SonicOS および SonicOSX 7

ユーザ

管理者ガイド

- - NSa および NSsp シリーズ

SONICWALL®

目次

1

ユーザ状況の設定

「**ユーザ > 状況**」ページには、ファイアウォール上の「**現在のユーザ**」の一覧が表示されます。「**現在のユーザ**」テーブルには、IPv4 と IPv6 の IP アドレスが設定/表示されます。

「**現在のユーザ**」テーブルには、以下の情報が表示されます。

- **ユーザ名**
- **IP アドレス**
- **セッション時間**
- **残り時間**
- **残り無動作時間**
- **種別/モード**
- **設定**
- **ログアウト**

トピック:

- 単一ユーザのログアウト
- 複数ユーザのログアウト
- 無動作ユーザの表示
- 未認証ユーザの表示
- ユーザ数の表示
- ユーザ リストの再表示

ユーザのログアウト

トピック:

- 単一ユーザのログアウト
- 複数ユーザのログアウト

単一ユーザのログアウト

ユーザをログアウトするには、以下の手順に従います

1. 「**ユーザ > 状況**」ページに移動します。
2. ログアウトするユーザを選択します。
3. 「**選択ユーザをログアウト**」をクリックします。

複数ユーザのログアウト

複数ユーザをログアウトするには、以下の手順に従います

1. 「**ユーザ > 状況**」ページに移動します。
2. 現在表示されているすべてのユーザを選択するには、リストの左上、**検索**アイコンのすぐ下にあるチェックボックスをオンにします。
3. 「**選択ユーザをログアウト**」をクリックします。

無動作ユーザの表示

既定では、動作中のユーザのみが「**ユーザ**」リストに表示されます。

無動作ユーザを表示するには、以下の手順に従います

1. 「**ユーザ > 状況**」ページに移動します。
2. リストの上にある「**無動作ユーザを含める**」の横のスライダーを選択します。
   無動作ユーザも「**ユーザ**」リストに表示されるようになります。

未認証ユーザの表示

未認証ユーザを表示するには、以下の手順に従います

1. 「**ユーザ > 状況**」ページに移動します。
2. リストの上にある「**未認証ユーザを表示する**」の横のスライダーを選択します。
   未認証ユーザも「**ユーザ**」リストの下にある個別の「**未認証ユーザ**」リストに表示されるようになります。

ユーザ数の表示

現在のユーザ数を表示するには、以下の手順に従います

1. 「**ユーザ > 状況**」ページに移動します。
2. 「**ユーザ**」リストの上にあるツールバーの右端の「**ユーザ数の表示**」アイコンを選択します。
   「**ユーザ数**」ウィンドウに以下が表示されます。
   - **ユーザ種別**
   - **アクティブ**
   - **停止中**
   - **合計**
3. 「**ユーザ数**」ウィンドウを閉じるには、ウィンドウの右上にある「X」を選択します。

ユーザリストの再表示

「ユーザ」リストを再表示するには、以下の手順に従います

1. 「**ユーザ > 状況**」ページに移動します。
2. 「**ユーザ**」リストの上にあるツールバーの右端の再表示アイコンを選択します。

2

ユーザの設定

通常の認証方式に加え、SonicOS/X では Lightweight Directory Access Protocol (LDAP) を使用してユーザを認証することができます。LDAP は Microsoft の Active Directory と互換性があります。

SonicWall 装置では、SonicWall のシングル サインオン エージェントを選択して、シングル サインオン機能を提供することができます。シングル サインオン (SSO) とは、ワークステーションへのシングル ドメイン ログインによる複数のネットワーク リソースへの特権的アクセスを提供する透過的なユーザ認証メカニズムです。SonicWall ネットワーク セキュリティ装置は、認証に Active Directory が使用されている場合に、ワークステーションの IP アドレスに基づいてユーザのアクティビティを識別するために、SonicWall シングル サインオン エージェント (SSO エージェント) による SSO 機能を提供します。SonicWall SSO エージェントは、Active Directory と同じドメイン内のコンピュータにインストールされている必要があります。

トピック:

ユーザ ログイン設定

トピック:

ログインの認証方法の設定

ログインの認証方法を設定するには、以下の手順に従います

1. 「**ユーザ > 設定**」ページに移動します。
2. 「**ログインの認証方法**」から次のいずれかの認証方法を選択します。

ローカル ユーザ	「ユーザ > ローカル ユーザ > ローカル グループ」ページを使用してローカル データベース内のユーザを構成する場合に選択します。ローカル ユーザおよびグループの設定の詳細については、「ローカル ユーザの設定」および「ローカル グループの設定」を参照してください。
RADIUS	ユーザ数が 1,000 人を超える場合、または SonicWall のユーザ認証にさらなるセキュリティを付加したい場合に選択します。ユーザ認証に RADIUS を使用することを選択する場合、ユーザは SonicWall に送るパスワードを暗号化するために HTTPS を使用して SonicWall にログインする必要があります。ユーザが HTTP を使用して SonicWall へのログインを試みた場合、ブラウザは自動的に HTTPS にリダイレクトされます。RADIUS の設定の詳細については、「RADIUS の設定」を参照してください。
RADIUS + ローカル ユーザ	認証に RADIUS と SonicWall ローカル ユーザ データベースの両方を使用する場合に選択します。RADIUS の設定の詳細については、「RADIUS の設定」を参照してください。
LDAP	Lightweight Directory Access Protocol (LDAP) サーバまたは Microsoft Active Directory (AD) サーバを使用してすべてのユーザ アカウント データを管理する場合に選択します。LDAP の設定の詳細については、「LDAP の設定」を参照してください。
LDAP + ローカル ユーザ	認証に LDAP と SonicWall ローカル ユーザ データベースの両方を使用する場合に選択します。LDAP の設定の詳細については、「LDAP の設定」を参照してください。
TACACS+	認証に Terminal Access Controller Access-Control System Plus (TACACS+) プロトコルを使用する場合に選択します。
TACACS+ + ローカル ユーザ	認証に Terminal Access Controller Access-Control System Plus (TACACS+) プロトコルと SonicWall のローカル ユーザ データベースの両方を使用する場合に選択します。

3. 「**更新**」を選択します。

シングル サインオン方式の設定

「**シングル サインオン方式**」には、使用可能な方式の状況が表示されます。方式を有効/無効にしたり、「**構成**」を選択してシングル サインオン方式を構成したりできます。以下の方式が使用可能です。

シングル サインオン方式を設定するには、以下の手順に従います:

1. 「**ユーザ > 設定**」ページに移動します。
2. 方式を有効または無効にしたり、「**構成**」を選択してシングル サインオン方式を構成したりします。次の方式が使用可能です。

SSO エージェント	認証に Active Directory を使用していて、SonicWall SSO エージェントが同じドメイン内のコンピュータにインストールされている場合、「**SSO エージェント**」を構成します。
ターミナル サービス エージェント	ターミナル サービスを使用していて、SonicWall ターミナル サービス エージェント (TSA) が同じドメイン内のターミナル サーバにインストールされている場合は、「SSO エージェント」を構成します。
ブラウザ NTLM 認証	SonicWall SSO エージェントまたは TSA を使わずにウェブ ユーザを認証したい場合は、「**ブラウザ NTLM 認証**」を構成します。ユーザは HTTP トラフィックを送信すると即時に識別されます。NTLM は MSCHAP 認証にアクセスするために RADIUS (LDAP を使う場合は LDAP) が構成されている必要があります。
RADIUS アカウント	ネットワーク アクセス サーバ (NAS) からアカウント サーバにユーザ ログイン セッション アカウント メッセージを送信する場合、「**RADIUS アカウント**」を構成します。
サードパーティ API	ユーザ ログイン/ログアウト通知をファイアウォールに受け渡すために、サードパーティ デバイスまたはスクリプト用の XML/JSON ベースの REST API を構成します。

3. 「**更新**」を選択します。

ユーザ名の大文字と小文字を区別して扱うよう設定する

ユーザ名の大文字と小文字を区別して扱うよう設定するには、以下の手順に従います

1. 「**ユーザ > 設定**」ページに移動します。
2. 「**ユーザ名の大文字と小文字を区別する**」を選択します。(このオプションは既定でオンになっています。)
3. 「**更新**」を選択します。

複数の場所からのユーザ ログインを許可しないよう設定する

一度に複数の場所からユーザがログインできないようにするには、以下の手順に従います

1. 「**ユーザ > 設定**」に移動します。
2. 「**多重ログインを禁止する**」をオンにします。(このオプションは、既定では選択されていません)
3. 「**更新**」を選択します。

パスワードが変更された直後にユーザを強制的にログインさせる

パスワードが変更された直後にユーザを強制的にログインさせるには、以下の手順に従います

1. 「**ユーザ > 設定**」に移動します。
2. 「**パスワードが変更された後に再ログインを強制する**」を選択します。(このオプションは、既定では選択されていません)
3. 「**更新**」を選択します。

最終ログイン以降のユーザ ログイン情報を表示する

最終ログイン以降のユーザ ログイン情報を表示するには、以下の手順に従います

1. 「**ユーザ > 設定**」ページに移動します。
2. 「**最終ログイン以降のユーザ ログイン情報を表示する**」を選択します。(このオプションは、既定では選択されていません)
3. 「**更新**」を選択します。

ワンタイム パスワード設定

ワンタイム パスワード設定を構成するには、以下の手順に従います

1. 「**ユーザ > 設定**」に移動します。
2. 「**ワンタイム パスワードの電子メール形式**」で、以下の電子メール形式から選択します。
   - **プレーン テキスト**
   - **HTML**
3. 「**ワンタイム パスワード形式**」で、以下のパスワード形式から選択します。
   - **英字**
   - **英数字**
   - **数字**

4. 「**ワンタイム パスワード長**」の開始フィールドと終了フィールドに、パスワードの最小長と最大長を入力します。長さは 4 ～ 14 文字にする必要があります。どちらのフィールドも既定値は 10 文字です。
5. 「**更新**」を選択します。

ユーザ ウェブ ログイン設 定 の構 成

トピック:

- 認証ページのタイムアウトの設定
- ブラウザのリダイレクト方法の設定
- ログイン ページへのリダイレクトの管理
- CHAP チャレンジを使用したユーザ認証
- 未認証ユーザのリダイレクト
- 認証バイパスへの URL の追加

認 証 ページのタイムアウト の設 定

ログイン認証ページが表示されている間はシステム リソースが消費されます。時間制限を設けてその間にログインしなければログイン ページを閉じるようにすることで、それらのリソースを解放します。

