service (ネットワーク トンネル サービス)**] エリアで、[**Configure (設定)**] をクリックします。[**Configure Network Tunnel Service (設定ネットワーク トンネル サービス)**] ページが表示されます。



3 [**IP address pools (IP アドレス)**] エリアで、IP アドレス プールを 1 つ以上作成します。詳細については、IP アドレス プールの構成を参照してください。

4 Web リソースのフィルタリングを有効にして構成するには、[**Web resource filtering (Web リソースのフィルタリング)**] エリアの [**Edit (編集)**] をクリックします。詳細については、Web リソースのフィルタリングの構成を参照してください。

5 カスタム接続を構成して、Connect Tunnel が現在または別のデフォルト アプライアンスやレルムにアクセスできるようにしたり、クライアントから接続可能な他のアプライアンスとレルムのリストを表示できるようにするには、[**Custom Connections (カスタム接続)**] エリアの [**New (新規)**] ボタンをクリックします。詳細については、カスタム接続の構成を参照してください。

6 接続障害時にネットワーク　トンネル　クライアントが接続できる代替サーバーを構成するには、[**Fallback servers (代替サーバー)**] エリアの [**New (新規)**] ボタンをクリックします。詳細については、代替サーバーの構成を参照してください。

IP アドレス プールの構成

IP アドレス プールは、ネットワーク トンネル クライアントへの IP アドレスの割り当てに使用されます。ユーザーが Connect Tunnel クライアントまたは OnDemand Tunnel エージェントを使用して接続する際、SMA アプライアンスによって、構成されているいずれかのアドレス プールからクライアント

に IP アドレスが割り当てられます。割り当てには、クライアントのコミュニティで許可されているプールのみが使用されます。コミュニティへどのように IP アドレスが割り当てられるかについては、IP アドレスの割り当てを参照してください。

IP アドレス プールの編集および削除については、AMC でのオブジェクトの追加、編集、コピー、削除を参照してください。

トピック:

- アドレス プールの割り当て方法
- IP アドレス プールの構成のためのベスト プラクティス
- 変換 IP アドレス プールの追加
- ダイナミック IP アドレス プールの追加
- 動的 RADIUS 割り当て IP アドレス プールの追加
- スタティック IP アドレス プールの追加

アドレス プールの割り当て方法

IP アドレスは、次のいずれかの方法で割り当てられるよう構成できます。

- 変換アドレス プール (Secure NAT)
- ルーテッド アドレス プール (DHCP)
- RADIUS 割り当てアドレス プール
- スタティック アドレス プール

変換アドレス プール (Secure NAT)

変換アドレス プールでは、アプライアンスがルータブルでない IP アドレスをクライアントに割り当て、安全なネットワーク アドレス変換 (Secure NAT) を使用して、これを、バックエンド トラフィック用に構成されている単一アドレスに変換します。アプライアンスは AMC で指定されたネーム サーバーを使用して、クライアント上に DNS と WINS の設定を定義します。Secure NAT では、クライアントのルータブルでないソース アドレスを、内部ネットワークのルータブルでない固定のシーケンス (2.0.0.2〜2.255.254.254) から単一の構成済みのアドレスに変換します。

変換アドレス プールを利用するメリットは次のとおりです。

- Secure NAT アドレス プールで必要となるのは、バックエンド アドレス 1 つのみです。このアドレスがすべてのリモート接続で共有されます。
- トンネル クライアント用に必要な IP アドレスが少なくて済みます。

このタイプのプールにおける制限は次のとおりです。

- すべてのネットワーク動作をクライアント側から始動する必要があります。そのため、この IP アドレス割り当て方法では、逆方向接続や相互接続を行うアプリケーション (SMS、VoIP、FTP など) がサポートされません。
- Windows ドメインの参照はサポートされません。ユーザーがネットワーク エクスプローラまたはネットワーク全体から Windows ドメインを参照しようとすると、リソースへのアクセスが認められていないことを示すエラー メッセージが表示されます。
- クライアント間の相互接続はサポートされません。

ルーテッド アドレス プール (DHCP)

ルーテッド アドレス プールでは、IP アドレスが DHCP サーバーからトンネル クライアントに動的に割り当てられます。DHCP アドレス プールの特徴は次のとおりです。

- 新しいリモート クライアントをサポートするための十分な予備アドレスの容量を持つ外部サーバーを必要とします。これらのプールは簡単に設定して維持することができ、またクライアントのアクティビティにほとんど制約を与えません。
- 逆接続および相互接続もサポートされますが、クライアントの IP アドレスが既知である必要があります。必要な場合は、DHCP サーバー上で DHCP クライアント ID を構成することによって、特定のクライアントに固定の DHCP アドレスを割り当てることもできます。クライアント ID はクライアントの構成時に生成されます。個別の ID を確認するには、DHCP サーバーのログを参照してください。

RADIUS 割り当てアドレス プール

一部のアプリケーションでは、割り当てられた IP アドレスとユーザーとの間に 1 対 1 の関係を必要とします。これは RADIUS サーバーによってサポートするのが最善です。RADIUS サーバーでは、認証の一環として、許可プロセス中に IP アドレスの割り当てが行われます。

この厳格な 1 対 1 の関連付けにより、次のような意図しない影響が生じる場合があります。

- 例えば、従業員が職場でアプライアンスにログインし、ログアウトし忘れている場合、自宅からログインしようとすると失敗します。IP アドレスは職場での最初のトンネル接続に関連付けられたままとなっています。オプションで、RADIUS サーバーを参照するコミュニティとレルムを AMC で構成して、RADIUS プールが枯渇している場合は他の IP アドレス プールを使用させることができます。
- 同じ RADIUS サーバーに対して認証を行うアプライアンスが 2 台あり、その両方が RADIUS プールを使用している場合、重複するアドレスの割り当てが行われて、その結果、複数のネットワーク競合が発生します。

スタティック アドレス プール

スタティック アドレス プールを使用すると、1 つまたは複数の静的 IP アドレス プールを指定することで、そこから IP アドレスがトンネル クライアントに割り当てられるようになります。スタティック IP アドレス プールをサブネットまたはアドレス範囲として構成することもできます。スタティック アドレス プールの特徴は次のとおりです。

- スタティック アドレス プールでは、アプライアンスの外部で構成作業を行う必要がなく、逆接続および相互接続もサポートされます。
- スタティック プールでは、同時リモート接続に対して 1 つずつバックエンド アドレスを識別する必要があります。(同時接続だけでなく) すべてのリモート クライアントをまかなえるだけの十分なアドレスがあり、アドレス衝突が発生していない場合、同じクライアントに通常同じアドレスが割り当てられるため、この方法は最も安定した方法になります。
- スタティック プールでは、トンネル接続が確立されている限り IP アドレスを割り当てたままにします。トンネルが切断された場合、切断から 2 分間、そのアドレスは同じクライアントにのみ再割り当て可能な状態に置かれます。2 分の経過後、そのアドレスはあらゆるクライアントに割り当て可能になります。アドレスの再割り当ては LRU (Least Recently Used) 方式で実行されます。
- Windows ドメインの参照がサポートされます。

IP アドレス プールの構成のためのベスト プラクティス

IP アドレス プールを構成するとき、次の点に留意する必要があります。

- アドレスが重複しないようにします。
  - スタティック IP アドレス プールを構成するときは、他のネットワーク リソースにすでに割り当てられている IP アドレスは指定しないでください。
  - ネットワーク トンネル クライアントが使用するよう構成している IP アドレスは、クライアント ネットワークですでに使用されている IP アドレスと競合する可能性があります。可能な限り、ユーザーのネットワークで使用されていることがわかっている IP アドレスは構成しないでください。
  - 変換 (Secure NAT) IP アドレス プールを構成するとき、内部インターフェースのサブネットで未使用のアドレスを必ず指定するようにしてください。
  - 複数のアプライアンスで RADIUS プールを使用しており、かつ、それらのアプライアンスが同一の RADIUS サーバーに対して認証を行う場合は、重複するアドレスの割り当てが発生します。
- ダイナミック DHCP またはスタティック IP アドレス プールを構成するとき、最大数の同時ユーザーに対応できるだけの、十分な IP アドレスがあることを確認します。例えば、同時ユーザーの最大数が 100 の場合、100 以上の IP アドレスが使用可能でなければなりません。

変換 IP アドレス プールの追加

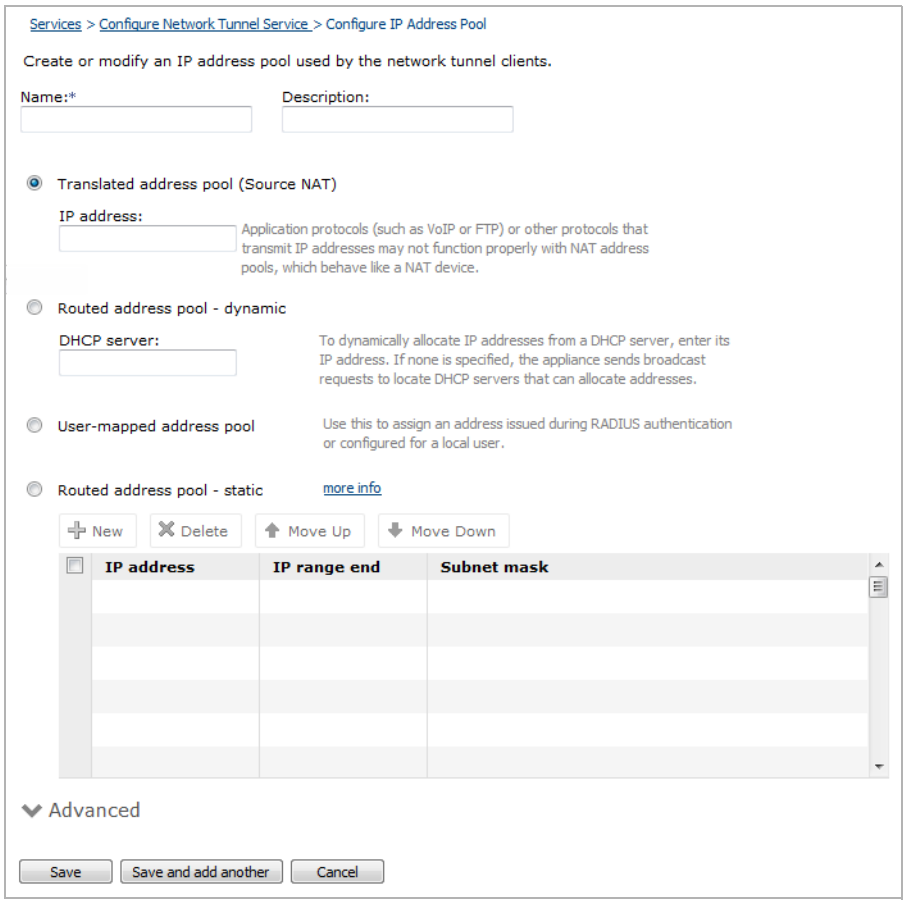
このセクションでは、セキュア ネットワーク アドレス変換 (Secure NAT) を使用して、変換 IP アドレス プールを作成する方法について説明します。

変換 IP アドレス プールを追加するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] の [**Network tunnel service (ネットワーク トンネル サービス)**] エリアで、[**Configure (設定)**] をクリックします。[**Configure Network Tunnel Service (設定ネットワーク トンネル サービス)**] ページが表示されます。

3 [**IP address pools (IP アドレス)**] エリアで、[**New (新規)**] をクリックします。[**Configure IP Address Pool (設定 IP アドレス プール)**] ページが表示されます。



4 [**Name (名前)**] フィールドにアドレス プールの名前を入力します。

5 [**Description (説明)**] フィールドに、アドレス プールについての分かりやすいコメントを入力します。

6 **Translated address pool (Source NAT) [変換アドレス プール (Secure NAT)]** をクリックします。

7 [**IP address (IP アドレス)**] フィールドに、すべてのクライアント トラフィックのソースとしてバックエンド サーバーに提示される Secure NAT アドレスを入力します。この IP アドレスが他の場所で使用されていないことを確認します。

8 [**Save (保存)**] を選択します。

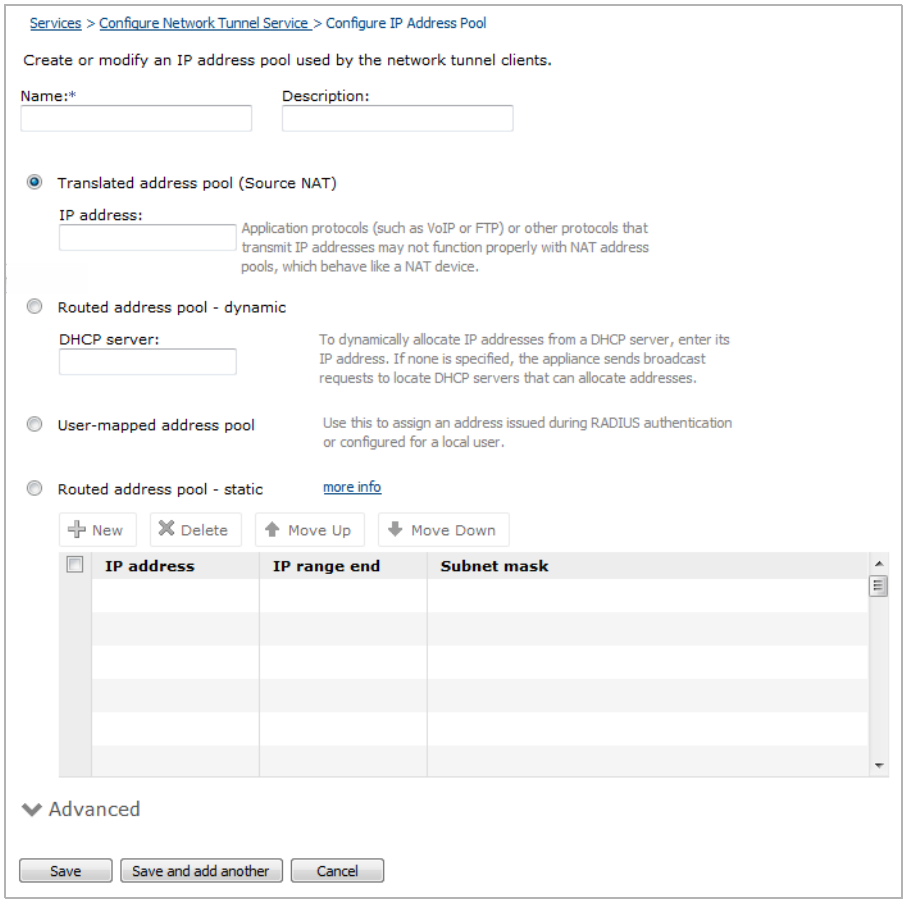
ダイナミック IP アドレス プールの追加

ダイナミック IP アドレス プールを追加するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] の [**Network tunnel service (ネットワーク トンネル サービス)**] エリアで、[**Configure (設定)**] をクリックします。[**Configure Network Tunnel Service (設定ネットワーク トンネル サービス)**] ページが表示されます。

3 [**IP address pools (IP アドレス)**] エリアで、[**New (新規)**] をクリックします。[**Configure IP Address Pool (設定 IP アドレス プール)**] ページが表示されます。



4 [**Name (名前)**] フィールドにアドレス プールの名前を入力します。

5 [**Description (説明)**] フィールドに、アドレス プールについての分かりやすいコメントを入力します。

6 [**Routed address pool - dynamic (ルーテッド アドレス プール - 動的)**] をクリックします。

7 [**DHCP server (DHCP サーバー)**] フィールドはデフォルトで空欄となっています。その場合、アプライアンスが、DHCP サーバーを探すためのブロードキャスト要求を送信し、見つかったサーバーを使用してアドレスを割り当てます。このボックスは、特定の DHCP サーバーを構成する必要がある場合を除き、空欄のままにしておきます。

8 [**Save (保存)**] を選択します。(DHCP アドレス プールは、この AMC ページの [**Advanced (詳細)**] 設定を無視します)。

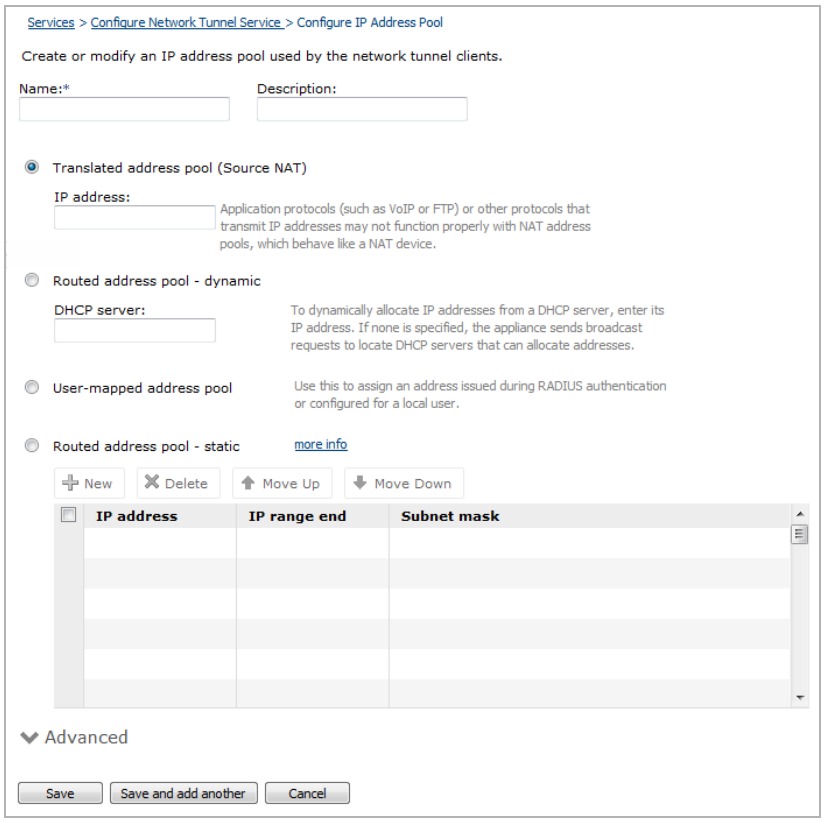
動的 RADIUS 割り当て IP アドレス プールの追加

RADIUS 割り当て IP アドレス プールを追加するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] の [**Network tunnel service (ネットワーク トンネル サービス)**] エリアで、[**Configure (設定)**] をクリックします。[**Configure Network Tunnel Service (設定ネットワーク トンネル サービス)**] ページが表示されます。

3 [**IP address pools (IP アドレス)**] エリアで、[**New (新規)**] をクリックします。[**Configure IP Address Pool (設定 IP アドレス プール)**] ページが表示されます。

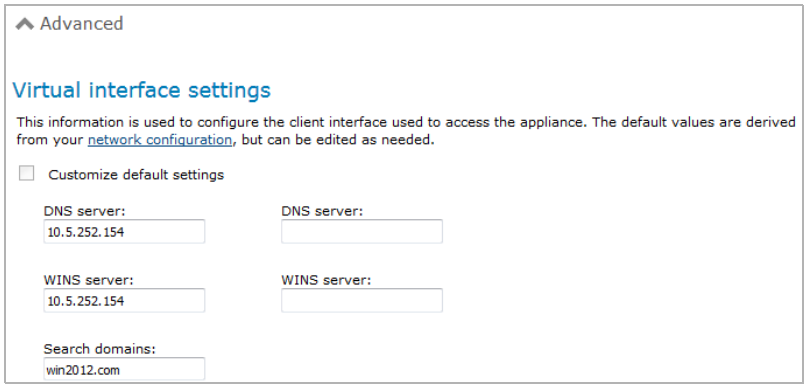


4 [**Name (名前)**] フィールドにアドレス プールの名前を入力します。

5 [**Description (説明)**] フィールドに、アドレス プールについての分かりやすいコメントを入力します。

6 [**RADIUS-assigned - dynamic (RADIUS 割り当て済み - 動的)**] をクリックしてプールを構成します。RADIUS サーバーでは、認証の一環として、許可プロセス中に IP アドレスの割り当てが行われます。この設定は、割り当てられた IP アドレスとユーザーとの間に 1 対 1 の関係を必要とするアプリケーションがある場合などに選択します。

7 (オプション) クライアント インターフェースを構成するために仮想インターフェースの設定を変更する場合は、[**Advanced (詳細設定)**] エリアをクリックして展開します。[**Virtual interface settings (仮想インターフェース設定)**] では、[**DNS server (DNS サーバ)**]、[**WINS server (WINS サーバ)**]、[**Search domains (検索ドメイン)**] が、[**Network Settings (ネットワーク設定)**] ページで定義されているのと同じ値であらかじめ構成されています。(詳細については、基本ネットワーク設定の構成を参照してください。)これらの設定を変更するには、[**Customize default settings (デフォルト設定のカスタマイズ)**] チェックボックスを選択してから、変更したい設定に対して適切な値を指定します。



8 [**Save (保存)**] を選択します。

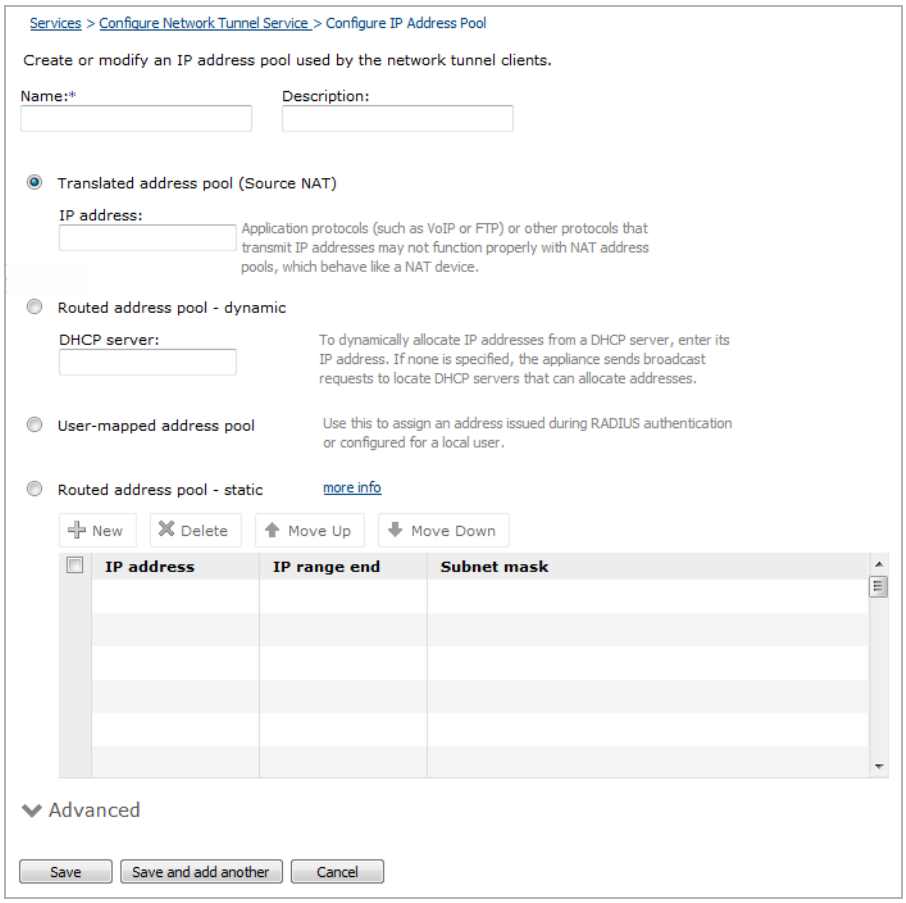
スタティック IP アドレス プールの追加

スタティック IP アドレス プールを追加するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] の [**Network tunnel service (ネットワーク トンネル サービス)**] エリアで、[**Configure (設定)**] をクリックします。

3 [**IP address pools (IP アドレス)**] エリアで、[**New (新規)**] をクリックします。[**Configure IP Address Pool (設定 IP アドレス プール)**] ページが表示されます。



4 [**Name (名前)**] フィールドにアドレス プールの名前を入力します。

5 [**Description (説明)**] フィールドに、アドレス プールについての分かりやすいコメントを入力します。

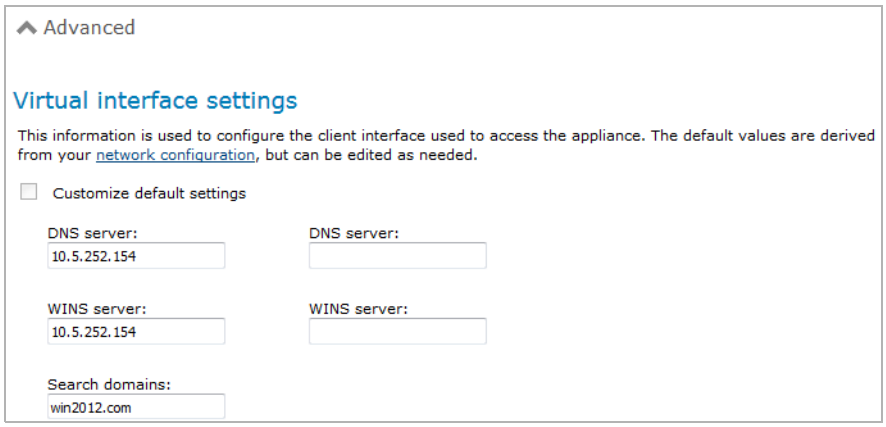
6 [**Routed address pool - static (ルーテッド アドレス プール - 静的)**] をクリックし、[**New (新規)**] をクリックします。

7 トンネル クライアントが使用できる IP アドレスを指定します。IP アドレスとサブネット マスクを、ドット区切りの 10 進数形式 (*n.n.n.n*) で入力します。

- 単一のホストを定義するときは、[**IP address (IP アドレス)**] にその IP アドレスを入力し、[**Subnet mask (サブネット マスク)**] に「255.255.255.255」を指定します。
- IP アドレスを範囲で指定するときは、[**IP address (IP アドレス)**] フィールドに開始アドレスを入力し、[**IP range end (IP アドレス範囲の終了)**] フィールドに終了アドレスを入力して、[**Subnet mask (サブネット マスク)**] を指定します。
- 完全なサブネットを定義するには、[**IP address (IP アドレス)**] フィールドにネットワーク アドレスを入力して、[**Subnet mask (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。サブネット マスクは、ある範囲に変換され、対応する値が入れられます。サブネットの IP アドレスが入力されている場合、それがネットワーク内の最初の使用可能アドレスに変換されますが、サブネットの真ん中のアドレスがそのまま使用されます。終了アドレスには、サブネットの最大の使用可能アドレスが入ります。

8 [**OK**] を選択します。このプールが、使用可能な IP アドレス プールのリストに追加されます。

9 (オプション) クライアント インターフェースを構成するために仮想インターフェースの設定を変更する場合は、[**Advanced (詳細設定)**] エリアをクリックして展開します。[**Virtual interface settings (仮想インターフェース設定)**] では、[**DNS server (DNS サーバ)**]、[**WINS server (WINS サーバ)**]、[**Search domains (検索ドメイン)**] が、[**Network Settings (ネットワーク設定)**] ページで定義されているのと同じ値であらかじめ構成されています。(詳細については、基本ネットワーク設定の構成を参照してください。)これらの設定を変更するには、[**Customize default settings (デフォルト設定のカスタマイズ)**] チェックボックスを選択してから、変更したい設定に対して適切な値を指定します。



10 [**Save (保存)**] を選択します。

Web リソースのフィルタリングの構成

Web リソースのフィルタリングを使用すると、定義された IP アドレスとポートに対して追加処理を実行して、HTTP トラフィックを検出できます。HTTP 要求が検出されると、Web サーバーの接続に対してポリシーとシングル サインオン ロジックが適用されます。

Web リソースのフィルタリングを使用すると、管理者が ExtraWeb に定義したものと同じ URL ベースのルールをトンネル セッションに適用できます。また、Web アプリケーションへのアクセス時にシングル サインオン機能を利用することもできます。

Web リソースのフィルタリングが有効になっていない場合、Web アクセスとトンネル アクセスで利用できるポリシーは同じではありません。Web アクセスの場合は、Web プロキシおよびポート マップ クライアントのすべての変換アクセスと HTTP アクセスについて、URL ポリシーを評価できます。トンネル経由で接続しているユーザーの場合、IP レイヤのリダイレクションは IP アドレスに基づくポリシーのみを許可します。複数の Web アドレスまたは名前空間が単一の Web サーバーでホストされている導入環境では、すべての Web コンテンツが、単一の IP アドレスまたはアドレス プールでアクセス可能です。IP レイヤのみをベースとしたポリシーでは、管理者が複数の名前空間の間でポリシーを区別することはできません。Web リソースのフィルタリングを有効にすると、トンネル セッションに対して、ポリシーで IP ベースのルールに加えて URL ベースのルールも使用できるようになります。

Web リソースのフィルタリングを構成するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] エリアで、[**Network tunnel service (ネットワーク トンネル サービス)**] の下の [**Configure (設定)**] をクリックします。

3 [**Web resource filtering (Web リソースのフィルタリング)**] エリアで、[**Edit (編集)**] をクリックします。[**Configure Tunnel Web Policy (設定 Tunnel Web ポリシー)**] ページが表示されます。

4 [**Enable web resource filtering (ウェブ リソースのフィルタリングを有効にする)**] チェック ボックスを選択して、トンネル サービスにおいて、Web ネットワークのトラフィックを含んでいる可能性のあるポートですべてのクライアント トラフィックをチェックさせます。

5 [**Save (保存)**] を選択します。

カスタム接続の構成

デフォルトでは、Connect Tunnel は、自身のダウンロード元のレルムとアプライアンスにアクセスするよう構成されます。カスタム接続のオプションを追加することにより、別のデフォルト アプライアンスまたはレルムにアクセスするよう Connect Tunnel を構成できるほか、クライアントから接続可能な他のアプライアンスやレルムのリストを表示するよう Connect Tunnel を構成することもできます。

カスタム接続を構成するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

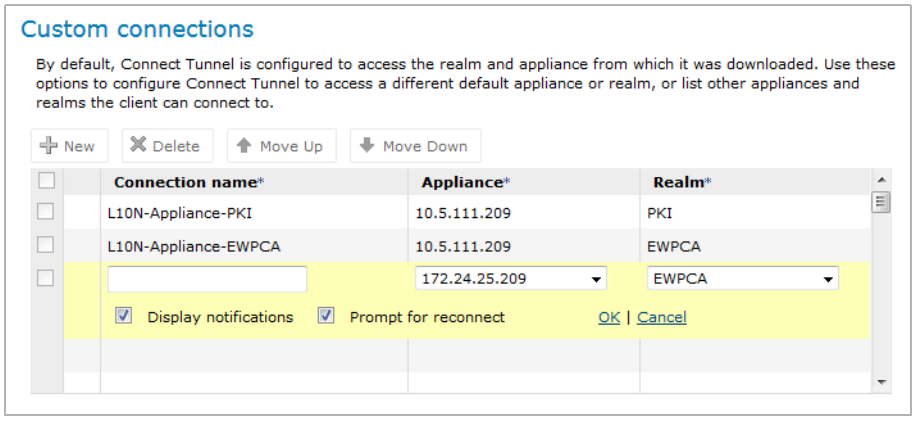
2 [**Access services (アクセス サービス)**] エリアで、[**Network tunnel service (ネットワーク トンネル サービス)**] の下の [**Configure (設定)**] をクリックします。

3 [**Custom Connections (カスタム接続)**] エリアで、[**New (新規)**] をクリックしてカスタム接続を追加します。

4 接続の種別を選択します。

- このアプライアンスへの接続
- 別のアプライアンスへの接続

[**Custom connections (カスタム接続)**] テーブルに、接続名、アプライアンス、およびレルムのフィールド (編集可能) が表示されます。



5 [**Connection name (接続名前)**] フィールドに、このカスタム接続に付ける分かりやすい名前を入力します。

6 [**Appliance (装置)**] フィールドに、アプライアンスの FQDN または IP アドレスを入力します。

7 [**Realm (レルム)**] フィールドに、レルム名を入力します。

8 このカスタム接続の使用時に通知を表示する場合は、[**Display notifications (通知を表示)**] チェックボックスを選択します。

9 切断時にユーザーにこのカスタム接続への再接続のプロンプトを表示する場合は、[**Prompt for reconnect (再接続のプロンプトを表示)**] チェックボックスを選択します。

10 [**OK**] を選択します。

11 複数のカスタム接続がリストされている場合に、接続の順序を変更するには、カスタム接続の横にあるチェック ボックスを選択してから [**Move Up (上に移動)**] または [**Move Down (下に移動)**] をクリックします。新しい順序でリストが更新されます。

12 カスタム接続を削除するには、その接続の横にあるチェック ボックスを選択してから [**Delete (削除)**] をクリックします。

代替サーバーの構成

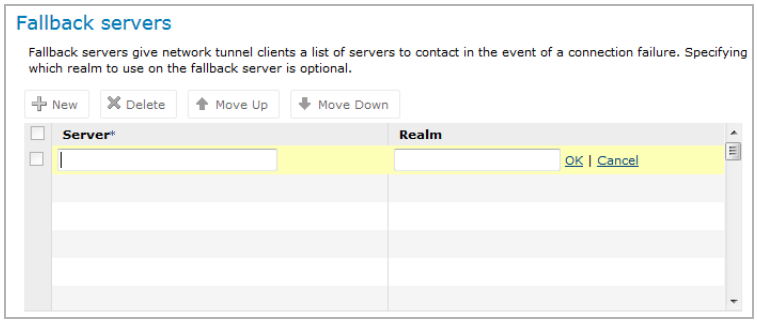
代替サーバーは、ネットワーク トンネル クライアントに、接続障害時に接続するサーバーのリストを提供します。

代替サーバーを構成するには

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] エリアで、[**Network tunnel service (ネットワーク トンネル サービス)**] の下の [**Configure (設定)**] をクリックします。

3 [**Fallback servers (代替サーバー)**] エリアで、[**New (新規)**] をクリックして代替サーバーを追加します。[**Fallback servers (代替サーバー)**] テーブルに、サーバーおよびレルムのフィールド (編集可能) が表示されます。



4 [**Server (サーバ)**] フィールドに、代替サーバーの IP アドレスを入力します。

5 代替サーバーで使用するレルムを指定するには、[**Realm (レルム)**] フィールドにレルム名を入力します。レルムの指定はオプションです。指定されていない場合は、プライマリのレルムが使用されます。

6 [**OK**] を選択します。

7 複数の代替サーバーがリストされている場合に、サーバーの順序を変更するには、サーバーの横にあるチェック ボックスを選択してから [**Move Up (上に移動)**] または [**Move Down (下に移動)**] をクリックします。新しい順序でリストが更新されます。

8 代替サーバーを削除するには、その代替サーバーの横にあるチェック ボックスを選択してから [**Delete (削除)**] をクリックします。

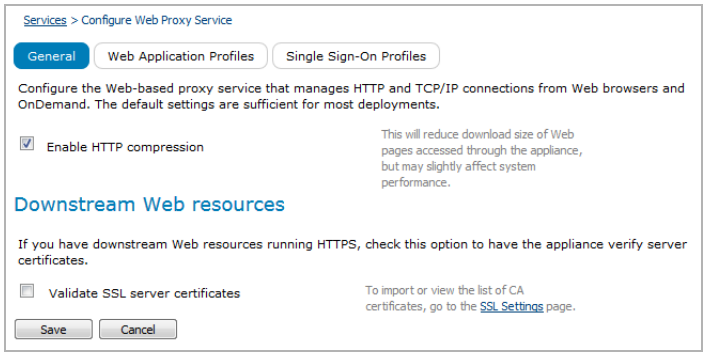
Web プロキシ サービスの構成

このセクションでは、Web リソースへのアクセスを管理するサービスの構成方法について説明します。Web プロキシ サービスは、Web プロキシ アクセス、変換 Web アクセス、カスタム ポート マッピング Web アクセス、およびカスタム FQDN マッピング Web アクセスを提供します。

Web プロキシ サービスを構成するには、

1 メイン ナビゲーション メニューの [**System Configuration (システム構成)**] で、[**Services (サービス)**] をクリックします。

2 [**Access services (アクセス サービス)**] エリアで、[**Web proxy service (Web プロキシ サービス)**] に対する [**Configure (設定)**] をクリックします。



3 HTML、XML、CSS ファイルがアプライアンスからクライアントに送られるとき、あらかじめこれらのファイルを圧縮したい場合、[**General (一般)**] タブで [**Enable HTTP compression (HTTP 圧縮を有効にする)**] を選択します。圧縮を行うと、アプライアンス経由でアクセスする Web ページのダウンロード サイズは小さくなりますが、システムのパフォーマンスが低下する可能性があります。

圧縮を有効にすると、システムのパフォーマンスに影響する可能性があります。

4 [**Downstream Web resources (ダウンストリーム Web リソース)**] を構成します。

- Web プロキシ サービスで、バックエンド Web サーバーの証明書の妥当性をチェックするようにしたい場合は、[**Validate SSL server certificates (SSL サーバー証明書を検証)**] を選択します。この設定を有効にすると、証明書の CN がホスト名と合致し証明書が有効であることを、アプライアンスが確認するようになります。Secure Mobile Access ダウンストリーム HTTPS を使用している場合は、この機能をできる限り有効にしてください。
- 証明書をバックエンド Web サーバーに発行した CA をリストするアプライアンスのルート証明書の詳細を表示する場合または証明書をインポートする場合は、[**SSL Settings (SSL 設定)**] リンクをクリックします。CA 証明書の管理については、CA 証明書を参照してください。

メモ：Web アプリケーション プロファイルの構成方法については、Web アプリケーション プロファイルの追加を参照してください。

Android アプリケーションのアクセス制御 - 任意のバージョンを許可する

SMA は、モバイル クライアントの任意のバージョンを Android Application Access Control (AAC) で実行できるようにします。

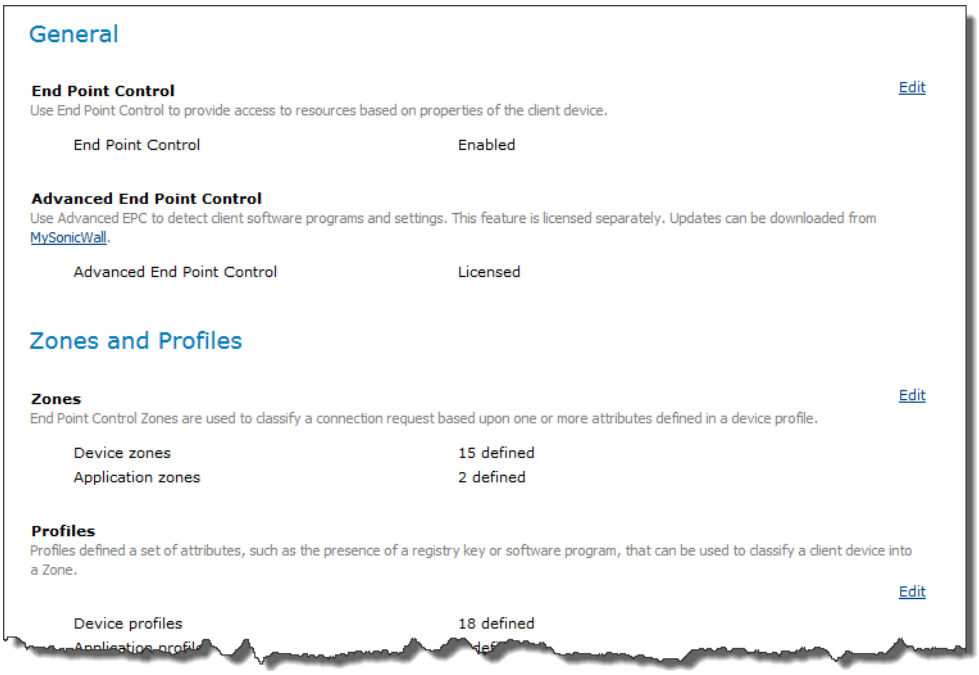
Apple iOS では、クライアント アプリケーションのどのバージョンでもネットワークにアクセスすることができます。これは、Apple がアプリケーション ストアの開発者に厳格な監査とレビューのプロセスを強いることから、iOS は本質的に信頼できるからです。

しかし、Android では、どのバージョンのクライアント アプリケーションでもネットワークにアクセスできるようになると、リスクが高まります。それにもかかわらず、Android のユーザーは、デバイス上のアプリケーションを更新する頻度が高いため、クライアントのどのバージョンでもネットワークにアクセスできるようにする必要があります。

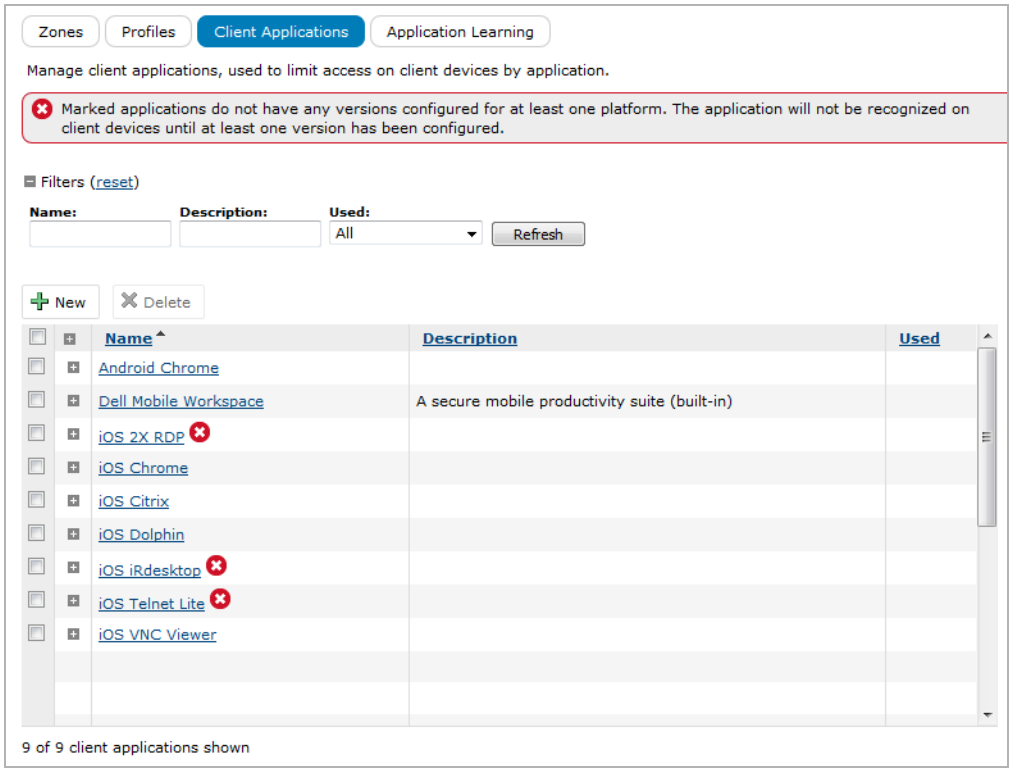
クライアント アプリケーションの任意のバージョンでのネットワーク アクセスの許可は、[**Client Applications (クライアント アプリケーション)**] で有効にします。

