SOPHOS

Cybersecurity made simple.

ユーザー ポータル ヘルプ

目次

(2019/04/15)

1 はじめに

名前、ログイン情報、メールアドレス、ユーザーグループメンバーシップなどユーザーの個人情報は、ユーザーの登録時に管理者が設定します。ユーザーグループでは、グループのメンバーに、サーフィン量、アクセス時間量、ネットワークトラフィック量を定義するポリシーセットを適用します。サーフィン量ポリシーは、ユーザーアカウントの有効期日を定義し、アクセス時間ポリシーは、インターネットを使用できる合計時間数を定義します。データトランスファーポリシーは、アップロードおよびダウンロードするデータトランスファーの上限を定義します。

管理者もユーザーも上記のユーザー情報を閲覧できます。管理者がユーザーの詳細を表示するには、デバイスで**「認証」 > 「ユーザー」**の順にアクセスします。ユーザーが詳細を表示するには**「ユーザーポータル」**にアクセスします。

ユーザポータルのアクセス

https://<ソフォスデバイスの IP アドレス> を閲覧するか、「キャプティブポータル」ページで「ユーザーポータルはこちらをクリック」をクリックすると、ユーザーポータルにアクセスできます。ポータルには、ユーザーのログイン情報でログオンします。

注
認証サービスを使用する必要のある外部ユーザーは、ユーザーポータルへのアクセスを取得する前に、キャプティブポータルにログインする必要があります。外部ユーザーは、https://<ソフォスデバイスの IP アドレス>:8090 からキャプティブポータルにアクセスできます。ログインすると、外部ユーザーがユーザーポータルにアクセスできるようになります。

2 個人設定

2.1 パスワードの変更

「**パスワード変更**」ページで、パスワードを変更することができます。

Device Administrator はユーザーが登録する時に、名前、ログイン情報、メールアドレスなどの個人情報を設定します。この情報の一部を変更することができます。

1. **「個人」「パスワードの変更」**の順にアクセスします。
2. このページには以下の情報があります：

ユーザー名

ユーザーがユーザーポータルのアクセスに使用する名前を表示します。

現在のパスワード

現在のパスワードを入力します。

新しいパスワード

新しいパスワードを入力します。再度パスワードを入力して確認してください。

3. **「保存」**をクリックします。

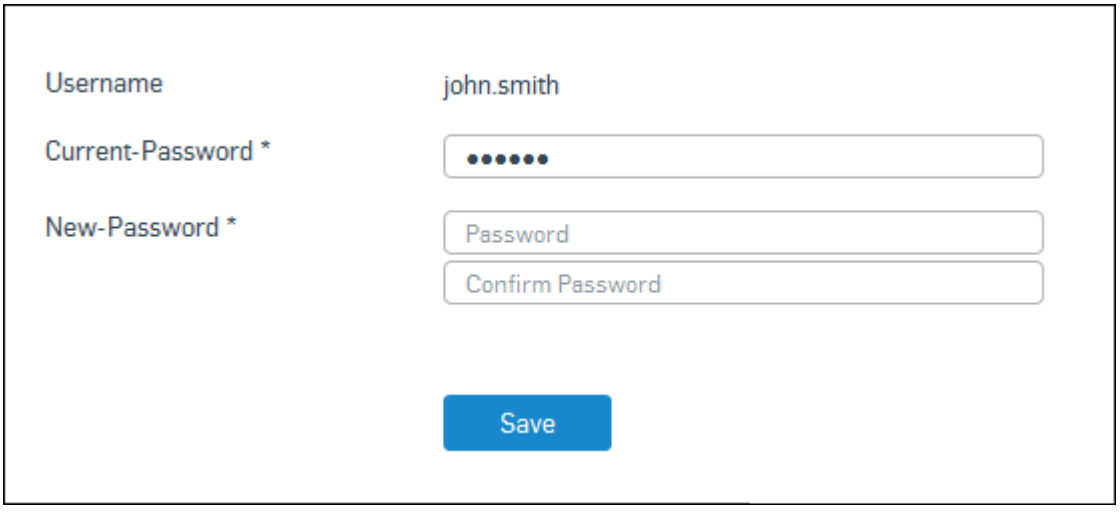

図 1：パスワードの変更

2.2 個人情報

「**個人情報**」ページでは、デバイスに保存されている個人情報を更新できます。

Device Administrator はユーザーが登録する時に、名前、ログイン情報、メールアドレスなどの個人情報を設定します。この情報の一部を変更することができます。