認証ページのタイムアウトを設定するには、以下の手順に従います

1. 「**ユーザ > 設定**」に移動します。
2. 「**認証ページの表示時間 (分)**」フィールドには、ユーザがユーザ名とパスワードを使ってログインするまでの制限時間、つまりログイン ページがタイム アウトするまでの分数を入力します。ログイン ページがタイム アウトすると、再度ログインを試みる前に行うべきことを知らせるメッセージが表示されます。既定値は 1 分です。
3. 「**更新**」を選択します。

ブラウザのリダイレクト 方 法 の設 定

ブラウザのリダイレクト方法を設定するには、以下の手順に従います

1. 「**ユーザ > 設定 > ウェブ ログイン**」に移動します。
2. ユーザのブラウザを最初に SonicWall 装置のウェブ サーバにどのようにリダイレクトするを決めるために、「**ブラウザをこのデバイスにリダイレクトする経路**」から、以下のオプションのいずれかを選択します。
    - **インターフェースの IP アドレス** – ブラウザを装置のウェブ サーバ インターフェースの IP アドレスにリダイレクトする場合に選択します。このオプションは、既定では選択されています。
    - **インターフェース IP アドレスの逆引き DNS 調査によるドメイン名** – クリックすると、装置のウェブ サーバのインターフェース、IP アドレス、DNS 名、TTL (秒) が表示されます。このオプションは、既定では選択されていません。
    - **構成されたドメイン名** – 選択すると、「**システム > 管理**」ページで構成したドメイン名へのリダイレクトが有効化されます。

ⓘ **補足:** このオプションは、「**システム > 管理**」ページでドメイン名を指定した場合にのみ使用できます。指定していない場合、このオプションはグレーアウトされます。構成されたドメインへのリダイレクトを有効にするには、「**システム > 管理**」ページでファイアウォールのドメイン名を設定します。リダイレクトが許可されるのは、インポートした証明書がそのページで HTTPS ウェブ管理用として選択されている場合です。

- **管理証明書の名前** — これを選択すると、構成されたドメイン名へのリダイレクトが適切な署名済み証明書により有効化されます。この管理証明書の名前へのリダイレクトが許可されるのは、インポートした証明書がそのページで HTTPS ウェブ管理用として選択してある場合です。

  ⓘ **補足:** このオプションは、「**システム > 管理**」ページの「**ウェブ管理設定**」セクションで証明書を HTTPS 管理用としてインポートした場合にのみ使用できます。指定していない場合、このオプションはグレーアウトされます。

  ⓘ **ヒント:** インポートした管理証明書を使用する場合は、このオプションを使います。管理証明書を使用する予定がなければ、「**構成されたドメイン名**」を選択します。

  HTTPS 管理を行う際、ブラウザで無効な証明書の警告が表示されないようにするには、証明機関によって適切に署名された証明書（管理証明書）をインポートする必要があります。内部的に生成された自己署名証明書はこの目的には合いません。この証明書は、当該装置およびそのホストドメイン名を対象として生成されたものでなければなりません。適切に署名された証明書は、装置のドメイン名を取得する最善の方法です。

  管理証明書を使用する場合、証明書に関する警告が表示されないようにするには、ブラウザを IP アドレスではなく、そのドメイン名へリダイレクトする必要があります。例えば、インターネットをブラウズしていて `https://gateway.SonicWall.com/auth.html` のログインにリダイレクトされた場合、装置上の管理証明書によって装置が実際に `gateway.sonicwall.com` だとわかるので、ブラウザはそのログイン ページを表示します。しかし、リダイレクト先が `https://10.0.02/auth.html` の場合は、証明書の示す装置が `gateway.sonicwall.com` であってもブラウザはそれが正しいか判断できないので、代わりに証明書に関する警告を表示します。

3. 「**更新**」を選択します。

ログイン ページへのリダイレクトの管理

リダイレクトを制限することで、SonicWall 装置のウェブ サーバに過剰な負荷がかかる可能性が回避されます。ログイン ページへのリダイレクトを制限しないと、HTTP/HTTPS 接続がリダイレクトされる場合に、一部の不正ユーザが高い比率で何回も繰り返しページを開く可能性があるからです。

ログイン ページへのリダイレクトを管理するには、以下の手順に従います

1. 「**ユーザ > 設定 > ウェブ ログイン**」に移動します。
2. 「**ユーザのリダイレクトを制限する**」フィールドに、ユーザ 1 人あたりの 1 分間におけるリダイレクトの最大回数を入力します 既定値は 10 回です。
3. 同じページへのリダイレクトをさらに制限するには、「**同じページの反復的な取得をリダイレクトしない**」オプションを選択します。このオプションは、既定では選択されています。
4. セッションを暗号化する必要がない場合は、「**ログイン完了時にユーザを HTTPS から HTTP にリダイレクトする**」を選択します。
5. 「**更新**」を選択します。

CHAP チャレンジを使用したユーザ認証

RADIUS 認証を使用している場合 (かつ RADIUS サーバが RADIUS 認証をサポートしている場合)、ウェブ ログイン時に CHAP チャレンジを使用してユーザを認証することができます。HTTP 経由で CHAP チャレンジを使用して認証を行うログインは保護されているので、必ずしもログインに HTTPS を強制する必要はありません。

SonicWall 装置へのログインにこのメカニズムを使用する管理者は、実行できる管理作業が制限されます。一部の管理作業では、装置がユーザのパスワードを認識している必要がありますが、リモート認証サーバによる CHAP 認証ではパスワードを利用できません。したがって、このオプションが有効になっていると、管理ユーザ グループに所属するユーザは、管理目的でログインする場合に HTTPS を介して手動でログインしなければならないことがあります。この制限は組み込みの **admin** アカウントには適用されません。

ⓘ **ヒント:** LDAP を使用している場合は、通常、以下の方法でこのメカニズムを利用できます。

- ログインの認証方法を「RADIUS」に設定します。
- RADIUS に関する設定を行う際に、ユーザ グループ メンバーシップの設定メカニズムとして LDAP を選択します。

CHAP チャレンジを使用してユーザを認証するには、以下の手順に従います

1. 「**ユーザ > 設定 > ウェブ ログイン**」に移動します。
2. 「**RADIUS CHAP モードでのログインを許可する**」を選択して、ログイン種別を有効にします。
   ⓘ **補足:** このオプションは、「**ログインの認証方法**」が「**RADIUS**」または「**RADIUS + ローカル ユーザ**」の場合にのみ選択可能です。このオプションは、既定では選択されていません。
3. 「**更新**」を選択します。

未認証ユーザのリダイレクト

認証されていないユーザからの HTTP/HTTPS トラフィックを SonicWall 固有のログイン ページではなく所定の URL にリダイレクトすることができます。

認証されていないユーザからの HTTP/HTTPS トラフィックをリダイレクトするには、以下の手順に従います。

1. 「**認証されていないユーザを外部ログイン ページ URL にリダイレクトする**」を選択します。このオプションを使用すると、ユーザを外部の認証システムで認証できるようになります。このオプションは、既定では選択されていません。
   ⓘ **ヒント:** 認証されていないユーザだけをリダイレクトできるようにするには、この状況に対応する 1 つ以上のアクセス ルールを作成する必要があります。
   ⓘ **補足:** その後、外部システムは SSO 用のサードパーティ API や RADIUS アカウントを使用してユーザの名前と資格情報をファイアウォールに渡すことができるので、アクセス制御やログ記録といったアクティビティでユーザが特定されるようになります。
2. このオプションを選択すると、「**URL**」フィールドが表示されます。このフィールドにリダイレクト先の URL を入力します。
3. ゾーンのゲスト設定で構成されたキャプティブ ポータルに関連するオプションを構成するには、「**ゲスト キャプティブ ポータルのウェブ ログイン設定**」までスクロールします。

4. キャプティブ ポータルでのゲスト認証で、認証ページをフレームとしてポータル ホスト ページに表示できるようにするには、「**フレーム形式の認証ページを許可する**」を選択します。このオプションは、既定では選択されていません。
5. 「**更新**」を選択します。

認証バイパスへの URL の追加

SonicOS/X ゲスト サービスは、保護されたネットワークに対するアクセスをゲスト ユーザに与えることなく、ゲスト ユーザがネットワークを通じて直接インターネットに接続できるようにします。これを行うために、SonicOS/X はユーザのコンピュータの IP アドレスを使用します。

IP アドレスを識別子として使用することは、ゲスト ユーザ トラフィックがネットワーク ルータを通過する場合に役立ちます。この場合、送信元 MAC アドレスはルータの MAC アドレスに変わるからです。これに対し、ユーザの IP アドレスは変わらずに通過します。

MAC アドレスのみを使って識別を行う場合、同じルータを通る 2 つのクライアントは同じ MAC アドレスでネットワーク セキュリティ装置に到達します。その結果、一方のクライアントが認証されると、もう一方のクライアントからのトラフィックも認証済みとして処理され、ゲスト サービス認証をバイパスすることになります。

識別にクライアント IP アドレスを使用することで、ルータ デバイスを経由するすべてのゲスト クライアントが個別に認証を要求されるようになります。

アクセス ルールに HTTP URL ユーザ認証バイパスを追加するには、以下の手順に従います

1. 「**ユーザ > 設定 > 認証バイパス**」に移動します。
2. 「**追加**」を選択します。「**URL の追加**」ページが表示されます。
3. 「**URL の追加** 」フィールドに URL を入力します。
4. 「**追加**」を選択します。変更命令の確認のポップアップが表示されます。
5. 「**OK**」をクリックします。
6. 「**更新**」を選択します。

ユーザ セッション設定

以下の設定は、SonicWall ネットワーク セキュリティ装置を通して認証されるすべてのユーザに適用されます。

ユーザ セッションの設定を構成するには、以下の手順に従います

1. 「**ユーザ > 設定 > ユーザ セッション**」に移動します。

ファイアウォールを介して認証されるすべてのユーザに適用される設定を構成するには

1. 「**ユーザ > 設定 > ユーザ セッション**」に移動します。
2. 「**無動作時タイムアウト (分)**」フィールドで、無動作状態が一定期間続いたらユーザをファイアウォールからログアウトさせる時間の長さを指定します。既定値は 15 分です。
3. 「**無動作時のユーザ ログアウトを防ぐために次のサービスからのトラフィックを許可しない**」から、無動作ユーザのログアウトを阻止するサービスまたはサービス グループ オプションを選択します。このオプションを有効化すると、ユーザはログアウトではなく非アクティブ化されるので、システムのオーバーヘッドが減り、

寿命が超過した認証済みユーザを再度識別する場合に生じる遅延が回避されます。無動作ユーザはシステム リソースを消費しませんが、「**ユーザ> 状況**」ページには表示されます。既定は「**なし**」です。

4. 以下の「**ユーザが識別されていない接続のログ記録**」オプションで、実行するログ記録の種類（「**ユーザ名をログに記録しない**」または「**ユーザ名をログに記録する**」）を選択し、必要に応じてログ ユーザ名も選択します。
   - **SSO がユーザの識別に失敗した場合: ユーザ名をログに記録する ー 不明 SSO 失敗**（既定値）
   - **SSO をバイパスする接続の場合: ユーザ名をログに記録する ー SSO バイパス**（既定値）