Android 上で任意のバージョンのクライアント アプリケーションを許可するには

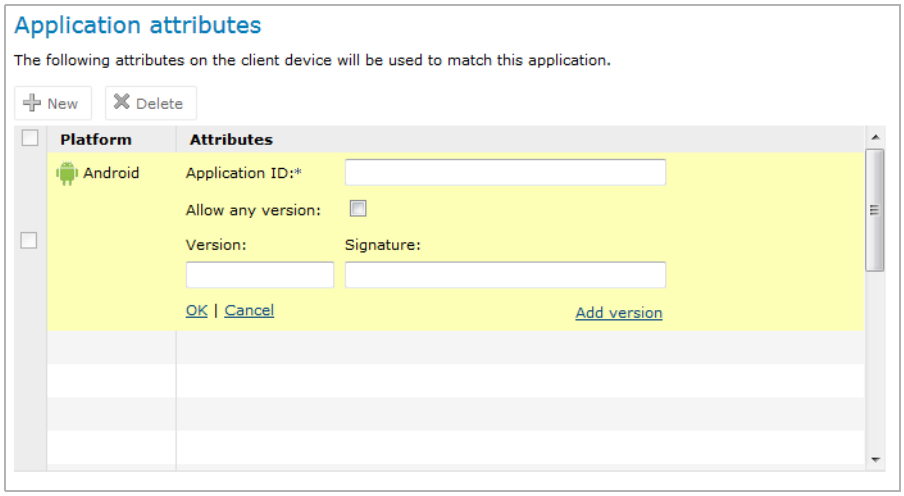
1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**End Point Control**] をクリックします。



2 [**Application Control (アプリケーション制御)**] で、[**Client Applications (クライアント アプリケーション)**] の [**Edit (編集)**] をクリックします。[**Client Application (クライアント アプリケーション)**] ページが表示されます。



3 [**Application attributes (アプリケーション属性)**] の [**New (新規)**] をクリックし、メニューから [**Android**] を選択します。



4 [**Application ID (アプリケーション ID)**] フィールドにアプリケーション ID を入力します。

5 [**Allow any version (任意のバージョンを許可する)**] チェックボックスを選択します。

6 [**Save (保存)**] を選択します。

ターミナル サーバー アクセス

SMA アプライアンスは、個別の Windows Terminal Services または Citrix サーバー、Citrix サーバー ファームに対する Web ベース アクセスをネイティブ サポートしています。Native Access Module には別途ライセンスが必要です。ライセンスの購入については、チャネル パートナーまたは Secure Mobile Access の販売担当者までお問い合わせください。

トピック:

- ターミナル サーバー リソースへのアクセスの提供
- サーバー ファーム リソース
- Citrix アクセス用ブラウザ専用モード
- ターミナル サーバー アクセスのアクセス制御ルールおよびリソースの定義
- グラフィカル ターミナル エージェントの管理
- グラフィカル ターミナル ショートカット

ターミナル サーバー リソースへのアクセスの提供

Web ベース グラフィカル ターミナル エージェントを使用すると、ネイティブ アプリケーション プロトコルを使用してターミナル サーバーにアクセスできるようになります。例えば、Citrix サーバーにアクセスする際、クライアントは固有の (HTTP でない) Citrix プロトコルを使用して、クライアントからサーバーへトラフィックを送信します。したがって、ターミナル サーバー リソースに対するアクセスを提供するとき、Secure Mobile Access のいずれかのアクセス方式 (Web プロキシ エージェント、

OnDemand プロキシ エージェント、いずれかのトンネル クライアント) をプロビジョニングするよう WorkPlace を構成する必要があります。変換 Web アクセスのみを提供するよう WorkPlace を構成している場合、固有のアプリケーション プロトコルにアクセスする上で必要なネットワーク トランスポートがクライアント PC にないため、ターミナル リソースが使用できなくなります。アクセス方式の構成の詳細については、コミュニティに対するアクセス方式の選択を参照してください。

Windows Terminal Services または Citrix サーバーでホストされているアプリケーションでは、シングル サインオンを有効にすることができます。このような構成にすると、ユーザーの WorkPlace ログイン クレデンシャルが、サーバーでパブリッシュされているすべてのアプリケーションに渡されることになります。シングル サインオンを無効にした場合、別のログイン ページが表示され、ターミナル サーバーでホストされているアプリケーションにアクセスする前に、必要なクレデンシャルを指定しなければならなくなります。

ターミナル サーバー リソースへのアクセスを有効にする場合は、次のような基本手順を実行します。

1 ターミナル サーバー リソースおよびアクセス ポリシーの定義

最初に、個別の Windows Terminal Services または Citrix サーバー、あるいは Citrix サーバー ファームを定義し、これらのリソースをアクセス制御ルールに追加します。

- 各ホストまたは Citrix サーバー ファーム オブジェクトを AMC でリソースとして定義する必要があります。ネットワークに、同様の名前を持つ Citrix サーバーのセットが含まれている場合、ワイルドカード文字を使用し、複数のサーバーを含む 1 つのリソース オブジェクトを定義することで、作業時間を短縮できます。

  Citrix サーバー ファームを構成している場合、アプリケーションをリソースとしてホストしている個別の Citrix サーバーについても定義する必要があります。Citrix サーバー ファームの定義については、Citrix サーバー ファーム リソースの追加を参照してください。

- 他のリソースと同様の方法で、アクセス制御ルールでリソースを参照します。個別の Windows Terminal Services または Citrix サーバーにターミナル サーバー アクセスを提供する方法については、ターミナル サーバー アクセスのアクセス制御ルールおよびリソースの定義を参照してください。

2 適切なグラフィカル ターミナル エージェントのインストールまたは更新

ユーザーが、WorkPlace から Citrix または Windows Terminal Services リソースへの接続を開始するとき、アプライアンスは、アプライアンスで提供されている適切なバージョンのエージェントがユーザーのコンピュータ上にインストールされているかどうか判定し、必要に応じて、エージェントを自動的にインストールまたは更新します。適切なグラフィカル ターミナル エージェントが AMC で構成されている必要があります。エージェントの管理については、グラフィカル ターミナル エージェントの管理を参照してください。

3 ターミナル サーバー リソースを参照する WorkPlace ショートカットの作成

Windows Terminal Services または Citrix ホストには、ユーザーが WorkPlace のショートカットをクリックしたときに展開される Web ベースのエージェントからアクセスします。グラフィカル ターミナルの WorkPlace ショートカットの構成については、グラフィカル ターミナル ショートカットを参照してください。

サーバー ファーム リソース

SMA アプライアンスでは、個々の Citrix サーバー、ロードバランシングされた 1 つまたは複数の Citrix サーバー ファーム、または VMware サーバーを指定できます。

トピック:

- Citrix サーバー ファーム リソースの追加
- VMware View リソースの追加

Citrix サーバー ファーム リソースの追加

このセクションでは、Citrix サーバー ファームをリソースとして定義する方法について説明します。Citrix サーバーへのターミナル サーバー アクセスの提供については、ターミナル サーバー アクセスのアクセス制御ルールおよびリソースの定義を参照してください。

ユーザーが Citrix リソースにアクセスできるようにするには、最初に、アプライアンスに 2 つの Citrix エージェント (Windows で動作する ActiveX コントロール、およびクロスプラットフォームの Java アプレット) を構成します。エージェントのファイルがアプライアンスにアップロードされると、ユーザーが WorkPlace から初めて Citrix リソースにアクセスする際に、適切な Citrix クライアントが自動的にプロビジョニングされるようになります。詳細については、グラフィカル ターミナル エージェントの管理を参照してください。アプライアンスでは、Citrix クライアントがサポートするすべてのデスクトップ オペレーティング システムおよびアプリケーションがサポートされています。小型携帯端末はサポートしていません。

個別の Citrix サーバーごとに、カスタム ICA ファイルを指定できます。

Citrix サーバー ファームは、次のシステム要件を満たしている必要があります。

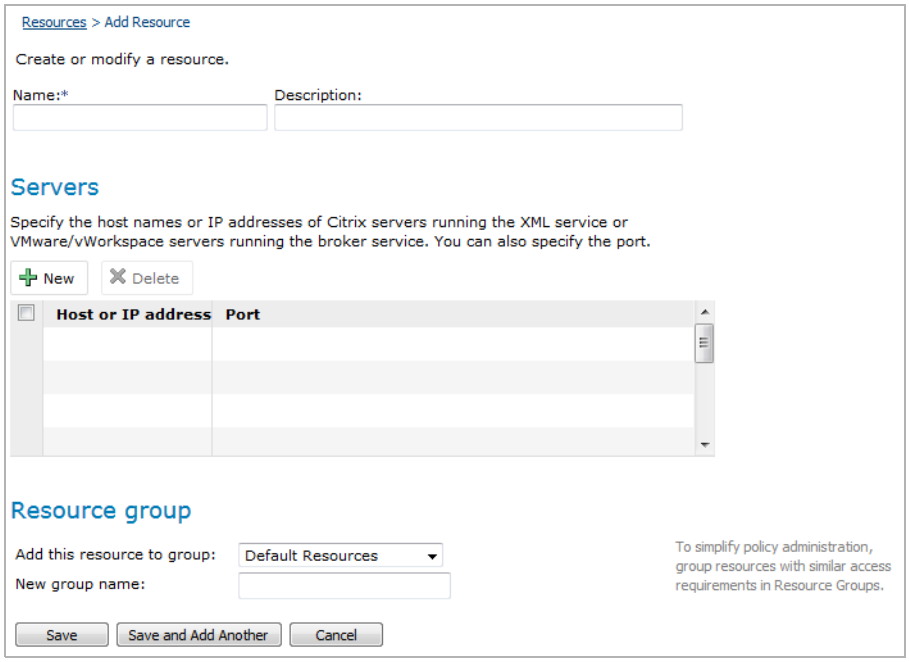
- Citrix XenApp
- Citrix XML サービスが動作していること

ユーザーが、Citrix サーバー ファームに対する WorkPlace ショートカットをクリックすると、独立した WorkPlace ウィンドウが現れ、サーバーでホストされているリソースが表示されます。WorkPlace Web インターフェースでは、ユーザーがファーム内の Citrix サーバーでホストされているアプリケーションを参照して作業するうえで必要なサービスを提供します。他の Web インターフェースを展開する必要はありません。ユーザーはこれらのリソースを参照してリンクをクリックすることで、アプリケーションを自動的に起動できます。Citrix アプリケーションは、Citrix クライアントのウィンドウに表示されます。

Citrix サーバー ファーム リソースを追加するには

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

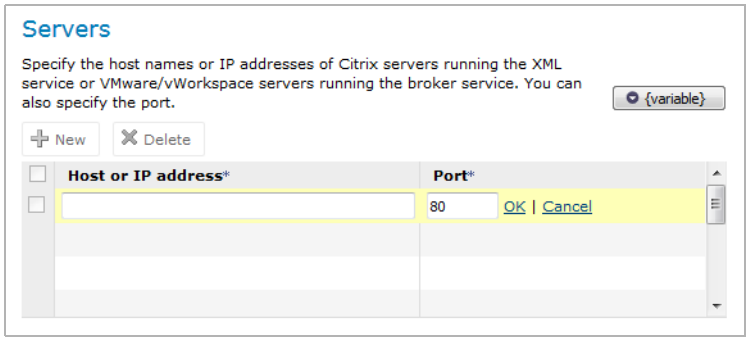
2 [**Resources (リソース)**] ページで [**New (新規)**] をクリックして、リストから [**Server farm (サーバー ファーム)**] を選択します。[**Add Resource - Server (リソースの追加 - サーバー)**] ページが表示されます。



3 [**Name (名前)**] フィールドにサーバー ファームの名前を入力します。

4 [**Description (説明)**] フィールドに、サーバー ファームについての分かりやすいコメントを入力します。この手順はオプションですが、説明を入力しておくと後でリソースのリストを参照する際に役立ちます。

5 [**Servers (サーバー)**] の下にある [**New (新規)**] をクリックし、サーバー ファームに入れるサーバーを指定します。各サーバー ファームには、Citrix XenApp サーバーを 1 つ以上入れる必要があります。



a [**Host or IP address (ホストまたは IP アドレス)**] フィールドに、Citrix XenApp サーバーのホスト名または IP アドレスを入力します。

b [**Port (ポート)**] フィールドに、アプライアンスが Citrix XenApp サーバー上の XML ブラウザ サービスに接続する際に使用されるポート番号を入力します。デフォルトのポート番号は「**80**」です。

c [**OK**] を選択します。サーバーが、ファームのサーバー リストに追加されます。

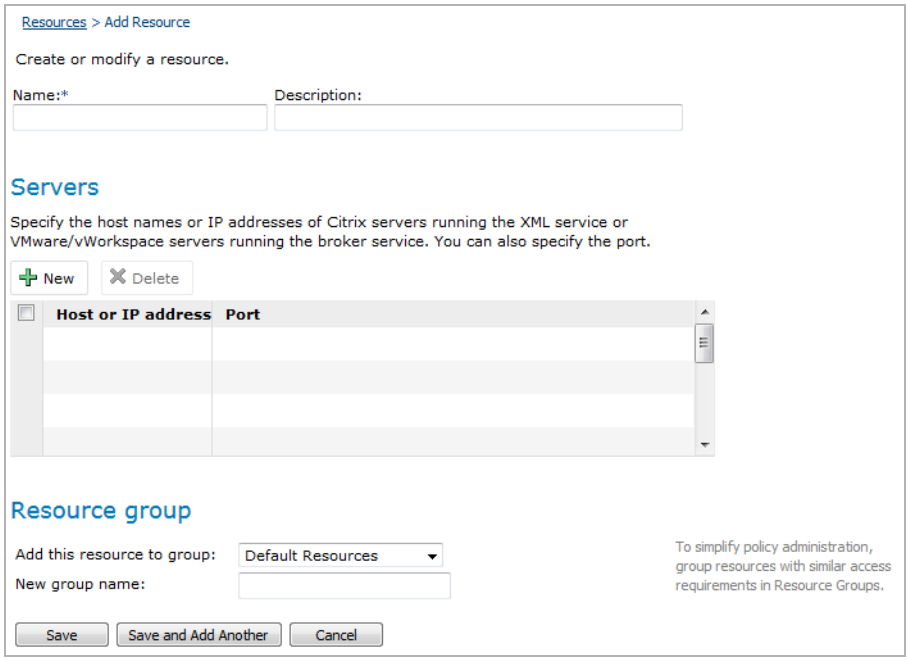
6 [**Save (保存)**] を選択します。

VMware View リソースの追加

VMware View リソースを追加するには

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。

2 [**Resources (リソース)**] ページで [**New (新規)**] をクリックして、リストから [**Server farm (サーバーファーム)**] を選択します。[**Add Resource - Server (リソースの追加 - サーバー)**] ページが表示されます。



3 [**Name (名前)**] フィールドに Vmware View の名前を入力します。

4 オプション。[**Description (説明)**] フィールドに、VMware View についての分かりやすいコメントを入力します。

5 [**Citrix or VMware servers Citrix (または VMware サーバー)**] の下の [**New (新規)**] をクリックし、VMware View に含まれている VMware サーバーを指定します。各 View には 1 台以上のサーバーが含まれている必要があります。

   a [**Host or IP address (ホストまたは IP アドレス)**] フィールドに、VMware サーバーのホスト名または IP アドレスを入力します。

   b [**Port (ポート)**] フィールドに、アプライアンスが VMware サーバーのサービスに接続する際に使用されるポート番号を入力します。デフォルトのポート番号は「*80*」です。

   c [**OK**] を選択します。

6 [**Save (保存)**] を選択します。

VMware View クライアントを追加するには

1 AMC のメイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**Agent Configuration (エージェント設定)**] をクリックします。

2 [Other agents (その他エージェント)] エリア > [Graphical terminal agents (グラフィカル ターミナル エージェント)] で、[**Configure (設定)**] をクリックします。

3 [**VMware View clients (VMware View クライアント)**] エリアで、[**Browse...(参照...)**] をクリックしてエージェント ファイルに移動します。それぞれのエージェント ファイルを選択します。

4 [**Save (保存)**] を選択します。

Citrix アクセス用ブラウザ専用モード

ユーザーは、Citrix Native Access Module を使用して Citrix アプリケーションにアクセスしています。Citrix リソースを設定するということは、エンドユーザーがメンテナンスが面倒な ActiveX または Java エージェントを使用する必要があることを意味します。Citrix は、Firefox および Chrome ブラウザから XenApp および XenDesktop に接続するために使用できる HTML5 ブラウザ ベースのレシーバーを開発しました。SMA は、エンドユーザーがこれらのバックエンド アプリケーションに簡単にアクセスできるように、SMA アプライアンスから Citrix HTML5 レシーバーを簡単に設定する方法を提供します。

管理者は Citrix HTML5 ベースのレシーバーを利用することで、アプライアンス内の Citrix StoreFront URL を URL リソースとして設定できます。ユーザーは、ホスト マップまたはポート マップ方法 (リバース プロキシ) を使用して URL を起動し、資格情報を提供し、StoreFront の HTML5 ビューにリダイレクトされます。

HTML5 レシーバーは、Firefox および Chrome ブラウザでのみ動作します。

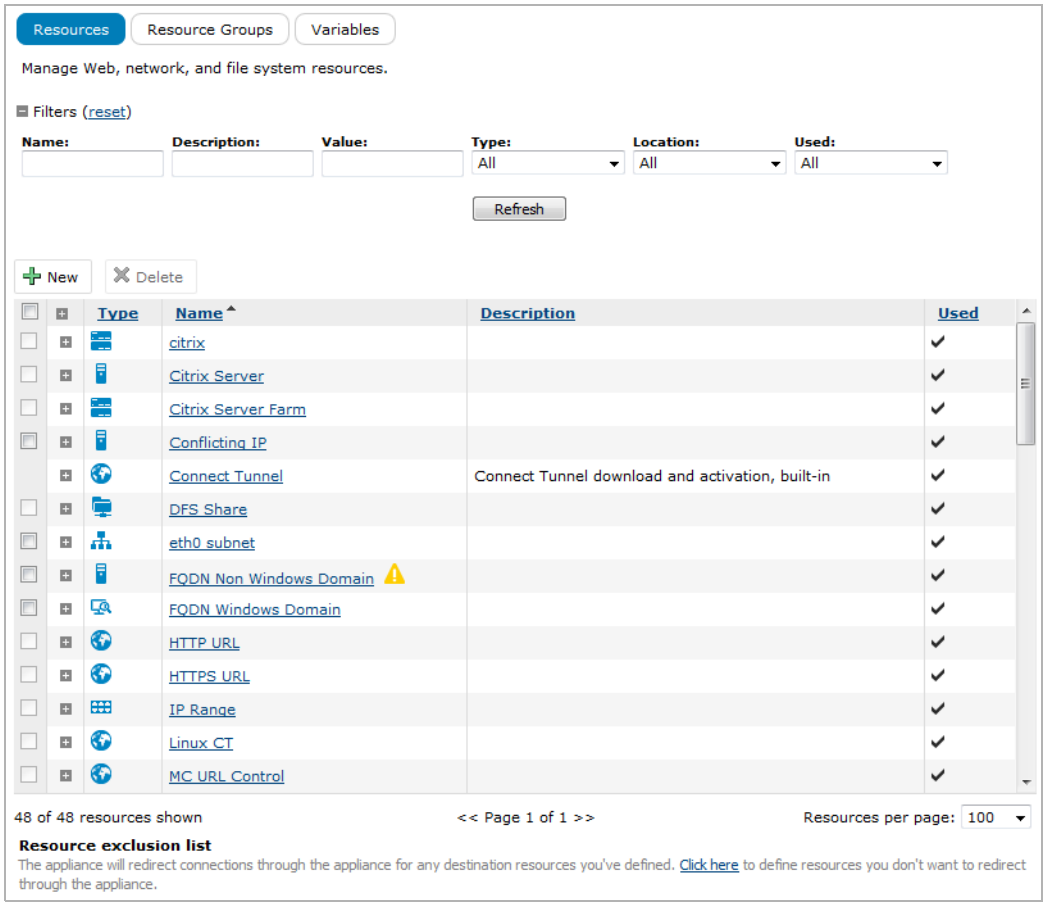
トピック:

- Citrix HTML5 レシーバーの URL の設定
- WorkPlace での Citrix HTML5 レシーバーのショートカットの設定

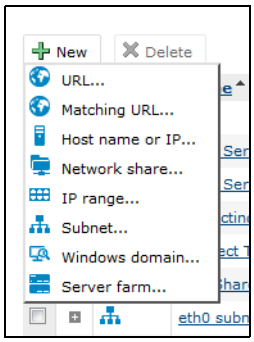
Citrix HTML5 レシーバーの URL の設定

Citrix HTML5 レシーバーの URL を設定するには

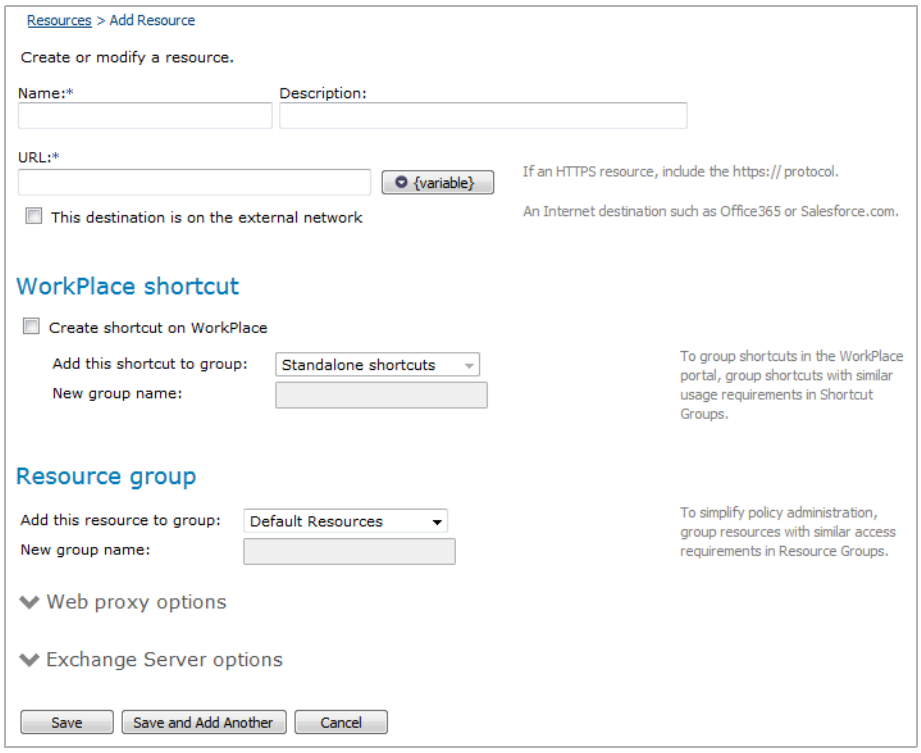
1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Resources (リソース)**] をクリックします。



2 [**New (新規)**] ボタンをクリックします。ドロップダウン メニューが表示されます。



3 [**URL**] を選択します。[**Add Resource URL (リソース URL の追加)**] ダイアログが表示されます。



4 [**Name (名前)**] フィールドに、この URL リソースの名前 (「Citrix HTML5 レシーバー」など) を入力します。

5 [**URL**] フィールドに、Citrix HTML5 レシーバーの URL を入力します。

6 このリソースが外部ネットワーク上にある場合は、[**This destination is on the external network (この宛先は外部ネットワーク)**] チェックボックスを選択します。

7 [**Create shortcut on WorkPlace (Workplace 上にショートカットを作成)**] チェックボックスを選択します。

8 [**Custom access (カスタム アクセス)**] パネルのドロップダウン メニューから、[**Access this resource on a custom port (カスタム ポートでこのリソースにアクセス)**] を選択します。

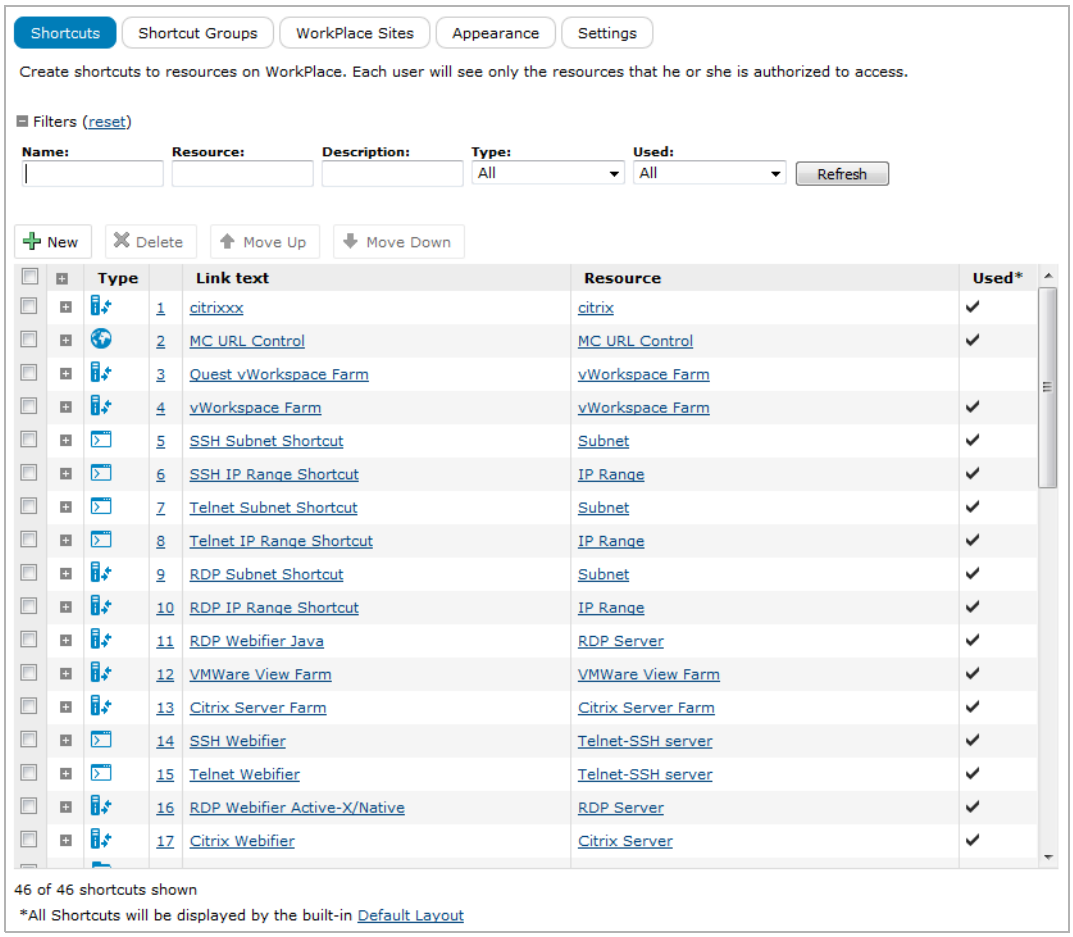
9 [**Port (ポート)**] フィールドに、必要なポート番号を入力します。

10 [**Save (保存)**] を選択します。

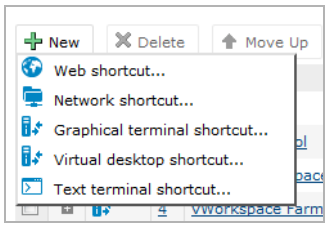
WorkPlace での Citrix HTML5 レシーバーのショートカットの設定

WorkPlace で Citrix HTML5 レシーバーのショートカットを設定するには

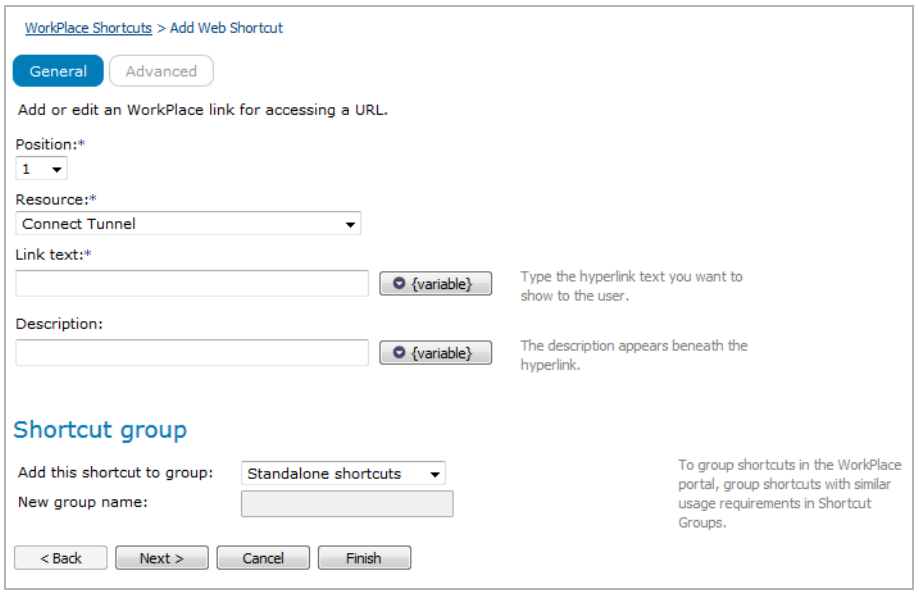
1 AMC のメイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックし、[**Shortcuts (ショートカット)**] タブをクリックします。



2 [**New (新規)**] ボタンをクリックします。ドロップダウン メニューが表示されます。

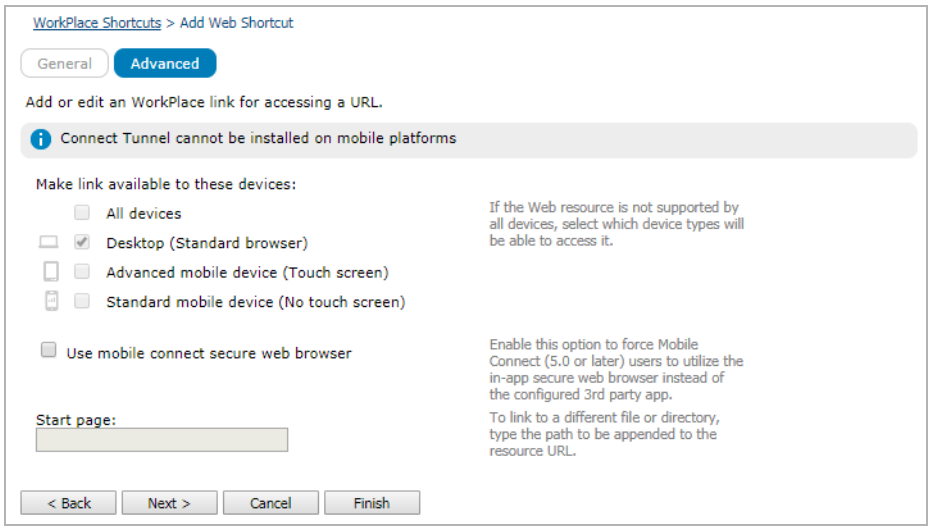


3 [**Web shortcut (Web ショートカット)**] を選択します。[**Edit Web Shortcut (Web ショートカットの編集)**] ダイアログが表示されます。



4 適切なフィールドに、Citrix HTML5 レシーバーの名前と説明を入力します。

5 [**Next (次へ)**] をクリックすると、[**Advanced (詳細)**] ページが表示されます。



6 [**All devices (すべてのデバイス)**] チェックボックスを選択します。

7 [**Start page (開始ページ)**] フィールドに、Citrix HTML5 レシーバーの URL を入力します。

```
/citrix/store2web
```

8 [**Save (保存)**] を選択します。

ターミナル サーバー アクセスのアクセス制御ルールおよびリソースの定義

このセクションでは、アクセス制御ルールを定義してターミナル サーバー リソースを作成することにより、ユーザーにターミナル サーバー アクセスを提供する方法について説明します。詳細については、アクセス制御ルールおよびリソースの追加を参照してください。

ターミナル サーバー リソースを定義するには

1 AMC のメイン ナビゲーション メニューの [**Security Administration (セキュリティ管理)**] で、[**Access Control (アクセス制御)**] をクリックします。

2 「**New (新規)**」をクリックします。[**Add/Edit Access Rule (アクセス ルールの追加/編集)**] ページが表示されます。

3 [**Number (番号)**] フィールドに、アクセス ルール リスト内でのルールの位置を示す番号を入力します。

4 [**Action (動作)**] ボタンを使用して [**Permit (許可)**] を指定します。

5 [**Basic settings (基本設定)**] で、次のように情報を指定します。

   a [**User (ユーザ)**] が選択されていますが、そのままにしておきます (これにより、リソースへのアクセスを試行するユーザーにルールが適用されます)。

   b [**From (送信元)**] フィールドでは、ルールを適用する対象ユーザーを指定します。この例では、値を「*Any user*」のままとしています。

   c [**To (送信先)**] フィールドで、[**Edit (編集)**] をクリックし、このルールに対する対象リソースを指定します。[**Resources (リソース)**] ダイアログが表示されます。

   d [**New (新規)**] をクリックして、リストから「**Host name or IP (ホスト名または IP)**」を選択します。同じ IP サブネットに複数のターミナル サーバーがある場合は、[**IP range (IP 範囲)**] または [**Subnet (サブネット)**] を選択できます。[**Add/Edit Resource (リソースの追加/編集)**] ページが表示されます。

   e リソースの名前を入力します。例えば、「`terminal server`」と入力します。

   f [**Host name or IP address (ホスト名または IP アドレス)**] フィールドに、ターミナル サーバーのホスト名または IP アドレスを入力します。

   g [**Save (保存)**] を選択します。[**Add/Edit Resource (リソースの追加/編集)**] ページが閉じます。

6 「**完了**」をクリックします。

グラフィカル ターミナル エージェントの管理

このセクションでは、SMA アプライアンス経由でターミナル サーバー リソースに対してユーザー アクセスを提供するグラフィカル ターミナル エージェントを構成する方法について説明します。WorkPlace 経由でターミナル サーバーへのアクセスを提供する方法については、グラフィカル ターミナル ショートカットを参照してください。

トピック:

- Windows Terminal Services エージェントの管理
- VMware View クライアントの管理

Windows Terminal Services エージェントの管理

[**Configure Graphical Terminal Agents**] ページの [**Windows Terminal Services agents (Windows ターミナル サービス エージェント)**] セクションで示されているように、SMA アプライアンスでは、Windows クライアント マシンにインストールされているネイティブの RDP クライアントか、アプライアンスにあらかじめインストールされているクロスプラットフォームの Java ベース Windows Terminal Services エージェントのいずれかを、自動的に使用します。クロスプラットフォームのエージェントはアプライアンスで使用するようにカスタマイズされており、更新できません。ネイティブの Windows RDP クライアントは、Microsoft の自動更新によりクライアント マシンで更新されます。

Citrix エージェントの管理

ユーザーが Citrix リソースにアクセスできるようにするには、アプライアンスに 2 つの Citrix エージェント (Windows 上で稼働する ActiveX コントロールと、クロスプラットフォームの Java アプレット) を構成する必要があります。

アプライアンスでそれぞれの Citrix エージェントを構成する場合、エージェント ファイルをアプライアンスにアップロードします。SMA アプライアンスは、ユーザーが初めて WorkPlace から Citrix リソースにアクセスする際に、Citrix エージェントをプロビジョニングします。

Citrix エージェントをインストールするには

1 AMC のメイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**Agent Configuration (エージェント設定)**] をクリックします。

2 [**Other agents (その他エージェント)**] エリアの [**Graphical terminal agents (グラフィカル ターミナル エージェント)**] で [**Configure (設定)**] をクリックします。[**Configure Graphical Terminal Agents (グラフィカル ターミナル エージェントを設定)**] ページが表示されます。

3 ActiveX エージェントを指定するには、[**Citrix agents (Citrix エージェント)**] の下にある [**Windows (ActiveX control) (Windows (ActiveX コントロール))**] を次のように設定します。

   a [**Agent file (エージェント ファイル)**] フィールドに、エージェント ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します。

   b [**Save (保存)**] をクリックして、ファイルを SMA アプライアンスに転送します。

4 Mac OS X エージェントを指定するには、[**Citrix agents (Citrix エージェント)**] の下にある [**Mac OS X**] を次のように構成します。

   a [**Agent file (エージェント ファイル)**] フィールドに、エージェント ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します。

   b [**Save (保存)**] をクリックして、ファイルを SMA アプライアンスに転送します。

5 Java エージェントを指定するには、[**Citrix agents (Citrix エージェント)**] の下にある [**Cross-platform (Java applet) (クロスプラットフォームの Java アプレット)**] エリアを次のように構成します。

a [**Agent file (エージェント ファイル)**] フィールドに、エージェント ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します。

b [**Save (保存)**] をクリックして、ファイルを SMA アプライアンスに転送します。

VMware View クライアントの管理

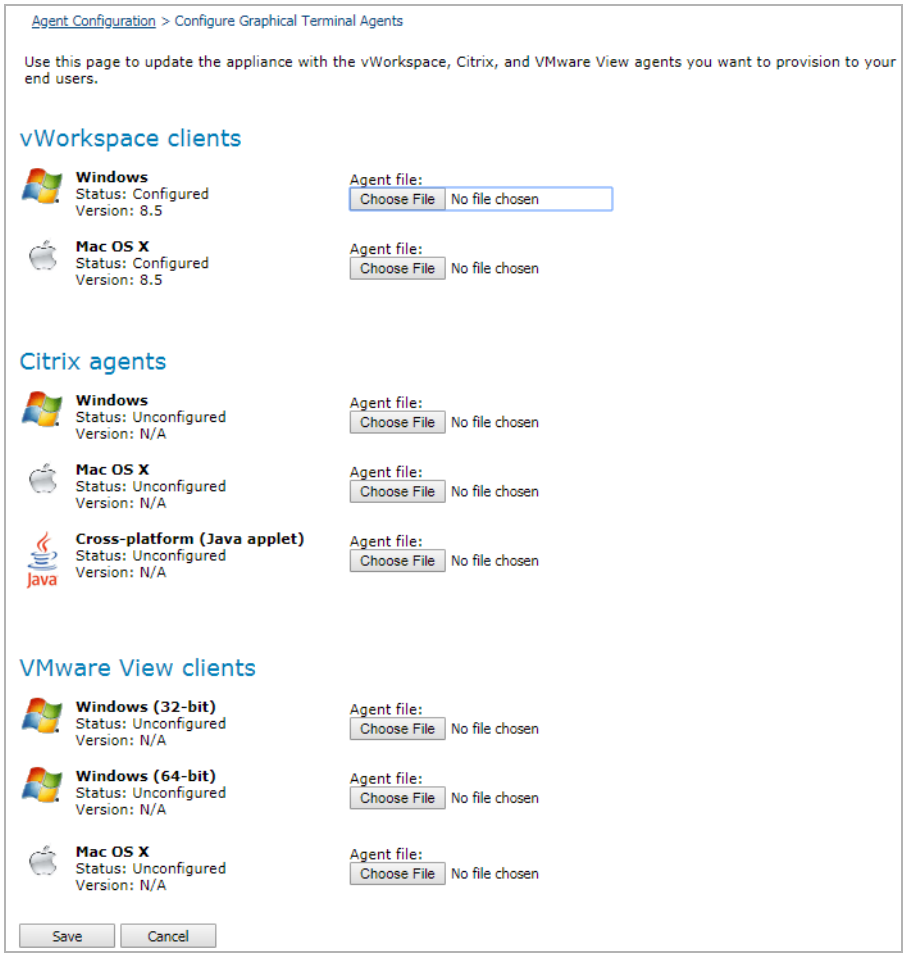
32 ビット版および 64 ビット版 Windows のユーザーが VMware リソースにアクセスできるようにするには、アプライアンスに 2 つの VMware View クライアント (32 ビット Windows クライアントと 64 ビット Windows クライアント) を構成する必要があります。

アプライアンスでそれぞれの VMware View クライアントを構成するには、エージェント ファイルをアプライアンスにアップロードします。SMA アプライアンスは、ユーザーが初めて WorkPlace から VMware View リソースにアクセスする際に、VMware View エージェントをプロビジョニングします。

VMware エージェントをインストールするには

1 AMC のメイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**Agent Configuration (エージェント設定)**] をクリックします。

2 [**Other agents (その他エージェント)**] エリアの [**Graphical terminal agents (グラフィカル ターミナル エージェント)**] で [**Configure (設定)**] をクリックします。[**Configure Graphical Terminal Agents (グラフィカル ターミナル エージェントを設定)**] ページが表示されます。



3 32 ビット版 Windows 向け VMware View クライアント用のエージェントを指定するには、[**VMware View clients (VMware View クライアント)**] の下にある [**Windows (32-bit)**] 設定を次のように構成します。

   a [**Agent file (エージェント ファイル)**] フィールドに、エージェント ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します。

   b [**Save (保存)**] をクリックして、ファイルを SMA アプライアンスに転送します。

4 64 ビット版 Windows 向け VMware View クライアント用のエージェントを指定するには、[**VMware View clients (VMware View クライアント)**] の下にある [**Windows (64-bit)**] エリアを次のように構成します。

   a [**Agent file (エージェント ファイル)**] フィールドに、エージェント ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します。

   b [**Save (保存)**] をクリックして、ファイルを SMA アプライアンスに転送します。

5 Mac OS X 向け VMware View クライアント用のエージェントを指定するには、[**VMWare View clients (VMware View クライアント)**] の下にある [**Mac OS X**] エリアを次のように構成します。

   a [**Agent file (エージェント ファイル)**] フィールドに、エージェント ファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します。

   b [**Save (保存)**] をクリックして、ファイルを SMA アプライアンスに転送します。

グラフィカル ターミナル ショートカット

グラフィカル ターミナル ショートカットを作成すると、Windows Terminal Services ホストまたは Citrix ホストで提供されるリソースに対して、ユーザーが Web ベースでアクセスできるようになります。ターミナルリソースに対するショートカットを作成するときは、あらかじめそのリソースを定義する必要があります (詳細については、リソースの追加およびCitrix サーバー ファーム リソースの追加を参照してください)。また、適切なグラフィカル ターミナル エージェントが AMC で指定されている必要もあります。詳細については、グラフィカル ターミナル エージェントの管理を参照してください。

このセクションでは、個別の Citrix または Windows Terminal Services ホスト、および Citrix サーバー ファームに対するグラフィカル ターミナル ショートカットを構成する方法について説明します。

トピック:

- 個別のホストに対するグラフィカル ターミナル ショートカットの追加
- サーバー ファームへのグラフィカル ターミナル ショートカットの追加

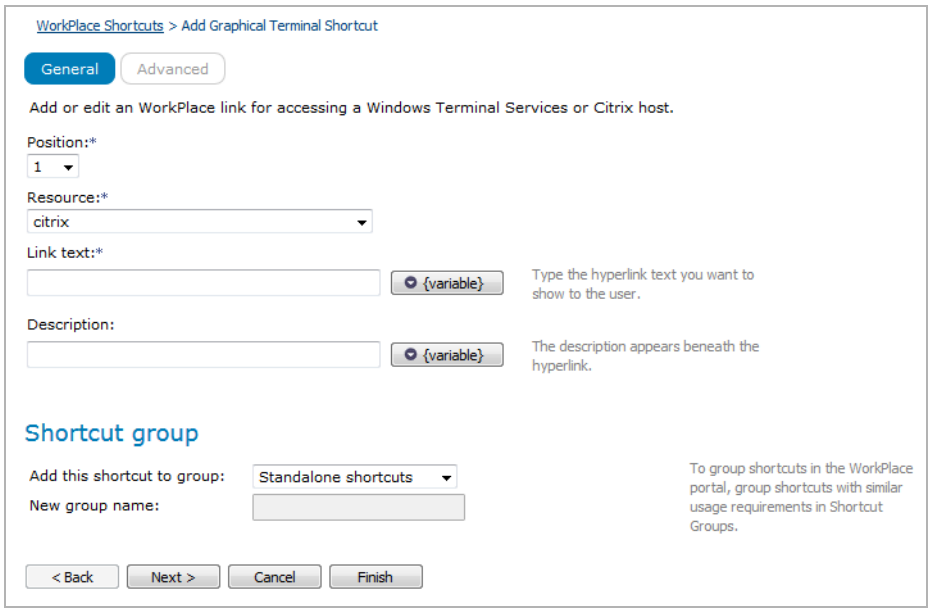
個別のホストに対するグラフィカル ターミナル ショートカットの追加

このセクションでは、個別の Windows Terminal Services または Citrix ホストに対するグラフィカル ターミナル ショートカットを構成する方法を説明します。Citrix サーバー ファームに対するグラフィカル ターミナル ショートカットの構成については、サーバー ファームへのグラフィカル ターミナル ショートカットの追加を参照してください。