1. **「個人」「個人情報」**の順にアクセスします。
2. このページには以下の情報があります：

ユーザー名

ユーザーポータルにアクセスするときの名前が表示されます。

名前

ユーザーの名前を入力します。

メール

管理者が設定したメールアドレスが表示されます。

3. **「保存」**をクリックします。

図 2：個人情報

3 クライアントのダウンロード

「**ダウンロードクライアント**」ページには、必要クライアントをすべてダウンロードできるリンクが含まれています。

デバイスにはユーザー認証の様々なオプションが含まれています。ユーザーにネットワークリソースへのアクセスが提供される前に、ユーザー全員が認証されます。ユーザー認証は、ローカルデータベース、Active Directory、LDAP、RADIUS、TACACS、eDirectory、NTLM またはこれらの組み合わせを使用して実行できます。デバイスは Windows の認証情報を使用して認証可能な Transparent Authentication の SSO (Single Sign On) もサポートしているため、ユーザーは 1 回ログインすればネットワークリソースにアクセスすることができます。SSO は Active Directory および Citrix またはターミナルサービス環境で使用できます。

キャプティブポータル、Windows、Linux、Macintosh、Android、iOS プラットフォーム用の認証クライアントまたは SSO (Single Sign On) を使用してデバイスを認証できます。

このページから次のクライアントをダウンロードすることができます。

シングルサインオン

管理者のみがご利用いただけます。

Sophos Single Sign-On Client - ユーザーは組織のネットワークとデバイスに同時にログオンできます。ユーザーのマシン上でクライアントをインストールする必要があります。

Sophos Transparent Authentication Suite - Windows の認証情報を使用して認証可能な Transparent Authentication を可能にします。ユーザーは 1 回ログインすればネットワークリソースにアクセスすることができます。ユーザーのマシン上でクライアントをインストールする必要はありません。

Sophos Authentication for Thin Client - ネットワーク認証情報を使用して認証可能な Transparent Authentication を、Citrix またはターミナルサービス環境を利用するユーザーが使えるようにします。ユーザーは 1 回ログインすればネットワークリソースにアクセスすることができます。ユーザーのマシン上でクライアントをインストールする必要はありません。

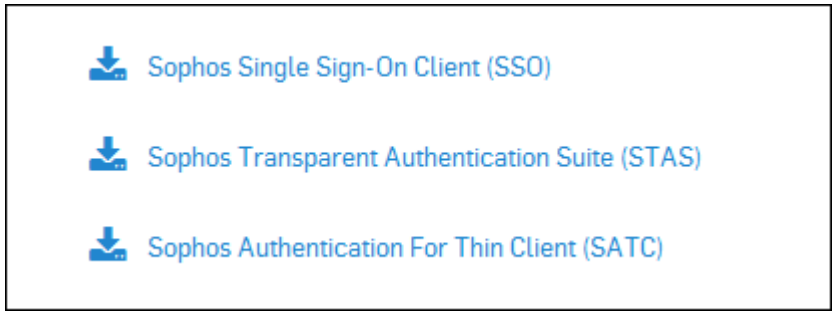

図 3：シングルサインオン

認証クライアント

ユーザー全員がご利用いただけます。

Windows 向けのダウンロード - Windows OS を使用しているユーザーが、デバイスにログオンし、デバイス内に設定されているポリシーに従って、ネットワークリソースとインターネットにアクセスできるようになります。

MAC OS X 向けのダウンロード - Macintosh OS X 以降のシステムを使用しているユーザーが、デバイスにログオンし、デバイス内に設定されているポリシーに従って、ネットワークリソースとインターネットにアクセスできるようになります。

Linux 32 向けのダウンロード - 32 ビットの Linux オペレーティングを使用しているユーザーが、デバイスにログオンし、デバイス内に設定されているポリシーに従って、ネットワークリソースとインターネットにアクセスできるようになります。

Linux 64 向けのダウンロード - 64 ビットの Linux オペレーティングを使用しているユーザーが、デバイスにログオンし、デバイス内に設定されているポリシーに従って、ネットワークリソースとインターネットにアクセスできるようになります。

iOS/Android クライアントの CA のダウンロード - デバイスとの安全な接続を構築するために、iOS または Android システムにインストールする電子証明書をダウンロードできます。

注
iOS/Android 向けの認証クライアントは、それぞれ App Store/Play ストアからダウンロードできます。Android の Google Chrome では、クライアントはダウンロードできません。ユーザーは別のブラウザを使用するか、Admin が Google Chrome の信頼できる機関として提供するデフォルトの認証局 (CA) をインストールしなければなりません。あるいは、ユーザーはダウンロードリンクを長押しして、オプション「リンクを保存」を選択します。