     ⓘ **補足:** このオプションは、「**シングル サイン オン認証設定の強制**」ダイアログの「**SSO バイパス**」セクションで設定できます。
   - 発信元が外部である接続の場合:「**ユーザ名をログに記録しない**」(既定値)。「**ユーザ名をログに記録する**」を選択した場合、既定のユーザ名は「**不明 (外部)**」です。
   - その他の識別できない接続の場合:「**ユーザ名をログに記録しない**」(既定値)。「**ユーザ名をログに記録する**」を選択した場合、既定のユーザ名は「**不明**」です。
5. ユーザが SonicWall 装置からログアウトした後も残るユーザの接続をどう処置するかを「ログアウト時の残りのユーザ接続に対する動作」オプションで指定します。

	動作	
ログアウトの種類	**ユーザ認証 1 を必要とする接続の場合**	**その他の接続 2 の場合**
無動作によるログアウト時の動作	• 接続を維持（既定値） • 接続を終了 • 次の時間経過後に終了: ... 分	• 接続を維持（既定値） • 接続を終了 • 次の時間経過後に終了: ... 分
能動的/報告対象ログアウト時の動作	• 接続を維持 • 接続を終了（既定値） • 次の時間経過後に終了: ... 分	• 接続を維持 • 接続を終了 • 次の時間経過後に終了: 15 分（既定値）

1. 特定のユーザのみを許可するアクセス ルールによる接続に対して適用されます。
2. 特定のユーザ認証要件を備えていないその他の接続に対して適用されます。

以下に対しては、別の動作を設定できます。

- 無動作によるログアウト（ユーザがドメイン/コンピュータにログインしたままのこともあれば、そうでないこともある）。
- ユーザによる能動的なログアウト、または SonicWall ネットワーク セキュリティ装置へのユーザ ログアウトの報告（後者は通常、ユーザがドメイン/コンピュータからログアウトしたことを意味する）。

6. 「**更新**」を選択します。

トピック:

- SSO で認証されたユーザのユーザ セッションの設定
- ウェブ ログイン用ユーザ セッションの設定

SSO で認証されたユーザのユーザ セッションの設定

SSO で認証された無動作ユーザの処置を指定するには、以下の手順に従います

1. 「**ユーザ> 設定 > ユーザ セッション**」に移動します。
2. SonicWall ネットワーク セキュリティ装置から SSO メカニズムを通して識別されたユーザを、そのユーザからのトラフィックをまだ受け入れていない段階で、無動作状態にしてリソースが消費されないようにするには、「**ログインの通知時にトラフィックを送信するまではユーザを無動作状態にする**」をオンにします。ユーザの無動作状態はトラフィックを受け取るまで続きます。このオプションは、既定では選択されています。

   SSO メカニズムによっては、SonicWall ネットワーク セキュリティ装置がユーザを能動的に再識別する仕組みを提供していない場合があり、そのようなメカニズムで識別されたユーザからトラフィックが送られてこないと、装置が最終的にユーザのログアウト通知を受け取るまで、ユーザは無動作状態のままになります。それ以外の再識別可能なユーザは、無動作状態のままトラフィックを送信しないと、一定期間を超過したときに寿命超過で削除されます（後述の説明を参照）。
3. 能動的にログインして SSO で識別されたユーザが無動作によりタイムアウトした場合、再識別されなければユーザは無動作状態に戻ります。何も処置しなければ無動作によりログアウトするところのユーザを無動作状態に戻すには、「**無動作タイムアウト時にすべてのユーザをログアウトさせるのではなく無動作状態にする**」をオンにします。これを行うと、オーバーヘッドが減り、動作状態に復帰するユーザを再識別する場合に生じる遅延が回避されます。このオプションは、既定で選択されています。
4. 無動作ユーザが寿命超過処置の対象となる場合、無動作状態のままトラフィックを送信しなかったとき寿命超過で削除されるまでのタイムアウト時間（分）を設定できます。具体的には、「**無動作ユーザを寿命超過させる時間（分）**」をオンにし、フィールドにタイムアウト時間を入力します。この設定は既定で選択されています。最小タイムアウト値は 10 分、最大値は 10000 分、デフォルト値は **60** 分です。

   ⓘ **補足:** 無動作ユーザと動作中のユーザを区別する理由はユーザの管理に使われるリソースの消費を抑えるためであり、寿命超過タイマーは 10 分間隔で更新されます。そのため、無動作ユーザが実際に削除されるまでの時間は、ここで設定した時間よりも最大で 10 分長くなる可能性があります。
5. 「**更新**」を選択します。

ウェブ ログイン用ユーザ セッションの設定

ウェブ ログイン用ユーザ セッションの設定を構成するには、以下の手順に従います

1. 「**ユーザ > 設定 > ユーザ セッション**」に移動します。
2. **ウェブ接続のログイン セッション時間の制限を有効にする:** ログイン ページがタイムアウトする前にユーザがウェブ ログインによりファイアウォールにログインする時間を制限するには、このオプションをオンにし、「**ログイン セッション時間の制限（分）**」フィールドに時間を分単位で入力します。この設定は既定で選択されています。既定値は **30** 分です。

   セッションがタイム アウトすると、再度ログインを試みる前にログアウトするよう促すメッセージが表示されます。
3. 「**ログアウト ボタン付きユーザ ログイン状況ウィンドウを表示する**」を選択し、ユーザ セッションが継続している間、「**ログアウト**」ボタンのある状況ウィンドウを表示します。ユーザがセッションからログアウトするには、「**ログアウト**」をクリックする必要があります。このオプションは、既定では選択されていません。

   ⓘ **補足:** ユーザのセッション中は、このウィンドウをずっと開いておかなければなりません。ウィンドウを閉じると、ユーザはログアウトします。

ⓘ **重要:** このオプションを有効化しないと、状況ウィンドウは表示されず、ユーザがログアウトできないことがあります。その場合は、ログイン セッション時間の制限を設けてユーザを最終的にログアウトさせなければなりません。

「**(分) ごとにユーザ ログイン状況ウィンドウを更新する**」には、ログイン セッションの残りの分数が表示されます。ユーザは、数値を入力して「**更新**」を選択することで、残りの分数を短く設定し直すこともできます。

このオプションを有効化すると、そのウィンドウから送られてくるハートビートを監視するメカニズムも有効化し、ログアウトせずに切断されたユーザを検知してログアウトさせることができます。
重要: このオプションを有効化しないと、ユーザがログアウトできないことがあります。ログイン セッション時間の制限を設けて、ユーザを最終的にログアウトさせるようにしてください。

4. 「**ユーザ ログイン状況ウィンドウがハートビートを送信する間隔 (秒)**」フィールドに、SonicWall ネットワーク セキュリティ装置にハートビートを送り返す頻度を指定します。このハートビートは、SonicWall ネットワーク セキュリティ装置に接続状況を通知するもので、状況ウィンドウが表示されている限り、送信され続けます。既定値は 120 秒です。
5. 「**切断されたユーザの検出を有効にする**」を選択すると、SonicWall ネットワーク セキュリティ装置は接続が有効でなくなったユーザを検出すると、そのセッションを終了します。このオプションは、既定ではすでに選択されています。
6. 「**ユーザ ログイン状況ウィンドウから次の時間ハートビートがなかった場合に切断とみなす (分)**」フィールドで、ハートビートからの応答がなかった場合に、ユーザ セッションを終了するまでの時間を設定します。ユーザ セッションを終了するまでの遅延時間は、最小 1 分、最大 65535 分で、既定値は 10 分です。
7. 認証されていない VPN ユーザの DNS アクセスを許可するには、「**Allow unauthenticated VPN users to access DNS (認証されていない VPN ユーザの DNS アクセスを許可する)**」を選択します。
8. ログイン状況ウィンドウを個別のポップアップ ウィンドウとして表示したくない場合は、「**ポップアップではなく、同一ウィンドウ内にユーザのログイン状況ウィンドウを開く**」を選択します。このオプションは、既定では選択されていません。
9. LDAP オプションが有効な場合、LDAP のサーバから読み込みオプションが選択可能になります。以下のオプションがあります。
    - 「**Automatically update the schema configuration (スキーマの設定を自動的に更新する)**」
    - 「**Export details of the schema (スキーマの詳細をエクスポートする)**」
10. 「**更新**」を選択します。

アカウント

SonicOS/X は、RADIUS アカウントと TACACS+ アカウントの両方をサポートしています。RADIUS サーバと TACACS+ サーバの両方が構成されている場合、ユーザのアカウント メッセージは両方のサーバに送信されます。

トピック:

- RADIUS アカウントの設定
- TACACS+ アカウントの設定

RADIUS アカウントの設定

トピック:

RADIUS アカウント情報のサーバへの送信

RADIUS アカウント情報をサーバに送信するには、以下の手順に従います

1. 「**ユーザ > 設定 > アカウント**」に移動します。
2. 「**RADIUS アカウント**」の横の「**構成**」を選択します。
3. RADIUS サーバを追加するには、以下の手順に従います:
    a. 「**サーバの追加**」を選択します。「**設定**」ページが表示されます。
    b. 「**ホスト名または IP アドレス**」フィールドに、ホスト名または IP アドレスを入力します。
    c. [**ポート**] フィールドに、ポート番号を入力します。
    d. 「**共有鍵**」フィールドと「**事前共有鍵の確認**」フィールドに、共有鍵を入力します。
    e. 「**詳細**」タブの「**ユーザ名の形式**」リストから、ユーザ名の形式を選択します。
        - **ユーザ名**
        - **ユーザ名@ドメイン**
        - **ドメイン¥ユーザ名**
        - **ユーザ名.ドメイン**
    f. 「**保存**」をクリックします。「RADIUS アカウント」テーブルが更新されます。

    追加する RADIUS サーバごとに、これらのステップを繰り返します。
4. 「**一般設定**」を選択します。
5. 「**RADIUS アカウント サーバ タイムアウト (秒)**」フィールドに、タイムアウトの最大値を秒単位で入力します。既定値は **5** 秒です。
6. 「**再試行**」フィールドに再試行の最大数を入力します。既定値は **3** です。
7. 「RADIUS アカウント」テーブルに表示されているすべてのサーバにアカウント データを送信するには、「**アカウント データをすべてのサーバに送信する**」を選択します。
8. 有効にする RADIUS サーバごとに、「**有効**」をクリックします。
9. 「**更新**」を選択します。