個別のホストに対するグラフィカル ターミナル ショートカットを追加するには

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**Shortcuts (ショートカット)**] ページで [**New (新規)**] をクリックし、リストから [**Graphical terminal shortcut (グラフィカル ターミナル ショートカット)**] を選択します。[**Add Graphical Terminal Shortcut (グラフィカル ターミナル ショートカットを追加)**] ページの [**General (一般)**] サブページが表示されます。



3 [**Position (位置)**] フィールドに、リスト内でのショートカットの位置を指定します。

4 [**Resource (リソース)**] ドロップダウン メニューで、このショートカットがリンクしているホストまたは IP アドレス リソースを選択します。このメニューには、使用可能な定義済みリソースが含まれています(**URL** リソースおよび**ネットワーク共有**リソースは、グラフィカル ターミナル ショートカットを関連付けることができないため、表示されません)。

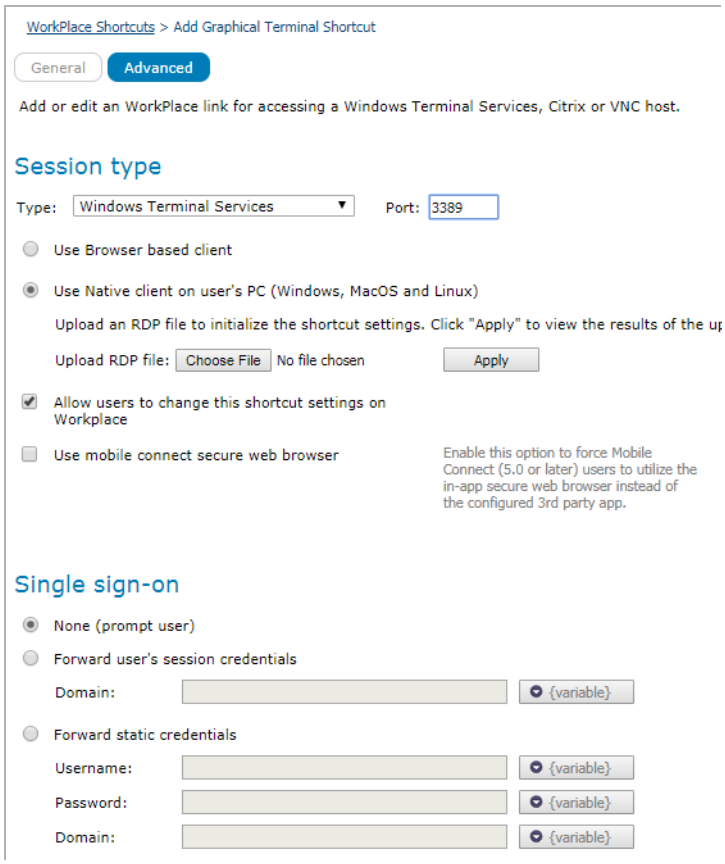
5 ユーザーはこのハイパーリンク テキストをクリックしてグラフィカル ターミナル リソースにアクセスします。ハイパーリンク (ユーザーはこのハイパーリンクをクリックしてリソースにアクセスします) を入力し、オプションで、そのリンクの説明 (リンクの横に表示されます) を入力します。これらのエントリには変数を含めることができます。

   a [**Link text (リンク テキスト)**] フィールドに、ユーザーに表示するハイパーリンク テキストを入力します。例えば、選択したリソースがユーザーのホーム ディレクトリの Windows ドメインの場合は、「`Home directory`」と入力します。変数を使用すると、リンクの後ろに実際のパスを表示できます。[**{variable}**] をクリックし、リストから [**{URL_REF_VALUE}**] を選択します。[**Insert (挿入)**] をクリックすると変数がリンク テキストに追加されます。再度 [**{variable}**] をクリックするとリストが閉じます。

   b [**Description (説明)**] フィールドに、ショートカットについての分かりやすいコメントを入力します。説明の入力はオプションですが、入力しておくとユーザーがリソースを識別しやすくなります。例えば、変数を使用して、そのユーザーに固有の内容にすることができます。[**Description (説明)**] のエントリの例と、WorkPlace でユーザー (この例では *LGeorge*) に表示される説明のテキストを以下に示します。

```
{Session.userName}'s user directory -> LGeorge's user directory
```

6 ショートカットを現在の設定で保存するときは [**Finish (完了)**] をクリックし、他の構成設定を表示するときは [**Next (次へ)**] をクリックします。[**Add Graphical Terminal Shortcut (グラフィカル ターミナル ショートカットを追加)**] ページの [**Advanced (詳細設定)**] タブが表示されます。



7 [**Session type (セッション種別)**] で、開始するセッションのタイプを指定します。

- Windows Terminal Services ホストとの接続を開始する場合は、[**Windows Terminal Services (Windows ターミナル サービス)**] をクリックします。[**Port (ポート)**] フィールドには、Windows ターミナル サービス接続のポート番号を入力します。シームレスに再接続を試行する場合は、[**Automatically reconnect if session is interrupted (セッションが中断された場合に自動的に再接続する)**] チェックボックスを選択します。
- 個別の Citrix ホストへの接続を開始する場合は、[**Citrix**] をクリックします。[**Port (ポート)**] フィールドに、接続のポート番号を入力します。オプションで、[**Custom ICA file (カスタム ICA ファイル)**] を指定できます (このファイルのパスを入力するか、[**Browse (参照)**] をクリックしてファイルの場所を指定します)。カスタム ICA ファイルには、Citrix ホストに対する追加の構成設定が含まれています。

8 [**Single sign-on (シングル サインオン)**] で、ユーザー クレデンシャルがホストに渡される方法を指定します。ユーザー クレデンシャルを転送すると、ユーザーが複数回ログインする (アプライアンスへアクセスするためにログインし、ホストへアクセスするために再度ログインする) 必要がなくなります。

- シングル サインオンをオフにし、その代わりにユーザーにクレデンシャルを要求するときは、[**None (なし)**] をクリックします。
- WorkPlace で認証に使用されるユーザー名とパスワードをホストに渡すときは、[**Forward user's session credentials (各ユーザーの個別のユーザー名とパスワードを転送)**] をクリックします。

- すべてのユーザーについて同じユーザー名とパスワードを転送するには、[**Forward static credentials (静的資格情報を転送)**] をクリックします。すべてのユーザーに転送するには、静的なユーザー名、パスワード、ドメインを [**Username (ユーザ名)**]、[**Password (パスワード)**]、[**Domain (ドメイン)**] に入力します。

9 ユーザーがグラフィカル ターミナル ショートカットをクリックしたときにアプリケーションを自動的に起動させる場合は、[**Startup options (起動オプション)**] を指定します。

- [**Start application (起動アプリケーション)**] フィールドに、起動するアプリケーションのパスを入力します。
- アプリケーションで作業ディレクトリが必要な場合は、[**Working directory (作業ディレクトリ)**] ボックスにそのパスを入力します。

10 [**Display properties (表示プロパティ)**] を次のように指定します。

- [**Screen resolution (画面解像度)**] ドロップダウン メニューで、そのアプリケーションに対する適切な解像度を選択します。デフォルト解像度は「**1024 x 768 pixels**」です。カスタム解像度を設定するには、[**Custom...(ユーザ定義...)**] を選択して、右側に表示されるフィールドに希望のピクセル値 (幅 x 高さ) を入力します。サポートされる解像度の最小値は 640x480 ピクセル、最大値は 4096x2048 ピクセルです。
- **Terminal Services (ターミナル サービス)** に対するショートカットの場合、ユーザーが画面解像度を変更できるようにするには [**Allow users to select a different resolution**] チェックボックスを選択します。ユーザーは、Workplace でショートカット自体のリスト ボックスから解像度を選択できるようになります。Citrix ショートカットの場合、このチェックボックスは無効になっています。
- [**Color depth (色深度)**] リストで、色深度を選択します。デフォルト設定は「**Lowest (8-bit)**」です。

  メモ：色深度の設定を高くするとパフォーマンスが低下する可能性があります。

11 必要に応じて、[**Resource redirection (リソースのリダイレクト)**] を設定します。

- [**Allow access to local drives (ローカル ドライブへのアクセスを許可する)**] チェックボックスを選択すると、ユーザーはセッション中にローカル ドライブにアクセスできるようになります。
- [**Allow access to local printers (ローカル プリンタへのアクセスを許可する)**] チェックボックスを選択すると、ユーザーはセッション中にローカル プリンタにアクセスできるようになります。
- [**Bring remote audio to local computer (リモート デバイスの音声をローカル コンピュータ上で再生する)**] チェックボックスを選択すると、ユーザーはセッション中にリモートの音声にアクセスできるようになります。音声のリダイレクションはネットワーク リソースを多く消費するため、パフォーマンスが低下する可能性があることに注意してください。デフォルトではオフになっています。
- [**Share clipboard between local and remote computers (ローカル コンピュータとリモート コンピュータでクリップボードを共有する)**] チェックボックスを選択すると、ユーザーは双方向でクリップボードの内容のコピーと貼り付けができるようになります。デフォルトでは、この機能が有効になっています。

12 「**Finish (完了)**」をクリックします。

メモ：

- Citrix ホストに対するショートカットでシングル サインオンを有効にすると、ユーザーの認証クレデンシャルがクライアントに転送されるようになるため、セキュリティ上、危険にさらされる可能性があります。
- Windows Terminal Services エージェントの Java オープンソース版では、[**Resource redirection (リソースのリダイレクト)**]オプションはサポートされていません。
- アプリケーションおよびデータのセットへの読み取り専用アクセスを提供するショートカットでは、クリップボードの共有を有効にすることは適切ではありません。

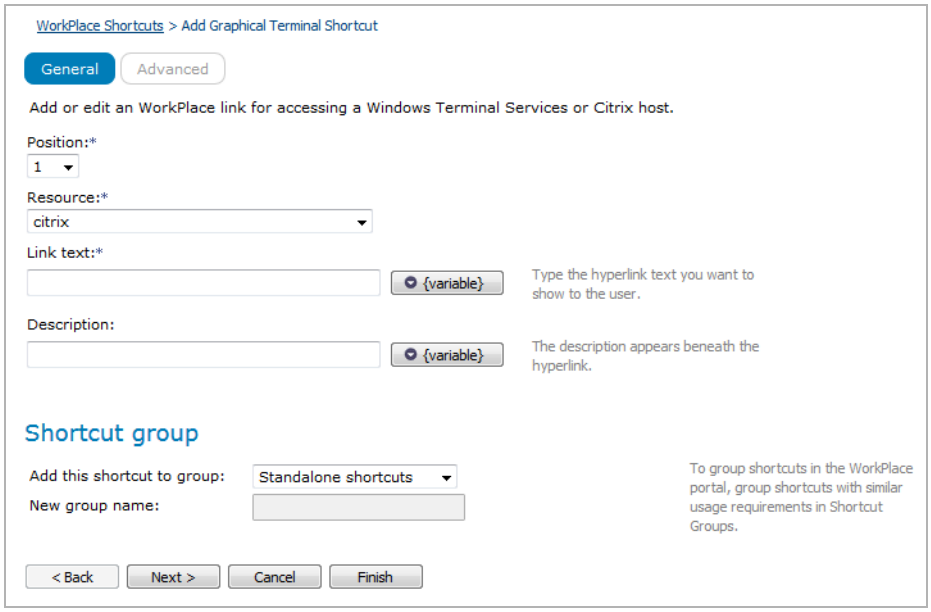
サーバー ファームへのグラフィカル ターミナル ショートカットの追加

このセクションでは、Citrix サーバー ファームに対するグラフィカル ターミナル ショートカットを構成する方法について説明します。個別の Citrix または Windows Terminal Services ホストに対するグラフィカル ターミナル ショートカットの構成については、個別のホストに対するグラフィカル ターミナル ショートカットの追加を参照してください。

サーバー ファームに対するグラフィカル ターミナル ショートカットを追加するには

1 メイン ナビゲーション メニューの [**User Access (ユーザー アクセス)**] で、[**WorkPlace**] をクリックします。

2 [**New (新規)**] をクリックし、リストから [**Graphical terminal shortcut (グラフィカル ターミナル ショートカット)**] を選択します。[**Add Graphical Terminal Shortcut (グラフィカル ターミナル ショートカットを追加)**] ページが表示されます。



3 [**Position (位置)**] フィールドに、リスト内でのショートカットの位置を指定します。

4 [**Resource (リソース)**] ドロップダウン メニューで、このショートカットにリンクするリソースを選択します。このリストには、使用可能な定義済みリソースが含まれています(**URL** リソースおよび**ネットワーク共有**リソースは、グラフィカル ターミナル ショートカットを関連付けることができないため、表示されません)。

5 [**Link text (リンク テキスト)**] フィールドに、ハイパーリンク テキストを入力します。

6 ユーザーはこのハイパーリンク テキストをクリックしてグラフィカル ターミナル リソースにアクセスします。ハイパーリンク (ユーザーはこのハイパーリンクをクリックしてリソースにアクセスします) を入力し、オプションで、そのリンクの説明 (リンクの横に表示されます) を入力します。これらのエントリには変数を含めることができます。

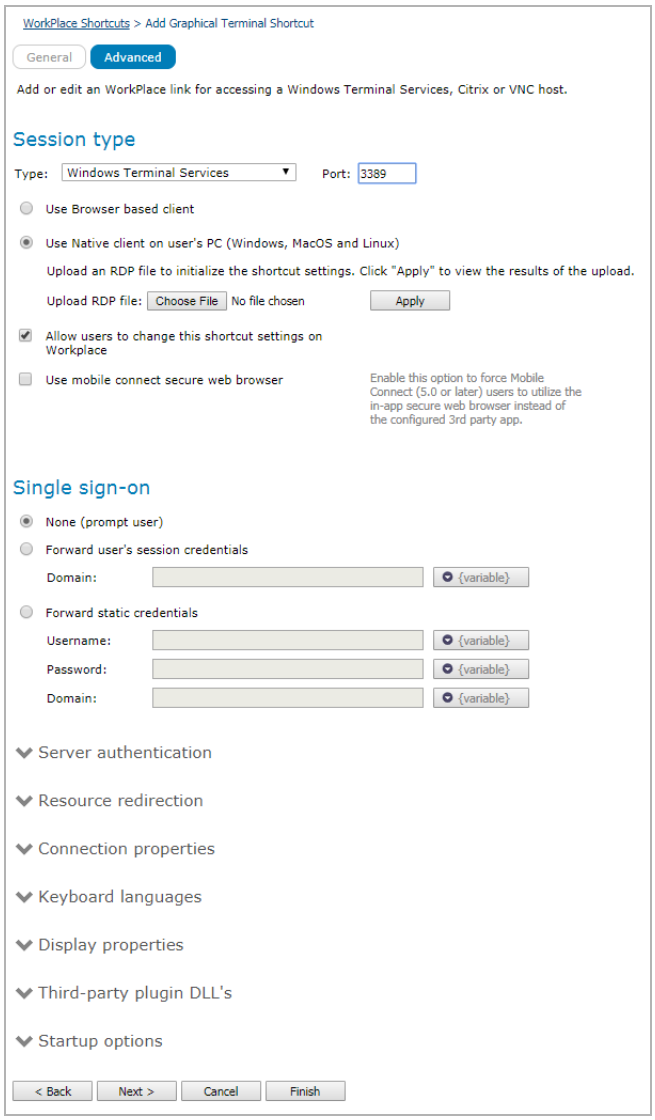
   a [**Link text (リンク テキスト)**] フィールドに、ユーザーに表示するハイパーリンク テキストを入力します。

   b [**Description (説明)**] フィールドに、ショートカットについての分かりやすいコメントを入力します。説明の入力はオプションですが、入力しておくとユーザーがリソースを識別しやすくなります。例えば、変数を使用して、そのユーザーに固有の内容にすることができます。[**Description (説明)**] のエントリの例と、WorkPlace でユーザー (この例では *LGeorge*) に表示される説明のテキストを以下に示します。

```
{Session.userName}’s user directory -> LGeorge’s user directory
```

WorkPlace において、グループを設定してユーザー向けのリソースをまとめることができるほか、各ショートカットを個別に表示することもできます。[**Shortcut group (ショートカット グループ)**] エリアで、新しいショートカットを新規または既存のグループに追加します。このショートカットを単独で WorkPlace に表示するには、[*Standalone shortcuts*] グループに追加します。(ショートカットの表示順序は [**Configure WorkPlace Layout (WorkPlace のレイアウトを設定)**] ページで変更できます。詳細については、WorkPlace レイアウトの作成または編集を参照してください)。

7 ショートカットを現在の設定で保存するときは [**Finish (完了)**] をクリックし、他の構成設定を表示するときは [**Next (次へ)**] をクリックします。[**Add Graphical Terminal Shortcut (グラフィカル ターミナル ショートカットを追加)**] ページの [**Advanced (詳細設定)**] タブが表示されます。



8 必要な場合は、[**Port (ポート)**] に別の値を指定して、Citrix クライアントと WorkPlace との間での ICA トラフィックの送信に使用するポートを変更できます。デフォルト ポートは **1494** です。

9 [**Single sign-on (シングル サインオン)**] で、ユーザー クレデンシャルがホストに渡される方法を指定します。ユーザー クレデンシャルを転送すると、ユーザーが複数回ログインする (アプライアンスへアクセスするためにログインし、ホストへアクセスするために再度ログインする) 必要がなくなります。

- シングル サインオンをオフにし、その代わりにユーザーにクレデンシャルを要求するときは、[**None (なし)**] をクリックします。
- WorkPlace で認証に使用されるユーザー名とパスワードをホストに渡すときは、[**Forward user's session credentials (各ユーザーの個別のユーザー名とパスワードを転送)**] をクリックします。
- すべてのユーザーについて同じユーザー名とパスワードを転送するには、[**Forward static credentials (静的資格情報を転送)**] をクリックします。すべてのユーザーに転送するに

は、静的なユーザー名、パスワード、ドメインを [**Username (ユーザ名)**]、[**Password (パスワード)**]、[**Domain (ドメイン)**] に入力します。

10 ユーザーの WorkPlace ログイン クレデンシャルを、Citrix サーバー ファームでホストされている、すべてのパブリッシュ アプリケーションに転送するときは、[**Enable SSO to Citrix applications (Citrix アプリケーションへの SSO を有効にする)**] チェック ボックスを選択します。Citrix アプリケーションでシングル サインオンを有効にすると、ユーザーの利便性は向上しますが、ユーザーのパスワードがクライアント コンピュータに一時的にクリアテキストで保存されるようになるため、セキュリティが危険にさらされる可能性があります。

11 [**Display properties (表示プロパティ)**] を次のように指定します。

- [**Screen resolution (画面解像度)**] リストで、そのアプリケーションに対する適切な解像度を選択します。デフォルト設定は [**1024 x 768 pixels**]です。
- [**Color depth (色深度)**] リストで、色深度を選択します。デフォルト設定は [**16-bit**] です。

  メモ：色深度設定を高くするとダウンロード速度が低下する可能性があります。

12 「**Save (保存)**」を選択します。

メモ：Citrix ホストに対するショートカットでシングル サインオンを有効にすると、ユーザーの認証クレデンシャルがクライアントに転送されるようになるため、セキュリティ上、危険にさらされる可能性があります。

第 8 部

Mobile Connect

- SMA と Mobile Connect の使用

11

SMA と Mobile Connect の使用

SMA と Mobile Connect の使用について

Mobile Connect には、iOS、OS X、Android でのアプリケーション アクセス制御 (アプリごとの VPN とも呼ばれます) に関する一般的な設計上の制約と実装上の問題があります。以下の情報は、Mobile Connect を SMA アプライアンスに接続するように設定する際に知っておく必要のある考慮事項と警告を示しています。

Mobile Connect の詳細については、お使いのデバイス用の『*Mobile Connect ユーザー ガイド*』(SonicWall サポートから入手可能です) を参照してください。

一般的な制限事項

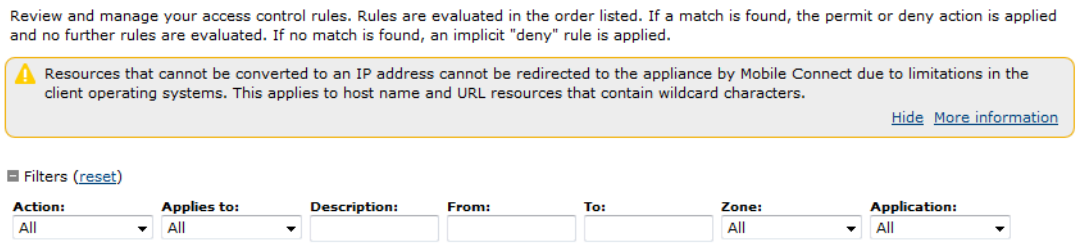
トピック:

ホスト名のリダイレクト

Mobile Connect は、サポートされているすべてのプラットフォームで DNS 監視 (Windows/Mac OSX/Linux の場合は Connect Tunnel など) を実行できますが、ルートを追加できません。現在のバージョンでは、「対応する IP リソースがありません」というメッセージが記録されます。さらに、Mobile

Connect では動的ルーティングがサポートされていません。

- Mobile Connect には他のクライアント (Windows/Mac/Linux) のような動的ルーティングが含まれないため、ユーザーがアクセスするホストまたはドメインに対応するすべての IP サブネットまたは範囲を AMC のリソースとして追加し、宛先ホストまたはドメインへのアクセスが必要なユーザー/グループに適切なアクセス制御ルールを含める必要があります。
- Mobile Connect は動的ルーティングを処理できないため、Secure Mobile Access 11.x.0 以上には、ワイルドカードを含むリソースが機能しないという警告が含まれています。



スプリット トンネルを使用した DNS ルーティング

スプリット トンネルでは、VPN DNS サフィックス検索ドメインに一致する DNS 要求のみが VPN DNS サーバーを使用します。VPN DNS サフィックスと一致しないドメインへの要求は、ローカル (3G/WiFi 接続) DNS サーバーに送られます。これは、E-Series SMA、SMB SMA、および UTM のすべてのサーバーアプライアンスへの接続に当てはまります。これは Apple の iOS の制限事項です。

DNS サフィックスの例: `example.com`

- `www.example.com` に対するクエリは VPN DNS サーバーを使用
- `intranet.corp.example.com` に対するクエリは VPN DNS サーバーを使用
- `www.google.com` に対するクエリはローカル DNS サーバーを使用
- `i2.examplecorp.com` に対するクエリはローカル DNS サーバーを使用

スプリット トンネル モードでは、AMC に CEM エントリを追加することで、この動作を無効にすることができます。

リダイレクト オールを使用した DNS ルーティング

トンネル オール モード (リダイレクト オールとも呼ばれます) では、すべての DNS 要求が優先され、VPN DNS サーバーが使用されます。

Mobile Connect の一般的な制限事項

Mobile Connect は、アプリケーションがユーザーまたはアプリケーションがアクセスを許可されていない企業ネットワーク上の何かにアクセスしようとしているときに、エンドユーザーにメッセージを提供していません。現在、このようなアクセス要求は何も表示されずに破棄されています。SonicWall はこの制限事項を認識しており、今後のリリースでこの種の条件でより多くの情報とメッセージをユーザーに提供するために Mobile Connect を強化するよう努めています。

ファイル

Mobile Connect 3.0 では、新しいファイル ブックマークを使ったファイルへの安全なモバイル アクセスを導入しています。ファイル ブックマークを使用すると、まずサーバーで設定されるファイル ポリシーを確認して強制的に実行し、ファイルを Mobile Connect アプリケーション内に安全にダウンロードして表示することで、ファイルへの安全なアクセスを可能にします。サーバーで設定されるポリシーには、ファイルを印刷するか、クリップボードにコピーするか、サードパーティのアプリケーションで開くか、iOS デバイスに安全にキャッシュするかの制御が含まれます。ディレクトリのナビゲーションを可能にするために、ファイル ブックマークをフォルダまたはファイル共有のルート ディレクトリに作成することもできます。

アプリケーション アクセス 制御

アプリケーション アクセス制御は、Android および iOS/Mac OSX プラットフォームで、SonicWall Secure Mobile Access に対して次のように動作します。

- VPN で制御されるアプリケーション
- iOS/Mac OS X 固有の制限事項
- Android 固有の制限事項
- Windows RT MC の制限事項

VPN で制御されるアプリケーション

Mobile Connect ユーザーがアプリケーションの承認を削除すると、そのアプリケーションは VPN で制御されるアプリケーションではなくなります。このアプリケーション経由でのそれ以降のアクセスは、VPN で制御されるアプリケーションではなかったかのように動作します。アプリケーションの選択または選択解除は、即座に有効になります。Mobile Connect を切断して再接続する必要はありません。

アプリケーション アクセス制御を使用している場合、ユーザーがアプリケーションの承認を削除すると、使用が承認されたアプリケーションを使用してネットワーク リソースまたは個人 Web サイトに引き続きアクセスできるのでしょうか。

例えば、ユーザーが Chrome (使用が承認されたアプリケーション) で企業リソースにアクセスしているとき、次の手順が実行されます。

1 Chrome を選択すると、Chrome は企業ネットワーク経由でトラフィックを送信できます。

2 Chrome を選択解除すると、クライアントはトンネル経由でユーザーのトラフィックが企業ネットワークに送信されないことを保証します。

3 Chrome が選択されているかどうかにかかわらず、企業ネットワーク上ではない場所にユーザーが移動した場合、トラフィックはユーザーの通常のネットワーク インターフェースから送信されます。企業ネットワーク上ではない場所とのトラフィックのやりとりにトンネルを使用することはありません。つまり、アプリケーション アクセス制御を使用している場合、SMA は常に**スプリット トンネル**を使用し、**リダイレクト オール**を使用することはありません。

4 ユーザーがアクセスを許可された企業ネットワーク内の宛先へのトラフィックは、アプリケーションが選択されている場合はトンネルに配信され、選択されていない場合は破棄されます。企業ネットワーク内の宛先へのトラフィックが、ユーザーのデバイスの通常のインターフェースから送信されることはありません。

チェックボックスは、トラフィックを破棄するか、トンネルに送信するかのみを制御します。トラフィックをどこに送信するかを決定することはできません。そのような動的ルーティングは、現在のクライアント インターフェースではサポートできません。

制御下にあるアプリケーションが VPN の影響を受けないということは、厳密には正しくありません。Mobile Connect クライアントが実行されてサーバーに接続されている場合は、あらゆるアプリケーション (リストされていないものも含む) から企業ネットワーク上の IP アドレス宛のすべてのトラフィックがキャプチャされます。リストされていないアプリケーションからのトラフィックは破棄されます。これは、IP アドレスの衝突がある場合に重要です。アプリケーション アクセス制御で同じ問題が発生する可能性があり、制御下にあるかどうかにかかわらず、ユーザーのデバイス上のすべてのアプリケーションに影響します。

iOS/Mac OS X 固有の制限事項

Apple によって Mobile Connect に追加の制限事項が課せられることもあります。SonicWall は、管理者とユーザーのための BYOD をさらに強化するために、これらの制限事項のいくつかについて Apple と引き続き協力しています。制限事項の例を次に示します。

- iOS と Mac OSX 上の Mobile Connect は、プロキシ ベースのメカニズムを使用してアプリケーション データを企業ネットワークにリダイレクトします。これには、SonicWall が認識している特定のサーバー側スケーリングに関する制限事項があります。SonicWall は、iOS および Mac OSX デバイスの BYOD 管理者とユーザーに最適なソリューションを見つけるために、Apple と引き続き協力しています。
- バージョン情報は、iOS および Mac OSX のアプリケーション学習中には提供されません。バージョン情報を取得するには、App Store でアプリの詳細を表示します。

Android 固有の制限事項

Google には、Apple が iOS および Mac OSX について行っているような、Android 向けのアプリごとの VPN サポートが組み込まれていません。したがって、Mobile Connect は独自のメカニズムを使用して、Android デバイスでアプリごとの VPN 機能とランタイム検証を実行します。SonicWall は、Android 内のアプリごとの VPN により包括的なアプローチを提供し、管理者とユーザーのための BYOD をさらに強化するために、Google と引き続き協力しています。

Windows RT MC の制限事項

- Windows RT MC はアプリケーション アクセス制御をサポートしていません。
- EPC サポートは限定的です。

サポートされる EPC プロファイル

エンド ポイント制御ポリシーのチェックは、VPN 接続が確立される前に実行されます。Mobile Connect は、サポートされる EPC プロファイルの属性をサポートしています。

サポートされる EPC プロファイル

Android	iOS	Mac OSX
アンチウィルス アプリ	アプリケーション	アンチウイルス プログラム
パーソナル ファイアウォール アプリ	クライアント証明書	アンチスパイウェア プログラム
アプリケーション	ディレクトリ名	パーソナル ファイアウォール プログラム
クライアント証明書	周辺機器 ID	アプリケーション
ディレクトリ名	ファイル名	クライアント証明書
周辺機器 ID	iOS バージョン	ディレクトリ名
ファイル名		周辺機器 ID
Android バージョン		ファイル名
		Mac OS バージョン

IPV6 の制限事項

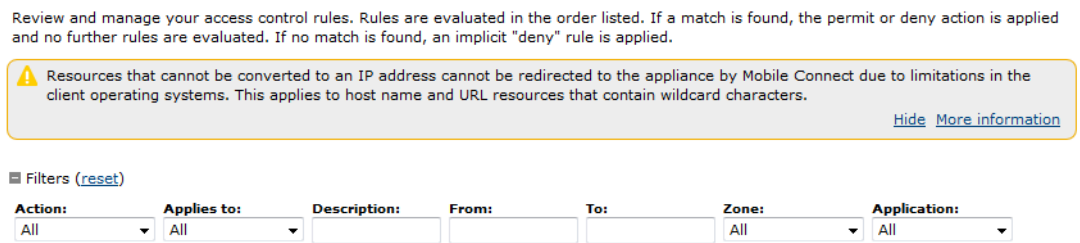
デバイスに IPv4 と IPv6 があり、DNS ホスト名がアプライアンスの IPv6 レコードに解決される場合、Mobile Connect は IPv6 を使用してアプライアンスと通信します。それ以外の場合は、IPv4 に戻ります。

URL 制御に関する注意

以下のフィールドの内容は、Mobile Connect の機能に悪影響を及ぼします。

- `http` または `https` を使用してサーバー フィールドをセットアップすると、Mobile Connect の障害の原因となります。
- レルム名の制限事項により、ホスト名または URL にワイルドカードを含めずに、URL の形式が正しく設定されている必要があります。

ワイルドカードが Mobile Connect の操作を妨げる可能性のあるさまざまなページには、警告が表示されます。



URL 制御を使用すると、他のモバイル アプリケーションが特別な URL を使用して Mobile Connect にアクション要求を渡すことができます。これらのアクション要求は、VPN 接続エントリを作成し、VPN 接続を実行または切断できます。例えば、別のアプリケーションで Mobile Connect を起動し、必要に応じて内部リソースにアクセスし、`mobileconnect://` または `sonicwallmobileconnect//` URL スキームを使用して切断することができます。URL 制御の一般的な例を次に示します。

- プロファイルの追加: `mobileconnect://addprofile[/]?name=ConnectionName&server=ServerAddress[&Parameter1=Value&Parameter2 =Value...]`
- 接続: `mobileconnect://connect[/]?[name=ConnectionName|server=ServerAddress][&Parameter1=Value&Parameter2 =Value...]`
- 切断: `mobileconnect://disconnect[/]`

詳細な情報は、ご使用のモバイル デバイス用の『SonicWall *Mobile Connect ユーザー ガイド*』に記載されています。

Trusted Network Detection の設定

iOS Connect On Demand 機能に対する Apple Trusted Network Detection (TND) の機能拡張は、iOS 6 で利用可能です。TND は、

- Connect On Demand 機能に対してのみ使用できます。
- ユーザーが信頼できるネットワーク上にいるかどうかを判断することで、Connect On Demand 機能を拡張します。
- iPhone 設定ユーティリティで設定します。
- Wi-Fi 接続にのみ使用されます。他の種類のネットワーク接続で動作する場合、Connect On Demand は VPN を接続するかどうかの判断に TND を使用しません。

Connect On Demand は、ユーザーがドメイン リストで指定されたホスト名で宛先にアクセスしようとするたびに、VPN 接続を開始します。例えば、「`*.example.com`」が**常時接続**リストにある場合、ユーザーが `internal.example.com` にアクセスすると、クライアントはデバイスが現在接続されているネットワークに関係なく、VPN 接続を開始します。TND は、サフィックスによる Trusted Network Detection に示すように、VPN とローカル DNS サーバーおよび DNS サフィックスを比較して、Mobile Connect を使用するか、VPN にダイヤルするかを決定します。

サフィックスによる Trusted Network Detection

DNS サフィックス	DNS サーバ	ログイン
なし	なし	拒否 - VPN なし
なし	同じ	拒否 - VPN なし
同じ	同じ	拒否 - VPN なし
同じ	同じ、およびその他	許可
同じ	異なる	許可
異なる	同じ	許可
一部	一部	許可

Trusted Network Detection と Connect On Demand の詳細については、Apple Inc. のマニュアルを参照してください。

接続に TND が使用できるかどうかを確認するには、[**Connection (接続)**] タブの [**Status (ステータス)**] 行の情報インジケータをタップします。利用可能な場合には、TND を有効/無効にするボタンが表示されます。

TND を設定するには:

1 [**Connection (接続)**] タブの [**Status (ステータス)**] 行の [**Info (情報)**] アイコンをタップします。

2 [**Connect On Demand**] がオンになっていることを確認します。

3 [**Trusted Networks (信頼されるネットワーク)**] をオンにします。

> **メモ：**Mobile Connect for iOS 3.0 では、ファイル ブックマークは SMA 7.5 以降のファームウェアを持つ SonicWall SMA アプライアンスでのみサポートされています。SMA および次世代ファイアウォールア プライアンスでのファイル ブックマークのサポートは、将来のリリースで予定されています。

第 9 部

付録

- アプライアンスのコマンドライン ツール
- トラブルシューティング
- アプライアンス保護のためのベスト プラクティス
- SAML ID プロバイダの設定
- ログ ファイルの出力フォーマット
- 多言語サポート
- SonicWall サポート

A

アプライアンスのコマンドライン ツール

ツールの概要

実行しなければならないほとんどの構成管理作業 (アプライアンス構成のバックアップとリストア、アップグレードの適用など) は、Web ベースのアプライアンス管理コンソール (AMC) の [**Maintenance** (メンテナンス)] ページを使用して行うことができます。このセクションでは、コマンドラインでの作業を好む管理者向けに、同様の作業を行うためのアプライアンス ツールについて説明します。アプライアンスのコマンドライン ツールを参照してください。

アプライアンスのコマンドライン ツール

ツール	目的
Setup Tool (`setup_tool`)	ノート型 PC または端末を使用し、シリアル接続を介して Setup Tool を実行することで、アプライアンスを構成します。 • Setup Tool による新しいアプライアンスの構成を参照してください。 **メモ：** `setup_tool` と `cluster_tool` は、`config_reset` に統合されます。
Backup Tool (`config_backup`)	現在の構成ファイルを保存します。 • 構成データの保存を参照してください。
Host Validation Tool (`checkhosts`)	アプライアンス リソースで参照されるホストのリストを表示し、それらがアクセス可能かどうか、および DNS で解決できるかどうかを示します。 • ホストの確認を参照してください。

構成データファイルの詳細および AMC での管理方法については、構成データの管理および システムのアップグレード、リセット、またはロールバックを参照してください。

Setup Tool による新しいアプライアンスの構成

新しいアプライアンスをセットアップする方法としては、アプライアンスの前面にある LCD 制御を使用して情報を入力することを推奨しています。これにより、Web ブラウザでアプライアンスに接続し、アプライアンス管理コンソール (AMC) にアクセスして Setup Wizard を実行できます。詳細については、電源投入とネットワークの基本設定を参照してください。

コマンドライン ユーティリティを使用したい場合は、ノート型 PC または端末を使用し、シリアル接続から Setup Tool を実行し、アプライアンスを構成できます。

トピック:

- Setup Tool の使用についてのヒント
- Setup Tool の使用

Setup Tool の使用についてのヒント

Setup Tool で作業する際のヒントをいくつか紹介します。

- イエスかノーで答える設問の場合、プロンプトの最後に `[y]` または `[n]` が付いています。対応する文字を入力して **Enter** を押すと、その次の設問が表示されます。
- 文字を削除するには、**Backspace** を押します。(Windows ベースの PC の場合、**Delete (削除)** キーで文字を削除することもできます)。
- IP アドレスまたはネットマスクを入力するとき、4 桁のオクテット (`w.x.y.z`) による標準 IP アドレス形式を使用します。Setup Tool では、基本エラー チェックが行われます (例えば、指定したゲートウェイがアプライアンスと同じサブネットにあるかどうかの確認など)。
- Setup Tool を終了して変更事項を破棄するときは「`q`」を押します。

Setup Tool の使用

コマンドラインから Setup Tool を実行するとき、Secure Mobile Access エンド ユーザー ライセンス契約 (EULA) を承認するよう求められます。また、root パスワードを作成し、IP アドレス、サブネット マスク、内部デフォルト ゲートウェイを指定することも求められます。

Setup Tool を実行するには、

1. アプライアンスとの間でシリアル接続を確立し (電源投入とネットワークの基本設定を参照)、電源ボタンを押してアプライアンスをオンにします。
2. アプライアンスが構成されていない場合、または Factory Reset Tool や Config Reset を使用してリセットした直後の場合、Setup Tool が自動的に動作を開始します。
3. ログインするよう求められたら、ユーザー名に「`root`」と入力します。**Enter** を押して次のページに移ります。
4. 内部インターフェースの IP アドレス、サブネット マスク、(オプションで) ゲートウェイを入力するよう求められます。このインターフェースは、Web ブラウザからアプライアンスに接続し、AMC を使用してセットアップを継続するときに使用します。

   `IP` アドレス:

   - 内部 (プライベート) ネットワークに接続する内部インターフェースの IP アドレスを入力して、**Enter** を押します。

   `Subnet mask:`

   - 内部ネットワーク インターフェースのネットマスクを入力して、**Enter** を押します。

   ゲートウェイ:

- AMC にアクセスする際、アクセス元のコンピュータがアプライアンスと異なるネットワーク上にある場合は、ゲートウェイを指定する必要があります。トラフィックをアプライアンスにルーティングするゲートウェイの IP アドレスを入力して、**Enter** を押します。

  アプライアンスと同じネットワークから AMC にアクセスしている場合は、そのまま **Enter** を押します。

5 ここまで入力した情報を確認するよう求められます。現在の値で良ければそのまま **Enter** を押します。値を変更したい場合は新しい値を入力してから **Enter** を押します。

6 最後に、変更を保存して適用するよう求められます。

- **Enter** を押して、変更を保存します。

この時点で、Setup Tool が変更を保存し、必要なサービスを再起動します。また、これまで指定した情報を使用して SSL 鍵を生成します (SSH では、リモート SSH クライアントおよびサーバーと交換するセキュリティ鍵が必要です)。Setup Tool を使用して SSH を構成したら、これらの鍵を生成していることを示すメッセージが表示されます。

この間、フィードバックはほとんどありません。Setup Tool が反応しなくなったと思い込まずに、そのまましばらくお待ちください。Setup Tool が終了したら、初期セットアップが完了したことを示すメッセージが表示されます。このメッセージには、AMC にアクセスするための URL も示されます。

構成データの保存とリストア

アプライアンスには、構成データを保存しリストアするためのコマンドライン管理ツールが多数用意されています。

- Config Backup Tool - 現在の構成ファイルを保存します。
- Config Restore Tool - 保存されている構成ファイルをリストアします。

AMC を使用して構成データを保存およびリストアする方が簡単で便利ですが、AMC でインポートおよびエクスポートできるデータは、コマンドライン ツールで保存、リストアできるデータの一部だけです。AMC方法とコマンドライン ツール では、この 2 つの方法を比較しています。

AMC方法とコマンドライン ツール

構成項目	AMC	コマンドライン ツール
アクセス ポリシー	x	x
証明書	x	x
WorkPlace スタイルのカスタマイズ	x	x
ノード固有のネットワーク設定	x	x

トピック:

- 構成データの保存
- ホストの確認

構成データの保存

バックアップ ファイルは、圧縮された tar ファイル (デフォルト: /var/backups/cfgback.tgz) に保存されます。特にシステムを何度もカスタマイズするような場合は、システムを定期的にバックアップすることが推奨されます。

Backup Tool を使用して構成をバックアップするには、

1 SSH またはシリアル接続を使用してアプライアンスに接続し、「root」としてログインします。

2 「config_backup」と入力し、次のオプション パラメータのいずれかを指定します。

```
config_backup [-t <tarfile>] [-q] [-d <debuglevel>] [-h]
```

構成バックアップのパラメータ

パラメータ	説明
-t *<tarfile>*	構成をバックアップするファイルを指定します。このパラメータは、デフォルト ファイル (/var/backups/cfgback.aea) と異なるバックアップ ファイルにバックアップする場合にのみ必要となります。 リストア プログラムは、リストア時に通常デフォルト ファイルを検索するため、このパラメータを設定することは推奨されません。
-q	確認プロンプトをオフにします (バックアップを「静かに (quiet)」行います)。通常、既存のバックアップ ファイルを上書きするか尋ねられます。
-d *<debuglevel>*	バックアップ操作の際に表示する情報の量を指定します。*<debuglevel>* には「0」(情報を表示しない) から「10」(すべての情報を表示する) までの整数を指定します。デフォルトは「1」(標準的な情報量) です。
-h	使用可能なパラメータを示すヘルプ リストを表示します。

Config Backup Tool を実行したら、システムの構成ファイルが、上記で指定した名前と場所のバックアップ ファイルに保存されます。同じ場所にバックアップ ファイルがすでに存在する場合は、上書きしても良いか尋ねられます (-q パラメータを使用していない場合)。

メモ： Update Tool を使用して新しいシステム アップデートをインストールした場合、構成が自動的にバックアップされます。その場合、管理者が手動で作成したバックアップは上書きされません。

安全性を高めたい場合は、SCP などのプログラムを使用して .tgz ファイルをアプライアンスから別の場所 (ネットワーク上のドライブやリムーバブル ディスクなど) にコピーします。

Backup Tool をスクリプトに追加することにより、バックアップを自動化できます。その場合、-q パラメータを使用して、確認プロンプトが出ないようにします。