図 4：認証クライアント

Apple iOS 向け CISCO™ VPN クライアントの設定

Cisco VPN クライアントが有効にされており、ログインしたユーザーに許可されている場合にのみ利用可能です。

CISCO™ VPN クライアントは CISCO が開発したソフトウェアで、リモートワーカーのためのセキュリティの高いリモート接続として、暗号化された VPN トンネルを確立します。「**インストール**」をクリックして、Cisco VPN クライアント用の SF 関連設定をご使用の iOS デバイスにインストールします。クライアントがと SF デバイスと通信できるように、この設定をクライアントにインポートします。

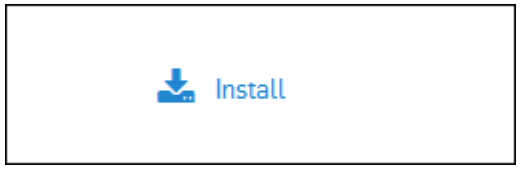

図 5：Apple iOS 向け Cisco VPN クライアントの設定

SPX アドイン

この機能は、メールプロテクションの有効な登録がある場合にのみご利用いただけます。

この機能は、Sophos Firewall モデル XG105 以上、Cyberoam モデル CR25iNG 以上およびすべての Sophos UTM モデルでご利用になれます。

「Sophos Outlook Add-in のダウンロード」をクリックし、SPX アドインをダウンロード、インストールします。SPX アドインを使うと、社外に送信する機密情報を含むメッセージを簡単に暗号化することができます。このアドインは、ユーザーの Microsoft Outlook ソフトウェアとシームレスに統合されるため、ユーザーは Sophos Firewall (SF) メールプロテクションからメッセージを暗号化しやすくなります。

Outlook でアドインをインストールするには、次のステップを行ってください。

1. ファイルを一時フォルダに解凍します。
2. インタラクティブインストールの場合、setup.exe を実行します (ユーザーは入力するように指示されます)。
3. 自動インストールの前提条件：
   - Windows XP、Windows Vista、Windows 7、Windows 8 (32 ビットおよび 64 ビットの両方) のバージョンをサポートしています。
   - Microsoft Outlook 2007 SP3、2010 または 2013 (32 ビットおよび 64 ビットの両方) のバージョンをサポートしています。
   - Microsoft .NET Framework 4 Client Profile
   - Microsoft Visual Studio 2010 Tools for Office Runtime 4.0
4. それでは、インストーラを次のパラメータで実行してください: msiexec /qr /i SophosOutlookAddInSetupUTM.msi T=1 EC=3 C=1 I=1

図 6：SPX アドイン

4 SSL VPN

「SSL VPN」メニューは、リモートアクセスクライアントソフトウェアと構成ファイルをダウンロードし、クライアントレスアクセス経由で接続するため、Web を安全に閲覧することができます。

注

SSL VPNタブは、管理者があなたに SSL VPN を少なくとも一つ割り当てて初めて使用可能になります。

管理者が有効にした接続の種類に対応するリモートアクセスのオプションのみが表示されます。たとえば、SSL VPN リモートアクセスの使用を有効にした場合、**「SSL VPN クライアント」**セクションが表示されます。

各接続タイプは、別々のセクションに表示されます。接続タイプによって、それぞれのソフトウェアをダウンロードするための情報および/またはボタンが有効になります。

関連概念

セキュリティ保護された Web 閲覧 (p. 7)
「セキュリティ保護された Web 閲覧」メニューは、SSL VPN クライアントレスユーザーに SSL 経由で任意の URL にアクセスすることを許可します。

クライアントレスアクセスの接続 (p. 8)
「クライアントアクセスの接続」メニューはブラウザのみをクライアントとして使用し、ユーザーは事前構成した接続の種類を経由して、外部ソースから内部リソースにアクセスできます。

SSL VPN クライアント (p. 8)
「SSL VPN クライアント」メニューでは、SSL VPN クライアントソフトウェアや、管理者が選択した SFOS の設定に基づいて自動生成された設定ファイルをダウンロードすることができます。

4.1 セキュリティ保護された Web 閲覧

「セキュリティ保護された Web 閲覧」メニューは、SSL VPN クライアントレスユーザーに SSL 経由で任意の URL にアクセスすることを許可します。

管理者がクライアントレスポリシーに、このような URL のブックマークを作成する必要はありません。この機能は、SFOS の管理者がクライアントレスアクセスポリシーで**設定 > 「VPN」 > 「クライアントレスアクセス」**の順にアクセスし、**「Web アプリケーションの制限」**オプションを使用してアクティブ化/非アクティブ化することができます。