ユーザ アカウントの設定

RADIUS 用のユーザ アカウントを構成するには、以下の手順に従います

1. 1 つまたは複数のユーザ種別を選択します。
2. 「**RADIUS アカウントによって識別された SSO ユーザを含める**」は、既定では選択できません。これを選択できるようにするには、まず「**SSO で認証されたユーザ**」フィールドを選択します。
3. 「**包含**」リストから、含めるユーザを選択します。
   - **ドメイン ユーザ**
   - **ローカル ユーザ**
   - **ドメインおよびローカル ユーザ**
4. 中間更新を送信するには、「**中間更新を送信する**」を選択します。

RADIUS アカウントのテスト

RADIUS アカウントをテストするには、以下の手順に従います

1. 「**ユーザ > 設定 > アカウント**」に移動します。
2. 「**RADIUS アカウント**」の横の「**構成**」を選択します。
3. 「**テストするサーバの選択**」リストから、テストする RADIUS サーバを選択します。
4. 「**テスト**」リストから、テストする機能を選択します。
   - SSL VPN
   - **ユーザ アカウント**: 「**ユーザ**」と「**IP アドレス**」を入力します。
5. 「**テスト**」を選択します。
   「**テスト状況**」が更新され、返されたすべてのユーザ属性が「**返されたユーザ属性**」に表示されます。

RADIUS サーバの編集

RADIUS サーバを編集するには、以下の手順に従います

1. 「**ユーザ > 設定 > アカウント**」に移動します。
2. 「**RADIUS アカウント**」の横の「**構成**」を選択します。
3. 編集する RADIUS サーバの**編集**アイコンをクリックします。「**共有鍵**」フィールドと「**事前共有鍵の確認**」フィールドは淡色表示となり、変更できません。
4. 必要な変更を加えます。
5. 「**保存**」をクリックします。

RADIUS サーバの削除

サーバを 1 つ削除するには、以下の手順に従います

1. 「**ユーザ> 設定 > アカウント**」に移動します。
2. 「**RADIUS アカウント**」の横の「**構成**」を選択します。
3. 削除するサーバの行の右端にマウス ポインタを置くと、アイコンが表示されます。「**削除**」アイコンを選択します。確認メッセージが表示されます。
4. 「**確認**」をクリックします。

5. 「**更新**」を選択します。

1 つまたは複数のサーバを削除するには、以下の手順に従います

1. 「**ユーザ> 設定 > アカウント**」に移動します。
2. 「**RADIUS アカウント**」の横の「**構成**」を選択します。
3. 削除する「RADIUS アカウント」テーブル内のサーバを選択します。
4. 「**削除**」を選択します。確認メッセージが表示されます。
5. 「**確認**」をクリックします。
6. 「**更新**」を選択します。

TACACS+ アカウントの設定

SonicOS/X は TACACS+ アカウントの Start、Watchdog、および Stop メッセージをサポートしますが、TACACS+ アカウント プロキシはサポートしません。つまり、SonicOS/X はアカウント要求をアカウント サーバに転送しません。

TACACS+ アカウントを構成するには、以下の手順に従います

1. 「**ユーザ > 設定 > アカウント**」に移動します。
2. 「**TACACS+ アカウント**」の横の「**構成**」を選択します。
3. TACACS+ サーバを追加するには、「**サーバの追加**」を選択します。
4. 「**ホスト名または IP アドレス**」フィールドに、TACACS+ サーバのホスト名または IP アドレスを入力します。
5. 「**ポート**」フィールドに、サーバのポート番号を入力します。既定値は 49 です。
6. 「**共有鍵**」フィールドと「**事前共有鍵の確認**」フィールドに、共有鍵を入力します。
7. この TACACS+ サーバを使用する準備ができたら、「**有効**」を選択します。
8. 「**保存**」をクリックします。

3

パーティションの設定と管理

ⓘ | **補足:** 「**ユーザ > パーティション**」は、パーティション処理が SonicWall 装置に対して構成されている場合にのみ表示されます。

認証パーティションのツリーを展開すると、そのパーティションに割り当てられているサーバ、クライアント、エージェントが表示されます。

以下のツリーを展開できます。

- すべてのテーブル エントリ – 見出しのチェックボックスの横にある三角形をクリックします。
- 1 つ以上のテーブルエントリ – それぞれの展開アイコンをクリックします。

トピック:

認証パーティション設定

このセクションは認証パーティション処理を有効または無効にします。

- 認証パーティション処理が無効になっていると、その他のセクションは表示されません。
- 認証パーティション処理が有効になっている場合、2 つの検索機能と 2 つの追加セクション (「認証パーティション」および「認証選択ポリシー」) も表示されます。

認証パーティション

ⓘ | **補足:** このセクションは、認証パーティション処理が有効になっている場合にのみ表示されます。

このセクションには、認証パーティションのテーブルが表示され、パーティションの作成、編集、削除、管理を行うことができます。ここで構成するパーティションにより、どのユーザでどの認証サーバが使用されるかが制御されます。

パーティションのツリーを展開すると、そのパーティションに割り当てられているサーバ、エージェント、クライアントを表示できます。

選択用チェックボックス	テーブルにある 1 つ以上のパーティションやサブパーティションを選択できます。テーブル見出しにあるチェックボックスをオンにすると、「既定」パーティションを除くすべてのエントリが選択されます。
名前	認証パーティションの名前を指定します。サブパーティションは、名前の前に**リンク**アイコンが表示されます。
親パーティション	サブパーティションに対する親の認証パーティションを指定します。親パーティションの場合、この列は空欄になります。
ドメイン	パーティションまたはサブパーティションが属するドメインを指定します。「**既定**」パーティションの場合、この列は空欄になります。
コメント	パーティションの追加時に入力したコメントが表示されます。「**既定**」パーティションに対するコメントは、「**自動作成された既定パーティション**」です。
構成	パーティションの**編集**アイコン、**選択**アイコン、**削除**アイコンが表示されます。 ⓘ | **補足:** 「**既定**」パーティションでは、**削除**アイコンが淡色表示になっています。
パーティションの追加	認証パーティションまたはサブパーティションを追加するための「認証パーティションの追加」ポップアップ ダイアログを表示します。
自動割り当て	まだ割り当てられていないすべての LDAP サーバ、RADIUS サーバ、SSO エージェント、TSA、および RADIUS アカウント クライアントをその IP アドレスまたはホスト名に基づいて、関連するパーティションに自動的に割り当てます。
パーティションの削除	選択されている認証パーティションまたはサブパーティションを削除します。 ⓘ | **補足:** 「**既定**」パーティションは削除できません。

このテーブルには、認証パーティションが必ず 1 つは存在します。それは自動生成された「**既定**」パーティションです。このパーティションは削除できません。ただし、既定パーティションを編集して、サーバ、エージェント、クライアントや、サブパーティションを選択することは可能です。認証パーティションを無効にした場合、すべての LDAP サーバ、SSO エージェント、TSA、および RADIUS アカウント クライアントは「**既定**」パーティションに割り当て直されます。これらは、認証パーティションを再び有効化する際に割り当て直す必要があります。なお、RADIUS サーバは影響を受けないので、割り当てられたパーティションにとどまります。

トピック:

- パーティションとサブパーティションの追加
- パーティションとサブパーティションの削除

パーティションとサブパーティションの追 加

パーティションを追加するには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」セクションで、**追加**アイコンをクリックします。「**認証パーティションの追加**」ダイアログが表示されます。
3. 「**パーティション名**」フィールドに、意味のある分かりやすい名前を入力します。名前は 1 ～ 32 文字の英数字で指定します。

4. 「**パーティション種別**」で、認証パーティションを次のどれにするかを選択します。
    - **最上位レベルのパーティション**
    - **サブパーティション**
        1. 「**親パーティション**」ドロップダウン メニューが使用可能になります。
        2. このドロップダウン メニューから親パーティションを選択します。既定のパーティションは「Default」です。

            ⓘ | **ヒント:** インストールに複数のパーティションが存在しない場合は、サブパーティションを「Default」パーティションのサブパーティションとして作成します。
5. 「**ドメインの追加/編集**」フィールドの横の「**追加**」アイコンをクリックします。「**ドメインの追加**」ダイアログが表示されます。
6. 「**ドメイン名を入力**」フィールドにドメイン名を入力します。
7. 「OK」をクリックします。
8. 追加するドメインごとに、これらのステップを繰り返します。
9. 必要に応じて、「コメント」フィールドにコメントを入力します。
10. 「**保存**」をクリックします。

パーティションやサブパーティションは「**認証パーティション**」テーブルに追加されます。サブパーティションは、その親パーティションのすぐ後に配置され、**リンク** アイコンによってサブパーティションであることがわかります。

パーティションとサブパーティションの削除

ⓘ | **補足:** このセクションでは、パーティションという語がパーティションとサブパーティションの両方を指します。

1 つのパーティション、複数のパーティション、またはすべてのパーティションを削除できます。1 つのパーティションを削除した場合、そのサーバ、エージェント、クライアントは「**既定**」パーティションへの再割り当てが行われます。

ⓘ | **補足:** 「**既定**」パーティションは削除できません。

トピック:

- 単一パーティションの削除
- 複数パーティションの削除
- すべてのパーティションの削除

すべてのパーティションの削除

すべてのパーティション (既定を除く) を削除するには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」テーブルで、テーブルの左側の列の上部にあるチェックボックスをオンにします。すべてのパーティションが選択されます。
3. 「Default」パーティションの選択を解除します。

    ⓘ | **補足:** 「Default」パーティションは削除できません。「Default」パーティション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。
4. 「**パーティションの削除**」を選択します。確認メッセージが表示されます。
5. 「OK」をクリックします。

すべてのサーバ、エージェント、クライアントは「Default」パーティションへ再割り当てされます。

複数パーティションの削除

複数のパーティションを削除するには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」テーブルで、削除する認証パーティションのチェックボックスを選択します。複数のパーティションを選択できます。
3. 「**パーティションの削除**」を選択します。確認メッセージが表示されます。
4. 「OK」をクリックします。

単一パーティションの削除

パーティションを 1 つ削除するには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」テーブルで、削除するパーティションの「**構成**」列にある**削除**アイコンを選択します。確認メッセージが表示されます。
3. 「OK」をクリックします。

パーティション選択ポリシー

補足: このセクションは、認証パーティション処理が有効になっている場合にのみ表示されます。

このセクションには、認証パーティションの選択に影響を与えるポリシーのテーブルが表示され、ポリシーの作成、作成したポリシーの削除と編集を行うことができます。こうしたポリシーにより、認証されるユーザの物理的な場所に基づいて「**認証パーティション**」テーブル内のパーティションが選択されます。選択パーティション内のドメインとの照合が利用できないドメイン名を持つユーザを認証する際、そのユーザのパーティションはこうしたポリシーによって設定されたユーザの物理的な場所に基づいて選択されます。こうした選択ポリシーは、認証デバイスをその物理的な場所に基づいてパーティションに自動的に割り当てるためにも使用されます。