ホストの確認

AMC で作成されるアクセス制御ルールの多くでホスト リソースをポイントしています。ルールが評価されるたびに、アプライアンスではそのようなホストを DNS で解決しようとします。アプライアンスでリソースの追加、削除、変更が行われると、一部のリソースが不要になったり、完全にアクセスできなくなったりすることがあります。解決できないホストがあると、パフォーマンス低下も生じる可能性があります。

アプライアンスで (SSH を使用して) コマンドラインから実行できる「checkhosts」というスクリプトが /usr/local/extranet/bin にあります。このツールは、機能しないホストやアクセスできないホストについてレポートするため、ポリシー評価が最も効率的になるようにリソースやアクセス制御リストを更新するのに役立ちます。

コマンド構文のヘルプを表示するには、次のように入力してください。

```
<appliance prompt>:/usr/local/extranet/bin/checkhosts -h
```

B

トラブルシューティング

トラブルシューティングの概要

ここでは、一般的なトラブルシューティングの方法を紹介し、アプライアンス管理コンソール (AMC) で使用できるトラブルシューティング ツールについて説明します。コア ネットワーキング サービス (DHCP、DNS、WINS など) の障害は予測不能な障害に発展します。

AMC の [**User Sessions (ユーザ セッション)**] ページを使用すると、アプライアンスやアプライアンスの HA ペアのセッションを監視、トラブルシューティング、終了できます。セッションの詳細をまとめて分類できますが、必要があれば、デバイスの分類方法や理由の詳細を表示できます。約 24 時間分のデータが保存され、削除または変更された項目であっても表示されます。ユーザー アクセスとポリシー詳細の表示を参照してください。

一般的なネットワーキングの問題

ネットワーキングの問題のトラブルシューティングのヒントは、解決方法ごとに分類されています。ping ユーティリティを使用する場合は、[**Configure Basic Network Settings (基本ネットワーク設定の設定)**] ページで [**Enable ICMP pings (ICMP Ping を有効にする)**] が有効になっていることを事前に確認してください。これら表にはいくつかのヒントを挙げています。

ネットワーキングの問題のトラブルシューティングのヒント

ユーティリティ	トラブルシューティングのヒント
外部インターフェースの ping	外部インターフェースに ping して、ネットワーク接続を確認します。ホストの IPv4 または IPv6 アドレスには ping できるのに、ドメイン名にはできない場合、名前解決に問題があります。ping コマンドは、コマンドラインまたは AMC 内から発行できます (ping コマンドを参照)。
外部インターフェースでのネットワーク トラフィックのキャプチャ	外部インターフェースがアプライアンスに到着し返されることを確認するために、tcpdump をベースとする、AMC のネットワーク トラフィック ユーティリティを使用します。このネットワーク トラフィック データをテクニカル サポートに送信することも、Wireshark のようなネットワーク プロトコル アナライザを使用して検証することもできます。詳細については、ネットワーク トラフィックのキャプチャを参照してください。
ネットワーク ゲートウェイの ping	外部インターフェースや内部ゲートウェイを ping します。ping コマンドは、コマンドラインまたは AMC 内から発行できます。詳細については、ping コマンドを参照してください。
ping を使用した DNS のテスト	DNS で問題が発生した場合は、最初にクライアントの DNS 解決が動作しているかどうかを確認します。 1 クライアント マシンがインターネットにアクセスできることを確認します。 2 DOS コマンド プロンプトに「ping google.com」と入力します。次のような応答が表示されます。 Pinging google.com [*nnn.nnn.nnn.nnn*] 基本的な DNS 機能が動作していると、角括弧内の IP アドレスが DNS ルックアップによって解決され、基本的な DNS がクライアントで動作していることを確認できます。DNS が動作していないと、ping プログラムが数秒間一時停止してから、ホスト google.com が見つからなかったというメッセージが表示されます。
DNS を使用したアプライアンス ホスト名の解決	DNS の問題がまだ発生する場合、DNS がアプライアンス ホスト名を解決できるかどうかを確認します。上記の ping の手順を繰り返しますが、「google.com」をアプライアンスのホスト名に置き換えます。 ping が次を見つけた場合、 • ping がホスト名のアドレスを見つけられない場合、そのホスト名を処理するはずの DNS サーバーをトラブルシューティングします。ホスト名をアプライアンスの外部インターフェースの IP アドレスに置き換えて、クライアント接続に問題がないか確認します。 • ping がホスト名のアドレスを見つけたのに応答が表示されない (Request timed out (要求がタイムアウトしました)) 場合、ICMP エコーがクライアントとアプライアンスの間のいずれかのホップでブロックされている可能性があります。
ARP の消去	新しい IP アドレスを最近割り当てた場合、ローカルのアドレス解決プロトコル (ARP) キャッシュがファイアウォールやルータなどのネットワーク デバイスから消去されていることを確認します。こうすることで、これらのネットワーク デバイスが古い IP-MAC アドレス マッピングを使用しなくなります。

ネットワーキングの問題のトラブルシューティングのヒント: ハードウェア

ハードウェア	トラブルシューティングのヒント
ケーブル	すべてのネットワーク ケーブルをチェックして、破損しているケーブルがないことを確認します。
ファイアウォールのバイパス	ネットワーク アドレス変換 (NAT) を使用している場合、ファイアウォールによってブロックされる可能性があります。ケーブルを使用して物理インターフェースでノート型 PC をアプライアンスに接続することで、ファイアウォールを一時的にバイパスして、ネットワーク接続を確認します。 このように接続できない場合は、ノート型 PC をアプライアンスの外部インターフェースと同じネットワーク セグメントに (できるだけアプライアンスに近い位置に) 置きます。
スイッチ ポートの構成	SCP ファイルのコピーが遅かったり、Web プロキシやネットワーク トンネル サービスのパフォーマンスが遅かったりする場合、アプライアンスのインターフェース設定とアプライアンスが接続されているスイッチ ポートの構成が異なるために問題が発生している可能性があります。スイッチが誤ってデュプレックス モードを検出している可能性があります (例えば、アプライアンスがフル デュプレックスに構成されているのにスイッチがハーフ デュプレックスを検出しているなど)。Cisco のドキュメントには、同社製のスイッチのこのような問題について記載されています。 この問題を解決するには、オート ネゴシエーションを無効にします。その代わりに、スイッチ ポートを構成して、アプライアンスと一致する設定を静的に割り当てます。両方のスイッチ ポートと両方のアプライアンス インターフェースの設定 (必要であれば、内部と外部) をチェックする必要があります。1 つのインターフェース/スイッチ ポートが一致していないだけでも、パフォーマンスに影響します。 ネットワーク レイテンシが発生していて、アプライアンス/スイッチ ポートの構成は正しい場合、ネットワークの他の場所に問題があります。アプリケーション レベルの問題である可能性もあります (Web プロキシやネットワーク トンネル サービスがアクセスする DNS サーバーの名前解決が遅いなど)。

ネットワーキングの問題のトラブルシューティングのヒント : サードパーティの解決策

サードパーティの解決策	トラブルシューティングのヒント
トラフィックがフィルタリングで除外されていないことの確認	接続失敗時のログ ファイル */var/log/kern.iptables* の内容を確認します。パケットがアプライアンスに到着しているのに **iptables** (アプライアンスで動作するファイアウォール) によってドロップまたは拒否されている場合は、次のコマンドを実行して、**iptables** ルールセットを確認します。 `iptables -L -n -v` **iptables** によってフィルタリングされているトラフィックは、ロギングされますが、外部 syslog サーバーには転送されません。

ダウンロード済みのアップグレード ファイルの確認

システムのアップグレード、リセット、またはロールバックに記載されているように、AMC を使用して、更新バージョンをインストールできます。アップデートがローカル コンピュータに正しく転送されたことを確認するには、.zip ファイルから抽出した .md5 ファイル内のチェックサムと比較します。

PC の MD5 チェックサムを確認するには、Windows ベースまたは Java ベースのユーティリティを使用します。例えば、Microsoft の場合は、File Checksum Integrity Verifier (FCIV) という名前のサポート対象外のコマンドライン ユーティリティを同社のサイトで提供しています。

PC 上のダウンロード済みファイルを確認するには、

1 DOS コマンド プロンプトを開き、次のように入力します。これにより、ダウンロードしたファイルのチェックサムが返ります。

```
fciv <upgrade_filename>.bin
```

2 メモ帳などのテキスト エディタを使用して、対応する .md5 ファイル (MySonicWall Web サイトからダウンロードしたファイル) を開きます。

```
notepad <upgrade_filename>.bin.md5
```

3 2 つのチェックサムを比較します。一致すれば、アップデートを正しく続行できます。一致しない場合は、ダウンロードし直して結果のチェックサムを比較します。それでも一致しない場合は、SonicWall のテクニカル サポートにお問い合わせください。

アプライアンス上のダウンロード済みファイルを確認するには、

1 次のコマンドを入力すると、ダウンロード済みのファイルのチェックサムが返されます。

```
md5sum < 更新ファイル名 >.bin
```

2 対応する .md5 ファイルを開きます。

```
cat <upgrade_filename>.md5
```

3 2 つのチェックサムを比較します。

エージェント プロビジョニングのトラブルシューティング (Windows)

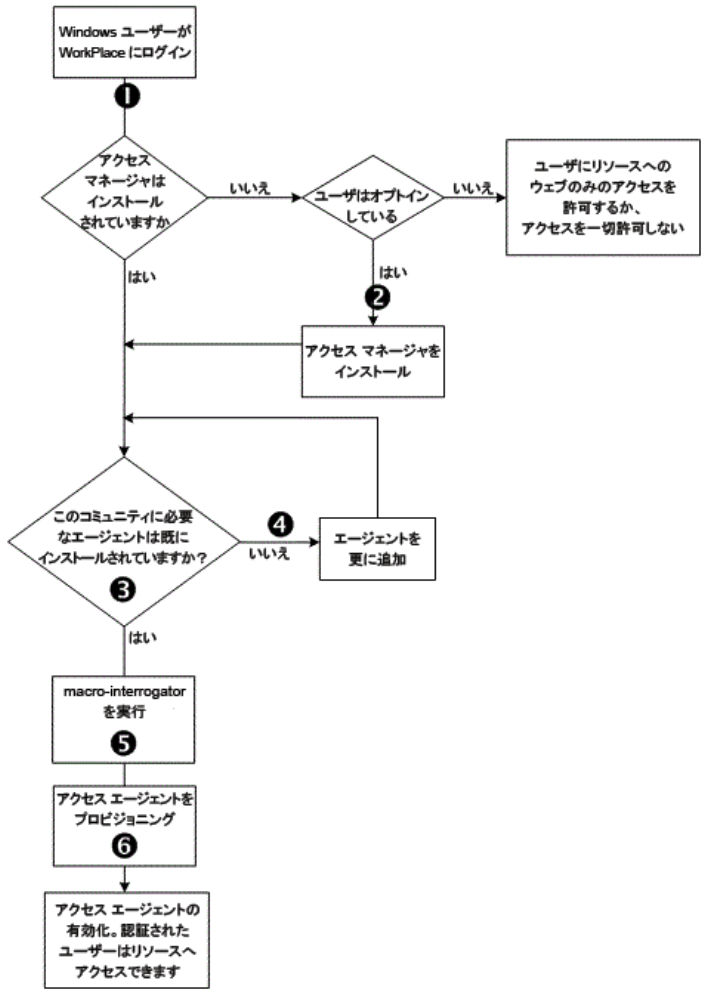
Secure Endpoint Manager (SEM) は、Windows ユーザーによる WorkPlace へのログイン時に EPC とアクセス エージェントをプロビジョニングするコンポーネントです。プロビジョニング時に問題があれば、クライアント インストール ログ (ユーザー名で識別) にエラーが記録され、これを AMC で確認できます。

App データ フォルダにアクセスするには、**Start (スタート) > Run (実行)** をクリックし、「%appdata%」と入力して **Enter** を押します。

プロビジョニング プロセス は、プロビジョニング プロセスの概要を紹介します。ステップ 2 ～ ステップ 6 では、epiBoostrapper.log という名前のファイル

(\Documents and Settings*<username>*\Application Data\Secure Mobile Access\LogFiles\ に保存されています) に情報が追加されます。

プロビジョニング プロセス



エージェント プロビジョニングのトラブルシューティングを行うには:

1 Micro-interrogation (JavaScript が使用され、プラットフォームとブラウザの基本情報が取得されます。)

- Microsoft の OS か? ActiveX が有効か? そうでない場合は、Java が有効か?
- どちらも使用できない場合、エラー メッセージがユーザーに提示されます。

2 MSI (Microsoft Windows Installer) 形式の自己解凍実行可能ファイルである `epiBootstrapper.exe` を取得します。この実行可能ファイルには、ステップ 5 で使用される Macro-interrogator も含まれます。

3 Advanced EPC エージェントのリストを取得し、インストールします。最小でも、`OPSWAT.msi` がインストールされます。

4 コミュニティで必要であれば、追加の Advanced EPC エージェントを取得します。

5 Macro-interrogation: Advanced EPC とその他のデバイス プロファイルの属性 (特定のファイル名や Windows レジストリ キーなど) の両方を検索します。

6 エージェント (例えば、データ保護や OnDemand トンネルなど) をプロビジョニングします。

関連トピックについては、次を参照してください。

- クライアント インストール ログ (Windows)
- クライアントおよびエージェント プロビジョニング (Windows)

AMC の問題

AMC で最もよくあるエラーの 1 つは、構成を変更した後に適用するのを忘れるという問題です。変更後に適用されていない状態の場合は常に、AMC の右上に [**Pending changes (保留中の変更)**] リンクが表示されます。このリンクをクリックして [**Apply Changes (変更の適用)**] をクリックすると、サービスが自動的に再起動します。

AMC の問題のトラブルシューティング

問題番号	解決法
AMC にアクセスできない	AMC にアクセスできない場合は、アプライアンスの内部ネットワーク インターフェースにケーブルを接続し、ネットワークを経由せずに AMC にアクセスできることを確認します。このように接続できない場合は、ノート型 PC を内部インターフェースと同じネットワーク セグメントに (できるだけアプライアンスに近い位置に) 置きます。 それでも AMC にアクセスできない場合は、URL に `https://` プロトコル識別子が付いていることを確認します。また、ポート番号 8443 が URL に含まれていることを確認します。
内部ネットワークで AMC にログインできない	ブラウザから内部ネットワークの AMC にログインできない場合は、クライアントからアプライアンスの内部インターフェースの IP アドレスへのトラフィックが実際に内部インターフェースに到着していることを確認します。`tcpdump` をベースとする AMC のネットワーク トラフィック ユーティリティを使用すると、内部インターフェース (`eth0`) のトラフィックをキャプチャできます。クライアントが AMC へのアクセスを試行すると、クライアントの IP アドレスからのトラフィック TCP SYN パケットはポート 8443 に渡されます。詳細については、ネットワーク トラフィックのキャプチャを参照してください。

AMC の問題のトラブルシューティング

問題番号	解決法
ログインできない	「Invalid Login Credentials（無効なログイン クレデンシャル）」というエラーで AMC ログインが失敗する場合は、ユーザー名とパスワードの綴りが正しいことを確認します。パスワードでは大文字と小文字が区別されます。**Caps Lock** や **Num Lock** が押されていないことを確認します。
CPU 使用率のスパイクが発生している	LDAP または AD 認証サーバーで、ネストされたグループ ルックアップを使用している場合、ルックアップ結果を必ずキャッシュするようにしてください。ディレクトリ ツリー全体を検索すると、時間がかかり、アプライアンスと認証サーバーの両方で CPU 使用率が増加します。

認証の問題

認証サーバーは、レルムで参照されます。

認証の問題のトラブルシューティング

問題番号	解決法
外部認証サーバーへのアクセス	tcpdump をベースとする AMC のネットワーク トラフィック ユーティリティを使用して、外部認証サーバーにアクセスできることを確認します。このネットワーク トラフィック データをテクニカル サポートに送信することも、Wireshark のようなネットワーク プロトコル アナライザを使用して検証することもできます。詳細については、ネットワーク トラフィックのキャプチャを参照してください。
認証サーバーのクレデンシャル	外部サーバーにアクセスするための正しいクレデンシャルが AMC に含まれていることを確認します。LDAP の場合は [**Login DN (ログイン DN)**] と [**Password (パスワード)**] の設定をチェックし、[**Test Connection (接続テスト)**] をクリックします。RADIUS の場合は [**Shared secret (事前共有鍵)**] の設定をチェックします。
認証サーバーのログ	認証サーバーのログを確認します。無効なクレデンシャルを入力していたり、接続に問題があったりしないことを確認します。
LDAP または AD 認証サーバーを使用したユーザー認証で時間がかかりすぎる、またはタイムアウトする	LDAP または AD サーバーでネストされたグループ ルックアップを使用している場合は、ルックアップの結果をキャッシュするようにしてください。ディレクトリの負荷を軽減し、パフォーマンスを向上させるには、[**Cache group checking (グループ チェックをキャッシュ)**] チェック ボックスを選択して、属性グループや静的グループの検索結果をキャッシュします。

エージェントでのパーソナル ファイア ウォールの使用

ファイアウォール製品によっては、Secure Mobile Access エージェントや EPC コンポーネントのプロビジョニング時にセキュリティ アラートが表示されるものもあります。これは、そのファイアウォールが (ポートとプロトコルに加えて) プロセスによってアウトバンド接続を制限しているためです。ほとんどの場合に、ユーザーは、アウトバンド接続を単純に「ブロック解除」または「許可」できます。

Connect Tunnel ユーザーは、パーソナル ファイアウォールを構成して、Secure Mobile Access VPN サービス (`ngvpnmgr.exe`) と Secure Endpoint Manager (`AventailComponents.exe`) がインターネットにアクセスできるようにし、SMA アプライアンスをホスト名または IP アドレスによって信頼されるホストまたはゾーンとして追加できるようにする必要があります。また、Windows Vista ユーザーは、`epiVista.exe` について例外を作成する必要があります。

Trend Micro 製品のように、権限が限定されているユーザーによるファイアウォール設定の上書きを許可しないファイアウォールもあります。ユーザーのアクセス権限が制限されている企業システムの場合、Secure Mobile Access VPN のインストール前にファイアウォールの設定を更新し、ユーザーがセキュリティ ダイアログ プロンプトに応答しなくてすむようにする必要がある場合があります。

企業レベルのパーソナル ファイアウォールのドキュメントをよく読んで、ファイアウォールのポリシーを判断してください。ファイアウォールの更新が必要な場合、すべてのプロセスがポート 443 でアプライアンスと通信できるルールが推奨されます。

Secure Mobile Access サービスの問題

実行中のサービスの簡単な要約を参照するには、メイン ナビゲーション メニューから [**Services**] をクリックします。

トピック:

- Web プロキシ サービスの問題
- Web プロキシ エージェントの問題
- トンネルの問題

Web プロキシ サービスの問題

- AMC のサーバー ログ レベルを一時的に [**Verbose (詳細)**] に上げます。(任意の AMC ページの右上にある [**Pending changes (保留中の変更)**] を必ずクリックしてから、[**Apply Changes (変更の適用)**] をクリックしてサービスを自動的に再起動してください。)
- Web プロキシ サービス ログを参照するには、メイン ナビゲーション メニューの [**Logging (ロギング)**] をクリックし、[**Log file (ログ ファイル)**] リストから [**Web proxy audit log (Web プロキシ監査ログ)**] を選択します。接続要求がログに記述されていることを確認します。
- DNS サーバーが AMC の Web プロキシ サービス [**Server name (サーバ名)**] を Web プロキシ サービス インターフェースに解決できることを確認します。AMC でルックアップ ツール (DNS ルックアップの使用を参照) することも、`nslookup` または `dig` コマンドをコマンド プロンプトから実行することもできます。
- ネットワークで NAT を使用して IP アドレスを変換している場合は、Web プロキシ サービス [**Server name (サーバ名)**] 設定に、NAT を使用して置換される外部 (またはパブリック) IP アドレスが含まれていることを確認します。

Web プロキシ エージェントの問題

Web プロキシ エージェントは、Internet Explorer 7.0 以降による Windows システム上の URL リソースに対するアクセスを提供します。WorkPlace の [**Connection Status (接続状態)**] エリアに [**Secure Mobile**

Access Web proxy (Web プロキシ)] と表示されていれば、クライアントで Web プロキシ モードがアクティブであることを表します。

Web プロキシ エージェントがクライアント マシンで正常に実行中であるかどうかをチェックするには、次の手順を実行します。

1 クライアント マシンで **Ctrl+Alt Delete** を押して、[**Task Manager (タスク マネージャ)**] をクリックします。

2 Windows のタスク マネージャの [**Processes (プロセス)**] リストにプロセス `ewpca.exe` がないかを調べます。このファイルが存在すれば、ネットワーク トラフィックを受信中でなくても、標準 Web モード アクセス エージェントが実行中です。

3 Web プロキシ エージェントがトラフィックを受け取っていることを確認するには、Internet Explorer を起動し、[**Tools (ツール)**] > [**Internet Options (インターネット オプション)**] を選択します。[**Connections (接続)**] タブで、[**LAN Settings (LAN 設定)**] またはアプライアンスへの接続に使用しているダイアルアップ/VPN 接続の [**Settings (設定)**] をクリックします。

4 接続タイプに対応する [**Settings (設定)**] ダイアログで、[**Use automatic configuration script (自動設定スクリプトを使用する)**] チェック ボックスが選択されていて、[**Address (アドレス)**] フィールドに次のアドレスが設定されていることを確認します。

   `http://127.0.0.1:<portnumber>/redirect.pac`

   Internet Explorer は、redirect.pac ファイルを使用して、Web プロキシ エージェントへの送信の接続を判断します。

5 `redirect.pac` ファイルによってリダイレクトされるリソース アドレスを表示するには、このファイルをエディタで開きます。このファイルは、クライアント マシンの次のフォルダに置かれています。

   `\Documents and Settings\<username>\Application Data\SMA1000\ewpca`

`redirect.pac` ファイルの「`//Redirection Rules//`」セクションには、標準 Web プロキシ エージェントによって送信される接続先として定義されているアドレスがリストされています。これらのアドレスは、AMC で定義されているネットワーク リソースと URL リソースのリストから取得されたものです。

トンネルの問題

このセクションでは、ネットワーク トンネル サービスとトンネル クライアントの問題のトラブルシューティング方法を説明します。

トピック:

- インストール
- 接続

参考資料:

- Windows クライアントのトラブルシューティング
- Macintosh と Linux の Tunnel Client のトラブルシューティング

インストール

インストールの問題のトラブルシューティング

問題番号	トラブルシューティングのヒント
Connect Tunnel クライアントがインストールされない	プロビジョニングされるクライアントは、クライアント コンピュータにインストール パッケージとして配備されます。インストール手順が失敗した場合、次のような問題がある可能性があり、それぞれに記載する方法で解決できます。 • システムがサポート対象外である。クライアント コンピュータのシステム ソフトウェアが Connect Tunnel クライアントでサポートされていることを確認します。 • クライアント ソフトウェアがシステム要件と一致していない。ユーザーが WorkPlace にアクセスできる場合、WorkPlace で使用できるクライアントをインストールします。 • ユーザーにローカルの管理者権限がない。Connect Tunnel クライアントをインストールするには、管理者権限が必要です。 • Connect Tunnel クライアントのインストール ログ ファイル (`ngsetup.log`) には、インストールの問題のトラブルシューティングに役立つ情報が記述されています。Windows Vista の場合、このファイルは、デフォルトでは非表示である `ProgramData` フォルダに置かれています。 `[drive:]\ProgramData\SMA1000\ngsetup.log`
OnDemand Tunnel エージェントがインストールされない	OnDemand Tunnel クライアントは、ユーザーが正しく構成されたレルムで認証された後に WorkPlace を閲覧すると、自動的にインストールされ、有効になります。通常、OnDemand Tunnel エージェントは、ユーザーの介入なしで動作するため、WorkPlace が実行中であれば、構成されているリソースにトンネル経由で安全にアクセスできます。OnDemand Tunnel エージェントのインストールまたは有効化が失敗した場合、次のような問題がある可能性があり、それぞれに記載する方法で解決できます。 • OnDemand Tunnel のインストールには、管理者権限が必要である。 • OnDemand Tunnel がこの Workplace レルムで有効にならない。AMC のメイン ナビゲーション ページで、[**Realms (レルム)**] をクリックします。[**Realms (レルム)**] ページに、アプライアンスに定義されているすべてのレルムのリストが表示されます。特定のレルムのネットワーク トンネル サービスに影響する設定を確認するには、レルムの名前をクリックします。[**Configure Realm (設定レルム)**] ページの [**Communities (コミュニティ)**] タブで、[**Access Methods (アクセス方法)**] エリアの [**Edit (編集)**] をクリックします。[**Network tunnel client (ネットワーク トンネル クライアント)**] チェックボックスが選択されていることを確認します。 • システムがサポート対象外である。クライアント コンピュータのシステム ソフトウェアが OnDemand Tunnel エージェントでサポートされていることを確認します。 • ブラウザがサポート対象外である。ユーザーが使用している Web ブラウザが OnDemand Tunnel エージェントでサポートされていることを確認します。システム要件については、クライアント コンポーネントを参照してください。

接続

接続の問題のトラブルシューティング

問題番号	トラブルシューティングのヒント
クライアントが接続できない	コミュニティが OnDemand Tunnel エージェントをサポートしていれば、OnDemand Tunnel エージェントは、ユーザーが WorkPlace で正常に認証された後に、自動的に起動します。 プロビジョニングされる Connect Tunnel は、トンネル セッションを開始するたびに有効にする必要があります。トンネル セッションは何時間もアクティブな状態を維持できます。ネットワーク接続が数秒以上中断されると、トンネル セッションが終了します。例えば、ネットワーク ケーブルが外れたり、ノート型 PC がスリープ状態になったり、ネットワーク リンクのビジー率が高くてレイテンシやパケット ドロップ率が高くなったりすると、中断が発生します。 Connect Tunnel クライアントや OnDemand Tunnel エージェントの接続が失敗する一般的な障害を、以下に説明します。 • アプライアンスに到達できない。Connect Tunnel ログイン ダイアログ ボックスで、[**Properties (プロパティ)**] をクリックします。[**Properties (プロパティ)**] ダイアログ ボックスで、[**Change (変更)**] の下にある [**Login group (ログイン グループ)**] をクリックします。アプライアンスにネットワーク経由で到達できる場合、使用できるレルムのリストが [**Select or enter your login (ログイン を選択または入力)**] に表示されます。アプライアンスに到着できない場合、少ししてから、「The remote network connection has timed out (リモート ネットワーク接続がタイムアウトしました)」というエラー メッセージが表示されます。 • 指定されたアプライアンス アドレスが正しくない。Connect ログイン ダイアログ ボックスで、[**Properties (プロパティ)**] をクリックします。[**Properties (プロパティ)**] ダイアログ ボックスで、[**Host name or IP address of your VPN (VPN のホスト名または IP アドレス)**] が正しいことを確認します。IP アドレスではなくホスト名が入力されている場合、クライアントがホスト名を解決でき、ホスト名がアプライアンスの外部インターフェースの IP アドレスに対応していることを確認します。 • アプライアンスが実行中ではない。アプライアンスが実行中であることを確認します。 • ユーザー名のレルムが無効である。有効なレルムがユーザーに構成されていることを確認します。 • 認証の失敗。ユーザーが正しい認証クレデンシャルを指定していることを確認します。 • クライアント サービスの障害。クライアント ログ (`ngsetup.log`) を取得し、状況の説明と一緒にそのログ ファイルを SonicWall に送信して、分析を依頼します。 • パーソナル　ファイアウォールがトンネル　トラフィックを許可しない。ユーザーのファイアウォールがアプライアンスの FQDN または IP アドレスへの接続を許可するように構成されていることを確認します。
クライアントは接続するが、リソースにアクセスできない	トンネルが確立されると、トンネルを示すアイコンがタスクバーの通知領域に表示されます。この段階で、クライアント コンピュータは、アプライアンスが到達でき、そのユーザーに許可されている、構成済みのすべてのリソースにアクセスできるようになります。クライアントがリソースに到達できない場合、次のような問題がある可能性があり、それぞれに記載する方法で解決できます。 • リソースが定義されていない。AMC で正しいリソースが定義されていることを確認します。 • ユーザーにリソースのアクセスが許可されていない。AMC で、アクセス制御ルールやレルムおよびコミュニティの割り当てを見直して、ユーザーにリソースへのアクセスが許可されていることを確認します。 • アプライアンスのルーティングがリソースに到達できない。アプライアンスとバックエンド リソースとの間に一般的なネットワークの問題がないことを確認します。 • サーバー ソフトウェアの障害。障害の時間を記録し、ネットワーク トンネル サービスが正しく機能しているかどうかを判断し、必要があれば詳細なトラブルシューティングの情報を収集します。

接続の問題のトラブルシューティング

問題番号	トラブルシューティングのヒント
クライアントは接続するが、突然切断される	Connect Tunnel や OnDemand Tunnel の接続は、確立されると、何時間もアクティブな状態が維持されます。ただし、いくつかの理由で、トンネルがそれより早く終了することがあります。トンネル接続が突然切断された場合、次のような問題がある可能性があり、それぞれに記載する方法で解決できます。 • トンネルがアイドル状態であったためにタイムアウトした。アプライアンスのリソースを無駄にしないために、一定時間アイドル状態になると、トンネルが切断されることがあります。 • 管理者がネットワーク トンネル サービスを停止または再起動した。AMC を使用する一般的な構成での処理であれば、確立されているトンネルには影響しません。確立時に有効だった構成で処理が継続します。ただし、アプライアンスの基本的なネットワーキングに影響する構成変更の場合は、既存のトンネルがドロップまたはハングするため、クライアント側で切断して復旧させる必要があります。 • ネットワーク トンネル サービス ログが Info レベル以上に設定されていると、ネットワーク サービスが停止するたびに「Reset Internal Interface and Addressing Information（内部インターフェースとアドレッシング情報のリセット）」というメッセージがログに記述されます。また、サービスが停止状態から起動されるたびに、「 Internal Interface eth0 Address *n.n.n.n* Netmask *n.n.n.n* BCastAddr *n.n.n.n* Subnet *n.n.n.n* (内部インターフェース eth0、アドレス n.n.n.n、ネットマスク n.n.n.n、BCastAddr n.n.n.n、サブネット n.n.n.n)」 (実際の IP アドレス値が設定されます) というメッセージがログに記述されます。ngutil ログの場合は、この同じ状況で「The server is shutting down（サーバーが停止します）」というテキストが記述されます。 • ネットワーク間トンネルが応答しない、または安定しない: トラフィックがクライアントとアプライアンスの間のいずれかのホップで使用可能な帯域幅を占有すると、パケットは、エンドポイントの TCP スタックまたは中間ルータの待ち行列で待機することになります。待ち行列が一杯である場合、パケットは破棄されます。 • ネットワーク トンネル サービスは、TCP SSL 接続経由でトラフィックを送受信します。TCP は、検証可能で使用可能である場合のみ、トラフィックを順番に転送することで、不安定なネットワークに対応できるように設計されています。TCP 実装では、ACK 応答がすぐに返されないと接続が破棄されることがあり、これは、Windows の TCP 実装にも当てはまります。接続が破棄されると、トンネル クライアントは一般的に、20 秒間は接続を透過的に再開しようとします。輻輳によって破棄された場合は、一般的に再開も失敗するため、ユーザーにはトンネルが終了したように見えます。 • クラスタのフェイルオーバが発生し、クライアントの再開が失敗した。クライアントの構成では、アクティブ ノードがスタンバイ ノードにフェイルオーバした場合、クライアントのトンネル再開メカニズムによって、クライアント接続が維持されます。クライアントは、トンネルの再開を 20 秒間試行した後に、試行を中止します。この時間内にフェイルオーバが完了しないと、トンネル接続が破棄されます。正常な終了では、クライアントは再開を試行しないため、すべてのトンネル接続が破棄されます。 • また、フェイルオーバ後のトンネル　クライアントが再開を試行している間に開始した新しいクライアント接続には、既存のクライアントが使用を再開しようとするアドレスが割り当てられます。アドレス割り当てのさまざまな特性によって状況は異なりますが、このような場合は、そのクライアントのトンネルの再開が破棄されます。
クライアントは接続するが、突然切断される (つづき)	• クライアント サービスの障害。クライアント サービス ソフトウェアに障害が発生すると、トンネルが破棄され、エラー ダイアログ ボックスが表示されます。クライアント ログを取得し、状況の説明と一緒にそのログ ファイルを SonicWall に送信して分析を依頼してから、サービスを再起動します。 • サーバー ソフトウェアの障害。アプライアンス トンネル ソフトウェアで障害が発生すると、アプライアンスは自動的にリブートするか、無限にハングする可能性もあります。 • リブートした場合は、/var/log/dump 内の番号付きのディレクトリにクラッシュ ダンプが出力されるため、この情報を取得して分析します。 • アプライアンスがリブートせずにハングした場合は、ハングする前にクラッシュ ダンプが成功している可能性があります。アプライアンスをリブートして、/var/log/dump をチェックして新しいクラッシュ ダンプを探し、この情報を取得して分析します。場合によっては、クラッシュが発生した状況を再現する必要があります。

接続の問題のトラブルシューティング

問題番号	トラブルシューティングのヒント
一般的なサーバーの問題	トンネルの問題は通常、最初にクライアント側で発生します。発生する可能性がある多くの問題は、AMC で、時には SSH コンソールやシステムのシリアル コンソールで、管理者のみが識別できます。詳細については、一般的なネットワーキングの問題を参照してください。
ネットワーク トンネル サービスが動作中でない	シリアル コンソールまたは SSH セッションで、次のように入力します。 `uscat /var/avt/vpn/status` ネットワーク トンネル サービスが構成され、動作中であれば、クライアントの仮想アドレス範囲の情報が表示されます。動作中でないと、シェル プロンプト以外に何も表示されません。ネットワーク トンネル サービスが動作中でない理由を判断する場合、次の項目が役立ちます。 • ライセンスが無効または期限切れである。アプライアンスのライセンスが無効である場合、ログイン後に、すべての AMC ページの右上にライセンス警告が表示されます。SonicWall に問い合わせて、ライセンスの問題を解決する必要がある可能性もあります。 • AMC またはコンソール プロンプトから停止された。AMC の [**Services (サービス)**] ページの [**Network Tunnel Service**] で、ネットワーク トンネル サービスを無期限に停止でき、サービスが停止しているかどうかを示す情報を表示できます。 • サービスが構成されていない、または正しく構成されていない。ネットワーク トンネル サービスには、仮想アドレスやクライアントへの割り当てに関連する情報を構成する必要があります。トンネル サービスの構成が完全でないと、サービスは動作しません。 • サーバー ソフトウェアの障害。ユーザー スペースのネットワーク トンネル サービス コンポーネントで障害が発生すると、一般的には、障害が発生したコンポーネントが再起動します。ログまたは `/var/log/core` のコア ファイルの情報を利用できます。カーネル コンポーネントの重大な障害が発生すると、一般的にクラッシュ ダンプが記録されます。 • クラスタの問題。クラスタ化されたアプライアンスは、クラスタ インターフェース経由での通信が可能である必要があります。安定した通信が可能でない場合、ペアの両方のノードがサービスを提供しようとするために障害が発生したり、両方がスタンバイ状態になってどちらもサービスを提供しなくなったりする可能性があります。

OnDemand の問題

このセクションでは、OnDemand (ポート マッピング) での問題のトラブルシューティング方法を説明します。

トピック:

- OnDemand の一般的な問題
- OnDemand の個別の問題

OnDemand の一般的な問題

OnDemand が正常に動作しない場合、次の診断を実行します。

- OnDemand のテスト
- OnDemand ログ ファイルの表示
- JRE バージョンの検出

- ブラウザでの Java の有効化
- Java コンソールの表示

OnDemand のテスト

OnDemand をテストするために、適切な URL に接続してアプレットを起動し、サポートされているアプリケーションを実行します。

テストでは、次の点を確認します。

- OnDemand が必要なネットワーク アクセス サービスと通信できること。
- Web プロキシ サービスの認証とアクセス制御が動作していること。
- OnDemand が自動的に接続を正しくリダイレクトすること。
- OnDemand が構成されているそれぞれのアプリケーションに接続を作成すること。
- 自動的に起動するように構成されている シンクライアント アプリケーションを OnDemand が起動すること。

OnDemand ログ ファイルの表示

Windows を使用するユーザーの場合、OnDemand の起動時にトラブルシューティング メッセージを含むログ ファイルが作成されます。ログ ファイルは、次の場所に保存されます。

```
%SystemRoot%\Documents and Settings\AllUsers\Application Data\SMA1000\Logfiles\
%SystemRoot%\Documents and Settings\<username>\Application Data\SMA1000\Logfiles\
```

JRE バージョンの検出

OnDemand が正しく動作しない場合、OnDemand でサポートされているバージョンの Java Runtime Environment (JRE) が動作していることを確認します。システム要件については、クライアント コンポーネントを参照してください。また、ユーザーのブラウザで Java が有効になっていることも確認します。ブラウザでの Java の有効化を参照してください。

クライアント コンピュータで動作中の JRE バージョンを検出するには、

- Windows 版 Internet Explorer: ブラウザの Java コンソールを開いて、JRE の情報を表示します。Java コンソールの表示を参照してください。
- Mac OS X のブラウザ: 「**Applications**」フォルダの「**Utilities**」フォルダを開き、「**Java**」フォルダを開きます。Java Plugin Settings プログラムを実行し、メニューから [**About (補足情報)**] をクリックして、動作中のバージョンの情報を確認します。

メモ：Windows の一部のバージョンには、JRE が含まれないことがあり、この場合には、エラー メッセージ (「`jview.exe must exist in \path or you need to set JAVA_HOME (jview.exe が \path に存在するか、JAVA_HOME に設定する必要があります)`」) が表示されます。このメッセージが表示されたにもかかわらず、JRE が Windows コンピュータに存在することがわかっている場合は、[**Environment Variables (環境変数)**] ダイアログで JAVA_HOME に JRE ディレクトリへのパスを設定します。詳細については、Windows のヘルプを参照してください。存在しない場合は、JRE を Windows コンピュータにインストールするか、他のコンピュータを使用する必要があります。

ブラウザでの Java の有効化

OnDemand アプレットが動作するためには、ユーザーのブラウザで Java が有効になっている必要があります。Internet Explorer の場合、Java はデフォルトで有効です。OnDemand が動作していない状態でデフォルトが変更されている可能性がある場合は、ブラウザのマニュアルに記載されている方法で有効にします。

Java コンソールの表示

OnDemand アプレットが起動しない場合、Java コンソールでその理由を確認できます。ユーザーのマシンで、使用している環境に合わせて、次の手順を実行します。

Java コンソールの表示: Windows-Sun JRE ユーザー

1 Sun Java Runtime Environment を実行しているユーザーは、タスクバー通知領域の [Sun Java] アイコンを右クリックすると、Java コンソールにアクセスできます。

2 [**Open Console (コンソールを開く)**] をクリックします。

Java コンソールの表示: Windows 版 Internet Explorer

1 [**Tools (ツール)**] > [**Internet Options (インターネット オプション)**] をクリックし、[**Advanced (詳細設定)**] タブをクリックします。

2 [**Microsoft VM**] の下で [**Java Console enabled (Java コンソールを使用する)**] と [**Java logging enabled (Java のログの使用)**] チェックボックスを選択し、[**OK**] をクリックします。

3 ブラウザを閉じて、もう 1 度開きます。

4 [**View (表示)**] メニューの [**Java Console (Java コンソール)**] をクリックします。

Java コンソールの表示: Mac OS X

1 [Applications (アプリケーション)] フォルダの [Utilities (ユーティリティ)] フォルダを開きます。

2 [Java] フォルダにある **Java Plugin 設定** プログラムを実行します。

3 **Java Plug-in コントロール パネル**で、[**General (一般)**] ページの [**Use Java console (Java コンソールを使用する)**] をクリックします。

OnDemand の個別の問題

このセクションでは、OnDemand の使用中に発生する可能性がある個別の問題のトラブルシューティングのヒントを説明します。

OnDemand の個別の問題のトラブルシューティング

問題番号	トラブルシューティングのヒント
OnDemand が起動しない	OnDemand を起動しようとしているコンピューターで、Java または JavaScript が Web ブラウザで有効になっていることを確認します。 Java がブラウザで有効である場合、OnDemand でサポートされているバージョンの Java Runtime Environment (JRE) を使用していることも確認します。システム要件については、クライアント コンポーネントを参照してください。 これらのオプションの両方が有効であっても OnDemand が起動しない場合、ユーザーのコンピュータで Java コンソールを開き、Java メッセージを参照します。問題の解決にあたって SonicWall テクニカル サポートへの問い合わせが必要な場合、これらのメッセージを確認するよう依頼されます。Java コンソールの表示を参照してください。
OnDemand でアプリケーションが正しく動作しない	ユーザーに、OnDemand [**Details (詳細)**] ページをチェックして、アプリケーション名がアクティブまたは非アクティブのどちらになっているかを確認するように依頼します。複数のアプリケーションが同じローカル IP アドレスおよびポートを使用するよう構成されていると、問題が発生する可能性があります。問題の詳細を参照するには、OnDemand [**Details (詳細)**] ページからログ メッセージをコピーして電子メールで送信するように、ユーザーに依頼します。
OnDemand がインストールされているが、アクティブにならない	Vista SP1 が動作するクライアント コンピュータで ActiveX と UAC (ユーザー アカウント制御) の両方が無効であると、Java がローカル コンピュータに一時ファイルのキャッシュを保存するように構成されている場合を除き、OnDemand をインストールできますが、アクティブにできません。キャッシュ設定を選択するには、コントロール パネルに移動して、Java コントロール パネルを開きます。[**Temporary Internet Files (インターネット一時ファイル)**] エリアで [**Settings (設定)**] をクリックし、[**Keep temporary files on my computer (コンピュータに一時ファイルを保持します)**] を選択します。
サーバー証明書の [**Accept (適用)**] ボタンを使用できない	状況によっては、ユーザーが受け入れられないサーバー証明書を OnDemand がユーザーに提示することがあります。証明書ページの [**Accept (適用)**] ボタンを使用できない場合、OnDemand は、サーバー証明書に問題があることを検出します。この問題の一般的な原因としては、次のようなものがあります。 • クライアント コンピュータとサーバーの間の日付/時刻の不一致。クライアント コンピュータと Web プロキシ サーバーの日付と時刻が正しいことを確認します。 • 証明書の有効期限が切れているか、まだ有効になっていない。 • 証明書情報がサーバー情報と一致していない。 • 証明書チェーンが無効である。

クライアントのトラブルシューティング

このセクションでは、Windows、Mac、Linux のクライアントでのトラブルシューティングについて説明します。

トピック:

- Windows クライアントのトラブルシューティング
- Macintosh と Linux の Tunnel Client のトラブルシューティング

Windows クライアントのトラブルシューティング

Secure Mobile Access インストーラ ソフトウェアは、Java または ActiveX によって、ユーザーのコンピュータにロードできます。このインストーラを他のすべての Secure Mobile Access ソフトウェア コンポーネントと一緒に削除するには、次の手順を実行します。

- ブラウザと Java の設定のリセット
- Secure Mobile Access のコンポーネントのアンインストール
- WorkPlace への再ログイン

ブラウザと Java の設定のリセット

次の手順で、ブラウザと Java の設定をリセットします。Internet Explorer、Google Chrome、および Firefox Mozilla のそれぞれの手順に従います。