安全なウェブブラウジングを利用するには、完全で有効な URL（例、http://www.google.com）を入力して、[**Go**]をクリックします。

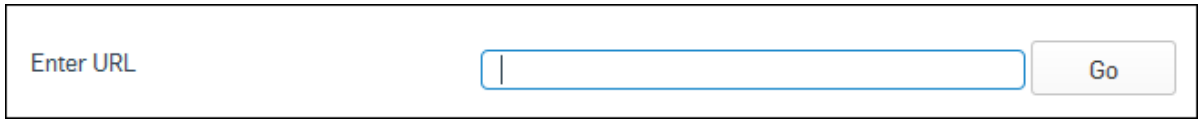

図 7：セキュリティ保護された Web 閲覧

関連概念

SSL VPN (p. 7)

「SSL VPN」メニューは、リモートアクセスクライアントソフトウェアと構成ファイルをダウンロードし、クライアントレスアクセス経由で接続するため、Web を安全に閲覧することができます。

4.2 SSL VPN クライアント

「SSL VPN クライアント」メニューでは、SSL VPN クライアントソフトウェアや、管理者が選択した SFOS の設定に基づいて自動生成された設定ファイルをダウンロードすることができます。

以下がダウンロード可能:

- Windows 用のクライアントと設定
- Windows 用の設定
- その他の OS 用の設定
- Android/iOS 用の設定

ソフトウェアパッケージをリモートクライアントにインストールすると、SSL VPN 接続をオープンできます。

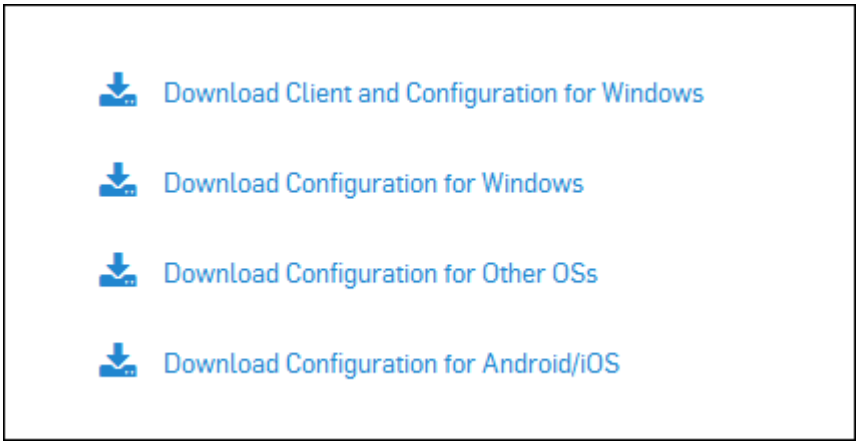

図 8：クライアント

関連概念

SSL VPN (p. 7)
「SSL VPN」メニューは、リモートアクセスクライアントソフトウェアと構成ファイルをダウンロードし、クライアントレスアクセス経由で接続するため、Web を安全に閲覧することができます。

4.3 クライアントレスアクセスの接続

「クライアントアクセスの接続」メニューはブラウザのみをクライアントとして使用し、ユーザーは事前構成した接続の種類を経由して、外部ソースから内部リソースにアクセスできます。

注
クライアントレスアクセス接続セクションは、管理者があなたに VPN 接続を作成し、許可するユーザーに追加して、はじめて利用可能になります。

クライアントレスアクセス接続セクションには、許可された接続がリストされます。アイコンは接続のタイプを表しています。

接続を使用するには、それぞれの接続ボタンを押してください。新しいブラウザウィンドウが開きます。接続に合わせたコンテンツとレイアウト。例えば、HTTP や HTTPS を開くとウェブサイトが含まれています。管理者が選択した設定によって、自分でログインする必要がある場合と、自動的にログインする場合があります。

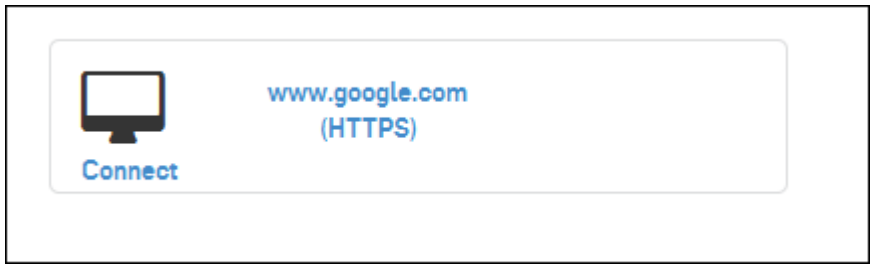

図 9：クライアントレスアクセスの接続

関連概念

SSL VPN (p. 7)