ⓘ | **補足:** 「**既定**」パーティションの「**既定**」選択ポリシーは削除できません

選択用チェックボックス	テーブル内の 1 つ以上のエントリを選択できます。テーブル見出しにあるチェックボックスをオンにすると、「**既定**」選択ポリシーのエントリを除くすべてのエントリが選択されます。
ゾーン	パーティション選択ポリシーに割り当てられているゾーンが表示されます。
インターフェース	認証パーティション選択ポリシーに割り当てられているインターフェースが表示されます。
ネットワーク	認証パーティション選択ポリシーに割り当てられているネットワークが表示されます。
パーティション	選択ポリシーが適用される認証パーティションが表示されます。
コメント	選択ポリシーの作成または編集時に入力したコメントがあれば表示されます。「**既定**」パーティションの選択ポリシーには、「**自動作成された既定ポリシー**」というコメントが付いています。
構成	**編集**アイコンと**削除**アイコンが表示されます。既定のポリシーではグレーアウトされています。

ポリシーの追加	認証パーティションまたはサブパーティション用の選択ポリシーを追加するための「**認証パーティション ポリシーを追加する**」ポップアップ ダイアログを表示します。
ポリシーの削除	選択されているポリシーを削除します。 **補足:**「**既定**」パーティション用のポリシーは削除できません。ポリシーが 1 つも選択されていない場合、「**削除**」はグレーアウトされています。

このテーブルには、選択ポリシーが必ず 1 つは存在します。「**既定**」パーティション用の自動生成された既定のポリシーです。このポリシーは、削除、優先順位の変更、編集ができません。ただし、適用されるパーティションの選択は可能です。

サーバ、エージェント、クライアントの割り当て

認証パーティションを追加した後は、サーバ、エージェント、クライアントをパーティションに割り当てることができます。同じ手順に従うことで、いつでも認証パーティションへの割り当てを行うこともできます。

割り当てられていないサーバ、エージェント、クライアントをパーティションに自動的に割り当てることができます。

トピック:

- サーバ、エージェント、クライアントの手動割り当て
- サーバ、エージェント、クライアントの自動割り当て

サーバ、エージェント、クライアントの手動割り当て

サーバ、エージェント、クライアントを手動で割り当てるには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」テーブルで、割り当てるパーティションの「**構成**」列で**選択**アイコンをクリックします。「**何を選択しますか?**」ダイアログが表示されます。
3. 割り当てるサーバ、エージェント、またはクライアントの種別を選択します。適切な「***partitionName* パーティションにサーバ/エージェント/クライアントの選択**」メニューには、使用可能なサーバ、エージェント、またはクライアントのリストが表示されます。
4. 以下のいずれかを実行します。
   - 「**利用可能**」リストからサーバ/エージェント/クライアントを選択し、右矢印を選択します。
   - Ctrl キーを押しながら各項目を選択して、「**利用可能**」リストから複数の項目を選択したうえで、右矢印を選択します。
   - 「**すべて追加**」を選択して、すべての項目を選択します。
5. 「**保存**」をクリックします。

サーバ、エージェント、クライアントの自動割り当て

「**自動割り当て**」ボタンを使用すると、まだ割り当てられていないサーバ、エージェント、クライアントをその IP アドレスまたはホスト名に基づいて関連するパーティションに割り当てることができます。

サーバ、エージェント、クライアントの自動割り当てを行うには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」テーブルで、未割り当てのサーバ、エージェント、クライアントを割り当てる認証パーティションのチェックボックスを選択します。複数のパーティションを選択できます。「**自動割り当て**」が使用可能になります。
3. 「**自動割り当て**」をクリックします。自動割り当てメッセージが表示されます。
4. 「OK」をクリックします。

パーティションの編集

「**既定**」パーティションを含むすべてのパーティションを編集できます。

パーティションを編集するには、以下の手順に従います

1. 「**ユーザ > パーティション**」へ移動します。
2. 「**認証パーティション**」テーブルで、変更する認証パーティションの「**設定**」列にある**編集**アイコンを選択します。「**認証パーティションの編集**」ダイアログが表示されます。
3. 「**パーティション名**」フィールドでは、パーティションの名前を変更できます。名前は 1 ～ 32 文字の英数字で指定します。
4. パーティションは、「**パーティション種別**」を変更することで、最上位レベルのパーティションからサブパーティションに、またはサブパーティションから最上位レベルのパーティションに変更できます。認証パーティションを次のどれにするかを選択します。
5. サブパーティションを持つ最上位レベルのパーティションは、そのサブパーティションをまず削除するか、別の最上位レベル パーティションに割り当て直すか、最上位レベルのパーティションにするかしないと、サブパーティションに変更することができません。
   - **最上位レベルのパーティション**
   - **サブパーティション**
     1. 「**親パーティション**」メニューが表示されます。
     2. 「**親パーティション**」ドロップダウン メニューから親パーティションを選択します。既定のパーティションは「Default」です。
6. ドメインを編集するには、以下の手順に従います:
   a. 編集するドメインを選択します。
   b. 「**編集**」を選択します。「**ドメインの編集**」ダイアログが表示されます。
   c. ドメイン名を変更します。
   d. 「OK」をクリックします。
7. ドメインを削除するには、以下の手順に従います:
   a. 削除するドメインを選択します。
   b. 「**削除**」を選択します。
8. ドメインを追加するには
   a. 「**ドメイン**」リストで、「追加」をクリックします。「**ドメインの追加**」ダイアログが表示されます。
   b. ドメイン名を 1 ～ 32 文字の英数字で入力します。
   c. 「OK」をクリックします。

9. 追加、編集、または削除するドメインごとに適切なステップを繰り返します。
10. 必要に応じて、「**コメント**」フィールドにコメントを入力します。
11. 「**保存**」をクリックします。

4

ゲスト サービスの設定

「ゲスト サービス」では、ゲスト アカウントの制限と設定を定義します。ゲスト アカウントとは、ユーザがネットワークにログインするための一時的なアカウントです。

ゲスト アカウントは、必要に応じて手動で作成するか、バッチで生成できます。一般的に、ゲスト アカウントには有効期限が設定されます。既定では、有効期限が切れた後にアカウントは削除されます。

トピック:

ゲスト プロファイルの追加

ゲスト プロファイルを追加するには、以下の手順に従います

1. 「**ユーザ > ゲスト サービス**」ページに移動します。
2. 「**ログアウト ボタン付きゲスト ログイン状況ウィンドウを表示する**」をオンにすると、ユーザがログインするごとにユーザのワークステーション上にユーザ ログイン ウィンドウが表示されます。ユーザは、ログイン セッション間、このウィンドウを開いたままにする必要があります。ウィンドウには、現在のセッションの残り時間が表示されます。ユーザは、ログイン状況ウィンドウ内の「**ログアウト**」を選択することにより、ログアウトできます。
3. ゲスト プロファイルを作成するには、「**ゲスト プロファイル**」リストの下にある「**ゲスト プロファイルの追加**」を選択します。「**ゲスト プロファイルの追加**」ウィンドウが表示されます。
4. 「**ゲスト プロファイルの追加**」ウィンドウで、以下のオプションを構成します。
    - **プロファイル名:** プロファイルの名前を入力します。
    - **ユーザ名開始文字列:** このプロファイルから生成される各ユーザ アカウント名の最初の部分を入力します。
    - **ユーザ名を自動生成する:** このオプションを選択すると、このプロファイルから生成されるゲスト アカウントに対して、ユーザ名が自動的に生成されます。通常、ユーザ名開始文字列に 2 または 3 桁の数字を付加した文字列がユーザ名となります。
    - **パスワードを自動生成する:** このオプションを選択すると、このプロファイルから生成されるゲスト アカウントに対して、パスワードが自動的に生成されます。生成されるパスワードは、一意な 8 文字の英字から構成される文字列です。

- **アカウントを有効にする:** このプロファイルから生成されるすべてのゲスト アカウントを作成時に有効にするには、このチェックボックスをオンにします。
- **アカウント期限切れ時に、アカウントを自動削除する:** アカウントの有効期限が切れたときに、アカウントをデータベースから削除するには、このチェックボックスをオンにします。
- **多重ログインを禁止する:** 任意の時点でアカウントの単一のインスタンスのみを使用できるようにするには、このチェックボックスをオンにします。既定では、新しいゲスト アカウントを作成するときに、この機能は有効になっています。単一のアカウントを使用して複数のユーザがログインできるようにする場合は、「**多重ログインを禁止する**」をオフにして、この強制を無効にします。
- **初回ログインの時点でアカウント有効期限を有効にする:** ユーザがアカウントに初回ログインするまで「アカウント存続期間」タイマーを遅延させるには、「**初回ログインの時点でアカウント有効期限を有効にする**」を選択します。このオプションは、既定では選択されていません。
- **アカウント存続期間:** この設定は、アカウントが失効するまで、セキュリティ装置上にアカウントを保持しておく期間を定義します。1 ～ 9999 の数値を「アカウント存続期間」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。
  - 分
  - 時間
  - 日

  既定値は 7 日間 です。

  「**自動削除**」が有効である場合、アカウントは有効期限が切れたときに削除されます。「**自動削除**」をオフにすると、アカウントは「**失効**」状態でゲスト アカウントのリストに残り、簡単に再びアクティブにすることができます。
- **無動作時タイムアウト:** アクティブ化されたゲスト サービス セッションでトラフィックが受け渡しされない期間の最大時間を定義します。この設定で定義した期間を過ぎるとセッションの有効期限が切れますが、アカウント自体は「**アカウント存続期間**」まではアクティブのままです。「**無動作時タイムアウト**」の値は、「**セッション存続期間**」で設定された値よりも大きくすることはできません。

  1 ～ 9999 の数値を「アカウント存続期間」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。
  - 分
  - 時間
  - 日

  既定値は **10 分**です。
- クォータ サイクル種別設定を指定する場合は、「**クォータ サイクル種別設定**」ドロップダウン メニューから選択します。
  - 循環しない（既定）
  - 日
  - 週
  - 月
- **セッション存続期間:** ゲスト ログイン セッションがアクティブになった後、アクティブである期間を定義します。既定では、アクティブ化はゲスト ユーザが最初にアカウントにログインするときに行われます。または、「**初回ログイン時にアカウントを有効にする**」をオフにすることによって、アカウントの作成時にアクティブにすることもできます。「**セッション存続期間**」には、「**アカウント存続期間**」より長い値を設定することはできません。

  1 ～ 9999 の数値を「**セッション存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。
  - 分

- 時間
- 日

既定値は 1 時間 です。

- ユーザが受信できるデータ量を制限するには、「**受信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」(既定) です。
- ユーザが送信できるデータ量を制限するには、「**送信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」(既定) です。
- **コメント**: 「**コメント**」フィールドには、コメントとして任意のテキストを入力できます。