- Cookie とキャッシュの消去
- セキュリティ ゾーンのデフォルトへのリセット
- 詳細設定のデフォルトへのリセット
- プライバシー設定のデフォルトへのリセット
- Java キャッシュの消去
- Java キャッシュの有効化

Cookie とキャッシュの消去

Internet Explorer でブラウザの Cookie とキャッシュを消去するには:

1 **Tools (ツール) > Internet Options (インターネット オプション)** をクリックします。

2 [**Delete Files (ファイルの削除)**] と [**Delete Cookies (Cookie の削除)**] をクリックします。

Mozilla Firefox でブラウザの Cookie とキャッシュを消去するには:

1 **Tools (ツール) > Clear Private Data (プライバシー情報の消去)** をクリックします。

2 少なくとも次の 3 つのチェックボックスを選択します。

- **Cookie**
- **キャッシュ:**
- **認証済みのセッション**

3 [**Clear Private Data Now ([プライバシー情報の消去)**] をクリックします。

Google Chrome でブラウザの Cookie とキャッシュを消去するには:

1 **Tools (ツール) > Clear browsing data (閲覧履歴を消去)** をクリックします。

2 少なくとも次の 3 つのチェックボックスを選択します。

- **Cookie と他のサイトやプラグインのデータを削除する**
- **キャッシュを空にする**

3 [**Clear browsing data (閲覧履歴を消去)**] をクリックします。

セキュリティ ゾーンのデフォルトへのリセット

Internet Explorer ですべての Web コンテンツ ゾーンのセキュリティ レベルをリセットするには:

1 **Tools (ツール) > Internet Options (インターネット オプション) > Security (セキュリティ)** タブをクリックします。

2 Web コンテンツ ゾーン (例えば、[**Internet (インターネット)**]) を強調表示し、[**Default Level (既定のレベル)**] ボタンをクリックします。この手順を、それぞれのゾーンについて実行します。

詳細設定のデフォルトへのリセット

Internet Explorer の詳細設定をリセットするには:

1 **Tools (ツール) > Internet Options (インターネット オプション) > Advanced (詳細)** タブをクリックします。

2 [**Restore Defaults (詳細設定を復元)**] ボタンをクリックします。

プライバシー設定のデフォルトへのリセット

Internet Explorer のプライバシー設定をリセットするには:

1 **Tools (ツール) > Internet Options (インターネット オプション) > Privacy (プライバシー)** タブをクリックします。

2 [**Default (既定)**] ボタンをクリックします。

Java キャッシュの消去

Windows システムで Java キャッシュを消去するには:

1 コントロール パネルで、[**Java**] をダブルクリックします。

2 [**Delete Files (ファイルの削除)**] ボタンをクリックします。

3 3 つのすべてのタイプの一時ファイルが削除対象として選択されていることを確認し、[**OK**] をクリックします。

Java キャッシュの有効化

デフォルトでは、一時ファイルのキャッシュがローカル コンピュータに保持されるように Java が構成されています。SMA アプライアンス経由のリモート アクセスで Java を使用している場合、このキャッシュが有効であることを確認します。

1 Windows コントロール パネルで、[**Java**] を開きます。

2 Java コントロール パネルで、[**Temporary Internet Files (インターネット一時ファイル)**] 領域の [**Settings (設定)**] をクリックします。

3 [**Keep temporary files on my computer (コンピュータに一時ファイルを保持します)**] を選択します。

Secure Mobile Access のコンポーネントのアンインストール

すべての Secure Mobile Access ファイルをアンインストールするには:

1 コンピュータを再起動します。この操作によって、ファイルがメモリにロードされていない状態になり、アンインストールが容易になります。

2 すべての Secure Mobile Access コンポーネントを削除します。

   a Windows エクスプローラで、`%WINDIR%\Downloaded Program Files\` を参照します。

   b `Secure Mobile Access Installer` ファイルを右クリックして、[**Remove (削除)**] を選択します。

   c Secure Mobile Access VPN Software をアンインストールします。コンピュータを再起動するよう要求されますが、この手順の最後のステップまで、再起動する必要はありません。

   d **Control Panel (コントロール パネル)**で、[**Add/Remove Programs (プログラムの追加と削除)**] を開きます。

   e それぞれの Secure Mobile Access コンポーネントを削除します。

3 Secure Mobile Access ソフトウェアが ActiveX または Java を使用してインストールされている可能性もあります (わからない場合は、両方の手順を実行してください)。

   ActiveX

   ステップ b をすでに実行した場合は、ここを飛ばして Java の手順に進みます。

   a Windows エクスプローラで、`%WINDIR%\Downloaded Program Files\` を参照します。

   b `Secure Mobile Access Installer` ファイルを右クリックして、[**Remove (削除)**] を選択し、[**OK**] をクリックます。

   c Secure Mobile Access VPN Software をアンインストールします。コンピュータを再起動するよう要求されますが、この手順の最後のステップまで、再起動する必要はありません。

   Java

   a Windows エクスプローラで、`%HOMEPATH%\Application Data\Aventail\EP\` を参照します。

   b `uninstall_ep.exe` をダブルクリックします。

   c Secure Mobile Access VPN Software をアンインストールします。コンピュータを再起動するよう要求されますが、この手順の最後のステップまで、再起動する必要はありません。

4 Windows エクスプローラで `%HOMEPATH%\Application Data\` を参照し、`Aventail` フォルダを右クリックして [**Delete (削除)**] を選択します。

5 コンピュータを再起動します。

WorkPlace への再ログイン

WorkPlace に再ログインし、Secure Endpoint Manager をインストールして、Secure Mobile Access コンポーネントがロードされるようにします。

クライアントまたはエージェントのインストール時に問題が発生すると、クライアント インストール ログにエラーが記録されます。Secure Endpoint Manager がインストールされていると、このログがアプライアンスに自動的にアップロードされ、AMC にリストされます。Access Manager がインストールされていない場合、インストール エラーが発生すると、ログ ファイルをアプライアンスにアップロードするよう要求されます。

追加のログ ファイルを取得するには:

1 `%HOMEPATH%\Application Data\` を参照します。

2 「`Aventail`」という名前のフォルダがあります。このファイルの内容を圧縮し、電子メールで SonicWall テクニカル サポートに送信します。

3 `%ALLUSERSPROFILE%\Application Data\` を参照します。

4 「`Aventail`」という名前のフォルダがあります。このファイルの内容を圧縮し、電子メールで SonicWall テクニカル サポートに送信します。

5 DOS ボックスを開きます (**Start (スタート) > Run (実行)** をクリックし、「`cmd`」と入力して Enter を押します)。

6 コマンド プロンプト ウィンドウに「`ngutil -all > ngutil.txt`」と入力します。

7 `ngutil.txt` ファイルを SonicWall テクニカル サポートに電子メールで送信します。

8 **Start (スタート) > Run (実行)** をクリックし、「`msinfo32`」と入力して Enter を押します。

9 [**System Summary (システムの概要)**] を強調表示し、**Start (開始) > Run (実行)** を選択します。エクスポートしたファイルを SonicWall テクニカル サポートに電子メールで送信します。

Macintosh と Linux の Tunnel Client のトラブルシューティング

Macintosh と Linux のトンネル クライアントの問題をトラブルシューティングする場合は、このセクションで説明するシステムおよびバージョンの情報をユーザーから入手します。ユーザーは、これらの情報を収集する前に、ソフトウェアをアンインストールして再インストールする必要があります。

トピック:

- Macintosh のシステムとアプリケーションの情報
- Linux のシステムとアプリケーションの情報

Macintosh のシステムとアプリケーションの情報

ユーザーからMacintosh のシステムとアプリケーションの情報にリストされる情報を入手します。

Macintosh のシステムとアプリケーションの情報

システム情報	調べる方法
オペレーティング システム	Apple メニューから [**About this Mac (この Mac について)**] を選択します。
Hostfino コマンド	ターミナル アプリケーション (Applications （アプリケーション） > Utilities （ユーティリティ）フォルダの) を開いて、「hostfino」と入力します。この操作によって、プロセッサとカーネルの情報や、使用可能メモリの大きさが表示されます。
OpenSSL	ターミナル アプリケーション (Applications （アプリケーション） > Utilities （ユーティリティ）フォルダの) を開き、次のように入力して、OpenSSL に関する情報を表示します。 `openssl version`
Safari ブラウザ	Saferi メニューから [**About Safari (Safari について)**] を選択します。
Java Virtual Machine (JVM)	1 [Applications （アプリケーション）] フォルダの [Utilities （ユーティリティ）] フォルダを開きます。 2 [Java] フォルダにある **Java Plugin 設定** プログラムを実行します。 3 **Java Plug-in コントロール パネル**で、[**General (一般)**] ページの [**Use Java console (Java コンソールを使用する)**] をクリックします。
システム プロファイラ	1 Apple メニューから [**About this Mac (この Mac について)**] を選択します。 2 [**More Info (詳しい情報)**] をクリックして [**System Profiler (システム プロファイル)**] を開きます。プロファイラには、コンピュータのハードウェアやインストールされているソフトウェアの詳細情報が表示されます。(印刷するように選択して) レポートをすべて出力すると、100 ページを優に超える可能性があります。

Connect Tunnel を起動する場合は、ログ ファイル `/var/log/AvConnect.log` と `/var/log/AventailConnectUI.log` にデバッグ情報が収集されるように設定されていることを確認します。デバッグ モードを有効にするには、Connect クライアントでデバッグ モードを有効にするか、コマンド プロンプトに移動して次のように入力します。

```
/Applications/AventailConnect.app/Contents/MacOS/startct.sh -d
```

Linux のシステムとアプリケーションの情報

問題を再現する前に、デバッグ ログを有効にし、現在のログを消去するように、ユーザーに依頼します。問題が再現されたら、ログを SonicWall サポートにエクスポートします。

[**General (一般)**] タブの [**Enable Debug Logging (デバッグ ロギングを有効にする)**] チェック ボックス、[**Clear Logs (ログの消去)**] ボタン、および [**Export Logs (ログのエクスポート)**] ボタンを使用して、これらの機能を実行します。

AMC のトラブルシューティング ツール

アプライアンスでのセッションの監視、トラブルシューティング、終了を実行できます。また、ユーザー名、レルム (認証サーバー)、コミュニティ、アクセス エージェント、トラフィック ロードなどでセッションをフィルタリングできるため、特定のセッションの要約を簡単に取得できます。ping、traceroute、DNS ルックアップ、ルーティング テーブル ビューアなどの基本ネットワーク ツールやネットワーク トレースの取得やフィルタリングも、バックエンド接続のトラブルシューティングに利用できます。

トピック:

- ユーザー セッションの表示
- DNS ルックアップの使用
- 現在のルーティング テーブルの表示
- ネットワーク トラフィックのキャプチャ
- ネットワーク トンネル クライアントのロギング ツール
- CEM 拡張機能の使用
- ping コマンド
- traceroute コマンド
- スナップショット ツール

DNS ルックアップの使用

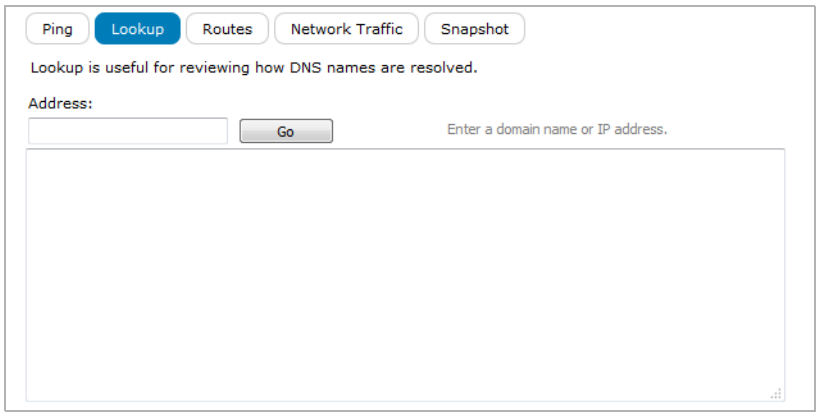
AMC のルックアップ ツールを使用すると、DNS による IP アドレスまたはホスト名の解決方法を確認できます。このツールは、DNS のさまざまな問題のトラブルシューティングに利用できます (例えば、DNS サーバーが動作中であるかどうかを確認できます)。

ルックアップ ツールでは、完全修飾ドメイン名または IP アドレスを使用して、ホストを指定します。ただし、[**Configure Name Resolution (名前解決の設定)**] ページ (AMC の [**Network Settings (ネットワーク設定)**] ページからアクセスできます) でデフォルト検索ドメインを 1 つ以上定義していれば、非完全修飾ホスト名を入力できます。名前解決の詳細については、名前解決の設定を参照してください。

DNS による IP アドレスまたはホスト名の解決方法を確認するには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Troubleshooting (トラブルシューティング)**] をクリックします。

2 [**Lookup (検索)**] タブをクリックします。



3 [**Address (アドレス)**] フィールドに、コマンドを発行するマシンの IP アドレスまたはホスト名を入力します。

4 「**実行**」を選択します。

現在のルーティング テーブルの表示

現在のルーティング テーブルを、AMC で表示できます。

現在のルーティング テーブルを表示するには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Troubleshooting (トラブルシューティング)**] をクリックします。

2 [**Routes (ルート)**] タブをクリックします。

3 「**実行**」を選択します。ルーティング テーブルが表示されます。

ネットワーク トラフィックのキャプチャ

tcpdump をベースとするこのネットワーク トラフィック ユーティリティを使用すると、アプライアンスに出入りするデータのパケット単位のリストをキャプチャできます。トラブルシューティングの経験がない場合は、このユーティリティでネットワーク トラフィック データのファイルを生成し、テクニカル サポートに送信してネットワークの問題のトラブルシューティングを依頼できます。トレース ファイルのトラブルシューティングや解読に精通している場合は、Wireshark などのネットワーク プロトコル アナライザを使用して、トラフィックを分析できます。

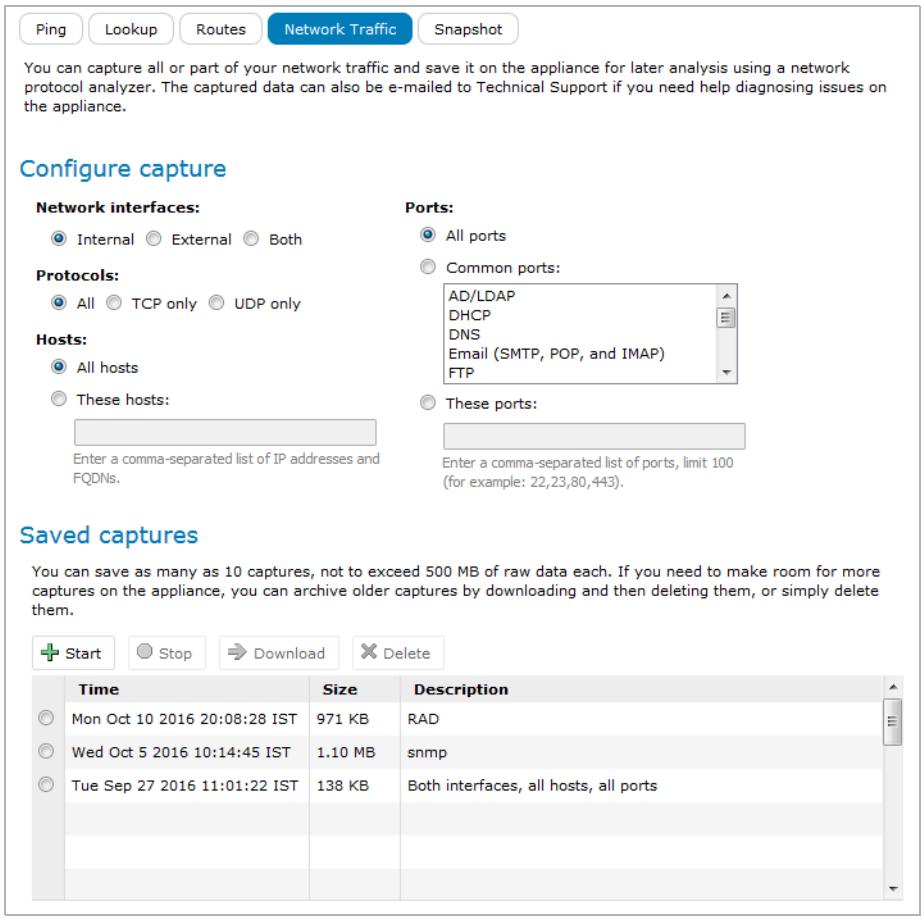
アプライアンスのすべてのネットワーク トラフィックをキャプチャすると、分析が困難になるほどの大量のデータがファイルに出力されます。可能であれば、フィルタを使用して、トラブルシューティングに使用するトラフィックだけに制限します。

次の例では、ホストとポート (この例では、Exchange サーバーと Web トラフィック) でフィルタリングする方法を紹介します。

アプライアンスのファイルにネットワーク トラフィックをフィルタリングし、キャプチャするには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Troubleshooting (トラブルシューティング)**] をクリックします。

2 [**Network Traffic (これらのホスト)**] タブをクリックします。



3 Exchange サーバーが送受信するトラフィックだけにキャプチャを制限するには、サーバーの完全修飾名あるいは IPv4 または IPv6 アドレスを [**These hosts (これらのホスト)**] フィールドに入力します。例えば、「`exchange.mycompany.com`」と入力します。

4 HTTP トラフィックだけをキャプチャするようにするには、[`Web (HTTP or HTTP/S)`] を [**Common ports (共通ポート)**] リストから選択します。これで、HTTP と HTTPS のポート (80、443、8080、および 8443) だけがキャプチャされます。

5 [**Start (スタート)**] をクリックして、トラフィックのキャプチャを開始します。1 回のキャプチャのサイズの上限は、未加工データで 500 MB です。キャプチャ ファイルのサイズが 100 MB になると別ファイルに「ロール オーバ」します (ファイルが大きいと、Wireshark などのパケット分析ツールでの処理が難しくなります)。1 つのキャプチャの合計サイズが 500 MB になると (それぞれが 100 MB の 5 つのファイル)、キャプチャが自動的に停止します。キャプチャの実行中、[**Size (サイズ)**] 列は上限にどれ位近づいているかを表します。

6 [**Stop (停止)**] をクリックして、トラフィックのキャプチャを停止します。キャプチャ ファイルは、アプライアンスに `.zip` ファイルとして保存され、ここに表示されます。(図の [**Size (サイズ)**] 列では、アプライアンスでファイルが使用している大きさを表します。これは圧縮された `.zip` ファイルのサイズであり、未加工データのサイズではありません。)保存できるファイル

の最大数は 10 で、キャプチャ ファイルがさらに追加されると、最も古いファイルがリストから削除されます。

7 キャプチャしたデータをダウンロードするには、分析またはテクニカル　サポートに送信するファイルに対応するボタンをクリックし、[**Download (ダウンロード)**] をクリックします。それぞれのキャプチャ ファイルは .zip ファイル (例えば、eth0.cap) で、キャプチャされたネットワーク トラフィックの概要と、使用されたフィルタとデータがキャプチャされた日時の概要が記述された readme テキスト ファイルが含まれます。

コメント： 内部インターフェース、ホスト： *exchange.mycompany.com*、選択ポート

```
Internal interface (eth0): enabled
External interface (eth1): disabled
Protocol: <All>
Hosts: exchange.mycompany.com
Ports: 80,443, 8080, 8443

開始時刻： 2007 年 8 月 15 日 水曜日 17:56:52 GMT
終了時刻： Wed Aug 15 2007 17:58:31 GMT
```

メモ：キャプチャされたネットワーク トラフィックは暗号化されておらず、パスワードやその他の機密情報が含まれている可能性があります。ダウンロードしたキャプチャの保存やセキュアではないインターネット接続経由での送信でセキュリティが心配である場合は、AMC のスナップショット ツールを代わりに使用します。ネットワーク キャプチャだけが含まれる部分的なスナップショットを作成し、結果の暗号化を選択できます。詳細については、スナップショット ツールを参照してください。

高可用性ペアの片方 (マスタ ノードまたはスレーブ ノード) のアプライアンスのネットワーク トラフィックをキャプデャできます。

ネットワーク トンネル クライアントのロギング ツール

ユーザーがいずれかのネットワーク トンネル クライアントを実行しているセッションをキャプチャするには、以下の手順を実行して結果を電子メールで送信するように、ユーザーに依頼します。Windows の手順は、Macintosh や Linux のユーザーの手順とは異なります。

Windows クライアント コンピュータで ngutil を実行するには、

1 コマンド プロンプトに移動します。**Start (スタート) > Run (実行)** をクリックし、[**Open (オープン)**] フィールドに「cmd」と入力して実行します。Windows Vista を使用している場合は、[**Start (スタート)**] をクリックしてから [**Start Search (検索の開始)**] フィールドに「cmd」と入力して実行します。

2 コマンド プロンプトで、次のコマンドを入力して、イベント ログを消去し、重大度レベルを設定します。

```
ngutil -reset -severity=debug
```

3 ネットワーク　トンネル　クライアントを起動し、システム管理者がログにキャプチャをしたいアクションを実行します。

4 コマンド プロンプトに「ngutil > log.txt」と入力して、バッファされたログ メッセージを現在のディレクトリの log.txt という名前のファイルに書き込みます。

5 log.txt ファイルを管理者に送信します。

6 または、ngutil -poll を実行すると、クライアント コンピュータのリアルタイムのログを参照できます。(**Ctrl-C** を押してログを停止します。)

メモ：「ngutil -tail=1000>client-log.txt」コマンドを入力するようにユーザーに依頼することもできます。このコマンドを実行すると、クライアント ログの最新の 1000 行が client-log.txt という名前のファイルにプレーン テキストで送信されます。

ngutil コマンドの構文の詳細を参照するには、コマンド プロンプトに「ngutil -help」と入力します。

クライアント コンピュータにセッション情報を保存するには (Macintosh または Linux)、

1 ネットワーク トンネル クライアントを起動し、システム管理者がログにキャプチャをしたいアクションを実行します。

2 クライアント デバイスで、AvConnect.log と AvConnectUI.log というファイルを探して、管理者に送信します。

CEM 拡張機能の使用

SonicWall テクニカル サポートから、Secure Mobile Access CEM (Configuration Extension Mechanism) の高度な URL 拡張機能を使用するよう依頼されることがあります。これらの CEM 拡張機能は、高度な AMC ページへのアクセスに使用するものです。テクニカル サポートから指示された場合のみ使用してください。

SonicWall サポートの連絡先はこちらです。https://www.sonicwall.com/ja-jp/support/

CEM の高度な機能

CEM (Configuration Extension Mechanism) は、メンテナンス リリースやホットフィックスで登場する機能をシンプルな構成で使用できるようにするための汎用的なメカニズムです。CEM ページでは、任意のキー値ペアを構成して、高度な機能を有効にできます。これらのキー値ペアは、パッチが生成されたそれぞれのサービスによって、拡張機能の構成ファイルから読み取られます (カスタム ドロップ、ホットフィックス、またはメンテナンス リリース)。

高度な機能は、SonicWall サポートの指示に従って使用してください。追加の指示については、SonicWall サポートにお問い合わせください。

ping コマンド

ping コマンドを使用して、ネットワーク接続を検証します。ping コマンドを実行すると、ICMP ECHO_REQUEST パケットがターゲット ホストに送信され、ホストから応答を待機します。

ping コマンドを実行するには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Troubleshooting (トラブルシューティング)**] をクリックしてから、[**Ping**] タブをクリックします。

2 [**Ping**] ページの [**Address (アドレス)**] フィールドに、ping の宛先であるマシンの IPv4 または IPv6 のアドレスまたはホスト名を入力します。

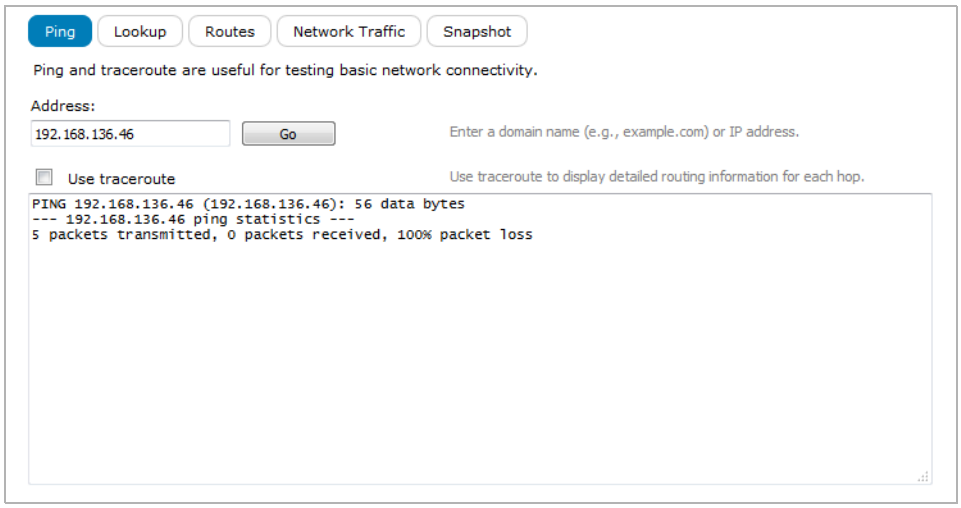
3 「**実行**」を選択します。AMC が ping コマンドを実行します。約 5 秒後に、ページの一番下の大きいボックスに結果が表示されます。ping コマンドがホストに到達できない場合、次のような結果が表示されます。

traceroute コマンド

traceroute コマンドを使用して、IP パケットが宛先に到着するまでに通過するゲートウェイを表示します。この情報は、ネットワークの障害ポイントの特定に役立ちます。

traceroute を実行するには

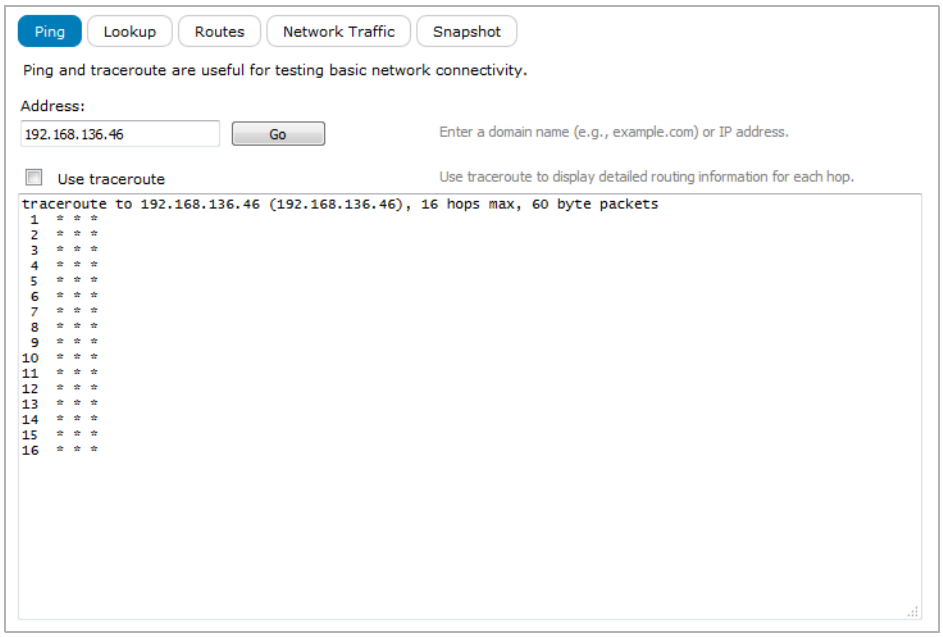
1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Troubleshooting (トラブルシューティング)**] をクリックしてから、[**Ping**] タブをクリックします。



2 [**Address (アドレス)**] フィールドに、`traceroute` コマンドを発行するマシンの IP アドレスまたはホスト名を入力します。

3 [**Use traceroute (traceroute を使用する)**] チェック ボックスを選択します。

4 「**実行**」を選択します。Traceroute から、最初のゲートウェイが始まって宛先で終了するホストのリストが返されます。



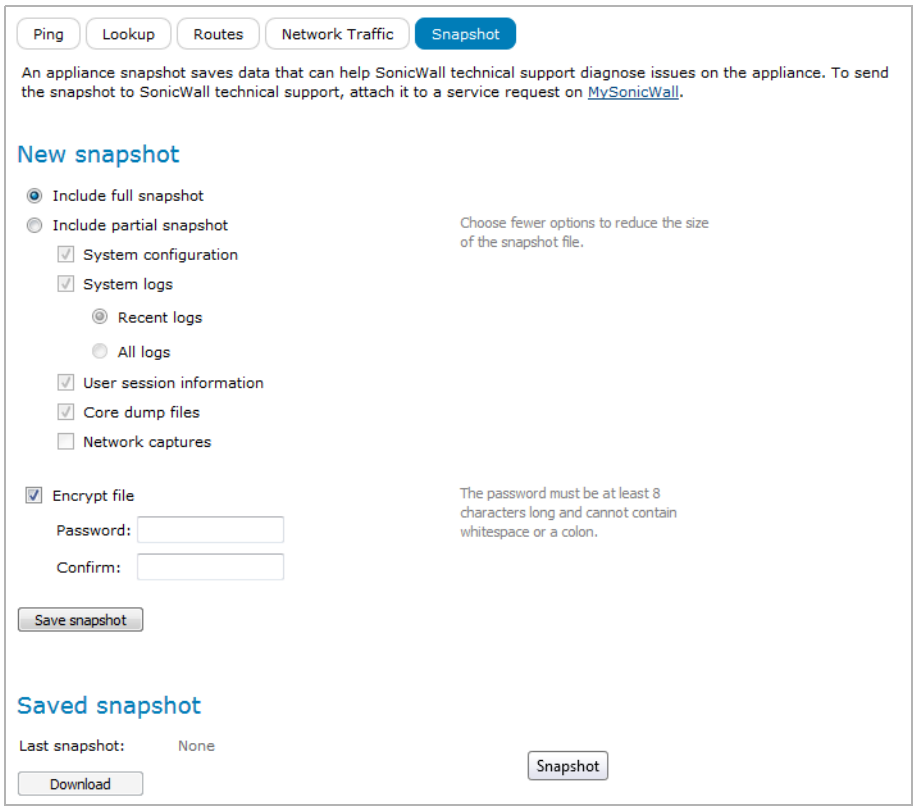
スナップショット ツール

構成の「スナップショット」は、アプライアンスで発生した問題について SonicWall テクニカル サポートやその他の IT 専門家に診断を依頼する際に役立ちます。このファイルは、コア ダンプ ファイルが含まれる場合は特に、とても大きくなることがあります (最後のステップの [File Download (ファイルのダウンロード)] ダイアログで大きさを確認できます)。

構成のスナップショットを保存するには、

1 メイン ナビゲーション メニューの [**Monitoring (監視)**] で、[**Troubleshooting (トラブルシューティング)**] をクリックします。

2 [**Snapshot**] タブをクリックします。



3 フル スナップショットまたは部分スナップショットを選択します。

4 すべてのシステム ログまたは最新の 4 つのシステム ログだけのどちらを保存するかを指定します。

5 [**Save snapshot (スナップショットの保存)**] をクリックします。「`snapshot.tgz`」という名前の zip アーカイブにファイルが保存されます。

6 SonicWall テクニカル サポートに送信する予定がある場合は、機密情報を保護するために、[**Encrypt file (ファイルの暗号化)**] を選択してください。テクニカル サポートがファイルを復号できるようにするために、このアーカイブに割り当てたパスワードを通知する必要があります。必ず、社内のセキュリティ要件を満足する方法 (例えば、電話やセキュアな電子メールなど) で送信してください。

7 [**Download (ダウンロード)**] リンクをクリックして、圧縮ファイルをローカルに保存します。

C

アプライアンス保護のためのベスト プラクティス

ネットワーク設定

次のベスト プラクティス リストにおける設定のほとんどは、AMC の [**Network Settings (ネットワーク設定)**] ページおよび [**Services (サービス)**] ページで構成できます。

- デュアル インターフェースを使用するようにアプライアンスを構成する
- デュアル ネットワーク ゲートウェイを使用するようにアプライアンスを構成する
- 両方のアプライアンス インターフェースをファイアウォールで保護する
- SSH サービスでは、厳格な IP アドレス制約を実施する
- SNMP サービスでは、厳格な IP アドレス制約を実施する
- SNMP コミュニティ文字列には、安全なパスフレーズを使用する
- ICMP トラフィックは無効にするか禁止する
- NTP サーバーを使用する
- アプライアンスが使用することになっているサーバー証明書を保護する

デュアル インターフェースを使用するようにアプライアンスを構成する

アプライアンスでは、外部インターフェースと内部インターフェースの両方が構成されている場合、最適なファイアウォール設定が可能になります。サービスは両方のインターフェースに分割されるため、AMC などの管理サービスはサービスを内部でのみリッスンします。Secure Mobile Access アクセス サービスなどのパブリック サービスは、外部でのみリッスンします。

デュアル ネットワーク ゲートウェイを使用するようにアプライアンスを構成する

デュアル ネットワーク ゲートウェイを使用すると、既存のネットワーク ルータを利用できます。そのため、アプライアンスの管理者の負担が減り、ネットワークが拡大、発展しても、ネットワーク構成の管理が容易になります。

両方のアプライアンス インターフェースをファイアウォールで保護する

- インターネットからのトラフィックは、ポート 80 とポート 443 でのみ許可します。
- アプライアンスは、顧客ネットワーク上の必要なリソースにのみアクセスできるようにします。
- 顧客ネットワークからは、信頼できる IP アドレスのみが AMC にアクセスできるようにします。

SSH サービスでは、厳格な IP アドレス制約を実施する

両方のネットワーク インターフェースが有効な場合、Secure Shell (SSH) は両方のインターフェースでリッスンします。SSH サービスのアクセスは、信頼できる管理ワークステーションの IP アドレスに制限するか、少なくとも内部ネットワークのアドレス範囲に制限します。

SNMP サービスでは、厳格な IP アドレス制約を実施する

両方のネットワーク インターフェースが有効な場合、Network Management Protocol (SNMP) は両方のインターフェースでリッスンします。SNMP サービスのアクセスは、信頼できる管理ワークステーションの IP アドレスに制限するか、少なくとも内部ネットワークのアドレス範囲に制限します。

SNMP コミュニティ文字列には、安全なパスフレーズを使用する

AMC の SNMP 構成では、ネットワーク管理ツールが SMA アプライアンスに照会するために使用する文字列を、[**Community string (コミュニティ文字列)**] フィールドで設定します。この値は、デフォルトで「**公開**」に設定されています。この文字列は、必ず安全なパスフレーズに変更するようにしてください。

ICMP トラフィックは無効にするか禁止する

両方のネットワーク インターフェースが有効な場合、Internet Control Message Protocol (ICMP) を有効にすると、他ユーザーがインターネットからアプライアンスを検出できるようになります。最も安全性の高いアプローチは、ICMP を無効にすることです。ICMP を有効にする場合は、ファイアウォールやその他のネットワーク デバイスを使用して ICMP Echo Request トラフィックを禁止する必要があります。

NTP サーバーを使用する

クロックを外部 Network Time Protocol (NTP) サーバーに合わせ、システム ログに正確なタイムスタンプが記録されるようにします。また、タイムベースのセキュリティ チェックサム (パスワードや証明書の有効期限など) が正常に動作するようにしておきます。

アプライアンスが使用することになっているサーバー証明書を保護する

アプライアンスのサーバー証明書を、他ユーザーがアクセスできる場所に残さないようにし、必ず強固なパスワードを使用して鍵が暗号化されるようにします。攻撃者がこの証明書を入手してしまうと、どのホストのものであるか把握されてしまい、機密データも解読されてしまいます。

アプライアンスの構成

次のベスト プラクティス リストにおける設定のほとんどは、AMC の [**Maintenance (メンテナンス)**] ページで構成できます。

アプライアンスのソフトウェア イメージを最新の状態にする

ホットフィックスやアップグレード ファイルには、セキュリティ関連の修正ファイルが含まれていることが多いため、[**Update (更新)**] ページを使用して速やかに適用するようにします。

定期的に構成をバックアップする

AMC で次のいずれかの方法を使用して、現在の構成を定期的にバックアップします。

- [**Import/Export (インポート/エクスポート)**] ページの [**Export (エクスポート)**] オプション。ローカル マシンへの現在の構成のエクスポートを参照してください。
- 必要であればバックアップをアプライアンスに保存できます。詳細については、現在の構成のアプライアンスへの保存を参照してください。

アプライアンス セッション

AMC セッションは、使用しない状態で 15 分経過すると自動的にタイムアウトします (タイムアウトまでの時間は変更できません)。AMC セッションを終了させるときは、AMC の右上隅にある [**Log out (ログアウト)**] をクリックします。(Web ブラウザを閉じてセッションを終了した場合、そのセッションは、15 分後にタイムアウトするまでの間ログインした状態でリストに表示されます)。

ただし、次のページについては、どちらも [**Auto-refresh (自動更新)**] が設定されているため、これが当てはまりません。

AMC セッション例外

AMC ページ	デフォルト自動更新設定
システム状況	1 分
ログ > ログの表示	1 分

[**Auto-refresh (自動更新)**] が「*オフ*」以外の時間間隔に設定されている場合、いずれかのページが表示されているときに更新動作が持続的に行われるため、15 分経過しても AMC セッションが自動的にタイムアウトしなくなります。これは、オートリフレッシュ モードを有効にした状態で、これら AMC のいずれかのページを表示させたまま席を外すと、AMC がタイムアウトしなくなるということを表しています。セキュリティを向上させるために、システム ステータスやログを表示し終わったら、AMC の他のページに必ず移るようにすることを推奨しています。

管理者アカウント

管理者アカウントを構成する場合、AMC のメイン ナビゲーション メニューで [**General Settings (一般設定)**] をクリックして、[**Administrators (管理者)**] エリアの [**Edit (編集)**] をクリックします。

強固なパスワードを使用する

パスワードは、8 文字以上にし、句読文字、大文字と小文字、数字などを組み合わせるようにします。

AMC 管理者パスワードを変更する

AMC 管理者パスワードは、初期インストールの際、root のパスワードと同じ値に設定されます。AMC 管理者パスワードは、Web ブラウザと AMC サーバーとの間の SSL トンネルで送信されるため、変更

することを推奨しています。プライマリ管理者 (ユーザー名が admin) のパスワードが変更されると、アプライアンスに (root として) 直接ログインするためのパスワードも変更されます。

管理者パスワードは頻繁に変更し、他人と共有しないようにする

特に必要でない限り、管理者パスワードを他人と共有しないようにします。他の管理者にアクセスを許可する必要がある場合は、個別の管理アカウントを作成します。1 人のユーザーが管理者アカウントを持つようにし、パスワードはエスクローとして預けるか、安全な場所に保管しておきます。

管理アカウントの数を制限し、管理権限は、信頼できる個人にのみ割り当てる

セカンダリ管理者のアクセスを制限します。役割ベースの管理により、プライマリ管理者は、セカンダリ AMC 管理者に対して、一定の制約付きで管理制御権限を付与できます。詳細については、管理者の役割の定義を参照してください。

アクセス ポリシー

アクセス ルールを作成、編集、順序変更するときは、AMC のメイン ナビゲーション メニューで [**Access Control (アクセス制御)**] をクリックします。ルールを作成するときは、次のガイドラインを使用します。

- 「最小限の権限」の原則に従う
- ルールの順序には特に注意を払う
- 最も範囲が狭いルールをリストの最初に配置する
- 「any」を含むルールは慎重に監査する

「最小限の権限」の原則に従う

ポリシー設計における最も安全なアプローチは、アクセスを許可したいリソースを個別にリストするというものです。「許可」ルールで指定されていないものはすべてアプライアンスで拒否されます。このアプローチは、「アクセス権は、ユーザーにデフォルトで与えるのではなく、明示的に与えなければならない」という、コンピュータ セキュリティの基本設計原理に基づくものです。

もう 1 つのアプローチは、制限されているリソースに対して「拒否」ルールを作成し、それ以外のすべてのリソースにはデフォルトでアクセスを許可するというものです。この場合、最終的に「拒否」ルールが処理されるまで、「拒否」ルールで指定されていないものはすべてアクセス可能になります。この方法の場合セットアップは簡単ですが、間違いが生じやすいためあまり安全とは言えません。

もちろん、許可ルールと拒否ルールを組み合わせて使用することもできます。その場合、ユーザーに対して、一部のリソースに対するアクセス許可を与えますが、他のリソースについてはアクセスを拒否します。

ルールの順序には特に注意を払う

アプライアンスは、アクセス制御ルールを順番に処理するため、アクセスを許可するか拒否するかという点でルールの順序が非常に重要になります。アプライアンスは、一致するものが見つかればその時点でルールの読み込みをやめます。セキュリティ ポリシーの設定を慎重に検討し、ルールを誤った順序で指定しないよう気を付けてください。

最も範囲が狭いルールをリストの最初に配置する

リストの最初に権限を付与する範囲の広いルールを配置すると、アプライアンスは、範囲が狭いルールを処理する前に一致を見つけてしまう可能性があります。一般に、最も範囲が狭いルールをリストの最初に配置するのがベストです。

「any」を含むルールは慎重に監査する

アクセスを特定のユーザーや特定のリソースに制限しないルールを作成する場合、「any」という言葉がアクセス制御リストで使用されます。

「any」がポリシー ルールで持つ意味について慎重に検討します。「許可」ルールの場合、「any」に適用される基準が多すぎると、セキュリティ ホールをさらすことにもなりかねません。一方、「any」で「拒否」ルールが多すぎる場合は、ネットワーク アクセスを不必要に制限してしまう可能性があります。

信頼ゾーンの設定

ユーザーのエンド ポイントで信頼のレベルに応じて異なるアクセス レベルを割り当てる「信頼ゾーン」を定義できます。接続要求が、AMC で設定されたデバイス プロファイルと比較され、適切なゾーンに割り当てられます。詳細については、End Point Control についてを参照してください。

信頼ゾーンを設定するには:

1. **拒否**ゾーンの設定拒否ゾーンは最初に評価されます。デバイス プロファイルとの一致がある場合 (デバイスで特定のファイルやレジストリ キーが見つかった場合など)、ユーザーはアクセスを拒否され、ログアウトします。詳細については、拒否ゾーンの作成を参照してください。
2. **隔離**ゾーンの設定プロファイルとの一致がないデバイスは、隔離ゾーンに入れられます (定義されている場合)。ユーザーに提示されるメッセージをカスタマイズできます。例えば、そのユーザーが隔離される理由や、ユーザーのシステムをセキュリティ ポリシーに準拠させる上で何が必要かを示すことができます。詳細については、隔離ゾーンの作成を参照してください。