「SSL VPN」メニューは、リモートアクセスクライアントソフトウェアと構成ファイルをダウンロードし、クライアントレスアクセス経由で接続するため、Web を安全に閲覧することができます。

5 インターネットの使用状況

このページではユーザーのインターネットの使用状況全体を表示します。

「**Iインターネットの使用状況**」は、インターネットサーフィンに必要な情報を表示します。

このページには次の詳細が表示されます。

- ユーザーグループ、1時間あたりの可能サーフィン合計時間、サーフィン定量使用期限、データ転送周期の更新日、インターネット合計使用時間、ゲストユーザーアカウント使用期限（ゲストユーザーとして登録している場合）などのポリシー情報。

図 10：ポリシー情報

- データ転送の割り当て量、使用した量、残りの量（アップロードとダウンロード）などの使用情報。

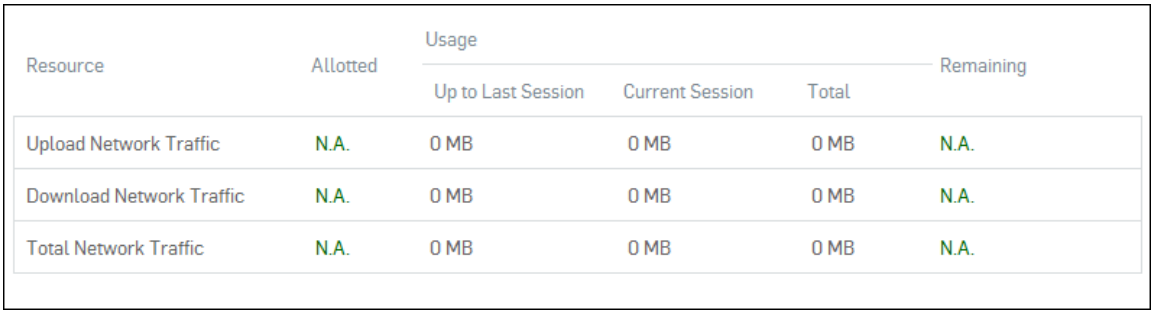

図 11：使用情報

- 月次使用 - サーフィン時間とデータ転送詳細

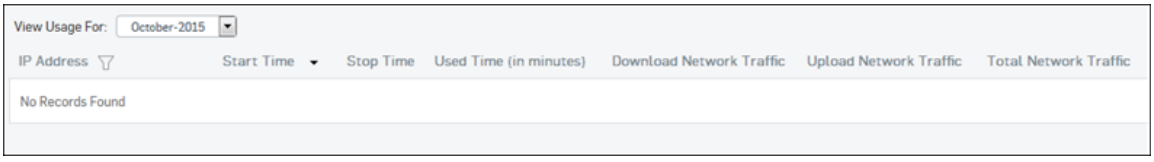

図 12：月次使用

上記の情報は、ユーザータイプにと設定されたポリシーよって、すべてが表示されるわけではありません。

6 隔離

「SMTP 隔離」には、隔離されているメールの完全リストが表示されます。これらのメールに対して、以下の操作を行うことができます。

- 期間、送信者、件名に基づいて並べ替える
- 表示されているオプションに基づいて、絞り込んで表示する
- リリースする
- 削除する

スパムとして隔離されたメールのリリース

隔離されたスパムのみをリリースすることができます。以下のいずれかの操作を行えます。

- メールの**「リリース」**をクリックします。
- メールを選択し、**「リリース」**を選択して、**「Go」**をクリックします。
- メールで届いた 隔離ダイジェストメール からリリースします。

注
マルウェアに感染したメールは、リリースしたり、ダウンロードすることはできません。

ファイアウォールはリリースされたメールをスキャンしてから、受信箱に配信します。

7 例外

「例外」では、送信者のメールアドレスを指定し、そのアドレスからのメールを許可またはブロックすることができます。

このページには次の詳細が表示されます。

- **許可されているメールアドレス**

  有効なメールアドレス (abc@example.com) またはワイルドカードとドメイン (*@example.com) を入力します。これらのアドレスからのメールは、スパムとマークされたり、隔離されたりすることがなくなります。この操作は、組織内の受信者全員に適用されます。