5. 「**更新**」を選択して、プロファイルを追加します。

ゲスト プロファイルの編 集

ゲスト プロファイルを編集するには、以下の手順に従います

1. プロファイルの「**構成**」列で**編集**アイコンをクリックします。
2. 「ゲスト プロファイルの追加」の手順を実行します。

ゲスト プロファイルの削 除

「Default」プロファイルを除くすべてのゲスト プロファイルを削除できます。

ゲスト プロファイルを削除するには、以下の手順に従います

1. 以下のどちらかを選択してください。
   - 削除するゲスト プロファイルのチェックボックス。
   - 「**ゲスト プロファイル**」テーブルの左上にあるチェックボックス。(「Default」プロファイルを除く) すべてのチェックボックスがオンになります。

   「**ゲスト プロファイルの削除**」が選択可能になります。
2. 「**ゲスト プロファイルの削除**」を選択します。確認メッセージが表示されます。
3. 「**更新**」を選択します。

5

ゲスト アカウントの設定

SonicWall セキュリティ装置上に構成されているゲスト サービス アカウントがリストされます。個々のアカウント、アカウントのグループ、またはすべてのアカウントを有効化/無効化するだけでなく、アカウントの自動削除機能を設定する、アカウントまたはセッションの失効日時を設定する、またはアカウントの追加、編集、削除、印刷を行うことができます。

トピック:

ゲスト アカウントの追加

新しいゲスト アカウントを追加するには、以下の手順に従います

1. 「**ユーザ > ゲスト アカウント**」ページに移動します。
2. ゲスト アカウント リストの下にある「**ゲスト アカウントの追加**」を選択します。
3. ゲスト アカウントについて、以下のパラメータを構成します。
    - **プロファイル**: このアカウントの生成に使用するゲスト プロファイルを選択します。
    - **名前**: アカウント名を入力するか、「**生成**」を選択します。生成される名前は、プロファイルに指定されているユーザ名開始文字列に 2 桁または 3 桁のランダムな数字が追加された文字列です。
    - **コメント**: わかりやすいコメントを入力します。
    - **パスワード**: ユーザ アカウントのパスワードを入力するか、「**生成**」を選択します。生成されるパスワードは、ランダムな 8 文字の英字から構成される文字列です。
    - **パスワードの確認**: パスワードを生成しなかった場合は、パスワードをもう一度入力します。
    - **ゲスト サービスの権限を有効にする**: 作成時にアカウントを有効にする場合は選択します。
    - **多重ログインを禁止する**: このオプションを選択すると、セキュリティ装置にログインするために同時に使用できるこのアカウントのインスタンスの数が 1 つに制限されます。選択していない場合は、複数のユーザがすぐにこのアカウントを使用できます。
    - **アカウント期限切れ時に、アカウントを自動削除する**: アカウントの有効期限が切れたときに、アカウントをデータベースから削除するには、このオプションをオンにします。
    - アカウント有効期限のカウントを開始するには、「**初回ログイン時にアカウントを有効にする**」を選択します。

- **アカウント存続期間**: この設定は、アカウントが失効するまで、セキュリティ装置上にアカウントを保持しておく期間を定義します。1 ～ 9999 の数値を「アカウント失効期日」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。
  - **分**
  - **時間**
  - **日**

  既定値は **7 日間** です。
- 「**アカウント期限切れ時に、アカウントを自動削除する**」を
  - 「**有効**」にすると、アカウントは有効期限が切れたときに削除されます。
  - 「**無効**」にすると、アカウントは、簡単に再びアクティブにできるように「**失効**」状態で「**ゲスト アカウント**」テーブルに残ります。
- アクティブ化されたゲスト サービス セッションでトラフィックが受け渡しされない期間の最大時間を定義するには、「**無動作時タイムアウト**」にタイムアウト時間を入力します。この設定で定義した期間を過ぎるとセッションの有効期限が切れますが、アカウント自体は「**アカウント存続期間**」まではアクティブのままです。「**無動作時タイムアウト**」の値は、「**セッション存続期間**」で設定された値よりも大きくすることはできません。

  ⓘ | **補足:** この設定は、プロファイルでの無動作時タイムアウトの設定より優先されます。

  1 ～ 9999 の数値を「アカウント存続期間」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。
  - 分
  - 時間
  - 日

  既定値は **10 分**です。

4. クォータ サイクル種別設定を指定する場合は、「**クォータ サイクル種別設定**」ドロップダウン メニューから選択します。
   - **循環しない**（既定）
   - **日**
   - **週**
   - **月**
5. ゲスト ログイン セッションがアクティブになった後、アクティブであり続ける期間を定義するには、「**セッション存続期間**」にその期間を指定します。既定では、アクティブ化はゲスト ユーザが最初にアカウントにログインするときに行われます。「**セッション存続期間**」には、「**アカウント存続期間**」より長い値を設定することはできません。

   ⓘ | **補足:** この設定は、プロファイルでのセッション有効期限の設定より優先されます。

   1 ～ 9999 の数値を「セッション存続期間」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。
   - **分**
   - **時間**
   - **日**

   既定値は **1 時間** です。
6. **受信制限 (0 で無効化)**: ユーザに受信を許可するメガバイト数を入力します。最小値の 0 を指定すると制限が無効化されます。最大は「**無制限**」（既定値）です。
7. **送信制限 (0 で無効化)**: ユーザに送信を許可するメガバイト数を入力します。最小値の 0 を指定すると制限が無効化されます。最大は「**無制限**」（既定値）です。

8. ユーザが受信できるデータ量を制限するには、「**受信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0（データを一切受信できない）～ 999999999 MB および「**無制限**」（既定）です。
9. ユーザが送信できるデータ量を制限するには、「**送信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0（データを一切受信できない）～ 999999999 MB および「**無制限**」（既定）です。
10. 「**更新**」を選択して、ゲスト アカウントを生成します。

ゲスト アカウントの編集

ゲスト アカウントを編集するには、以下の手順に従います

1. プロファイルの「**構成**」列で**編集**アイコンをクリックします。
2. 「ゲスト アカウントの追加」の手順を実行します。

ゲスト アカウントの削除

「Default」プロファイルを除くすべてのゲスト プロファイルを削除できます。

トピック:

- ゲスト アカウントの削除
- 複数ゲスト アカウントの削除
- すべてのゲスト アカウントの削除

ゲスト アカウントの削除

「Default」プロファイルを除くすべてのゲスト プロファイルを削除できます。

ゲスト アカウントを削除するには、以下の手順に従います

1. ゲスト アカウントの**削除**アイコンを選択します。確認メッセージが表示されます。
2. 「OK」をクリックします。

複数ゲスト アカウントの削除

「Default」プロファイルを除くすべてのゲスト プロファイルを削除できます。

1 つまたは複数のゲスト アカウントを削除するには、以下の手順に従います

1. 「**ユーザ > ローカル ユーザ**」または「**ユーザ > ローカル グループ**」に移動します。
2. 削除するゲスト プロファイルのチェックボックスをオンにします。
3. 「**設定**」列にある**削除**アイコンを選択します。確認メッセージが表示されます。
4. 「OK」をクリックします。

すべてのゲスト アカウントの削除

「Default」プロファイルを除くすべてのゲスト プロファイルを削除できます。

すべてのゲスト アカウントを削除するには、以下の手順に従います

1. 「**ゲスト アカウント**」テーブルのヘッダーにあるチェックボックスをオンにします。(「Default」プロファイルを除く) すべてのチェックボックスがオンになります。「**ゲスト アカウントの削除**」が選択可能になります。
2. 「**ゲスト アカウントの削除**」を選択します。確認メッセージが表示されます。
3. 「OK」をクリックします。

ゲスト状況の管理

「**ゲスト状況**」ページには、現在ログインしているすべてのゲスト アカウントの現在の状況が表示されます。

トピック:

- ゲストのログアウト
- すべてのゲストのログアウト

ゲストのログアウト

1 つまたは複数のゲストをログアウトするには、以下の手順に従います

1. 「**ユーザ > ゲスト状況**」に移動します。
2. リストから、ログアウトするゲストを選択します。
3. 右端にある「**ログアウト**」アイコンを選択します。

すべてのゲストのログアウト

すべてのゲストをログアウトするには、以下の手順に従います

1. 「**ユーザ > ゲスト状況**」に移動します。
2. 右端にある「**すべてログアウト**」アイコンを選択します。

6

ローカル ユーザおよびグループの設定

トピック:

認証とパスワードについて

トピック:

二段階認証の使用

多くのユーザ ログイン認証はワンタイム パスワード (OTP) を必要とします。SonicOS/X は、以下の方法で認証を提供します。

- 電子メールでユーザに送信されるワンタイム パスワード (OTP)
- 認証アプリケーションを使用する時間ベースのワンタイム パスワード (TOTP) 認証。
  この機能を使用するには、、以下の手順に従います
  - ユーザは自分のモバイル デバイスに TOTP クライアント アプリ (Google Authentication、DUO、Microsoft Authentication など) をダウンロードする必要があります。
  - 「**ユーザ設定**」ページの「**ワンタイム パスワード方式**」リストから「**TOTP**」を選択する必要があります。

初回ログイン パスワードの変更の強制

SonicOS/X では、ローカル ユーザの作成または編集時に、初回ログイン前にユーザにパスワードの変更を強制できます。ユーザまたはグループに対してログイン パスワードの変更を指定できます。

ローカル ユーザの設 定

ローカル ユーザは、SonicWall ネットワーク セキュリティ装置のローカル データベースに格納され、管理されるユーザです。「**ユーザ > ローカル ユーザとグループ**」では、すべてのローカル ユーザの表示、新しいローカル ユーザの追加、既存ローカル ユーザの編集を行うことができます。LDAP サーバからユーザをインポートすることもできます。

チェックボックス	個々のローカル ユーザを選択するために使います。
展開/折りたたみアイコン	既定では、ローカル ユーザのユーザ名のみがリストされます。「展開」アイコンを選択すると、ローカル ユーザが属するグループが表示されます。
名前	ローカル ユーザのユーザ名を一覧表示します。展開すると、ローカル ユーザが属するグループの名前が一覧表示されます。
ゲスト サービス	ローカル ユーザでゲスト サービスが有効になっているかどうかを緑色のチェックマーク アイコンで示します。
管理	ローカル ユーザで使用可能な管理機能の種別が表示されます。
VPN アクセス	各ローカル ユーザおよびそのローカル ユーザが属する各グループに関する「**コメント**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル グループの VPN アクセスの状況が、そのグループの各メンバーの状況と共に表示されます。
コメント	各ローカル ユーザおよびそのローカル ユーザが属する各グループに関する「**コメント**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル ユーザ/グループの構成または編集時に入力したコメントが表示されます。
クォータ	各ローカル ユーザの「**統計**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル ユーザの使用クォータが表示されます。
構成	各ローカル ユーザの「**編集**」アイコンと「**削除**」アイコンが表示されます。アイコンが淡色表示か無効になっている場合、その機能はそのローカル ユーザまたはローカル グループでは使用できません。