SSL 暗号の有効化

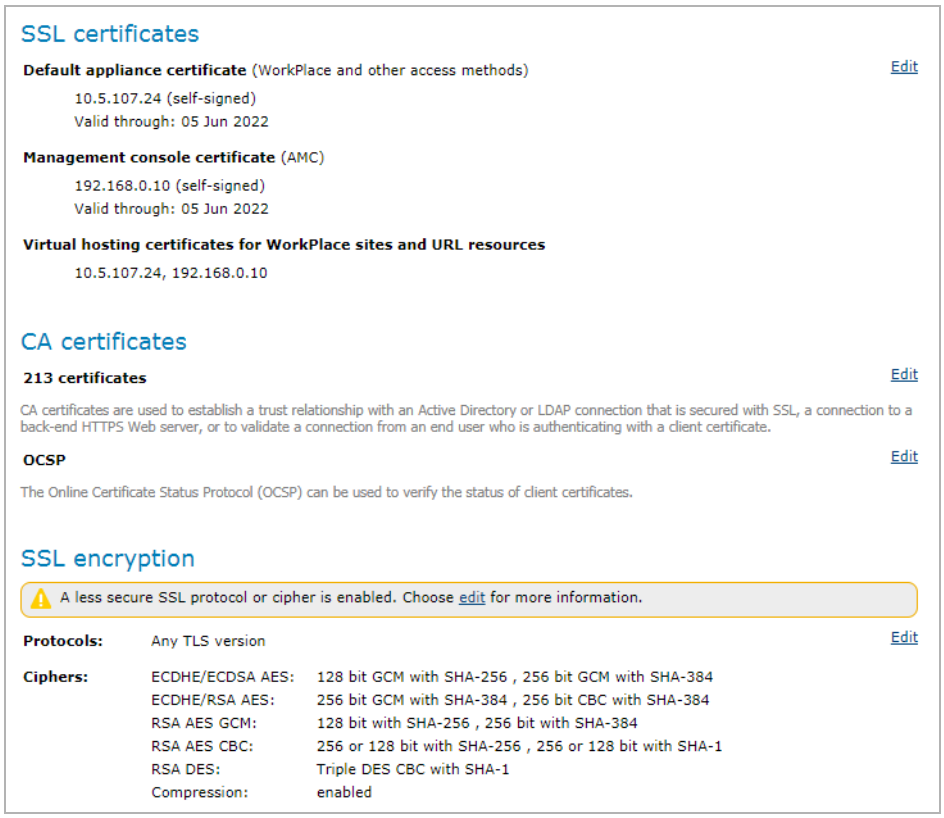
暗号化トラフィックのプロトコルや圧縮設定を構成する際には、1 つまたは複数の暗号を選択できます。アプライアンスでは、ユーザーの Web ブラウザでサポートされているもののうち、セキュリティとパフォーマンスのバランスが最も優れた暗号の組み合わせを使用します。目的の暗号を有効または無効にできます。

AMC、Workplace、Extraweb、および Tunnel はどれも、[**Configure SSL Encryption (SSL 暗号化の設定)**] ページで有効にされる SSL プロトコルに従い、接続クライアントのプロトコルと暗号を強制します。

互換性のない暗号やプロトコルにより、クライアント/ブラウザが SSL 接続のネゴシエートに失敗した場合、AMC は SSL 接続エラーを記録します。これらのメッセージはエラー レベルに記録され、管理者が SSL 互換性問題のトラブルシューティングを行うのに役立ちます。

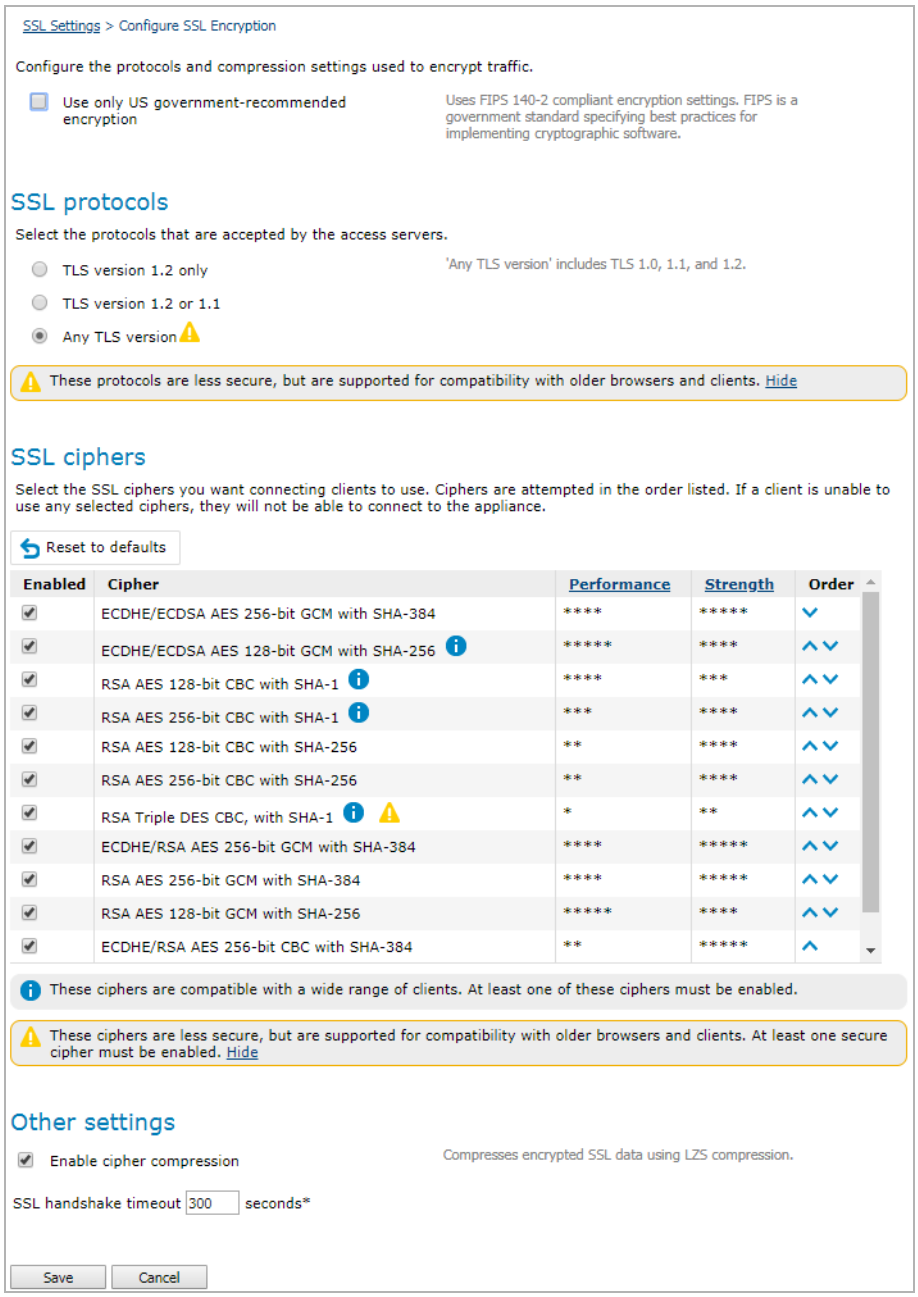
目的の SSL 暗号を有効または無効にするには:

1 **System Configuration (システム構成) > SSL Settings (SSL 設定)** ページに移動します。



メモ：警告は、安全性の低いプロトコルや暗号を有効にした場合にのみ表示されます。

2 SSL 暗号化で、**Edit (編集)** をクリックします。[**Configure SSL Encryption (SSL 暗号化の設定)**] ダイアログが表示されます。新規インストールでは、[**SSL ciphers (SSL の暗号)**] の下に示すように、デフォルトの SSL 暗号化の暗号が表示されます。



3 [**SSL ciphers (SSL の暗号)**] で、目的の暗号を選択します。

有効な SSL の暗号はすべて強制されます。

Suite B のサポート

Suite B とは、米国家安全保障局 (NSA) が、公開ネットワークを通過する情報のセキュリティと整合性を確保するために提供する暗号化アルゴリズムや暗号の群です。

Suite B はこれらの暗号の組み合わせを構成します:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

SMA アプライアンス用のSuite B はこの 2 つの暗号スイートと必要な ECDSA (Elliptic Curve Digital Signature Algorithm: 楕円曲線デジタル署名アルゴリズム) をサポートします。

新しい証明書署名リクエストまたは新しい自己署名証明書を作成する場合、RSA 証明書または ECDSA 証明書のどちらかを選択します。設定オプションは証明書の種類によって異なります。詳細については、Suite B の暗号の構成を参照してください。

有効な暗号とインストールした証明書の間で不一致が生じると、AMC は警告を表示して設定が有効にならないようにします。

SMA Tunnel クライアントとモバイル接続クライアントは Suite B の暗号をサポートします。

SSH 接続は、既存の SSH ネゴシエーション ルールに従って、2 つの Suite B の暗号を含む暗号を使用するようにネゴシエーションします。

Suite B の暗号は、仮想装置を含む現在サポートしているすべてのアプライアンス モデルで有効であり、利用可能です。

Suite B の暗号の構成

ここでは、Suite B の暗号を有効にし、適切な証明書を選択する方法を説明します。

トピック:

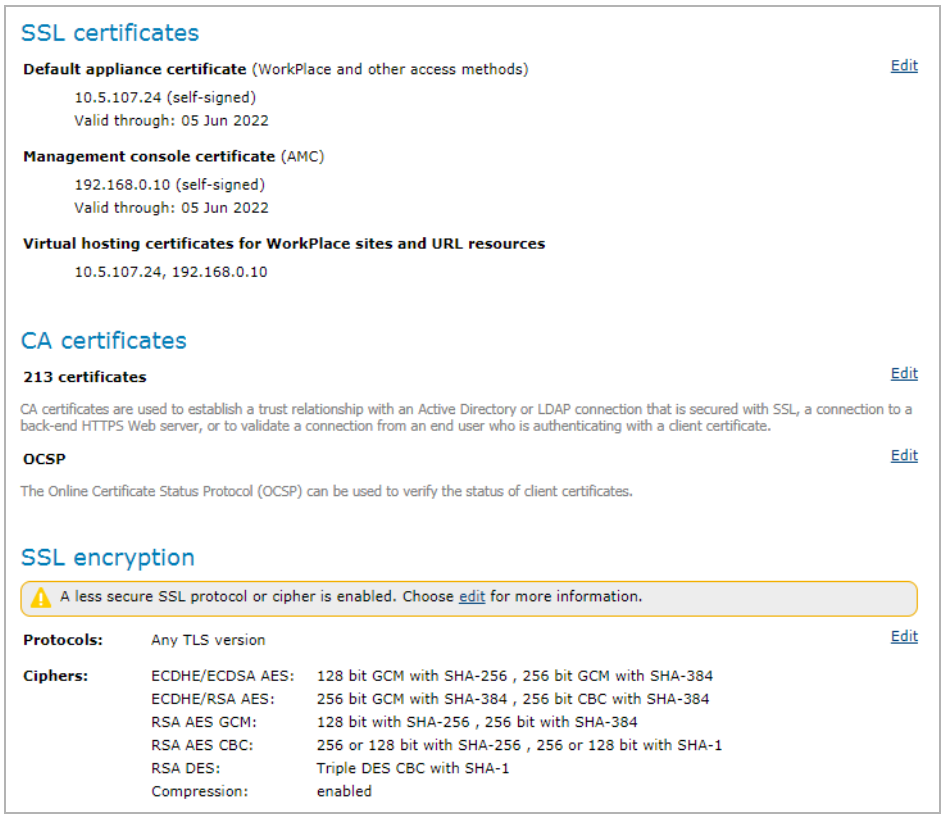
- Suite B の暗号の有効化
- 証明書の選択

Suite B の暗号の有効化

Suite B の暗号を有効にするには:

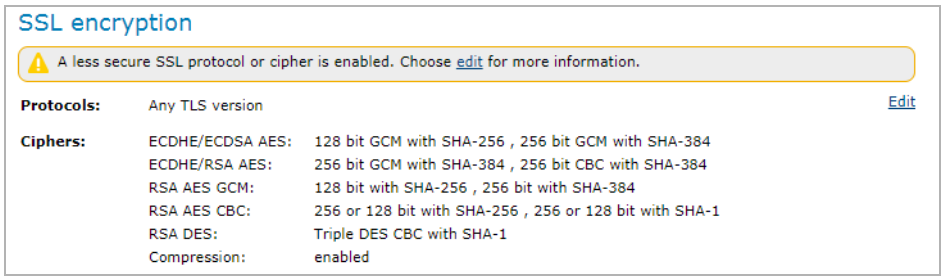
1 SMA アプライアンスで、[**System Configuration (システム構成) > SSL Settings (SSL 設定)**] ページに移動します。

2 [**SSL Encryption (SSL 暗号化)**] で**Edit (編集)** アイコンをクリックします。[**Configure SSL Encryption (SSL 暗号化の構成)**] ページが表示されます。



3 「**Reset to defaults (デフォルトにリセット)**」ボタンを選択します。利用可能な暗号が一覧表示され、Suite B の暗号は一覧の先頭に表示されます。

4 有効にする暗号のチェックボックスをオンにします。[**SSL Settings (SSL 設定)**] ページの[**SSL encryption (SSL 暗号化)**] パネルが更新されて、新たに追加された暗号の状況を示します。

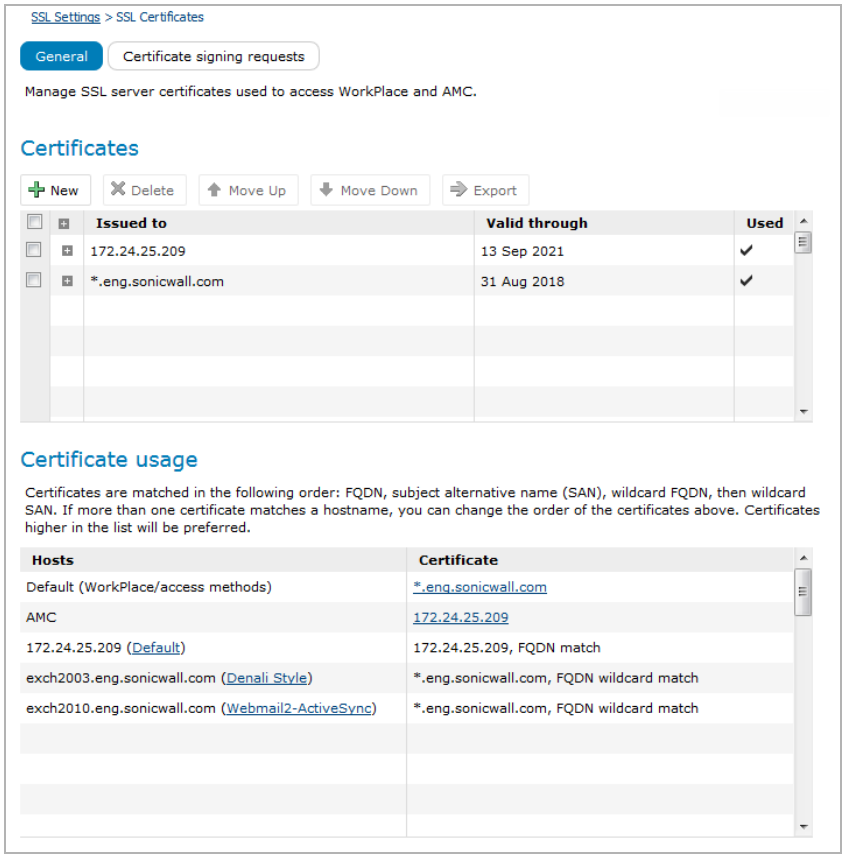


証明書の選択

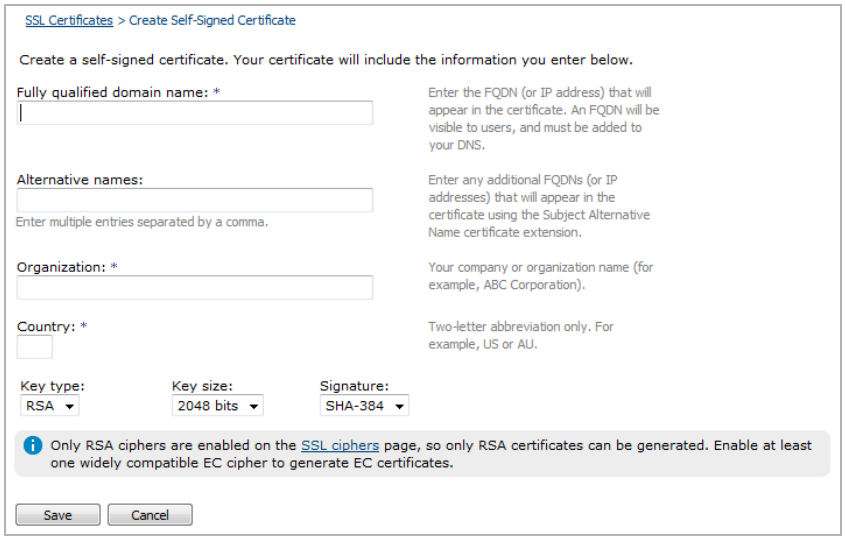
目的の証明書を選択するには:

1 SMA アプライアンスで、[**System Configuration (システム構成) > SSL Settings (SSL 設定)**] ページに移動します。

2 [**SSL Certificates (SSL 暗号化)**] で **Edit (編集)** アイコンを選択します。[**SSL Certificates (SSL 証明書)**]ページが表示されます。



3 **New (新規)** ボタンをクリックして、[**Create self-signed certificate... (自己署名証明書の作成...)**] を選択します。[**Create self-signed Certificate (自己署名証明書の作成)**] ダイアログが表示されます。



4 RSA 証明書にするには、**Key type (鍵種別)** ドロップダウン メニューで、[**RSA**] を選択します。既定の鍵種別は、RSA 暗号を有効にしていない場合を除き、**RSA** です。

5 **Key size (キー サイズ)**ドロップダウン メニューで、目的のサイズを選択します: **2048** ビットまたは **3072** ビット。

6 [**Signature (シグネチャ)**]ドロップダウン メニューで、目的の署名を選択します: **SHA-384** または **SHA-256**。

7 **ECDSA** 証明書にする場合は、**Key type (鍵種別)**ドロップダウン メニューで、**EC** を選択します。**Key type (鍵種別)**として**EC**を選択すると、他のオプションは**Prime size (プライム サイズ)**だけです。

8 必要に応じて **Prime size (プライム サイズ)** を選択します: **256** ビットまたは **384** ビット。

9 証明書の詳細を確認するには、[**SSL Certificates (SSL 証明書)**] ページに移動して、閲覧するデバイスのプラス記号をクリックします。詳細については次を参照してください:

- PSA 証明書は、証明書の**Key size (キー サイズ)** と**Signature (署名)** を示します。
- ECDSA 証明書は、証明書の**Prime size (プライム サイズ)** と **Signature (署名)** を示します。

クライアント アクセス

WorkPlace およびリソースへのユーザー アクセスを制御するには、以下の機能を使用します。

タイムアウト設定を変更する

一定時間内に再認証するようユーザーに求めるには、[**Credential lifetime (クレデンシャル存続期間)**] を設定します。AMC のメイン ナビゲーション メニューで [**General Settings (一般設定)**] をクリックし、[**Appliance options (装置オプション)**] エリアで [**Edit (編集)**] をクリックします。この設定は、すべての SSL セッションに適用されます。トンネル クライアントおよび OnDemand プロキシのセッションにも適用させるには、[**Network Tunnel Client Settings (ネットワーク トンネル クライアント設定)**] ページで [**Limit session length to credential lifetime (セッションの長さをクレデンシャルの有効期間に制限)**] を選択します。

End Point Control コンポーネントを展開する

Secure Mobile Access の End Point Control コンポーネントを使用すると、機密データが保護され、信頼されていない環境の PC からのアクセスを受けてもネットワークが危険にさらされることがなくなります。また、Cache Cleaner に非アクティブ タイマーが搭載されており、一定時間カーソルやポインタが動かず非アクティブな状態が続くと、そのユーザー接続が停止します。EPC はユーザー認証を補足するものあり、ユーザー認証の代わりに使用されることはありません。

連鎖式認証を使用する

セキュリティを向上させるため、Connect Tunnel ユーザーおよび Web ベース アクセスするユーザーに対して、単一のレルムにログインする際に 2 種類の認証方式を使用するよう求めることができます。例えば、RADIUS またはデジタル証明書を最初の認証方法として設定し、LDAP または Active Directory を 2 番目の認証方法として設定できます。設定方法については、連鎖式認証の構成を参照してください。

SecurID のような、強力な二要素認証方式を使用する

二要素認証では、ユーザーの身元や権限を確立するために 2 種類の独立した手段 (通常はユーザーが持っているものとユーザーが知っているもの) を使用します。例えば、SecurID トークンコード (ユーザーが持っているもの) とパスワードまたは PIN (ユーザーが知っているもの) を要求することによって認証を行うことができます。

D

SAML ID プロバイダの設定

SAML ID プロバイダの設定について

この付録は、SMA 認証サーバでの SAML (Security Assertion Markup Language) ID プロバイダの設定方法を説明します。

メモ：ID プロバイダ ユーザ インターフェース (UI) ページは、予告なしに変更されることがあり、本マニュアルで例として使用した UI ページと異なる場合があります。

本マニュアルの設定手順の一部では、手順を完了する前にインターネットからセキュリティ証明書をダウンロードしてインストールする必要があります。正しい証明書は、SMA アプライアンスの [**System Configuration > Authentication Servers (システム設定 > 認証サーバ)**] ページの [**Configure Authentication Server (認証サーバの設定)**] ダイアログの [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン リストから選択できるようになっている必要があります。

証明書のダウンロード 手順は、本マニュアルの設定手順を完了する前に実行する必要があります。どの証明書が必要かは、特定の ID プロバイダ (IdP) の設定手順で決まります。SAML 認証サーバーの設定を参照してください。

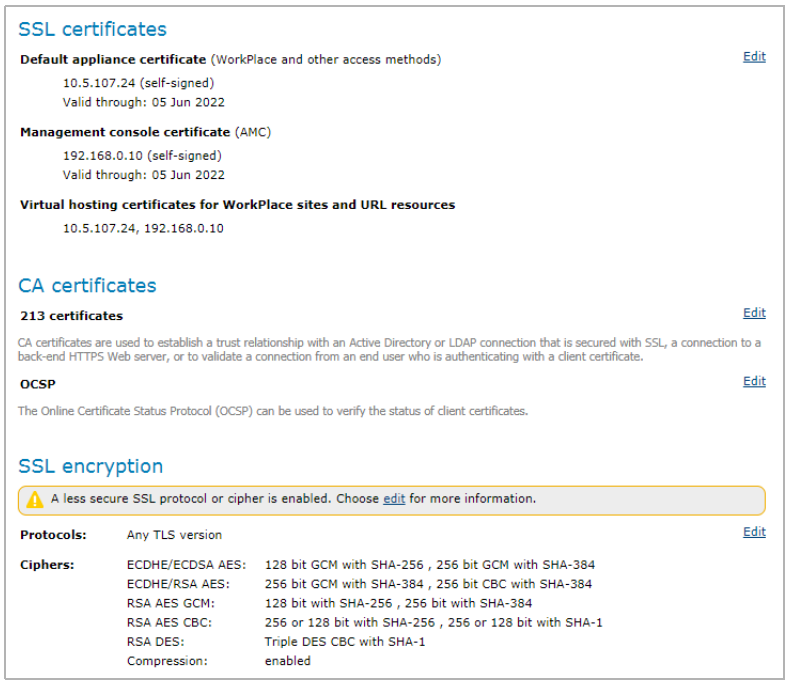
証明書のダウンロード

この手順は、設定手順で [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから証明書を選択する前に実行する必要があります。

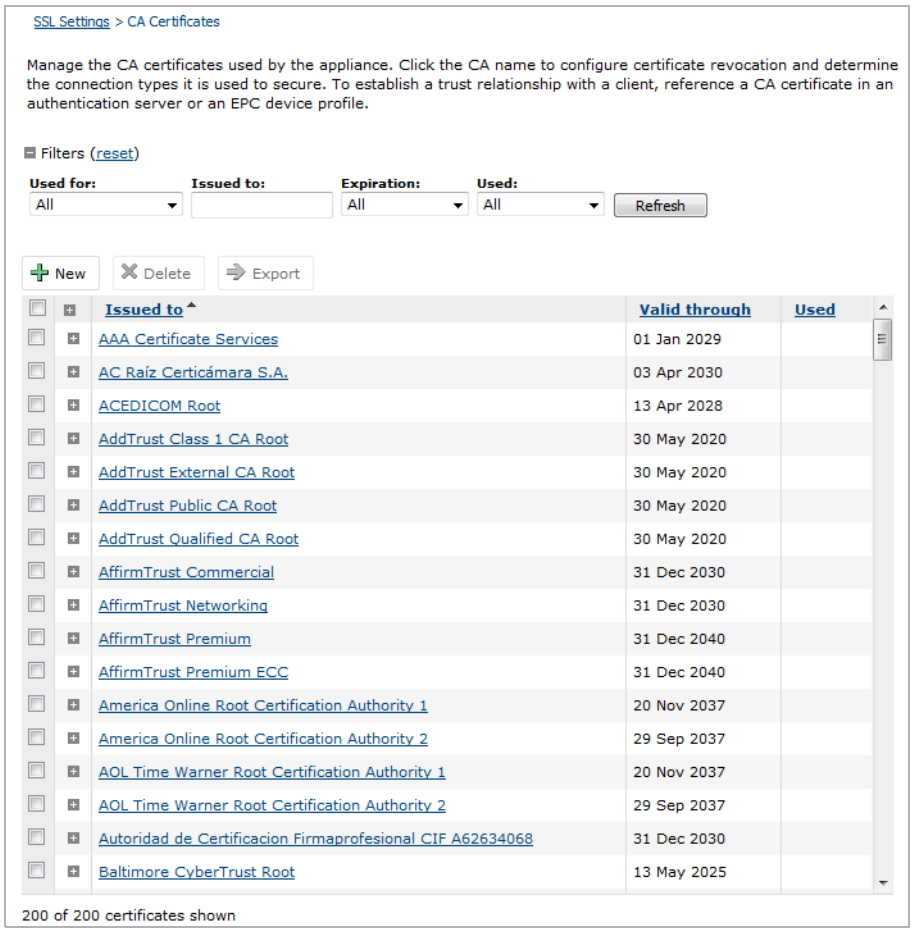
証明書をダウンロードしてインストールするには:

1 アプリケーション登録の際に表示される [**Configure Single Sign-on at <*APP_NAME*>** (<APP_NAME> でのシングル サインオンの設定)] ページから、目的の証明書をダウンロードします。

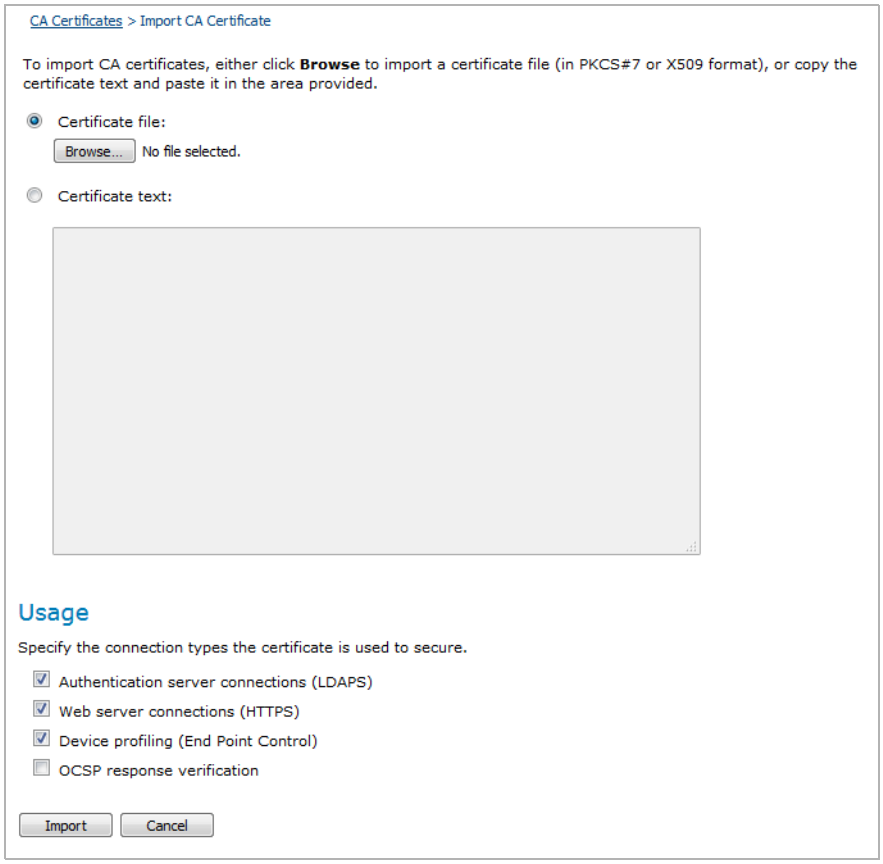
2 **System Configuration (システム構成) > SSL Settings (SSL 設定)** ページに移動します。



3 **[CA Certificates (CA 証明書)]**で、**<*番号*> 証明書**にある**[Edit (編集)]**をクリックします。**[CA Certificates (CA 証明書)]** ページが表示されます。



4 「**New (新規)**」をクリックします。[**Import CA Certificate (CA 証明書のインポート)**] ページが表示されます。



5 以下のいずれかのオプションを選択します。

a **証明書ファイル** を選択して目的の証明書を選択するために参照する。

b **証明書テキスト** を選択して、目的の証明書テキストを入力する。

6 「**インポート**」を選択します。

[**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューに証明書が表示されているはずです。

SAML 認証サーバーの設定

ここでは、各種 SAML 認証サーバ (IDP) を設定する方法を説明します。

これらの設定手順の一部では、SMA アプライアンスにすでに特定の証明書がダウンロードされてインストールされていて、[**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから利用できる必要があります。この手順については、証明書のダウンロードを参照してください。

トピック:

- Azure Active Directory
- 1 つの ID のクラウド アクセス マネージャ
- OneLogin

- Ping ID PingOne
- Salesforce

Azure Active Directory

ここでは、SMA 認証サーバとして Azure Active Directory (AD) を設定する方法を説明します。

トピック

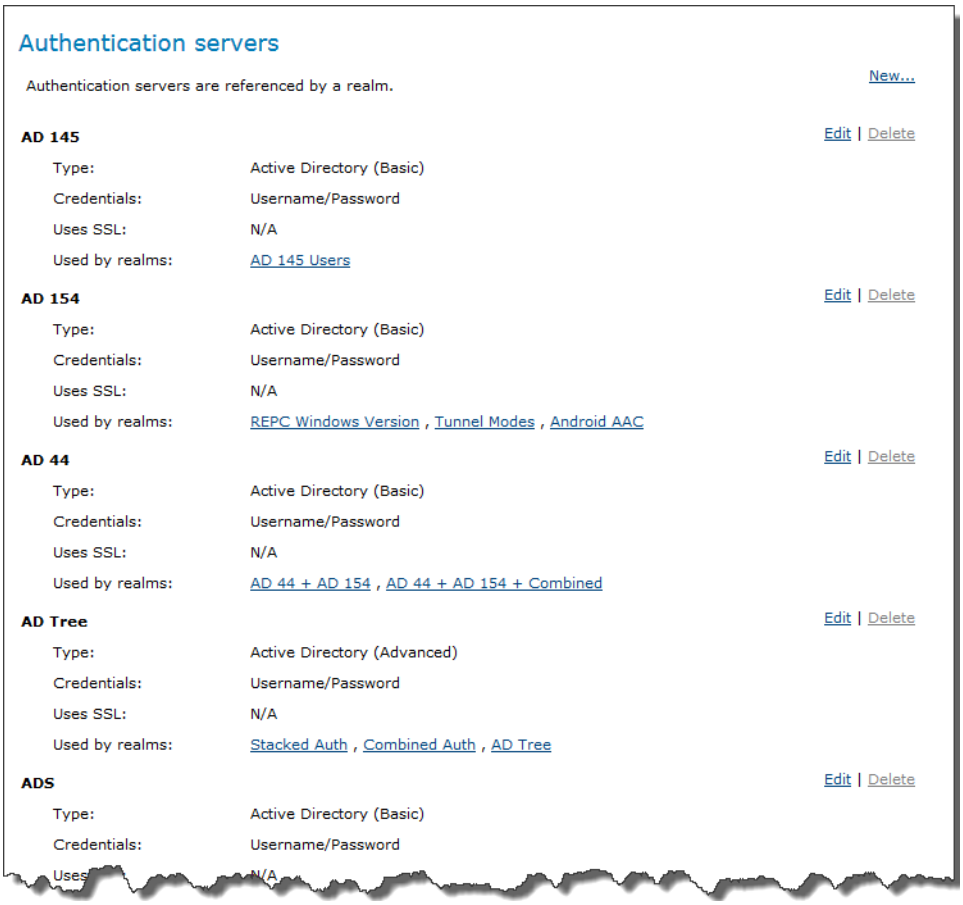
- SMA 認証サーバとしての Azure Active Directory の設定
- SMA アプリケーションを Azure Active Directory に追加する
- SMA アプリケーションのシングル サインオンの設定
- ユーザとグループの SMA アプリケーションへの割り当て

SMA 認証サーバとしての Azure Active Directory の設定

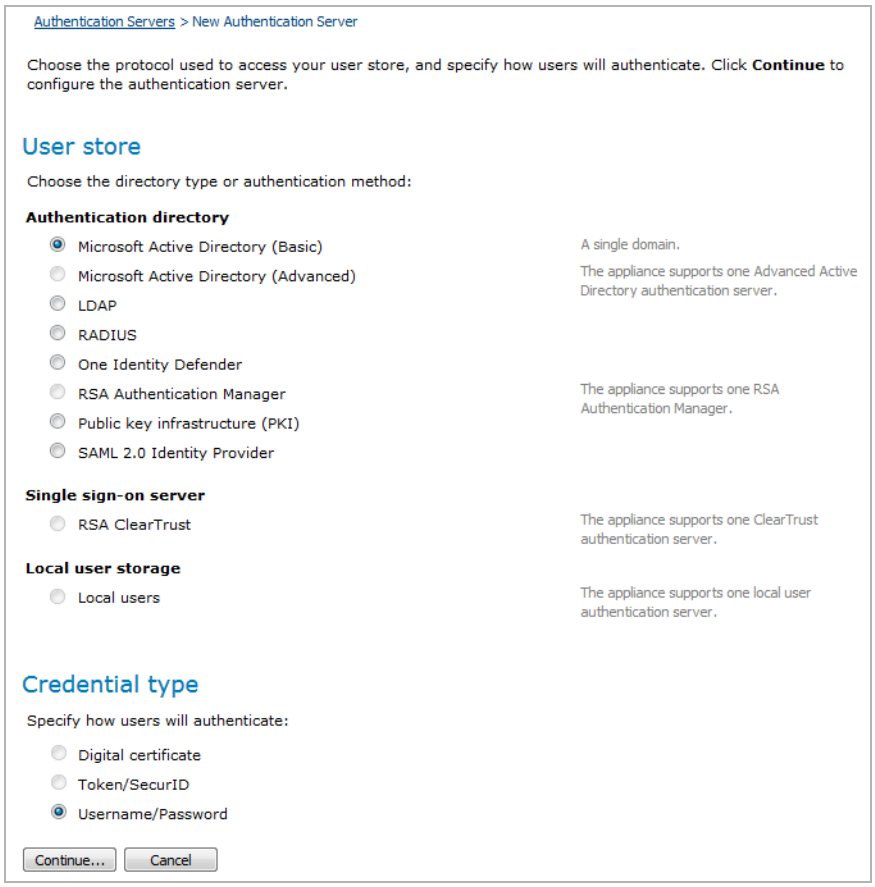
この手順では、SAML ID プロバイダとして Azure AD を設定し、SMA アプライアンス上で認証サーバを作成して設定します。

SMA 認証サーバとして Azure AD を設定するには:

1 SMA アプライアンスで、[**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページに移動します。

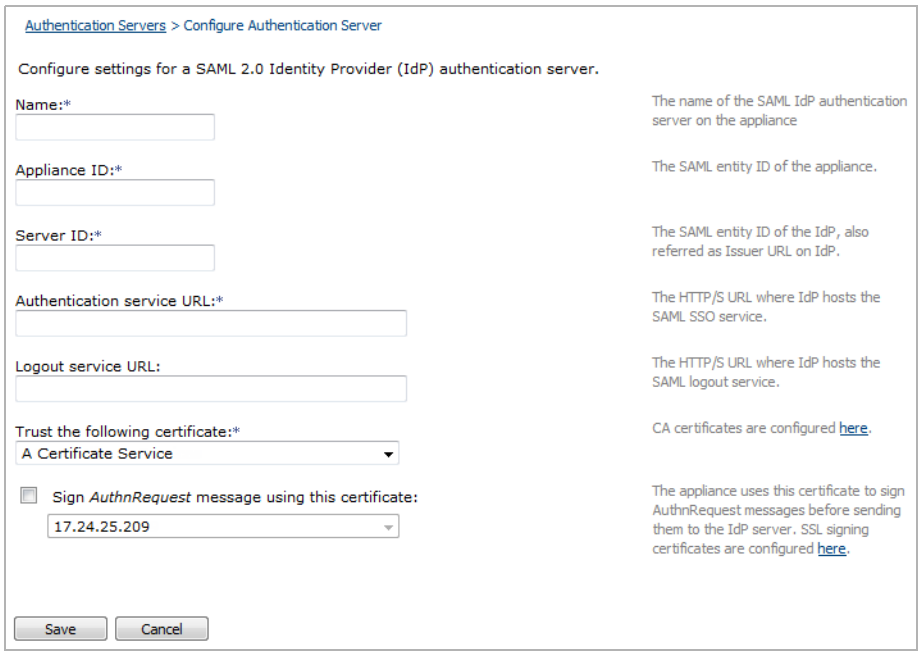


2 [**Authentication servers (認証サーバ)**] で [**New (新規)...**] をクリックします。[**New Authentication Server (新しい認証サーバー)**] ページが表示されます。



3 [**SAML 2.0 Identity Provider (SAML 2.0 ID プロバイダ)**] を選択します。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (認証サーバーの設定)**]ダイアログが表示されます。



以下のステップは、[**Configure Authentication Server (認証サーバの設定)**] ページでフィールドを設定する方法を説明します。

5 [**Name (名前)**] フィールドで、**Azure AD** を入力します。

6 [**Appliance ID (装置ID)**] フィールドで、[**Configure App Settings (アプリ設定の構成)**] ページの [**App ID URL (アプリ ID URL)**] フィールドまたは [**Issuer URL (発行者 URL)**] フィールドからアプライアンスの URL を入力します。例えば、`https://appliance.company.com` です。

7 [**Server ID (サーバ ID)**] フィールドで、[**Configure Single Sign-on at *<APP_NAME>* (*<APP_NAME>* でのシングル サインオンの設定)**] ページの [**Issuer URL (発行者 URL)**] フィールドからサーバの URL を入力します。例えば、「`https://sts.windows.net/db675175-89e4-40f3-xxxx-/`」と入力します。

8 [**Authentication service URL (認証サービス URL)**] フィールドで、[**Configure Single Sign-on at *<APP_NAME>* (*<APP_NAME>* でのシングル サインオンの設定)**] ページの [**Single sign-on service URL (シングル サインオン サービス URL)**] フィールドから URL を入力します。例えば、「`https://login.windows.net/db675175-89e4-40f3-xxxx-/saml2`」と入力します。

9 [**Logout service URL (ログアウト サービス URL)**] フィールドで、[**Configure Single Sign-on at *<APP_NAME>* (*<APP_NAME>* でのシングル サインオンの設定)**] ページの [**Single sign-on service URL (シングル サインオン サービス URL)**] フィールドから URL を入力します。例えば、*https://login.windows.net/db675175-89e4-40f3-xxxx-/saml2* です。

10 目的の証明書を [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから選択します。これは、[**Configure Single Sign-on at *<APP_NAME>* (<APP_NAME> でのシングル サインオンの設定)**] ページの [**Download certificate (証明書のダウンロード)**] になるはずです。

> **メモ**：[**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューに表示されるようにするには、まず、目的の証明書をダウンロードしてインストールする必要があります。設定方法については、証明書のダウンロードを参照してください。

11 (オプション) 必要に応じて [**Sign *AuthnRequest* message using this certificate (この証明書を使用して AuthnRequest メッセージに署名する)**] を選択してから、適切なアプライアンス証明書を選択します。

12 「**Save (保存)**」を選択します。

SMA アプリケーションを Azure Active Directory に追加する

SMA 認証サーバとして Azure Active Directory (AD) を設定した後、SMA アプリケーションを Azure AD サービスに追加する必要があります。

SMA アプリケーションを Azure AD に追加するには:

1 Azure AD にログインして、**Active Directory > *Directory (ディレクトリ)* > Applications (アプリケーション)** を選択します。

2 [**Add an application from the gallery (ギャラリーからアプリケーションを追加する)**] を選択します。[**Application Gallery (アプリケーション ギャラリー)**] で、左側の [**Custom (ユーザ定義)**] 種別を利用してユーザ定義アプリケーションを追加することができます。

3 [**Name (名前)**]フィールドに、SMA アプリケーションの名前を入力します。

SMA アプリケーションのシングル サインオンの設定

SMA アプリケーションの名前を入力したら、シングル サインオン オプションを設定できます。

SMA アプリケーションのシングル サインオンを設定するには:

1 Azure AD で、**SonicWall_SMA** アプリケーション ページに移動します。

2 [**Configure single sign-on (シングル サインオンの設定)**] を選択します。

3 SAML ベースの認証を設定するために、[**Microsoft Azure AD Single Sign-On (Microsoft Azure AD シングル サインオン)**] オプションを選択します。

4 [**Next (次へ)**] 矢印を選択します。[**Configure App Settings (アプリ設定の)**] ダイアログが表示されます。

5 3 つの URL フィールドに目的の URL を入力します:

- **SIGN ON URL (サインオン URL)** - アプライアンスの URL、例えば: `https://appliance.company.com`。
- **IDENTIFIER (識別子)** - [**Configure Authentication Server (認証サーバの設定)**] ダイアログの [**Appliance ID (アプライアンス ID)**] フィールドからの URL。SMA 認証サーバとしての Azure Active Directory の設定を参照してください。
- **REPLY URL (返信 URL)** - アプライアンス ACS URL、例えば: `https://appliance.company.com/saml2ssoconsumer`。

フィールドに必要な URL とその使用方法について説明したツール チップを表示するには、各フィールドのクエスチョン マーク アイコンをクリックします。

6 [**Next (次へ)**] 矢印を選択します。**Configure single sign-on at SonicWall_SMA (SonicWall_SMA でのシングル サインオンの設定)** ページには SMA アプリケーションを有効にして Azure AD から SAML トークンを受け取るのに必要な情報があります。

必要な値はアプリケーションによって異なります。アプリケーションの詳細については、SAML のマニュアルを確認してください。

シングル サインオン サービス URL と **シングル サインアウト サービス URL** はどちらも、この場合は Azure AD の SAML 要求処理のエンドポイントである、同じエンドポイントを解決します。

発行者 URL は SAML トークンの**発行者**フィールドからの URL です。

7 SMA アプリケーションを設定した後、[**Next (次へ)**] 矢印をクリックします。[**Single Sign-On Confirmation (シングル サインオンの確認)**] ページが表示されます。

8 チェック マークをクリックしてダイアログを閉じます。

ユーザとグループの SMA アプリケーションへの割り当て

SMA アプリケーションを、Azure AD を SAML ベースの ID プロバイダとして使用するように設定したら、テストを行う準備がほとんどできました。セキュリティ制御のため、Azure AD は、Azure AD を使用してアクセスする許可が直接、あるいはグループ経由で付与されるまでは、ユーザが SMA アプリケーションにサインインできるようにするトークンを発行しません。