- **ブロックされているメールアドレス**

  有効なメールアドレス (abc@example.com) またはワイルドカードとドメイン (*@example.com) を入力します。これらのアドレスからのメールは、組織内のすべての受信者に対してブロックされます。

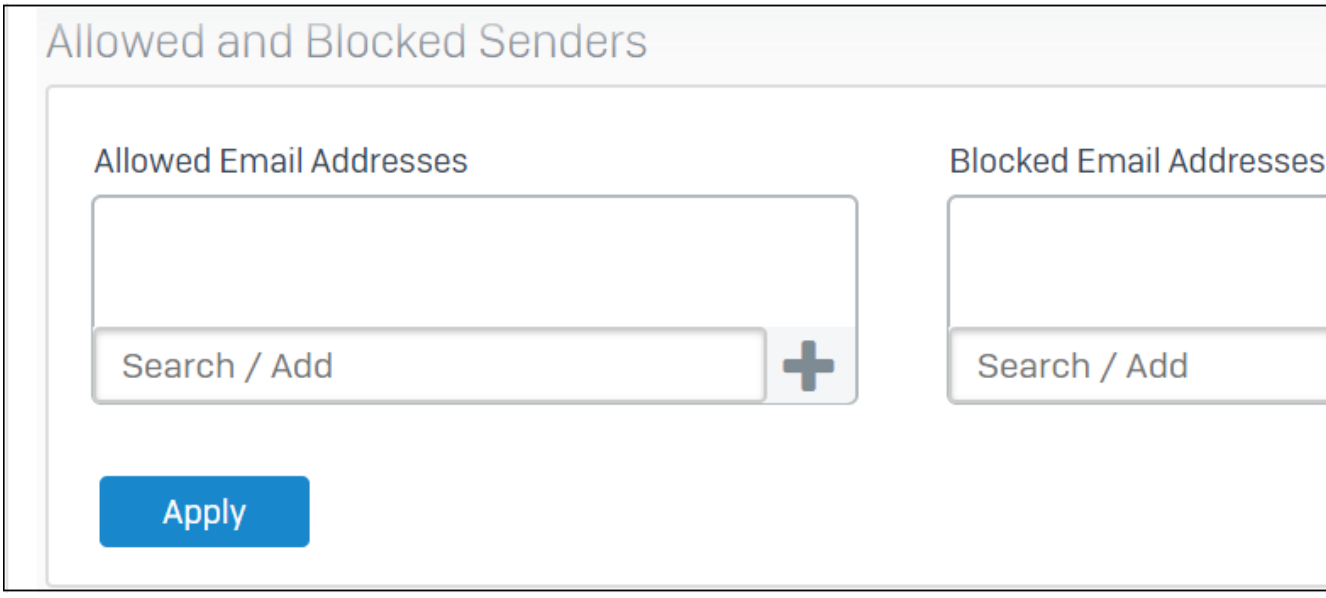

図 13：例外

8 ホットスポット

「ホットスポット」メニューでは、カフェ、ホテル、会社などの公共スペースで、時間制限およびトラフィック制限付きのインターネットアクセスをゲストに提供します。

「ホットスポット」タブは、管理者が**「当日有効パスワード」**または**「バウチャー」**タイプのホットスポットを作成した場合のみ表示されます。

このタブでは、ワイヤレスネットワークのゲストにホットスポットアクセス情報を提供できます。選択したホットスポットのタイプによって、汎用パスワードまたはバウチャーを生成して提供することができます。

関連タスク

当日有効ホットスポットタイプのパスワード (p. 14)
ホットスポットタイプのバウチャー (p. 15)
このページでは、固有のコードを含むバウチャーを作成する方法を説明します。バウチャーはプリントしてゲストに渡すことができます。作成したバウチャーのリストには、各バウチャーの利用法の概要が表示されており、管理するのに役立ちます。

8.1 当日有効ホットスポットタイプのパスワード

このページでは、ホットスポットの当日有効パスワードを作成する方法を説明します。

「パスワード」フィールドに、現在のパスワードが表示されます。これは1日に1度自動的に変わります。ただし、パスワードは手動で変更することができます。前のパスワードは直ちに無効になり、アクティブセッションは終了します。新しいパスワードは要求に応じて生成できます。

1. **「ホットスポット」**にアクセスします。
2. 「**ホットスポット**」ドロップダウンメニューから要求したホットスポットを選択します。
3. **「パスワード」**フィールドにパスワードを入力して、**「生成」**をクリックします。