認証と二段階パスワードの詳細については、「認証とパスワードについて」を参照してください。

トピック:

- すべてのユーザのクォータ制御
- ローカル ユーザの表示
- ローカル ユーザの追加
- ローカル ユーザの編集

すべてのユーザのクォータ制 御

ユーザのクォータ制御機能は、ユーザのアカウントに基づくクォータ制御を提供します。クォータは、セッション存続期間、または送受信トラフィック制限として指定できます。サイクル クォータでは、ユーザはアカウント クォータを使い切ると、次のサイクル（日、週、または月）が始まるまでインターネットにアクセスできなくなります。クォータ サイクルの設定が「**循環しない**」である場合、ユーザはクォータを使い切るとインターネットにアクセスできなくなります。

ローカル ユーザの表 示

「**ユーザ > ローカル ユーザとグループ**」では、ユーザが所属するすべてのグループを表示できます。ユーザの横の**展開**アイコンを選択すると、ユーザのグループ メンバーシップが表示されます。

ユーザ名の右側にある列には、ユーザの持つ権限が表示されます。展開表示では、ユーザが各権限を得ている元のグループが表示されます。

適宜、以下の操作を行います。

- 「**VPN アクセス**」列の**コメント** アイコンにマウス ポインタを重ねると、ユーザが VPN アクセス可能なネットワーク リソースが表示されます。
- 「**クォータ**」列の**統計**アイコンにマウス ポインタを重ねると、ユーザのクォータが表示されます。
- 展開表示で、ユーザの「**構成**」列にある**削除**アイコンをクリックして、グループからユーザを削除します。
  ⓘ | **補足:** グループから削除できないユーザのアイコンは、グレーアウトされています。
- ユーザの「**構成**」列にある**編集**アイコンを選択して、ユーザを編集します。詳細については、「ローカル ユーザの編集」を参照してください。
- ユーザの「**構成**」列にある**削除**アイコンをクリックして、その行のユーザまたはグループを削除します。
  ⓘ | **補足:** グループから削除できないローカル ユーザのアイコンは、グレーアウトされています。

「**ユーザ > ローカル ユーザおよびグループ**」ページの下部には、ローカル ユーザの総数が表示されます。

ローカル ユーザの追 加

ネットワーク セキュリティ装置の内部データベースにローカル ユーザを追加するには、「**ユーザ > ローカル ユーザとグループ**」ページを使用します。

ⓘ | **補足:** SSL VPN クライアントのユーザを作成するには、『*SonicOS/X 7 SSL VPN*』を参照してください。

トピック:

- ローカル ユーザ設定の構成
- ローカル ユーザ グループの設定
- ローカル ユーザの VPN アクセスの設定
- ローカル ユーザのユーザ クォータの設定

ローカル ユーザ設定の構成

ネットワーク セキュリティ装置の内部データベースにローカル ユーザを追加するには、「**ユーザ > ローカル ユーザとグループ**」ページを使用します。

ⓘ | **補足:** SSL VPN クライアントのユーザを作成するには、『*SonicOS/X 7 SSL VPN*』を参照してください。

データベースにローカル ユーザを追加するには、以下の手順に従います

1. 「**ユーザ > ローカル ユーザとグループ**」に移動します。
2. 「**ユーザの追加**」アイコンをクリックします。「**ユーザ設定**」ページが表示されます。
3. 以下の場合に、「**このユーザをドメイン ユーザにする**」を選択します。
   - 「このユーザをドメイン ユーザにする」が選択されている場合、このユーザ オブジェクトを使用して設定されるグループ メンバーシップ、アクセス権などが適用されるのは、名前付きのドメイン アカウント（RADIUS または LDAPにより認証済み）を使用してログインするユーザか、または SSO によりそのドメイン ユーザとして識別されるユーザです。これが選択されている場合、適用対象を特定のドメイン内で指定された名前を持つユーザ アカウントにするか、任意のドメイン内で指定された名前を持つユーザにするかを選択できます。
   - 「このユーザをドメイン ユーザにする」が選択されていない場合、これはローカル アカウントであり、そのユーザ オブジェクトを使用して設定されているすべてのものが、そのユーザ オブジェクトを使用してログインし、ローカルで認証されたユーザにのみ適用されます（この場合はパスワードがここで設定されている必要があります）。
4. 「**名前**」フィールドに、ユーザと関連付けられている名前を入力します。
5. 「**パスワード**」フィールドと「**パスワードの確認**」フィールドに、ユーザに割り当てられたパスワードを入力します。
6. 初回ログイン時にユーザにパスワードの変更を求める必要がある場合は、「**ユーザにパスワードの変更を強制する**」を選択します。このオプションは、既定では選択されていません。
7. 「**ワンタイム パスワード方式**」リストから、SSL VPN ユーザに二段階認証用のシステム生成パスワードを送信するよう要求する方式を選択します。

   ⓘ | **ヒント:** ローカル ユーザがワンタイム パスワードを有効にしていないのに、そのユーザが所属するグループで有効にしている場合には、そのユーザの電子メール アドレスが構成されていることを確認してください。電子メール アドレスが構成されていない場合、このユーザはログインできません。

   ⓘ | **ヒント:** このユーザに対する別のパスワード変更要求を回避するために、このオプションは最初のログインにのみ適用されます。

   - **無効**（既定）－「**ユーザにパスワードの変更を強制する**」を選択した場合、これを変更するためのダイアログが最初のログイン試行時に表示されます。
   - **電子メールでのワンタイム パスワード** － ユーザは、自分のユーザ名と最初のパスワードを入力した後に、電子メールで一時パスワードを受け取ります。パスワードを含む電子メールを受信したら、2 番目のパスワードを入力してログイン プロセスを完了できます。
   - **TOTP** － ユーザは自分のユーザ名と最初のパスワードを入力すると電子メールで一時パスワードを受け取りますが、この機能を使用するには、ユーザは自分のモバイル デバイスに TOTP クライアントアプリ（Google Authentication、DUO、Microsoft Authentication など）をダウンロードする必要があります。

     バインド解除 TOTP キーが表示されます。
8. ユーザがワンタイム パスワードを受信できるように、ユーザの電子メール アドレスを「**電子メール アドレス**」フィールドに入力します。

9. 必要に応じて、「**コメント**」フィールドに任意のコメントを入力します。
10. 「**保存**」をクリックします。

ローカル ユーザ グループの設定

ユーザをグループに追加するには、以下の手順に従います

1. 「**ユーザ > ローカル ユーザ**」ページに移動します。
2. 「**ユーザの追加**」を選択します。
3. 「**利用可能なユーザ グループ**」リストから、このユーザを含めるグループを選択します。
4. **追加**（右矢印）アイコンを選択して、ユーザを「**選択されたユーザ グループ**」リストに追加します。
   リソースを「**選択されたユーザ グループ**」リストから削除するには、グループを選択し、**削除**（左矢印）アイコンを選択します。すべてのグループからユーザを削除するには、**すべて削除**（二重左矢印）アイコンを選択します。

ローカル ユーザの VPN アクセスの設定

ローカル ユーザの VPN アクセスを構成するには、以下の手順に従います

1. 「**ユーザ > ローカル ユーザ**」ページに移動します。
2. 「**ユーザの追加**」を選択します。
3. 「**利用可能なネットワーク**」リストから、このユーザに既定で VPN アクセスを許可するネットワーク リソースを選択します。

   ⓘ **補足:** GroupVPN アクセス設定は、リモート クライアントおよび SSL VPN 仮想オフィスブックマークに影響します。
4. **追加**（右矢印）アイコンを選択して、リソースを「**選択されたネットワーク**」リストに追加します。
   リソースを「**選択されたネットワーク**」リストから削除するには、リソースを選択し、**削除**（左矢印）アイコンを選択します。すべてのリソースを削除するには、**すべて削除**（二重左矢印）アイコンを選択します。

ローカル ユーザのユーザ クォータの設定

ユーザのクォータを構成するには、以下の手順に従います

1. 「**ユーザ > ローカル ユーザとグループ**」に移動します。
2. 「**ユーザ クォータ**」タブをクリックします。
3. 「**クォータ サイクル種別設定**」リストから、以下を選択します。
   - **循環しない**（既定）
   - **日**
   - **週**
   - **月**
4. 「**セッション存続期間**」リストから、ゲスト ログイン セッションがアクティブになった後、アクティブであり続ける期間を指定します。既定では、アクティブ化はゲスト ユーザが最初にアカウントにログインするときに行われます。

5. 「セッション存続期間」リストから、期間の種別を選択します。
    - 分
    - 時
    - 日
6. 「**分/時/日**」フィールドに、期間を指定します。1 ～ 9999 の値を入力できます。
7. 「**受信制限**」フィールドに、ユーザが受信できるデータ量を MB 単位で入力します。範囲は 0（データを一切受信できない）～ 999999999 MB および「無制限」（既定）です。
8. 「**送信制限**」フィールドに、ユーザが送信できるデータ量を MB 単位で入力します。範囲は 0（データを一切送信できない）～ 999999999 MB および「無制限」（既定）です。
9. 「**保存**」をクリックします。

トピック:

- すべてのユーザのクォータ制御

ローカル ユーザの編 集

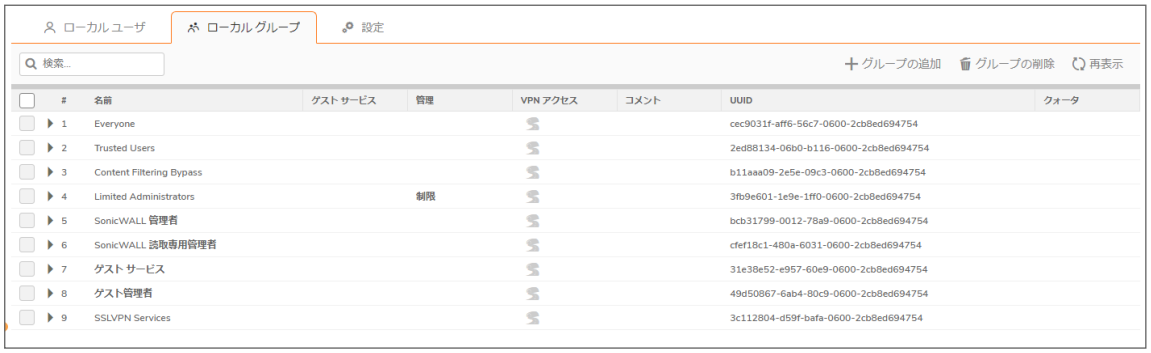
「**ユーザ > ローカル ユーザとグループ**」ページで、ローカル ユーザを編集できます。