SMA アプリケーションにユーザまたはグループを割り当てるには:

1 Azure AD で、[**Assign Users (ユーザの割り当て)**] ボタンをクリックします。

2 割り当てるユーザまたはグループを選択してから、[**Assign (割り当て)**] ボタンを選択します。

1 つの ID のクラウド アクセス マネージャ

ここでは、SMA 認証サーバとして 1 つの ID のクラウド アクセス マネージャ (CAM) 7.0 を設定する方法を説明します。

トピック

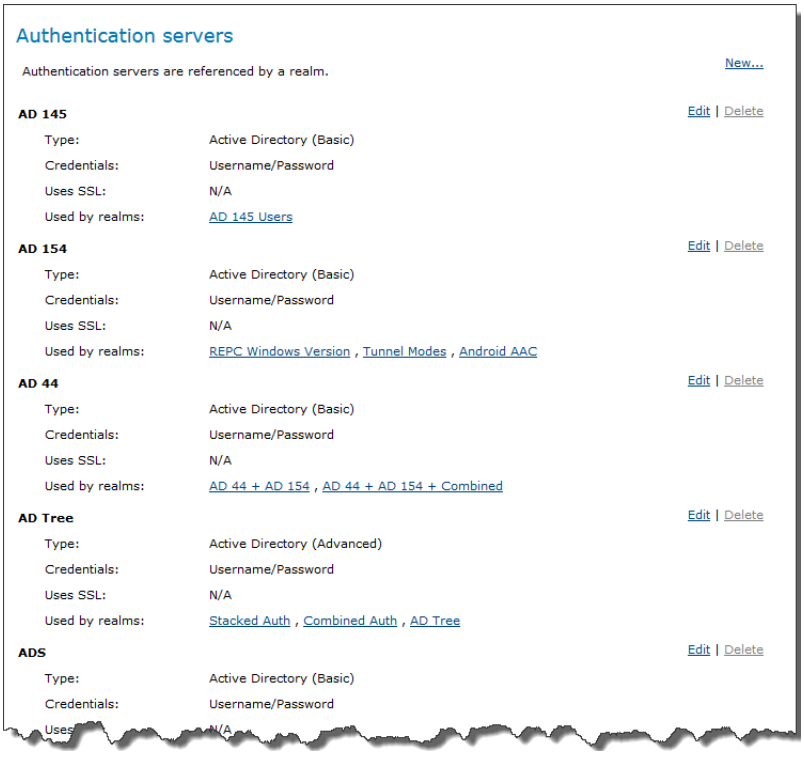
- SMA 認証サーバとしての 1 つの ID CAM の設定
- 1 つの ID のクラウド アクセス マネージャへの SMA アプリケーションの追加

SMA 認証サーバとしての 1 つの ID CAM の設定

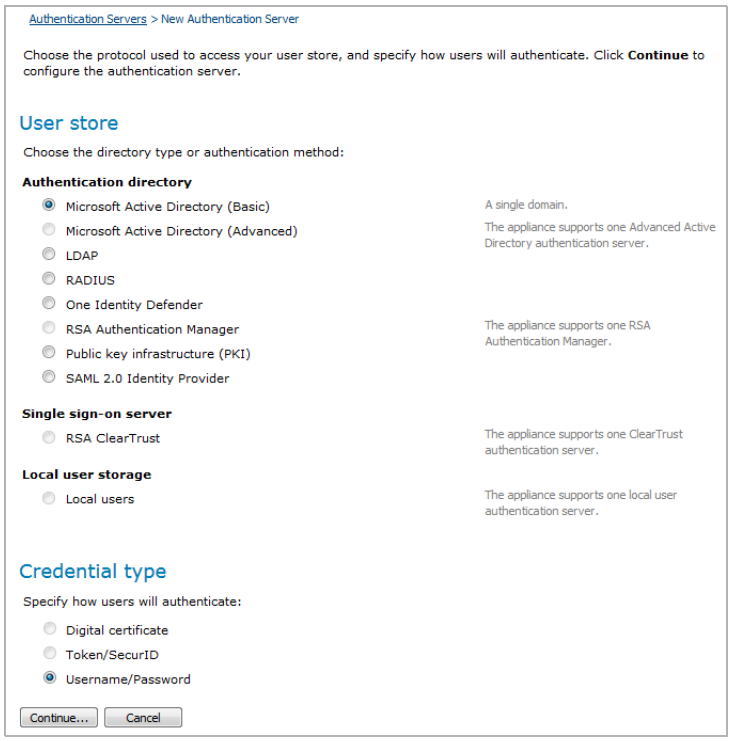
SMA アプライアンスとしての 1 つの ID のクラウド アクセス マネージャ (CAM) の設定は、SMA アプライアンスで 1 つの ID の CAM 認証サーバを設定することで行います。

SMA 認証サーバとして1 つの ID CAM を設定するには:

1 SMA アプライアンスで、[**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページに移動します。

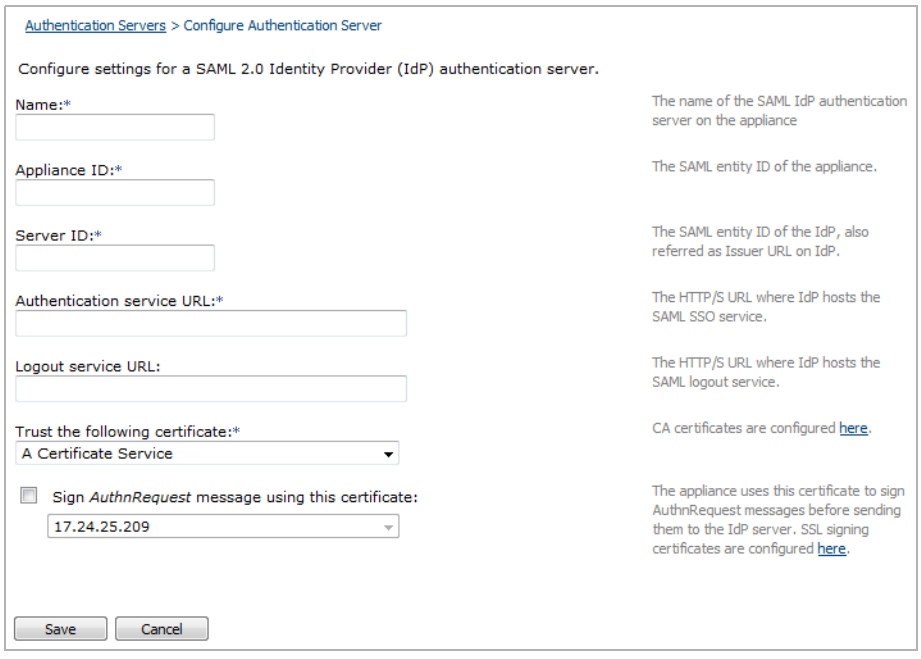


2 [**Authentication servers (認証サーバ)**] で、[**New (新規)**] を選択します。[**New Authentication Server (新しい認証サーバー)**]ダイアログが表示されます。



3 [**SAML 2.0 Identity Provider (SAML 2.0 ID プロバイダ)**] を選択します。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



[**One Identity Cloud Access Manager (1 つの ID のクラウド アクセス マネージャ)**] の[**Application Created (作成したアプリケーション)**] ページから、[**Configure Authentication Server (認証サーバの設定)**] ページのフィールドの値をいくつか取得できます。

以下のステップは、[**Configure Authentication Server (認証サーバの設定)**] ページでフィールドを設定する方法を説明します。

5 [**Name (名前)**] フィールドに、**CAM** と入力します。

6 [**Appliance ID (アプライアンス ID)**] フィールドには、[**Application Created (作成したアプリケーション)**] ページから**Audience/SP Identity (受講者/SP ID)** を入力します。例えば、「`https://appliance.company.com`」と入力します。

7 **Server ID (サーバ ID)** フィールドには、**Application Created (作成したアプリケーション)** ページから**Issuer Entity ID (発行者項目 ID)** または **IDP** を入力します。例えば、「`urn:cam.test.com.test.com/CloudAccessManager/RPSTS`」と入力します。

8 [**Authentication service ID (認証サービス ID)**] フィールドには、[**Application Created (作成したアプリケーション)**] ページから**IDP Login URL (IDP ログイン URL)** を入力します。例えば、「`https://sp16.test.com/CloudAccessManager/RPSTS/Saml2/Default.aspx`」と入力します。

9 [**Logout service URL (ログアウト サービス URL)**] フィールドには、**SSO URL** を入力します。例えば、「`https://cam.test.com.com/CloudAccessManager/RPSTS/Saml2/Default.aspx`」と入力します。

10 目的の証明書を [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから選択します。[**Application Created (作成したアプリケーション)**] ページの[**Certificate (Download Certificate) (証明書 (証明書のダウンロード))**] にある証明書になるはずです。

> **メモ**：このドロップダウン メニューに表示されるようにするには、まず、目的の証明書をダウンロードしてインストールする必要があります。設定方法については、証明書のダウンロードを参照してください。

11 (オプション) 必要に応じて [**Sign *AuthnRequest* message using this certificate (この証明書を使用して AuthnRequest メッセージに署名する)**] を選択してから、適切な証明書を選択します。

12 「**Save (保存)**」を選択します。

1 つの ID のクラウド アクセス マネージャへの SMA アプリケーションの追加

SMA 認証サーバとして 1 つの ID のクラウド アクセス マネージャ (CAM) を設定した後、SMA アプリケーションを 1 つの ID CAM サービスに追加する必要があります。

SMA アプリケーションを 1 つの ID CAM に追加するには:

1 1 つの ID CAM で、「ホームページ」に移動します。

2 [**Applications (アプリケーション)**] で、[**Add New (新規追加)**] を選択します。[**Create a New Application (新しいアプリケーションの作成)**] ページが表示されます。

3 [**Create a New Application (新しいアプリケーションの作成)**] ページで、[**Configure Manually (手動設定)**] を選択します。[**Back-end SSO Method (バックエンド SSO 方法)**] ページが表示されます。

4 [**Back-end SSO Method (バックエンド SSO 方法)**] で、[**Using SAML (SAML の使用)**] を選択します。

5 「**次へ**」を選択します。[**Federation Settings (連邦設定)**] ページが表示されます。

6 [**Federation Settings (連邦設定)**] で、次の URL を入力します:

   a [**Recipient (受信者)**] フィールドに、
   `https://appliance.company.com/saml2ssoconsumer` を入力します。

   b [**Audience/SP Identity (受講者/SP ID)**] フィールドに、
   `https://appliance.company.com` を入力します。

7 「**次へ**」を選択します。[**Subject Mapping (件名割付)**] ページが表示されます。

8 [**Subject Mapping (件名割付)**] で、デフォルトのオプション [**Users from "AD" can't log into this application (「AD」からのユーザはこのアプリケーションにログインできません)**] を選択したままにしておきます。

9 「**次へ**」を選択します。[**Claims Mapping (販売報告割付)**] ページが表示されます。

10 [**Claim Mapping (販売報告割付)**] セクションは空のままにしておきます。

11 「**次へ**」を選択します。[**External Access (外部アクセス)**] ページが表示されます。

12 [**External Access (外部アクセス)**] で、[**This application is external to my network (このアプリケーションはネットワークの外部です)**] を選択します。

13 「**次へ**」を選択します。[**Permissions (権限)**] ページが表示されます。

14 役割[**Permissions (権限)**] ページで、[**Allow Role Access (役割にアクセスを許可する)**] ボタンを使って目的の**Roles (役割)**を選択します。

15 「**次へ**」を選択します。[**Application Name (アプリケーション名)**] ダイアログが表示されます。

16 [**Application Name (アプリケーション名)**] フィールドに、SMA アプリケーションの名前を入力します。

17 「**次へ**」を選択します。[**Application Portal (アプリケーション ポータル)**] ページが表示されます。

18 [**Application Portal (アプリケーション ポータル)**] ページの [**SSO Mode (SSO モード)**] で、[**SP Initiated (開始側 SP)**] を選択します。

19 [**URL**] フィールドに、`https://appliance.company.com` を入力します。

20 必要な他のオプションを選択します。

21 「**完了**」をクリックします。[**Application Created (作成されたアプリケーション)**] ページが表示されます。

   [**Application Created (作成されたアプリケーション)**] ページには、SMA アプリケーションの設定に必要なすべてのシングル サインオンの詳細が表示されます。

OneLogin

ここでは、SMA 認証サーバとして OneLogin を設定する方法と、SMA アプリケーションを OneLogin サービスに追加する方法を説明します。

トピック:

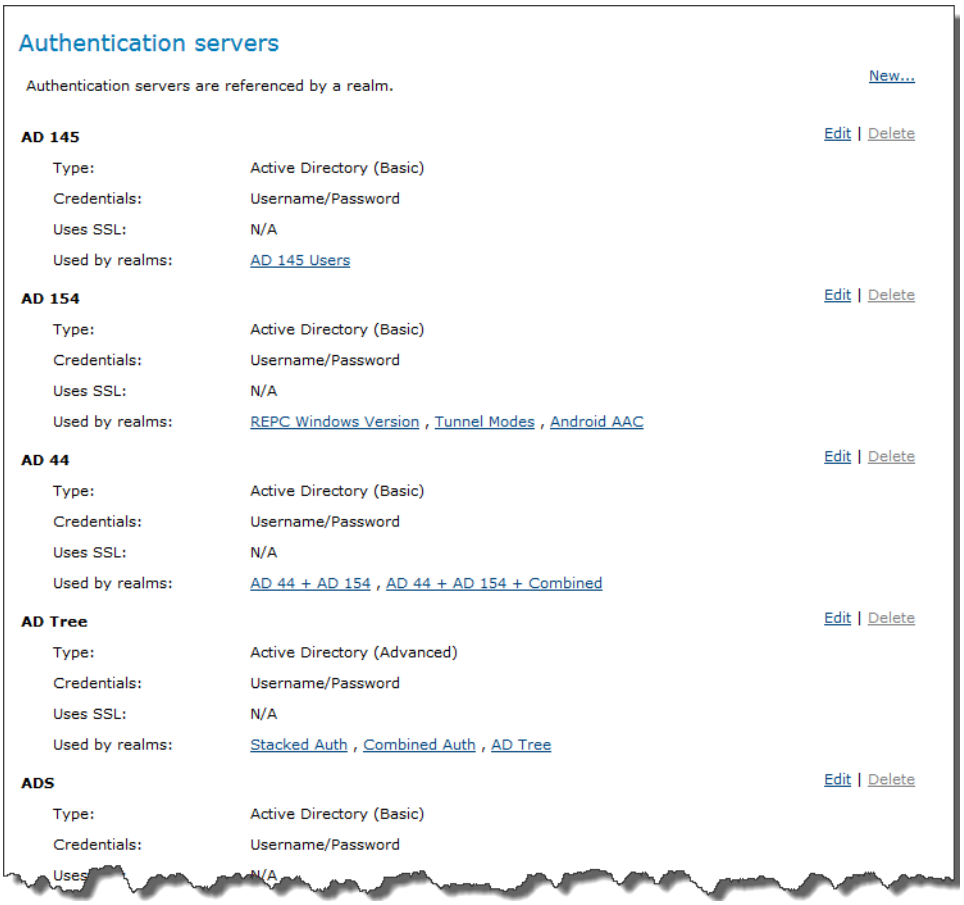
- SMA 認証サーバとしての OneLogin の設定
- SMA アプリケーションの OneLogin への追加

SMA 認証サーバとしての OneLogin の設定

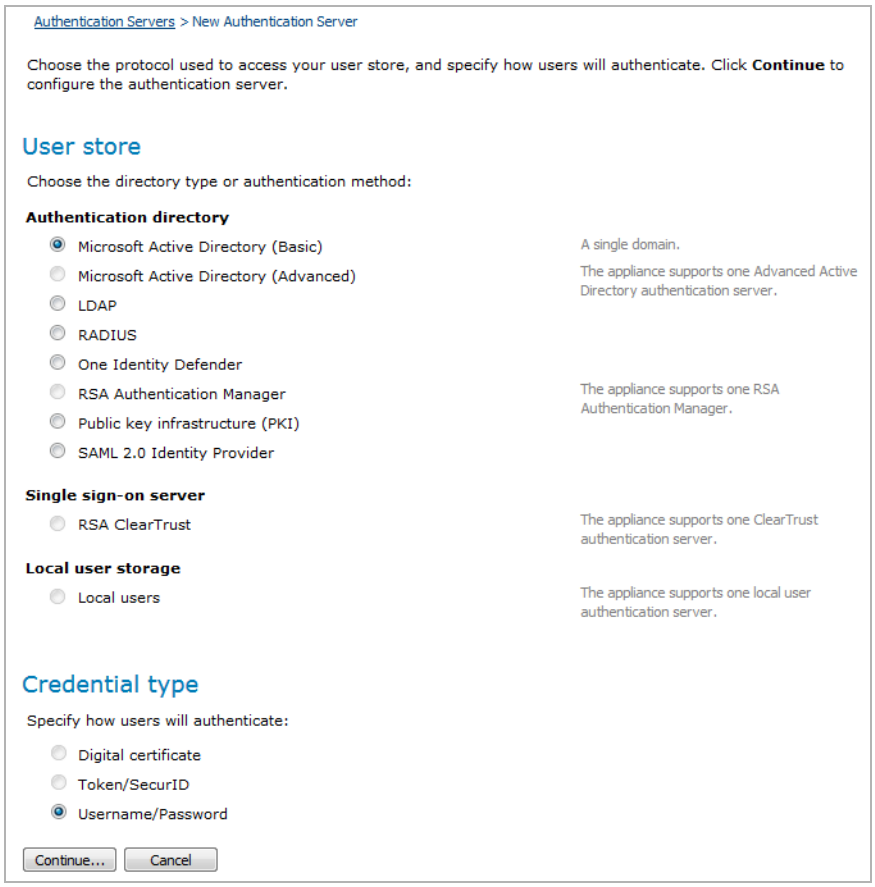
SAML ID プロバイダとしての OneLogin の設定は、SMA アプライアンスで OneLogin 認証サーバを設定することで行います。

SMA 認証サーバとして OneLogin を設定するには:

1 SMA アプライアンスで、[**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページに移動します。

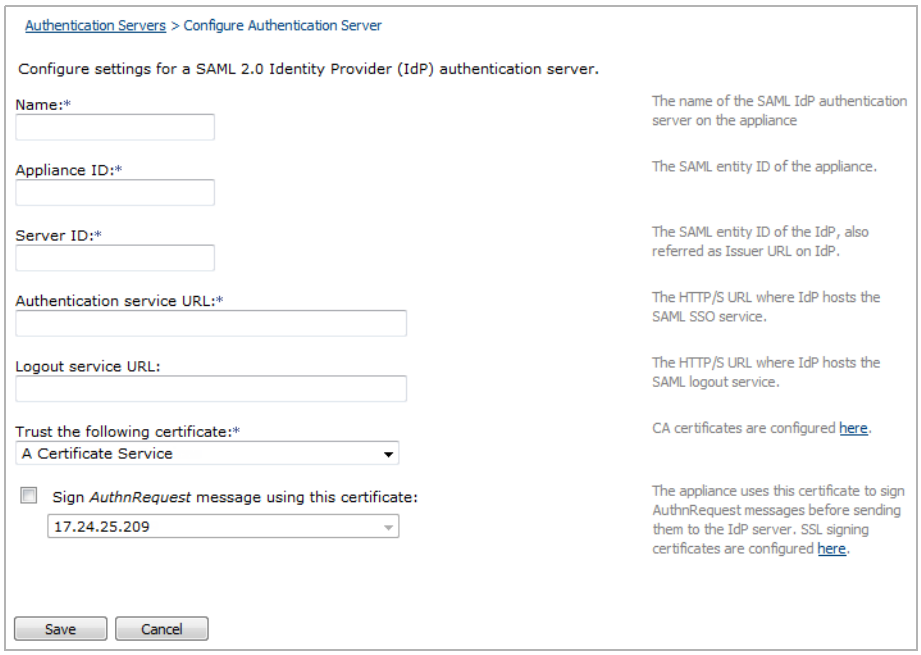


2 [**Authentication servers (認証サーバ)**] で、[**New (新規)**] を選択します。[**New Authentication Server (新しい認証サーバー)**]ダイアログが表示されます。



3 [**SAML 2.0 Identity Provider (SAML 2.0 ID プロバイダ)**] を選択します。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (認証サーバーの設定)**]ダイアログが表示されます。



以下のステップは、[**Configure Authentication Server (認証サーバの設定)**] ダイアログでフィールドを設定する方法を説明します。

5 [**Name (名前)**] フィールドに、**OneLogin_IDP** と入力します。

6 [**Appliance ID (アプライアンス ID)**] フィールドには、[**SonicWall VPN**] ページの [**Configuration (設定)**] タブから**Audience/SP Identity (受講者/SP ID)** を入力します。例えば、「`https://appliance.company.com`」と入力します。

7 [**Server ID (サーバ ID)**] フィールドには、[**SonicWall VPN**] ページの [**Configuration (設定)**] タブから **Issuer URL (発行者 URL)** を入力します。例えば、「`https://app.onelogin.com/saml/metadata/xxxx`」と入力します。

8 [**Authentication service URL (認証サービス URL)**] フィールドには、[**SonicWall VPN**] ページの **SSO** タブ から**IDP Login URL (IDP ログイン URL)** を入力します。例えば、「`https://company.onelogin.com/trust/saml2/http-post/sso/xxxx`」と入力します。

9 [**Logout service URL (ログアウト サービス URL)**] フィールドには、[**SonicWall VPN**] ページの **SSO** タブ から**SLO エンドポイント (HTTP)** を入力します。例えば、「`https://company.onelogin.com/trust/saml2/http-redirect/slo/xxxx`」と入力します。

10 [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから**X.509 証明書**を選択します。

> **メモ**：このドロップダウン メニューに表示されるようにするには、まず、この証明書をダウンロードしてインストールする必要があります。設定方法については、証明書のダウンロードを参照してください。

11 (オプション) 必要に応じて [**Sign *AuthnRequest* message using this certificate (この証明書を使用して AuthnRequest メッセージに署名する)**] を選択してから、適切なアプライアンス証明書を選択します。

12 「**Save (保存)**」を選択します。

SMA アプリケーションの OneLogin への追加

SMA 認証サーバとして OneLogin を設定した後、SMA アプリケーションを OneLogin サービスに追加する必要があります。

SMA アプリケーションを OneLogin サービスに追加するには:

1 OneLogin で、**ホーム**ページに移動します。[**Find Applications (検索アプリケーション)**] ページが表示されます。

2 [**Find Applications (検索アプリケーション)**] で、検索フィールドに「**sonicwall**」と入力して「Enter」を押します。[**Add Sonicwall VPN (Sonicwall VPNの追加)**] ページが表示されます。

3 [**Portal (ポータル)**] パネルで、[**Display Name (表示名)**] フィールドに「**SonicWall VPN**」と入力します。

4 [**Connectors (コネクタ)**] パネルで、[**Connector Version (コネクタ バージョン)**] として **SAML 2.0** を選択します。

5 「**Save (保存)**」を選択します。[**Sonicwall VPN**] ページが表示されます。

6 「**設定**」タブを選択します。

7 [**Appliance (アプライアンス)**] フィールドに、アプライアンスの FQDN を入力します。例えば、「`https://appliance.company.com`」と入力します。

8 [**SSO**] タブを選択します。

9 [**Enable SAML 2.0 (SAML 2.0 を有効にする)**] パネルでは、[**X.509 Certificate (X.509 証明書)**] フィールドで、[**View Details (詳細の表示)**] を選択します。[**Standard Strength Certificate (標準強度の証明書)**] ダイアログが表示されます。

10 CA 証明書を SMAアプライアンスにアップロードするには、[**Download (ダウンロード)**] ボタンを選択します。

Ping ID PingOne

ここでは、SMA 認証サーバとして Ping ID PingOne を設定する方法と、SMA アプリケーションを Ping ID PingOne サービスに追加する方法を説明します。

トピック:

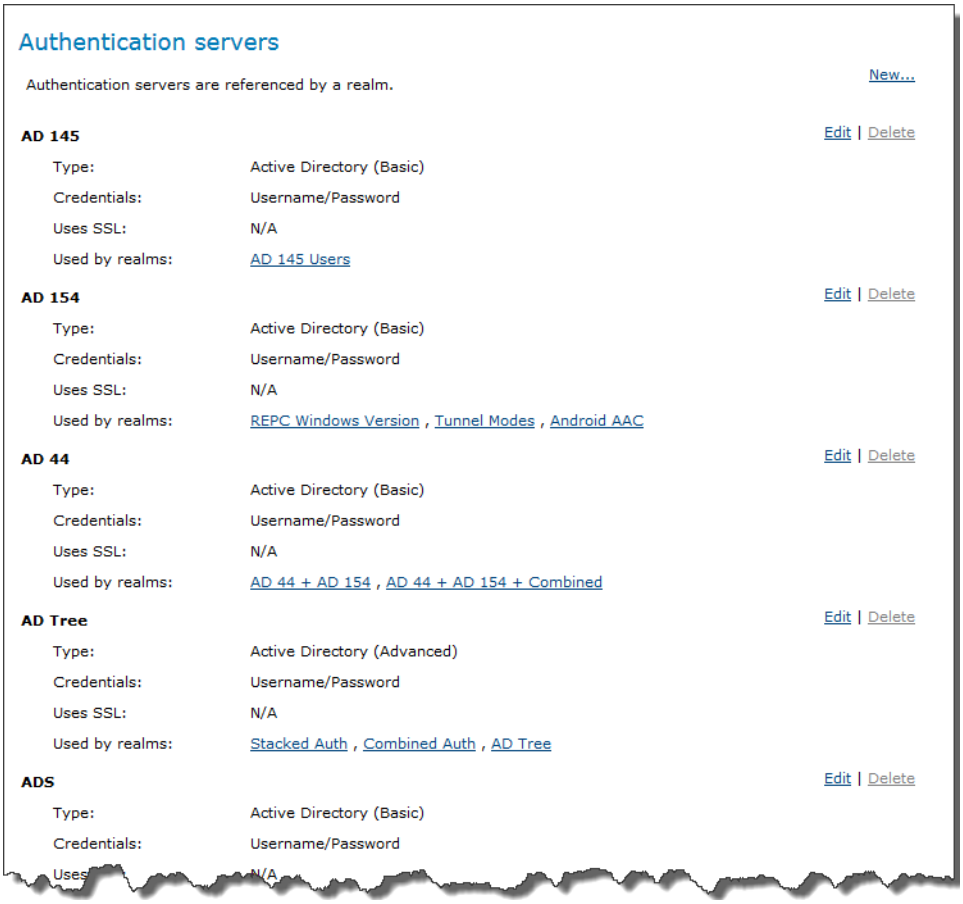
- SMA 認証サーバとしての Ping ID PingOne の設定
- SMA アプリケーションの Ping ID PingOne への追加

SMA 認証サーバとしての Ping ID PingOne の設定

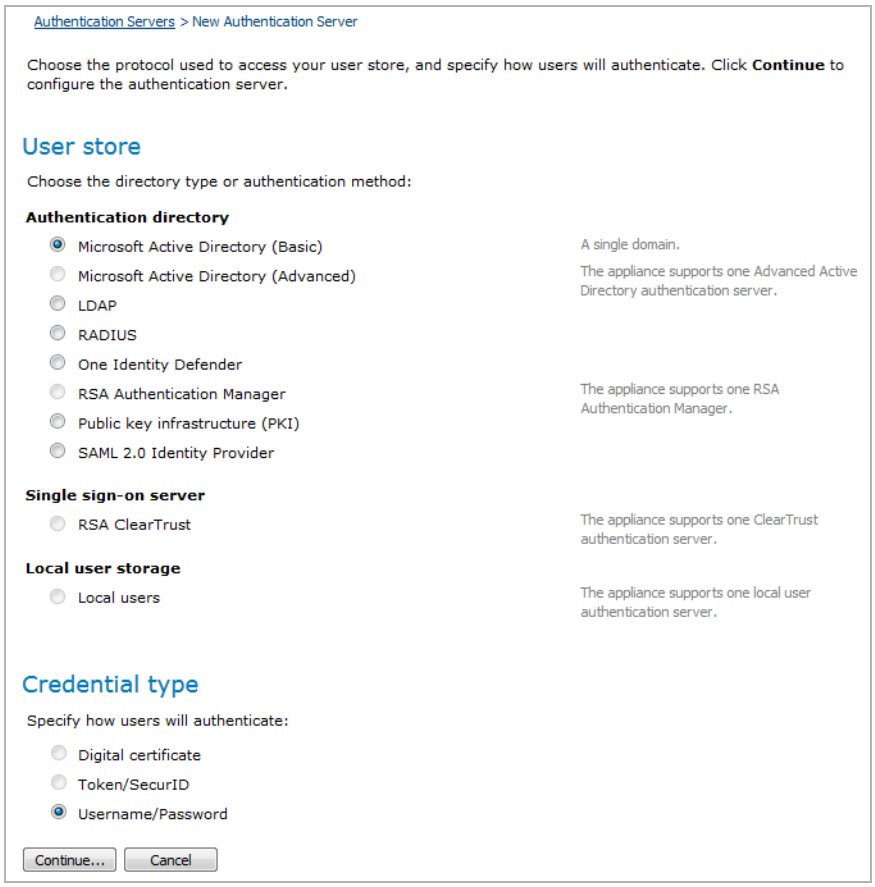
SAML ID プロバイダとしての Ping ID PingOne の設定は、SMA アプライアンスで Ping ID PingOne 認証サーバを設定することで行います。

SMA 認証サーバとして Ping ID PingOne を設定するには:

1 SMA アプライアンスで、[**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページに移動します。

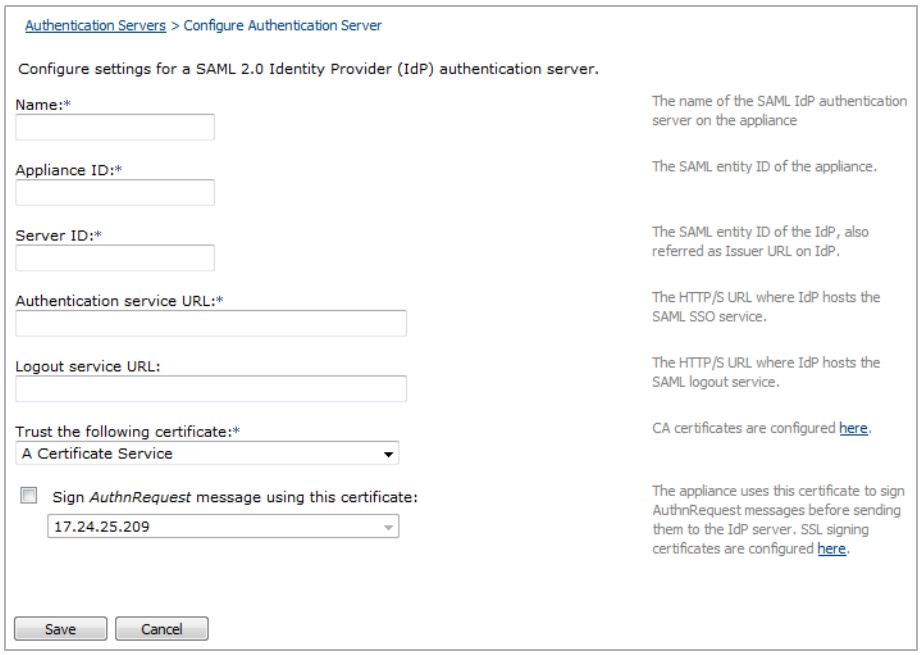


2 [**Authentication servers (認証サーバ)**] で、[**New (新規)**] を選択します。[**New Authentication Server (新しい認証サーバー)**] ページが表示されます。



3 [**SAML 2.0 Identity Provider (SAML 2.0 ID プロバイダ)**] を選択します。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (認証サーバーの設定)**]ダイアログが表示されます。



PingOne アプリケーション ページのフィールドから、このページのフィールドの値の大部分が取得できます。

以下のステップは、[**Configure Authentication Server (認証サーバの設定)**] ダイアログでフィールドを設定する方法を説明します。

5 [**Name (名前)**] フィールドに、「**PingOne_IDP**」と入力します。

6 [**Appliance ID (アプライアンス ID)**] フィールドには、[**PingOne**] アプリケーション ページから**entityId** を入力します。例えば、`http://junk.sonicwall.domain.com` です。

7 [**Server ID (サーバ ID)**] フィールドには、ダウンロードした XML ファイルから **EntityDescriptor** タグの **entityID**、例えば、「`https://pingone.com/idp/company`」を入力します。

8 [**Authentication service URL (認証サーバ URL)**] フィールドには、[**PingOne**] アプリケーション ページから**開始 シングル サインオン (SSO) URL** を入力します。例えば、「`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=734b784f-xxxxx`」と入力します。

9 [**Logout service URL (ログアウト サービス URL)**] フィールドには、ダウンロードした XML ファイルからの **SingleLogoutService** タグの**場所**属性から**ログアウト サービス URL** の値を入力します。例えば、「`https://sso.connect.pingidentity.com/sso/SLO.saml2`」と入力します。

10 目的の証明書を [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから選択します。これは **PingOne** アプリケーション ページからダウンロードされた**証明書**になるはずです。

> **メモ**：このドロップダウン メニューに表示されるようにするには、まず、目的の証明書をダウンロードしてインストールする必要があります。設定方法については、証明書のダウンロードを参照してください。

11 (オプション) 必要に応じて [**Sign *AuthnRequest* message using this certificate (この証明書を使用して AuthnRequest メッセージに署名する)**] を選択してから、証明書を選択します。

12 「**Save (保存)**」を選択します。

SMA アプリケーションの Ping ID PingOne への追加

SMA 認証サーバとして Ping ID PingOne を設定した後、SMA アプリケーションを Ping ID PingOne サービスに追加する必要があります。

SMA アプリケーションを Ping ID PingOne サービスに追加するには:

1 PingOne で、[**My Applications (アプリケーション)**] ページに移動します。

2 [**Add Application (アプリケーションの追加)**] で、[**New SAML Application (新しい SAML アプリケーション)**] を選択します。[**Applications Details (アプリケーションの詳細)**] パネルが開きます。

3 **アプリケーション名**を入力します。

4 **アプリケーションの説明**を入力します。

5 目的の**種別**を選択します。

6 [**Graphics (グラフ)**] で、目的の**アプリケーション ロゴ** と **アプリケーション アイコン**を選択します。

7 [**Continue to Next Step (次の手順に進む)**] をクリックします。[**Applications Configuration (アプリケーションの設定)**] パネルが開きます。

8 [**Protocol Version (プロトコル バージョン)**] では、**SAML v2.0** を選択します。

9 [**Assertion Consumer Service (ACS)**] フィールドには、 URL: `https://appliance.company.com/saml2ssoconsumer` を入力します。

10 **項目 ID** を入力します。

11 **アプリケーション URL** を入力します。これはアプライアンス URL と同じになるはずです。例えば、「`https://appliance.company.com`」と入力します。

12 [**Single Logout Binding Type (シングル ログアウト割り当て種別)**] では、[**Post**] を選択します。

13 「**次へ**」を選択します。[**SSO Attribute Mapping (SSO 属性割付)**] パネルが開きます。

14 [**Status (状況)**] 列では、アプリケーションの行を選択してアクティブにします。

15 [**Save & Publish (保存して公開)**] をクリックします。

16 [**Add new attribute (新しい属性の追加)**] を選択します。次のパネルが開きます。

17 CA 証明書を AMC へアップロードするには、証明書の**ダウンロード**をクリックします。

18 SAML メタデータの**Download (ダウンロード)**をクリックします。

19 「**完了**」をクリックします。

Salesforce

ここでは、SMA 認証サーバとして Salesforce を設定する方法と、SMA アプリケーションを Salesforce サービスに追加する方法を説明します。

トピック:

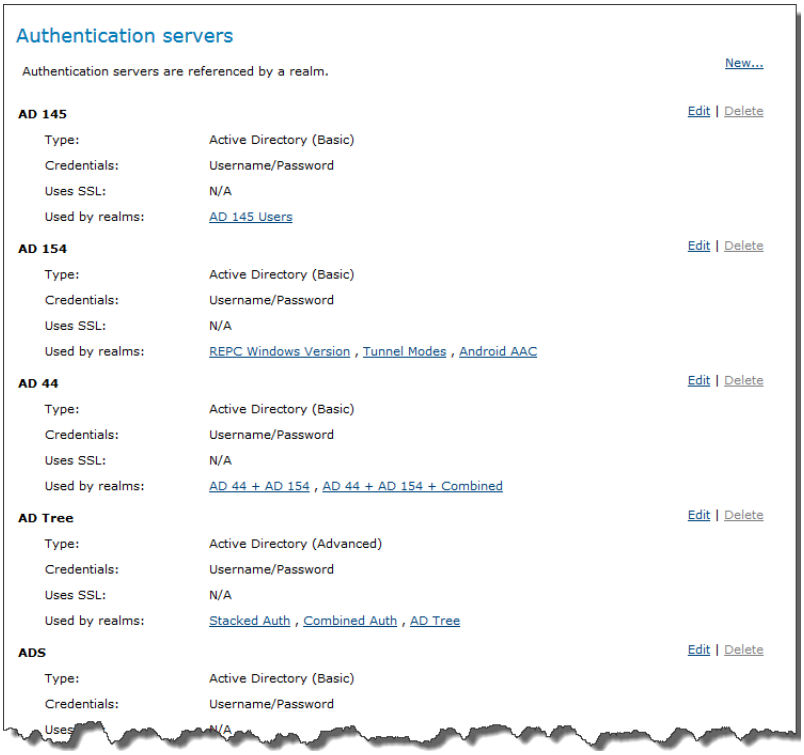
- SMA 認証サーバとしての Salesforce の設定
- SMA アプリケーションの Salesforce への追加

SMA 認証サーバとしての Salesforce の設定

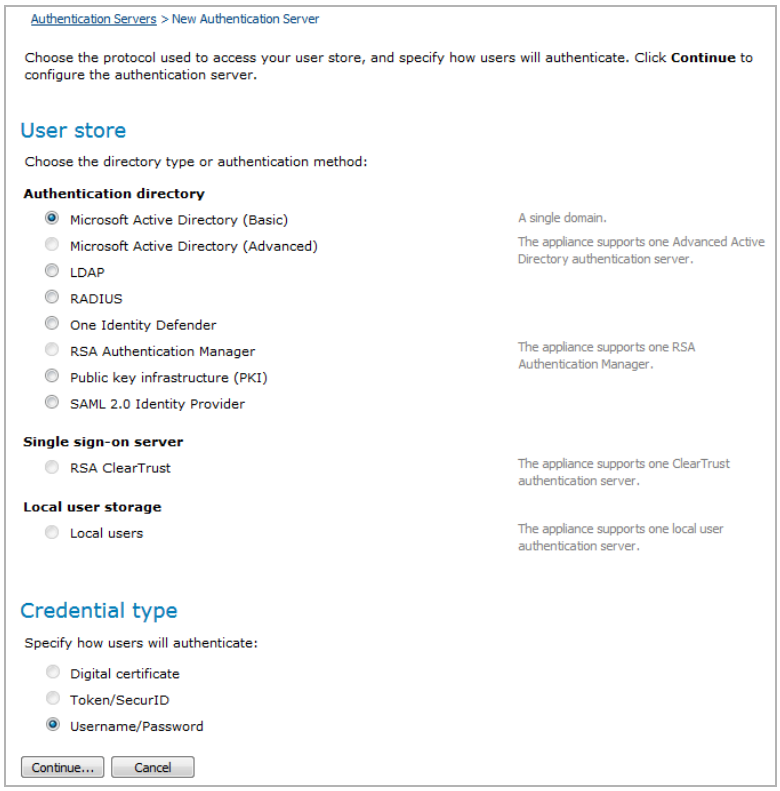
ここでは、SMA 認証サーバとして Salesforce を設定する方法を説明します。

SMA 認証サーバとして Salesforce を設定するには:

1 SMA アプライアンスで、[**System Configuration > Authentication Servers (システム構成 > 認証サーバー)**] ページに移動します。

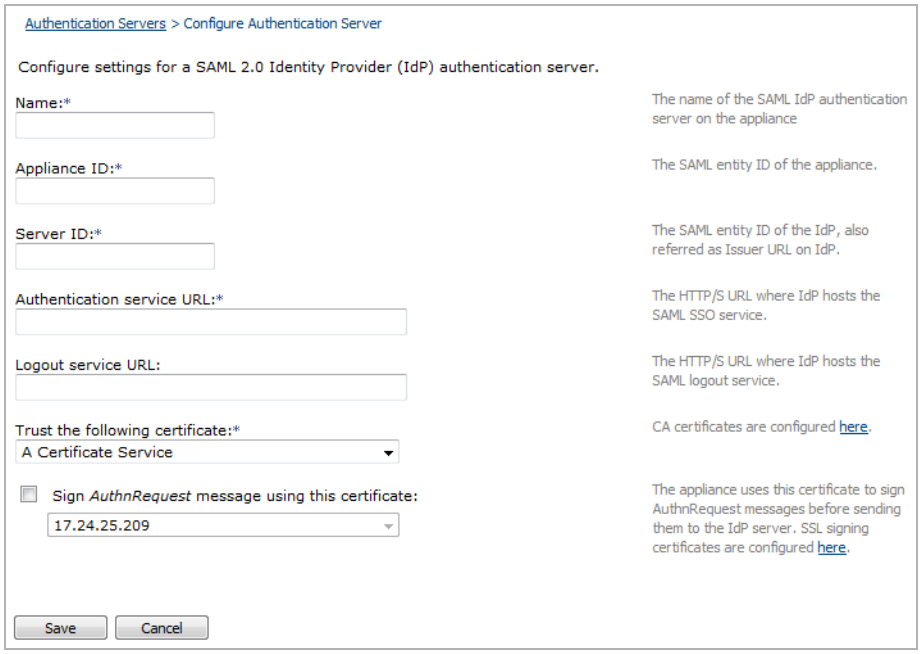


2 [**Authentication servers (認証サーバ)**] で、[**New (新規)**] を選択します。[**New Authentication Server (新しい認証サーバー)**] ページが表示されます。



3 [**SAML 2.0 Identity Provider (SAML 2.0 ID プロバイダ)**] を選択します。

4 [**Continue...(続ける...)**] を選択します。[**Configure Authentication Server (設定認証サーバ)**] ページが表示されます。



以下のステップは、[**Configure Authentication Server (認証サーバの設定)**] ダイアログでフィールドを設定する方法を説明します。

5 [**Name (名前)**] フィールドに、「**Saleforce_IDP**」と入力します。

6 [**Appliance ID (アプライアンス ID)**] フィールドに、[**Salesforce**] アプリケーション ページの[**Web App Settings (ウェブ アプリ設定)**] での**項目 Id**を入力します。例えば、「`https://application.company.com`」と入力します。

7 [**Server ID (サーバ ID)**] フィールドに、[**Web App Settings (ウェブ アプリ設定)**] での [**Salesforce**] アプリケーション ページから**発行者**を入力します。例えば、**Salesforce でのアプリケーション設定ごとに**、「`https://company.my.salesforce.com`」と入力します。

8 [**Authentication service URL (認証サーバ URL)**] フィールドには、[**Salesforce**] アプリケーション ページから**IdP開始側ログイン URL** を入力します。例えば、「`https://company.my.salesforce.com/idp/endpoint/HttpRedirect`」と入力します。