   注
   生成済みのデフォルトのパスワードを使用することもできます。

4. 「**メール送信**」スイッチのアクティブ化／非アクティブ化。

   注
   パスワードが管理者の指定したメール受信者へ送信されます。管理者がメールアドレスを指定していない場合、チェックボックスは利用できません。

5. 「**保存**」を指定して、新しく生成されたパスワードを保存します。

パスワードは直ちに変更されます。

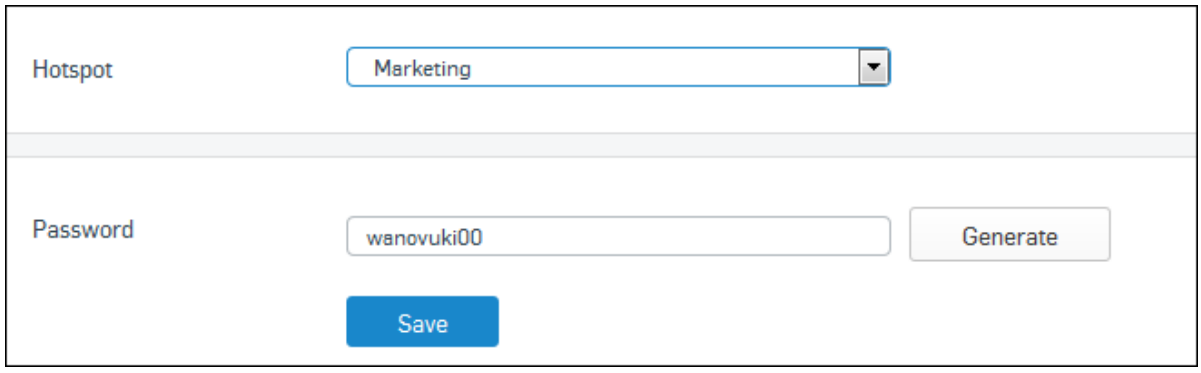

図 14：当日有効パスワード

関連概念

ホットスポット (p. 14)

「ホットスポット」メニューでは、カフェ、ホテル、会社などの公共スペースで、時間制限およびトラフィック制限付きのインターネットアクセスをゲストに提供します。

8.2 ホットスポットタイプのバウチャー

このページでは、固有のコードを含むバウチャーを作成する方法を説明します。バウチャーはプリントしてゲストに渡すことができます。作成したバウチャーのリストには、各バウチャーの利用法の概要が表示されており、管理するのに役立ちます。

このページでは、バウチャーを作成し、管理する方法について説明します。

1. **「ホットスポット」**にアクセスします。
2. 次の設定を指定します。

ホットスポット

バウチャーを作成したいホットスポットを選択します。

ホットスポットバウチャー定義

要求したバウチャー定義を選択します。

> **注**
> 有効なバウチャータイプは管理者が定義します。どのタイプを何の目的で使うかは会社が定義します。

件数:

このタイプのバウチャーの作成件数を入力します。

説明

バウチャーの説明を指定します。

印刷

バウチャーを直接印刷する場合にこのオプションを有効にします。

表示行数

印刷したいページサイズを選択します。

1 ページあたりのバウチャー数

1ページに印刷するバウチャーの数を選択します。デバイスはページ上のバウチャーを自動的に調整します。

QRコード付加

印刷するバウチャーに、バウチャーテキストデータに加えQRコードも印刷するよう要求することができます。QRコードは、コード化されたデータを含む四角の画像です。それをモバイルデバイスでスキャンすれば、必要なデータがフィールドにすでに入力されている、ホットスポットのログインページにアクセスできます。

3. 「**バウチャーの作成**」をクリックして、ユーザーが設定したセッティングでバウチャーを作成します。

バウチャーが生成されます。各バウチャーはすぐに、以下のバウチャーリストに新しい行として表示されます。設定によっては、直接印刷されます。各バウチャーにはユニークなコードが付いています。