ローカル ユーザを編集するには、以下の手順に従います

1. 「**ローカル ユーザ**」テーブルで、「**構成**」の下にあるユーザの**編集**アイコンをクリックします。「**ユーザ設定**」ページが表示されます。
2. 新しいユーザを追加する場合と同様に、「**設定**」、「**グループ**」、「**VPN アクセス**」、「**ブックマーク**」、「**ユーザ クォータ**」の各オプションを構成します。詳細については、「ローカル ユーザの追加」を参照してください。

ローカル グループの設 定

ローカル グループは、「**ローカル グループ**」テーブルに表示されます。ローカル グループの中には、変更可能でも削除できない既定のグループがあります。



チェックボックス	個々のローカル グループを選択するために使います。既定のローカル グループは変更できないので、対応するチェックボックスが淡色表示になっています。
展開/折りたたみアイコン	既定では、ローカル グループの名前だけが一覧表示されています 次のオプションがあります。

	• 「**展開**」アイコンを選択すると、リストが展開されてグループのすべてのメンバーが表示されます。メンバーを持たないローカル グループでは、そのグループの一覧の下に「メンバーなし」と表示されます。 • 「**折りたたみ**」アイコンを選択すると、ローカル グループのメンバーが隠されます。
名前	既定のローカル グループおよび構成されたローカル グループが名前順に一覧表示されます。 「**システム > 管理**」ページの「**複数の管理役割**」オプションが有効な場合、「**ユーザ > ローカル グループ**」ページには役割ベースの以下の既定の管理者グループが一覧表示されます。 • システム管理者 • 暗号化管理者 • 監査管理者
コンテンツ フィルタのバイパス	ローカル グループのコンテンツ フィルタをバイパスしているかどうかを緑色のチェックマーク アイコンで示します。このアイコンにマウス カーソルを合わせると、ツールチップが表示されます。 リモート ユーザの場合は、「**コメント**」アイコンに「リモート認証には適用されません」と表示されます。
ゲスト サービス	ローカル グループでゲスト サービスが有効になっているかどうかを緑色のチェックマーク アイコンで示します。このアイコンにマウス カーソルを合わせると、ツールチップが表示されます。 リモート ユーザの場合は、「**コメント**」アイコンに「リモート認証には適用されません」と表示されます。
管理	ローカル グループで使用可能な管理機能の種別が表示されます。このアイコンにマウス カーソルを合わせると、一覧表示された機能についてのツールチップが表示されます。 リモート ユーザの場合は、「**コメント**」アイコンに「リモート認証には適用されません」と表示されます。
VPN アクセス	各グループおよびそのグループの各メンバーに関する「**コメント**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル グループの VPN アクセスの状況が、そのグループの各メンバーの状況と共に表示されます。
コメント	ローカル グループのコメントが一覧表示されます。
UUID	接続されているデバイスの UUID が一覧表示されます。
クォータ	そのグループに割り当てられている使用クォータが表示されます。
構成	個々のローカル グループとグループ メンバーごとに「**編集**」アイコンと「**削除**」アイコンが表示されます。また、グループ メンバー全体の「**削除**」アイコンも表示されます。淡色表示のアイコンは、その機能がローカル グループまたはグループ メンバーで使用できないことを意味します。

トピック:

- 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 グループの追加

トピック:

- ローカル グループ設定の構成
- ローカル グループ設定の構成 – メンバー
- ローカル グループ設定の構成 – VPN アクセス
- ローカル グループ設定の構成 – 管理

ローカル グループ設定の構成

グループを追加または編集するには、以下の手順に従います

1. 「**ユーザ > ローカル グループ**」ページに移動します。
2. 「**グループの追加**」をクリックします。
3. 「**名前**」フィールドに、新しいローカル グループの名前を入力します。
4. 定義済みのユーザまたはグループの名前を編集することはできません。このフィールドはグレーアウトされています。
5. 「**ドメイン**」フィールドに、ドメイン名を入力します。ドロップダウン メニューからドメインを選択できます。リストにないドメイン名を入力する場合は、完全なドメイン名を入力する必要があります。そうしないと、エラー メッセージが表示されます。
6. 必要に応じて、「**コメント**」フィールドにローカル グループについてのコメントを入力します。
7. 必要に応じて、「ユーザのメンバーシップを LDAP ディレクトリのユーザの位置によって決定する」チェックボックスをオンにします。この設定が有効な場合、ログインしたユーザまたは SSO 経由で認証されたユーザには、LDAP サーバ上の対応するユーザ オブジェクトが「LDAP 位置」で指定した位置（または、その配下）にあれば、そのセッションの間、当該ユーザ グループへのメンバーシップが与えられます。この設定はデフォルトで無効になっています。

   ⓘ **ヒント:** 「メンバー」表示で、ローカル ユーザや他のグループを、このグループのメンバーにすることもできます。

   この設定を有効にすると、「**LDAP 位置**」フィールドがアクティブになります。

   a. 「**LDAP 位置**」フィールドに、LDAP ディレクトリ ツリー内の位置を入力します。位置の指定にはパス（domain.com/users など）または LDAP 識別名を使用できます。

      ⓘ **補足:** 「LDAP ユーザ グループ ミラーリング」を有効にした場合、ミラー ユーザ グループのこのフィールドは読み取り専用になり、ミラー元グループのLDAP ディレクトリ内の位置を示します。

   b. どちらかの「**ユーザの位置**」オプションに基づき、位置を選択します。

      - **指定された位置またはその配下**（既定値）
      - **指定された位置**

8. 必要に応じて、そのグループでワンタイム パスワードを要求するために、「**ワンタイム パスワード**」を選択します。この設定を有効にした場合は、ユーザの電子メール アドレスを設定する必要があります。
9. 「**更新**」を選択します。

ローカル グループ設定の構成 - メンバー

ローカル グループのメンバーを構成するには、以下の手順に従います

1. 「**ユーザ > ローカル グループ**」ページに移動します。
2. 「**グループの追加**」をクリックします。
3. 「**メンバー**」タブを選択します。
4. 「**利用可能なユーザ グループ**」リストで、このグループに所属するメンバーまたはグループを選択し、**追加**（右矢印）アイコンを選択します。

   すべてのユーザとグループを追加するには、**すべて追加**（二重右矢印）アイコンを選択します。

   ⓘ **補足:** 任意のグループを「Everyone」、「All LDAP Users」以外の他のグループのメンバーとして追加できます。グループを他のグループに追加する場合は、メンバーシップに注意してください。

   ユーザやグループを「**選択されたユーザ グループ**」リストから削除するには、ユーザやグループを選択し、**削除**（左矢印）アイコンを選択します。すべてのユーザとグループを削除するには、**すべて削除**（二重左矢印）アイコンを選択します。
5. 「**保存**」をクリックします。

ローカル グループ設定の構成 - VPN アクセス

ローカル グループの VPN アクセスを構成するには、以下の手順に従います

1. 「**ユーザ > ローカル グループ**」ページに移動します。
2. 「**グループの追加**」をクリックします。
3. 「**利用可能なネットワーク**」リストから、このグループに既定で VPN アクセスを許可するネットワーク リソースを選択します。

   ⓘ **補足:** GroupVPN アクセス設定は、リモート クライアントおよび SSL VPN 仮想オフィスブックマークに影響します。
4. **追加**（右矢印）アイコンを選択して、リソースを「**選択されたネットワーク**」リストに追加します。

   リソースを「**選択されたネットワーク**」リストから削除するには、リソースを選択し、**削除**（左矢印）アイコンを選択します。すべてのリソースを削除するには、**すべて削除**（二重左矢印）アイコンを選択します。

ローカル グループ設定の構成 - 管理

ローカル グループの管理を構成するには、以下の手順に従います

1. 「**ユーザ > ローカル グループ**」ページに移動します。
2. 「**グループの追加**」をクリックします。
3. 「**管理**」タブを選択します。
4. 別の管理グループへのメンバーシップを与えて新しいグループを管理グループにする場合は、「**メンバーはウェブ ログインで管理 UI に直にアクセスする**」を選択します。このオプションは、既定では選択されていません。
5. 「**このグループが読み取り専用管理者権限を付与し、別の管理グループのメンバーに使用される場合**」オプションは、読み取り専用管理者権限を付与するユーザ グループ（つまり、SonicWall Read-Only Admins グループまたはそのメンバーシップを持つグループ）のメンバーシップを取得したユーザがさらに別の管理ユーザ グループのメンバーシップを取得した場合の処理方法を制御します。ユーザに次の権限を与える

には、、以下の手順に従います:

- 読み取り専用の制限なしで他の管理グループによって設定された管理者権限を付与する場合は、「他のグループの管理者権限がこれに優先する（読み取り専用の制限はなくなる）」を選択します。このオプションを使うと、ユーザの既定のグループを読み取り専用管理グループとしておき、その中の特定のユーザだけを他の管理グループのメンバーにして読み取り専用の権限をオーバーライドすれば、それらのユーザが設定を行えるようになります。このオプションは、既定では選択されています。「ローカル ユーザ」テーブルのユーザの「管理」列に、他のグループを識別する指示語（制限、"完全" など）が表示されます。
- 他のグループによって設定された管理者権限レベルをメンバー ユーザに付与し、アクセスを読み取り専用に制限する場合は、「他のグループの管理者権限が読み取り専用に制限される」を選択します。「ローカル ユーザ」テーブルのユーザの「管理」列に、2 つの他のグループを識別する指示語（"読み取り専用の制限された" など）が表示されます。

ⓘ **ヒント:** 両方を混在させるには、SonicWall Read-Only Admins で最初のオプションを選択し、そのメンバーとなる別のグループを作成して 2 番目のオプションを選択します（逆ではうまくいきません）。

ⓘ **補足:** 読み取り専用管理グループのメンバーで、かつ他の管理グループに所属していないユーザには、読み取り専用に制限された（SonicWall Administrators の）完全なアクセス権が付与されます。

6. 「**保存**」をクリックします。

ローカル グループの編集

ローカル グループを編集するには、以下の手順を実行します

1. 「**ユーザ > ローカル グループ**」に移動します。
2. 編集するグループの「**設定**」列にある「**ユーザ グループの編集**」アイコンを選択します。「**ローカル グループ設定**」ダイアログが表示されます。
3. 「ローカル グループの追加」の手順を実行します。

7

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、次の URL を開きます:
https://www.sonicwall.com/ja-jp/support

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。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com 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 サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、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。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS および SonicOSX ユーザ 管理者ガイド – – NSa および NSsp シリーズ
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005633-30 Rev B

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、「SonicWall Inc.」を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035