9 目的の証明書を [**Trust the following certificate (以下の証明書を信頼する)**] ドロップダウン メニューから選択します。これは[**Identity Provider (ID プロバイダ)**] ページからダウンロードされた証明書になるはずです。

> **メモ**：このドロップダウン メニューに表示されるようにするには、まず、この証明書をダウンロードしてインストールする必要があります。設定方法については、証明書のダウンロードを参照してください。

10 (オプション) 必要に応じて [**Sign *AuthnRequest* message using this certificate (この証明書を使用して AuthnRequest メッセージに署名する)**] を選択してから、証明書の IP アドレスを入力します。

11 「**Save (保存)**」を選択します。

SMA アプリケーションの Salesforce への追加

SMA 認証サーバとして Salesforce を設定した後、SMA アプリケーションを Salesforce サービスに追加する必要があります。

SMA アプリケーションを Salesforce サービスに追加するには:

1 Salesforce にログインします。

2 [**App Setup > Create > Apps > Connected Apps Detail (アプリ設定 > 作成 > アプリ > 接続したアプリの詳細)**] ページに移動します。

3 [**Add (追加)**] を選択します。[**Settings (設定)**] ダイアログが表示されます。

4 [**Web App Settings (ウェブ アプリ設定)**] パネルで:

   a [**Start URL (開始 URL)**] には、「`https://appliance.company.com`」と入力します。

   b [**Enable SAML (SAML を有効にする)**] を選択します。

   c [**Entity ID (項目 ID)**] には、Workplace URL: `https://appliance.company.com` を入力します。

   d [**ACS URL**] には、「`https://appliance.company.com`」と入力します。

   e [**Subject Type (件名種別)**] には、[**Username (ユーザ名)**] を選択します。

   f [**Name ID Format (名前 ID 形式)**] には、「`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`」と入力します。

   g [**Issuer (発行者)**] には、「`https://company.my.salesforce.com`」と入力します。

5 「**Save (保存)**」を選択します。

6 [**App Setup > Create > Apps > Connected Apps Detail (アプリ設定 > 作成 > アプリ > 接続したアプリの詳細)**] ページで、[**Manage Profiles (プロファイルの管理)**] を選択します。

7 Salesforce アプリケーションへのアクセスを許可するユーザの種別を選択します。

8 「**Save (保存)**」を選択します。[**SonicWall SMA**] ページで、設定した Salesforce の設定を確認できます。

E

ログ ファイルの出力フォーマット

ログ ファイルの概要

SMA アプライアンスでは、システム イベントおよびユーザー イベントを一連のログ ファイルに記録します。ログ ファイルは、AMC を使用して参照できます。また、外部 syslog サーバーにメッセージを送信して参照することもできます (このプロセスについては、システム ロギングおよびモニタリングを参照してください)。このセクションでは、アプライアンスのコマンドライン インターフェースを使用して、ログ ファイルを手動で参照する方法、およびそれを解釈する方法について説明します。

ファイルの場所

SMA サービスのログ ファイル名には、アプライアンス内でのログ ファイル名のリストを示しています。最初の段階では、ローカル (`/var/log/aventail/`) に保管されます。

SMA サービスのログ ファイル名

Secure Mobile Access サービス	ファイル形式	ファイル名
システム メッセージ Web プロキシ サービス、ネットワーク トンネル サービス、ポリシー サーバーに対するメッセージ ログが記録されます。未登録デバイスのメッセージもこのログに記録されます。 システム メッセージ ログを参照してください。	syslog	access_servers.log
ネットワーク トンネル サービス[ねっとわーく とんねる さーびす] 接続活動についての情報、ネットワークにアクセスしたユーザーのリスト、ネットワーク トンネル サービスで転送されたデータの量が記録されます。 ネットワーク トンネル監査ログを参照してください。	SOCKS5LF	extranet_access.log
Web プロキシ サービス Web プロキシ監査ログを参照してください。	W3C CLF	extraweb_access.log
アプライアンス管理コンソール (AMC) 管理コンソールの監査ログを参照してください。	syslog	policy_audit.log management.log
クライアント インストール クライアント インストール ログ (Windows)を参照してください。	syslog	*<username>*@*<realm>*.log
WorkPlace WorkPlace ログを参照してください。	syslog	workplace.log wp_init.log
アップグレード ログ アプライアンスに加えたアップグレードがすべて記録されます。	テキスト	upgrade.log
移行ログ バージョン *<n.n.n>* からの移行時に記録されるログ メッセージであり、*/var/log/* に保管されます。	syslog	migrate_*<n.n.n>*.log

ログ ファイルのストレージ要件を最小限に抑えるために、ファイルがローテーションされます。ログ ローテーションの手順は、指定した頻度によって変動します。

ログのローテーション手順

周波数	手順
15 分おき	• 750MB 以上のログ ファイルがローテーションされます。 • syslog ログ ファイルが強制的にローテーションされます。 • ローテーションされるファイルは圧縮が有効になります。 • 圧縮率は、実際のファイル サイズの 0.10 % に設定されます。 • 各ファイルは、ローテーション後に圧縮されます。
毎日	• すべてのログ ファイルが強制的にローテーションされます。 • 7 日を経過したログ ファイルはすべて削除されます。

1 日以上前のログ ファイルは、非圧縮形式で保管されます。ログ ファイル名には、1 から 7 までの数値が割り振られた接尾辞が付けられます。こうすると、ログ ローテーションが毎日発生した場合、「7」の接尾辞が付くログ ファイルは一週間経過したことになります。例えば、

- `extraweb_access.log` が、Web プロキシ サービスの現在のログ ファイルです。
- `extraweb_access.log1` から `extraweb_access.log.7` が、それ以前のローテーションのログになります。

システム メッセージ ログ

システム メッセージ ログ (`/var/log/aventail/access_servers.log`) は、syslog 形式 (RFC 3164 を参照) で生成され、Web プロキシ サービス、ネットワーク トンネル サービス、ポリシー サーバー (他のサービスのポリシーを制御する内部サービス) のメッセージ ログを含んでいます。また、すべてのアクセス制御決定に関する詳細なメッセージも記述されます。つまり、ユーザーの要求がポリシー ルールと合致すると、そのときに実行された動作を示すログ ファイル エントリが記録されます。

次にメッセージ ログ エントリの例を示します。その後、各要素について説明しています。

```
[08/Nov/2016:07:16:24.312477 +0000] E-Class SRASSLVPN 002764 up 00000001 Info
System  CFG Pool Init STATIC/NAT id=1 name='HQ-pool2' gid='AV1160554493976A' ndns=2
nwins=2 nsuffix=0
```

システム メッセージ ログ フィールド

フィールド	説明
`[08/Nov/2016:07:16:24.312477 +0000]`	
正確なタイムスタンプ	このタイムスタンプは、サービス (Web プロキシ、ネットワーク トンネル、ネットワーク プロキシ、ポリシー) によってメッセージが生成された日時を示しています。このタイムスタンプは syslog で生成されるものより正確になります。これは、ロギング システムがメッセージを syslog に送信するとき、あらかじめバッファリングするためです。
`E-Class SRASSLVPN`	
アプライアンス名	この名前は、AMC の ([**Configure Basic Network Settings (基本ネットワーク設定の設定)**] ページの) [Network Settings (ネットワーク設定)] ページで変更できます。

システム メッセージ ログ フィールド

フィールド	説明
002764	
プロセス ID (PID)	動作しているすべてのアプライアンスには、プロセス ID (PID) が割り当てられています。この PID は、ログ エントリを生成したアプリケーションを識別します。
up	
アプリケーション ID	メッセージを生成したサーバー プロセスを識別します。次の ID があります。 • ap (API サーバー) • cp (SMA が配布するキャッシュ クライアント:ポリシー サーバー、クライアント クレデンシャル ストレージ) • dc (SMA が配布するキャッシュ サーバー:ポリシー サーバー、クライアント クレデンシャル ストレージ) • ev (ネットワーク トンネル サービス - カーネル コンポーネント) • ew (Web プロキシ サービス) • fm (フェイルオーバー モニター) • kp (ネットワーク トンネル カーネル モード ポリシー サーバー インターフェース) • ks (SSL デーモンに対するネットワーク トンネル カーネル モード インターフェース) • kt (カーネル トンネル コンポーネント) • ls (ログ サーバー) • ps (ポリシー サービス) (アクセス ポリシー決定の監査 も参照してください) • pt (ping/traceroute ツール) • uk (不明) • up (ネットワーク トンネル ポリシー サーバー デーモン) • us (ネットワーク トンネル ユーザー スペース SSL デーモン)
00000001	
コンテキスト ID	コンテキスト ID は、4 つのすべてのサービス (Web プロキシ、ネットワーク トンネル、ネットワーク プロキシ、ポリシー、WorkPlace) の関連ログを結合するために使用される一意の値です。単一のユーザー セッションに関連するすべてのメッセージを検索するとき、コンテキスト ID を使用できます。メッセージが特定のユーザー セッションに結合していない場合、00000010 未満の値が割り当てられます。この ID の最初の数値は、そのセッションを生成したサービスを表します。 • 0 (ポリシー サービス) • 1 (Web プロキシ サービス) • 3 (WorkPlace サービス)

システム メッセージ ログ フィールド

フィールド	説明
情報	
重要度	メッセージの重要度レベルは、次のいずれかになります。 • **エラー** - サーバーのシャットダウンや、他のコンポーネントとの通信障害を引き起こす問題。スタートアップ時の名前解決の問題は、このレベルでログに記録されます。 • **警告** - サーバーの動作には悪影響を与えない突発的な事象。例えば、RADIUS サーバーへのアクセスが一度だけ失敗した場合は、Info レベルでログに記録されますが、すべての試行が失敗した場合、そのエントリは Warning レベルでログ ファイルに追加されます。 • **情報** - 場合によっては記録する必要がない通常のイベント。例えば、特定のユーザーのログインや、特定のアクセス制御ルールとの一致などが該当します。 • **詳細** - Info メッセージと同様に、このレベルでは正常な動作を識別しますが、プロセスのステップがこれに含まれます。例えば、アクセス制御ルールを処理している場合、それぞれの不一致に対するメッセージは Verbose レベルになり、一致は Info として識別されます。
システム	
メッセージ タイプ	サーバーのどの部分でメッセージがログに記録されたかを示します。
`CFG Pool Init STATIC/NAT id=1 name='HQ-pool2' gid='AV1160554493976A' ndns=2 nwins=2 nsuffix=0`	
メッセージ テキスト	すべての識別情報の後に続くテキストが、メッセージです。 アクセス ポリシー決定のためのメッセージ テキストについては、アクセス ポリシー決定の監査を参照してください。

トピック:

- アクセス ポリシー決定の監査
- ログにおけるクライアント証明書エラーの表示
- End Point Control インタロゲーション
- 未登録デバイスのログ メッセージ

アクセス ポリシー決定の監査

システム メッセージ ログの主な用途に、アクセス ポリシー**決定**の監査に利用するというものがあります。ユーザーの要求がポリシー ルールと一致するたびに、アプライアンスは、実行したアクションに関するエントリをメッセージ テキスト フィールド (メッセージ ログの最後のフィールド) に書き込みます。

アクセス ポリシー決定のサンプル メッセージは次のようになります。

```
[09/Nov/2016:02:45:32.282637 +0000] E-Class SRASSLVPN 002421 ps 100004b3 Info
EWACL   User '(192.168.136.70 (Dominique Daba)@(Students)' connecting from
'192.168.136.70:37975' matched rule 'accessRule(AV1091719670706:preauth access
rule)', access to '127.0.0.1:455' is permitted.
```

接続要求がルールと一致すると、そのたびに、ログ メッセージが Info レベルで生成されます。ルールと一致しない要求は、Verbose レベルでログに記録され、一致するルールがない場合の要求は Warning レベルでログに記録されます。

ポリシー決定の場合、ログ メッセージ テキスト フィールド (前の例の `Info` より後のすべての部分) には、ログ メッセージ テキスト フィールドに示す情報が含まれます。

ログ メッセージ テキスト フィールド

フィールド	説明
`EWACL`	
ログ タイプ	評価されているアクセス ポリシー。ログ タイプは次の通りです。 • `CSACL` - クライアント/サーバー アクセス ポリシー • `EWACL` - Web アクセス ポリシー • `WPACL` - WorkPlace アクセス ポリシー • `NEACL` - ファイル システム アクセス ポリシー (WorkPlace の [Network Explorer] ページからアクセスするファイル共有)
`User '(192.168.136.70 (Dominique Daba)@(Students)'`	
ユーザー名	要求を出すユーザー。アプライアンスが複数のレルムを使用するよう構成されている場合、ユーザー名は「`(user)@(realm)`」の形式で記述されます。
`connecting from '192.168.136.70:37975'`	
要求の発信元	要求を出したユーザーのアドレス。
`matched rule 'accessRule(AV1091719670706:preauth access rule)'`	
一致ステータス	ルール一致ステータス (「`Matched`」または「`No Match`」) およびルールの ID。
`access to '127.0.0.1:455' is permitted`	
ルールの結果	詳細 ルールが一致した場合、このフィールドは空になります。ルールが一致しなかった場合、次のいずれかのメッセージが記述されます。 • Source Network is *<network>* (送信元ネットワークは <network> です) • Date/time specification *<time>* (日時の仕様 <time>) • User *<username>* not in User/Group List (ユーザー <username> がユーザー/グループのリストにありません) • Destination network is *<dest>* (送信先ネットワークは <dest> です) • Virtual Host is *<vhost>* (仮想ホストは <vhost> です) • Destination services dest is *<dest>* (対象サービスは <dest> です) • Command is *<command>* (コマンドは <command> です) • UDPEncrypt is *<true or false>* (UDPEncrypt は <true または false> です) • Key Length *<length from the policy rule>* requires a stronger cipher (鍵の長さ <length from the policy rule> では強力なサイファが必要です)

ルールが一致しない場合、一致するルールが見つからなかったことを示す Info レベルのメッセージが生成されます。

例

例 1 - Info レベルでの成功

```
[09/Nov/2016:02:45:32.712860 +0000] E-Class SRASSLVPN 002421 ps 10000531 Info
Session Authentication for user '(192.168.136.70 (Guest))@(Students)' SUCCESS for
realm 'Visitors'
```

例 2 - Info レベルでの失敗

```
[09/Nov/2016:04:27:40.965127 +0000] E-Class SRASSLVPN 002873 ps 00000003 Info
WPACL   User '(kevin figment)@(Students)' connecting from '192.168.136.70:0' found
no matching access rule, access to 'www.seattletimes.com:80' is denied.
```

ログにおけるクライアント証明書エラーの表示

アプライアンスが証明書チェーンを確認できない場合、システム メッセージ ログ ファイルに次のようなメッセージが記述されます。

```
[09/Nov/2016:21:28:14.610949 +0000] E-Class SRASSLVPN 001539 ps 10000042 Info System
Auth: CRL-CERT: Cert verification status = 0, err = 20 'unable to get local issuer
certificate'
```

このメッセージには、証明書チェックが失敗した理由を示すエラー コード (この場合「20」) が含まれます。クライアント証明書のエラー コードでは、このエラー コードについて説明しています。

クライアント証明書のエラー コード

コード	エラー メッセージ	説明
2	Unable to get issuer certificate	信頼されていない証明書の発行者証明書が見つかりません。
7	Certificate signature failure	証明書の署名が不正です。
9	Certificate is not yet valid	証明書が有効になっていません。
10	Certificate has expired	証明書の有効期限が切れています。
18	自己署名証明書	パスワード証明書が自己署名証明書であり、信頼されている証明書のリストにありません。
19	Self-signed certificate in certificate chain	信頼されていない証明書を使用して証明書チェーンを構築できますが、ルート証明書がローカルで見つかりません。
20	Unable to get local issuer certificate	通常、信頼されている証明書のリストが不完全であることを示しています。このエラーは、認証で中間証明書が使用される場合も発生します (ルート証明書が必要)。
21	Unable to verify the first certificate	チェーンに証明書が 1 つしか含まれずそれが自己署名証明書でないため、署名が確認できませんでした。
22	Certificate chain too long	証明書チェーンの長さが、指定されている最大深度を超えています。
23	Certificate revoked	証明書が失効済みです。
24	Invalid CA certificate	CA 証明書が無効です。CA でないか、拡張子が指定の目的と合致していません。

End Point Control インタロゲーション

システム メッセージ ログでは、ログ レベルが verbose に設定されているとき、クライアント EPC インタロゲーションの際に情報が収集されます。アプライアンスは、クライアントで特定のデバイス プロファイル属性の存在をチェックし、ログ ファイルにその照会および結果が記録されます。

次の例では、EPC が特定のアンチウイルス アプリケーション (Symantec Client Security、バージョン 9.x 以降) についてチェックしています。アプリケーションが見つからない場合は、この特定デバイスがデフォルト ゾーンに入れられます。

```
[04/Oct/2016:22:29:23.867093 +0000] E-Class SRASSLVPN 027186 uk 00000001 Verbose
System  ::API::QAABA145dFYNZimCKNWHB7p2q2Y=::(timwillis)@(Students)::CLIENT::
Interrogation: Evaluation of OPSWATAV AV1128462569762A [NortonAV.dll,Symantec
Corp.,Symantec Client Security,>=,9.x,,,,,FALSE] results: FALSE

04/Oct/2016:22:29:23.875781 +0000] E-Class SRASSLVPN 027186 uk 00000001 Verbose
System  ::API::QAABA145dFYNZimCKNWHB7p2q2Y=::(timwillis)@(Students):: Classified
into zone: Default zone
```

未登録デバイスのログ メッセージ

未登録デバイスのログ メッセージには、登録されていないデバイスについて、ユーザーによるログイン試行からデバイス ID が記録されます。AMC では、未登録デバイスのログ メッセージを XML 形式でエクスポートできます。[Logging (ログ)] ページで、[**Log file (ログファイル)**] ドロップダウン リストから [**Unregistered device log (未登録デバイス ログ)**] を選択して、[**Export (エクスポート)**] をクリックします。最初にフィルタや検索条件を適用することで、エクスポート ファイルのサイズを小さくすることができます。

また、別のシステムで、未登録デバイスのリストにアクセスし、XML 形式でエクスポートすることもできます。リストには、Web ブラウザで以下の URL を指定して直接アクセスできます。

```
https://(internal IP address)/UnregisteredDevices.xml
```

この URL では BASIC HTTP 認証が求められるため、少なくとも [Monitoring (監視)] カテゴリへの「View」アクセス権を持つ AMC ユーザーのクレデンシャルが必要です。

`curl` または `wget` コマンドを使用して、外部マシンからプログラムでリストを取得できます。

コマンド	構文
curl	`curl -k3u (user):(password) https://(internal IP):8443/UnregisteredDevices.xml`
wget	`wget --no-check-certificate --http-user=(user) --http-password=(password) https://(internal IP address):8443/UnregisteredDevices.xml`

これらのコマンドはどちらも SSL 証明書のチェックをオフにするため、自己署名証明書を使用している場合に便利です。

未登録デバイスのレポートを XML 形式で取得する際に使用される URL での定義内容は、次のとおりです。

URL	*https://<internal address>:8443/UnregisteredDevices.xml?parameter=value&parameter=value*	
認証		BASIC HTTP 認証。少なくとも [Monitoring] カテゴリへの「View」アクセス権を持つ AMC ユーザーのクレデンシャルが必要です。
パラメータ (全オプション)		
	ユーザ名	文字列、大文字と小文字の区別なし、デフォルト * (全ユーザー) この値がユーザー名に含まれるユーザーからのログインを検索します。例:`username=li` と指定すると、`Linda` や `Melinda` のエントリが返されます。
	レルム	文字列、大文字と小文字の区別なし、デフォルト * (全レルム) この値がレルム名に含まれるレルムへのログインを検索します。例 `:realm=Corp` と指定すると、`Corporate` や `Non-Corporate` のエントリが返されます。

プラットフォーム

文字列、以下に列挙した値

特定のプラットフォームのみを実行しているデバイスからのログインを検索します。

`all` - 全プラットフォーム (デフォルト)

`windows` - Windows デバイスのみ

`mac` - Mac デバイスのみ

`linux` - Linux デバイスのみ

`activeSyncMobile` - Exchange ActiveSync デバイスのみ

`mobilePhone` - 携帯電話のみ

`pda` - PDA デバイスのみ

`unknown` - プラットフォームが判断できないデバイスのみ

exported

文字列、以下に列挙した値

AMC または HTTP GET コマンドでエクスポートされたか、まだエクスポートされていないエントリを検索します。

`all` - エクスポートされたかどうかを問わず、全エントリが対象 (デフォルト)

`exported` - すでにエクスポートされたエントリのみ

`unexported` - まだエクスポートされていないエントリのみ

制限

件数、デフォルトは **1000**

このエントリ件数に検索を制限します。

deviceCount

番号、0-3、デフォルトは全エントリ

外部の AD/LDAP ストアで登録されているデバイスの特定の番号を使用するユーザーを検索します。

0 - 登録されているデバイスがないユーザー

`1` - 登録されているデバイスが 1 つのユーザー

`2` - 登録されているデバイスが 2 つのユーザー

`3` - 登録されているデバイスが 3 つ以上のユーザー

lastLoginTime

文字列、以下に列挙した値、デフォルトは`all`

現在の時刻に対して、特定の期間内にログイン試行があったユーザーを検索します。

`all` - すべてのログイン試行

`hour` - 過去 1 時間以内のログイン試行

`day` - 過去 1 日以内 (24 時間以内) のログイン試行

`week` - 過去 1 週間以内 (7 日以内) のログイン試行

ネットワーク トンネル監査ログ

ネットワーク トンネル監査ログには、トンネル接続全体のステータスやトンネル内でのフロー全体のステータスなど、接続活動に関する詳細な情報が記録されます。

メモ：2 種類のレコード タイプは、メッセージの 6 番目のフィールドに記述される言葉が「flow」か「tunnel」かで区別できます。

メッセージはディスク上の /var/log/aventail/extranet_access.log ファイルに保存されます。また、次のパラメータを含みます。

```
[source-ip:port] [authentication] "[username@realm]" "[date/time]" [version]
[command] [destination-ip:port] [status code] [bytes-received] [bytes-sent]
[connection duration] [imei]
```

この例は、ネットワーク トンネル サービス監査ログ ファイルのエントリを示しています。

```
12.230.158.210:1110 ssl:LDAP "fred figment" "13/Sep/2016:19:18:28 -0700" v1.1 flow:tcp
192.168.136.254:22 0 21722 60631 263 490236207159217
```

このログ エントリには、ネットワーク トンネル監査ログ フィールドに示すフィールド (スペースで区切られる) が含まれています。

ネットワーク トンネル監査ログ フィールド

フィールド	説明
source-ip:port	トンネル レコードの場合、このフィールドにはアウター トンネル接続の接続元アドレスが記述されます。フロー レコードの場合、このフィールドにはインナー フローの接続元アドレスが記述されます。これはトンネルが確立されるときにトンネル プールから割り当てられる仮想 IP アドレスです。 例: 12.230.158.210:1110
認証	ハイフン (-) は、TEAM クレデンシャル経由の再認証を示します。 **メモ**：TEAM クレデンシャルのネゴシエーションで使用される認証方式がトンネルでは認識されないため、値を明示できません。
"username@realm"	リソースにアクセスしているユーザーと、そのユーザーにログインされたレルム。このフィールドの形式は、使用される認証方式によって異なります。 例:"mfigment@employees"
"date/time"	接続開始の日付 (「日/月/年」形式) および時刻 (24 時間形式の時間、分、秒、 ミリ秒、GMT との時差で表されたタイム ゾーン)。 **メモ**：日付/時刻を含むレコードは、ログに記述されるまで時間がかかることがあります。 例: "13/Sep/2016:19:18:28 -0700"
バージョン	Connect または OnDemand Tunnel プロトコル バージョンを示します。「1.1」は現在サポートされているバージョンです。

ネットワーク トンネル監査ログ フィールド

フィールド	説明
command	実行されたコマンドのタイプ。ネットワーク トンネル サービスのログ ファイル エントリには、これらのコマンドが記述されます。 tunnel flow:tcp flow:udp flow:icmp
destination-ip:port	アクセス対象のリソースの IP アドレスおよびポート番号。フロー レコードの場合、これは TCP、UDP、または ICMP フローの接続先になります。トンネル レコードの場合、これはアプライアンスの外部アドレスになります (ポート番号は常に 0)。 例: 192.168.136.254:22
status code	「0」は成功を表します。 ステータス コードの詳細については、接続ステータス メッセージの監査を参照してください。
bytes-received	接続元から読み取られるバイト数。
bytes-sent	接続先に書き込まれるバイト数。
connection duration	Connection duration (秒) は、トンネルが閉じられた時間、TCP フローが TIME_WAIT 状態になった時間、UDP または ICMP フローがタイムアウトになった時間のいずれかに基づきます。
imei	すべての携帯電話に、メーカー、モデル タイプ、承認国などの情報を示す一意の 15 桁の IMEI コード (デバイス ID) が割り当てられます。IMEI は、ほとんどの電話で *#06# にかけると表示されます。また、バッテリ底面のコンプライアンス プレートにも示されています。 例: 352711-01-521146-5 IMEI コードが提供されないデバイスの場合は、プラットフォーム識別子が示されます。プラットフォーム識別子 (最初の文字) には次のものがあります。 W - Windows M - Mac L - Linux P - PDA A - AcitveSync Mobile X - 不明 (空欄) - 携帯電話

接続ステータス メッセージの監査

ネットワーク プロキシ/ トンネル監査ログには接続ステータス コードが含まれますが、これは、クライアント/サーバー接続の問題をデバッグする際に役に立ちます。ステータス コードは、ログ ファイルの destination-ip:port フィールドの直後のフィールドです (ログ ファイルのエントリ全体については、ネットワーク トンネル監査ログを参照してください)。接続ステータス コードでは各コードについて説明します。

接続ステータス コード

接続ステータス コード	説明
0	エラーが発生することなく、接続の試行が成功しました。
1	クライアントで無効な TEAM クレデンシャルが提示されました。
2	TEAM 要求をクライアントに送信できません。トンネル認証の交換、または PS 認証の交換でエラーが発生しました。
3	クライアントでのトンネル プロトコルが、アプライアンスでサポートされている最小要件を満たしていません。
4	TP エラーが発生したか、サポートされていない機能が要求されました。
5	セッションのアイドル時間が、構成やデフォルトでの許容時間を超えています。
6	使用できるアドレスがトンネル プールにありません。
9	トンネルの内部アドレスがないか (bad cfg)、realm_list (shouldn't happen) の問題が発生したか、クライアントがリソース リストを拒否しました。
10	クライアントのバージョンが合致しません。
11	利用できるトンネル プール アドレスがすべて、クライアントのネット作業環境と競合しており、回避できません。
12	クライアントに対する特別な「エラー」であり、即座の再開を必要とします。
65535	アクセス権が拒否されました。
65524	メモリ不足です。
65520	システムがビジーであり、セッションがドロップされました。
65514	内部で矛盾が生じており、予期しない状態が生じました。
65504	トンネル サービスが中止されました。
65432	ピアによって接続がリセットされました。
65429	接続されませんでした (内部エラー)。
65428	トンネル サービスがシャットダウンしました。
65426	タイムアウト (UDP フローの場合は特に、エラーとして考慮する必要はありません)。
65279	認証方式がありません。
65278	認証が失敗しました (ユーザーが不正なユーザー名/パスワードを入力した場合など)。
65277	認証 I/O が失敗しました。
65276	quiet モードで認証が失敗しました。
65275	クライアント接続が失われました。
65274	モジュールをロードできません。
65273	許可されていません (ポリシーによりアクセスが拒否されたなど)。
65272	暗号化障害。
65271	未知の障害。

例

ユーザーが不正なユーザー名/ パスワードを入力した場合、ログにエラー番号 65535 が記述されます。

```
192.168.2.69:3127 ssl "testing" "26/Feb/2017:21:31:51.947 +0000" none -:- 65535 385
0 14 352711-01-521146-5
```

タイムアウトが発生した場合、メッセージにエラー番号 65426 が含まれます。

```
192.168.2.69:3127 ssl "testing" "26/Feb/2017:21:31:51.947 +0000" none -:- 65426 385
0 1 352711-01-521146-5
```

クライアントからインターネットへのすべてのトンネル トラフィックはすべて (リダイレクト オール モードで動作している場合)、AMC の [**Configure Network Tunnel Service (ネットワーク トンネル サービスの設定)**] ページ ([**Enable route to Internet (インターネットへのルートを有効化)**]) で指定した IP アドレスを介してルーティングされます。このインターネットへのルートが使用できない場合は、接続ステータス コードとして「65504」が記述されます。

```
151.219.76.85:4827 - "(1248411)@(Radius)" "26/Jun/2016:17:54:14.916 +0000" 1.1
Flow:TCP 165.170.0.1:1503 65504 0 0 60 352711-01-521146-5
```

Web プロキシ監査ログ

Web プロキシ監査ログには、ネットワークにアクセスしたユーザーのリストや転送されたデータの量など、接続活動に関する詳細な情報が記録されます。

/var/log/aventail/extraweb_access.log ファイル メッセージは、World Wide Web Consortium (W3C) Common Log Format (CLF) で保管されます。CLF ログの詳細については、http://httpd.apache.org/docs/logs.html を参照してください。ログ メッセージには、これらのパラメータがあります。

```
[source-ip] [identity] [shortname@realm] [longname] [date/time] "[request]" [HTTP
return code] [bytes-sent] [imei]
```

次の例は、ネットワーク プロキシ/トンネル サービス監査ログ ファイルのエントリを示しています。

```
192.168.200.162 - (extranetuser)@(Translation)
(uid=extranetuser,ou=Users,dc=indigo,dc=com) [31/Mar/2017:09:08:09 -0700] "GET
http:/ /127.0.0.1:455/postauth/interrogator/AventailComponents.exe HTTP/1.1" 200
536016 "-"
```

このログ エントリには、Web プロキシ監査ログ フィールドに示すフィールド (スペースで区切られる) が含まれています。

Web プロキシ監査ログ フィールド

フィールド	説明
source-IP	Web プロキシ サービスにアクセスするコンピュータの IP アドレス (NAT が使用中の場合は、このフィールドに変換アドレスが含まれることがあります)。 例: 192.168.200.162
identity	このフィールドは、Web プロキシ サービスでは使用されません。常にダッシュ (「-」) が入ります。

Web プロキシ監査ログ フィールド

フィールド	説明
shortname@realm	ユーザーがログインしたら、このフィールドにはユーザー名とログイン レルムが (username@realm) の形式で示されます。 ユーザーがまだ認証されていない場合、または認証が不要なコンテンツ (WorkPlace ログイン ページ) にアクセスしている場合、このフィールドにはダッシュ (「-」) が入ります。認証が使用されていない (つまり AMC でレルムに対する [**Authentication server (認証サーバ)**] が [**None (なし)**] に設定されている) 場合、このフィールドには [**anonymous-user**] が入ります。 例: (extranetuser)@(Translation)
longname	ユーザーがログインしたら、このフィールドにはユーザーのロング ネームが示されます。LDAP および Active Directory のユーザー名が DN を使用して示されます。他のユーザー名は CN を使用して示されます。 ユーザーがまだ認証されていない場合、または認証が不要なコンテンツ (WorkPlace ログイン ページ) にアクセスしている場合、このフィールドにはダッシュ (「-」) が入ります。 例: (uid=extranetuser,ou=Users,dc=indigo,dc=com)
date/time	アプライアンスで要求を受け取った日付および時刻。 例: [16/Apr/2017:21:36:37 +0000]
request	HTTP 要求の 1 行目で、HTTP コマンド (GET や POST など)、要求されたリソース、HTTP バージョン番号が含まれます。 例: "GET /alias1/foo.gif HTTP/1.1"
HTTP-return-code	サーバーは、次のいずれかの戻りコードを返します。 • 2xx コードは、要求の成功を示します。 • 3xx コードは、ある種のリダイレクションまたはキャッシュされた応答を示します。 • 4xx コードは、エラーを示します (リソースが見つからない、要求が認証されていないなど)。 • 5xx コードは、サーバー エラーを示します。 これらのコードの詳細については、http://www.ietf.org/rfc/rfc2616.txt を参照してください。
bytes-sent	応答の本文で送信されたバイトの数 (HTTP ヘッダのサイズは含まれません)。
imei	すべての携帯電話に、メーカー、モデル タイプ、承認国などの情報を示す一意の 15 桁の IMEI コードが割り当てられます。IMEI は、ほとんどの電話で *#06#. にかけると表示されます。また、バッテリ底面のコンプライアンス プレートにも示されています。ユーザーに関連付けられている IMEI がない場合は、ダッシュ (-) がログ ファイルに記述されます。 例: 352711-01-521146-5

例

- 認証が失敗した場合 (ユーザーが不正なユーザー名やパスワードを入力するなどしたため)、戻りコード 200 ([**OK**] 、クライアント要求が理解されたことを示す) が付いた単一のメッセージがログに記述されます。要求を出したユーザーを唯一識別できるのは、メッセージに記録されている接続元 IP アドレスです。

```
192.168.2.69 - - [26/Feb/2017:21:43:30 +0000] "POST /__extraweb__authen
HTTP/1.1" 200 3610 352711-01-521146-5
```

認証が成功した場合も同様のメッセージが記述されますが、戻りコードが 302 (「検出」) になります。その直後に、ユーザーの認証クレデンシャルおよび戻りコード 200 を含む別のメッセージが続きます。

```
192.168.2.69 - - [26/Feb/2017:21:44:25 +0000] "POST /__extraweb__authen
HTTP/1.1" 302 206 352711-01-521146-5

192.168.2.69 - (jsmith)@(AD) [26/Feb/2017:21:44:25 +0000] "GET
/workplace/access/home HTTP/1.1" 200 15424
```

- ユーザーが正常に認証されたにもかかわらず、アクセス ルールによって Web リソースへのアクセスが拒否された場合、戻りコード 403 (「禁止」) を含むメッセージがログに記録されます。

```
192.168.2.69 - (jsmith)@(AD) [26/Feb/2017:21:52:25 +0000] "GET /dukes
HTTP/1.1" 403 3358 352711-01-521146-5
```

- ユーザーが正常に認証され、URL へのアクセスが許可された場合は、認証失敗時 (戻りコード *200*) とほぼ同じメッセージが記述され、さらにユーザーのクレデンシャルが含まれます。

```
192.168.2.69 - (jdoe)@(AD) [26/Feb/2017:21:51:03 +0000] "GET /dukes
HTTP/1.1" 200 262 352711-01-521146-5
```

管理コンソールの監査ログ

管理権限を持つユーザーは、AMC 監査ログを表示することにより、アプライアンスに対して実行された構成変更の履歴を確認できます。このログには、管理者が AMC で実行した構成変更の監査履歴も記録されます。AMC でこのログ (`/var/log/aventail/policy_audit.log`) を表示する場合は、管理監査ログの手順に従ってください。

また、AMC 関連の syslog 形式のログ ファイル(`/var/log/aventail/management.log`) もあります。

WorkPlace ログ

WorkPlace ログ (`/var/log/aventail/workplace.log`) は、Network Explorer によるファイル共有へのアクセスをトラブルシューティングする場合に使用すると便利です。また、Web ショートカットとネットワーク ショートカットが WorkPlace ポータル ページでどのように表示されるかについても確認できます。ファイル リソースへのアクセスも、Web プロキシ サービス ログ (`extraweb_access.log`) に記録されます。

WorkPlace ショートカットの例

ユーザーが WorkPlace にログインし、ショートカットが正常に表示されたとき、ログ ファイル エントリは次のようになります。

1 ユーザー名クレデンシャルが、セッション ID とあわせてログに記録されます (トラブルシューティングの際は、ユーザー名のみが検索されます)。

```
Feb 26 22:03:03 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:03:03,612] GOT:
CredentialsManager[teamSessionId=+kMs+1fJYyVOxJ8f/YO0gg==,teamcredentials=
{username=jdoe} ,credentials={}]
```

2 次に、ショートカット (この場合 Web ショートカット) の正常なロードを示すメッセージが記録されます。

```
Feb 26 22:03:03 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:03:03,615]
pcsession: <authorize:exit> uri=http://wemmet.internal.net status=SUCCESS
```

3 ネットワーク ショートカットの正常なロードは、次のように記録されます。

```
Feb 26 22:03:03 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:03:03,617]
pcsession: <authorize:exit> uri=smb://marshare01/marketing status=SUCCESS
```

(設定したアクセス ルールなどのために) ユーザーにショートカットが表示されない場合、アクセスの拒否は次のように処理されています。

1 ログイン時にユーザー名を検索します。

```
Feb 26 22:12:15 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:12:15,027] GOT:
CredentialsManager[teamSessionId=hZ98BEZxdyARJCtjkGl3lA==,teamcredentials=
{username=dsmith} ,credentials={}]
```

2 ロードできないショートカット情報をユーザーの WorkPlace ポータル ページで探します。次に Web ショートカットでの失敗した例を示します。

```
Feb 26 22:12:15 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:12:15,043]
pcsession: <authorize:exit> uri=http://wemmet.internal.net status=FAILURE
```

メモ：

- リソース共有へのアクセス (許可/ 拒否) も `extaweb_access.log` に記録されます。

  ```
  192.168.2.69 - (jdoe)@(AD) [26/Feb/2017:22:19:21 +0000] "GET
  /workplace/access/exec/file/view?path=smb://marshare01/marketing/
  reports.doc/ HTTP/1.1" 200 4608
  ```

- また、WorkPlace 関連の syslog 形式のログ ファイル (`/var/log/aventail/wp_init.log`) もあります。

F

多言語サポート

ネイティブ文字セットのサポート

このアプライアンスでは、拡張文字セット、つまり 2 バイト文字セットをサポートしています。そのため、ユーザー名、パスワード、リソース名、WorkPlace ショートカット、アクセス制御ルールについては、AMC で、拡張文字または 2 バイト文字を含むネイティブ文字セットで入力および表示できます。また、このアプライアンスでは、ユーザー名フィールドやパスワード フィールドなどのユーザー認証プロンプトについても、拡張文字または 2 バイト文字をサポートしています。

RADIUS ポリシー サーバーの文字セット

このアプライアンスでは、非英語文字セットを使用する RADIUS ポリシー サーバーによる文字エンコーディングをサポートしています。RADIUS 仕様の最新バージョン (RFC2865) では、すべてのテキスト フィールドで UTF-8 エンコード文字に対応することが求められています。ただし古いバージョンの RADIUS プロトコルでは、テキスト フィールドを 7 ビット US-ASCII で定義しています。AMC では、古いバージョンのプロトコルを使用する RADIUS サーバーもサポートするため、最も一般的に使用する文字セットのリストを選択できるようになっています。また、他の文字セットで入力することも可能です。

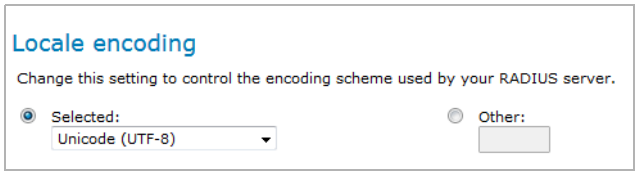
RADIUS サーバーの言語設定を変更するには、

1 メイン ナビゲーション ページから、[**Authentication Servers (認証サーバ)**] をクリックします。

2 構成したい RADIUS サーバーの横にある [**Edit (編集)**] をクリックします。(初めて AMC で RADIUS サーバーを構成する場合は、RSA サーバー認証の構成を参照してください)。

3 [**Configure Authentication Server (設定認証サーバ)**] ページで、[**Advanced (詳細)**] エリアを展開します。

4 [**Locale encoding (ロケールのエンコーディング)**] で次のように設定します。



- [**Selected (選択済み)**] リスト ボックスから文字セットを選択します (選択可能な文字セットについては、選択可能な RADIUS 文字セットを参照してください)。

- [**Other (その他)**] をクリックし、テキスト ボックスに文字セットの名前を入力します。入力できる文字セットのリストについては、サポートされているその他の RADIUS 文字セットを参照してください。

5 「**Save (保存)**」を選択します。

トピック:

- 選択可能な RADIUS 文字セット
- サポートされているその他の RADIUS 文字セット

選択可能な RADIUS 文字セット

[**Configure Authentication Server** (認証サーバーの設定)] ページの [**Selected (選択済み)**] リスト ([**Advanced (詳細)**] 設定の下) では、次の文字セットを選択できます。

選択可能な RADIUS 文字セット

文字セット	コード ページ
Arabic (アラビア語)	1256
Baltic (バルト語)	1257
Central European (中央ヨーロッパ語)	1250
Chinese Simplified (GBK) (簡体中国語)	936
Chinese Traditional (Big5) (繁体中国語)	950
Cyrillic (キリル文字)	1251
Greek (ギリシャ語)	1253
Hebrew (ヘブライ語)	1255
Japanese (Shift-JIS) (日本語)	932
Korean (韓国語)	949
Turkish (トルコ語)	1254
Unicode (UTF-8)	65001
Vietnamese (ヴェトナム語)	1258
Western (西欧語)	1252

サポートされているその他の RADIUS 文字セット

RADIUS サーバーで使用されるエンコーディング スキームを設定するときは、[**Configure Authentication Server** (認証サーバーの設定)] ページの [**Locale encoding** (ロケールのエンコーディング)] エリアで、サポートされているその他の RADIUS 文字セットに示す文字セットのいずれかを入力します。

サポートされているその他の RADIUS 文字セット

言語タイプ	サポートされている文字セット		
ヨーロッパ語	ASCII	ISO-8859-10	MacRoman
	ISO-8859-1	ISO-8859-13	MacCentralEurope
	ISO-8859-2	ISO-8859-14	MacIceland
	ISO-8859-3	ISO-8859-15	MacCroatian
	ISO-8859-4	ISO-8859-16	MacRomania
	ISO-8859-5	KOI8-R	MacCyrillic
	ISO-8859-7	KOI8-U	MacUkraine
	ISO-8859-9	KOI8-RU	MacGreek
		CP850	MacTurkish
		CP866	Macintosh
セム語	ISO-8859-6	MacHebrew	
	ISO-8859-8	MacArabic	
	CP862		
日本語	EUC-JP		
	ISO-2022-JP		
	ISO-2022-JP-2		
	ISO-2022-JP-1		
中国語	EUC-CN	BIG5-HKSCS	
	HZ	ISO-2022-CN	
	GB18030	ISO-2022-CN-EXT	
	EUC-TW		
	CP950		
Korean (韓国語)	CP949		
	ISO-2022-KR		
	JOHAB		
アルメニア語	ARMSCII-8		
グルジア語	Georgian-Academy		
	Georgian-PS		
タジク語	KOI8-T		
タイ語	TIS-620		
	CP874		
	MacThai		
ラオ語	MuleLao-1		
	CP1133		
Vietnamese (ヴェトナム語)	VISCII		
	TCVN		

サポートされているその他の RADIUS 文字セット

言語タイプ	サポートされている文字セット	
Unicode	UCS-2	UTF-16
	UCS-2BE	UTF-16BE
	UCS-2LE	UTF-16LE
	UCS-4	UTF-32
	UCS-4BE	UTF-32BE
	UCS-4LE	UTF-32LE
		UTF-7

G

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。

Secure Mobile Access 管理ガイド
更新日 - 2018 年 7 月
ソフトウェア バージョン - 12.1
232-004389-00 Rev A

索引

あ

い

え

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ろ

わ