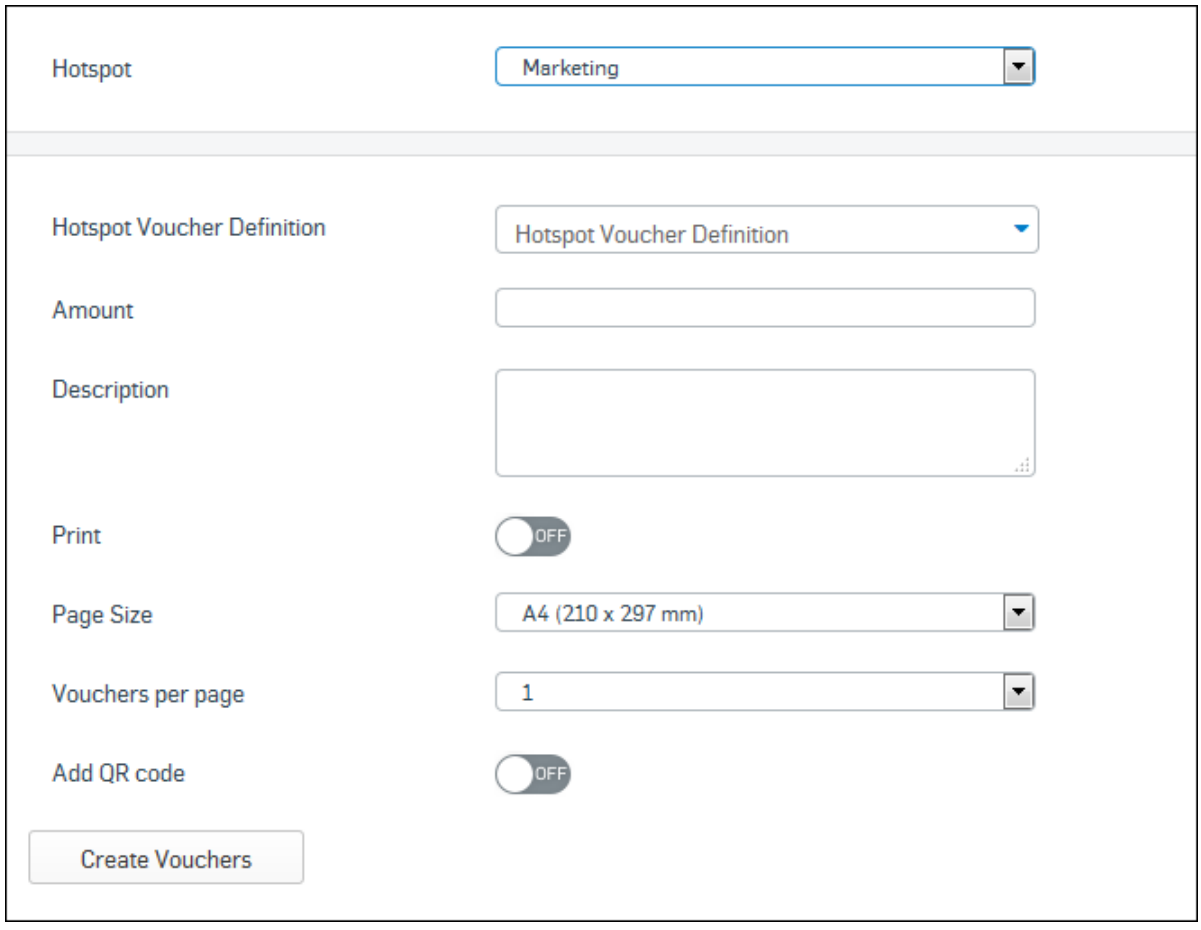

図 15：ホットスポットタイプのバウチャー

ここで、以下のバウチャーリストを管理できます。

関連概念

バウチャーリストの管理 (p. 17)
このページでは、**ホットスポット** タブのバウチャーリストの管理方法について説明します。

ホットスポット (p. 14)

「ホットスポット」メニューでは、カフェ、ホテル、会社などの公共スペースで、時間制限およびトラフィック制限付きのインターネットアクセスをゲストに提供します。

8.2.1 バウチャーリストの管理

このページでは、**ホットスポット** タブのバウチャーリストの管理方法について説明します。

バウチャーリストで、バウチャーを管理することができます。リストをソート、プリント、削除することができます。また、選択したバウチャーをエクスポートすることもできます。

- リストをソートするには、ソートしたいテーブルヘッダをクリックします。矢印は表が昇順で並んでいるか、降順で並んでいるかを示しています。
- バウチャーを印刷または削除するには、当該のバウチャーの横にあるチェックボックスを選択して、下にある適当なボタンをクリックします。

  注
  バウチャーは、管理者が指定した時間後に自動的に削除されます。

- バウチャーをエクスポートするには、当該のバウチャーの横にあるチェックボックスを選択して、下にある「**CSV をエクスポート**」のボタンをクリックします。ウィンドウが表示されるので、CSV ファイルを保存する場所を指定するか、直接開きます。選択したバウチャーは 1つの CSV ファイルに保存されます。ファイルをオープンする場合は、カラムの区切り文字として正しいキャラクターを選択するよう注意してください。

関連タスク

ホットスポットタイプのバウチャー (p. 15)
このページでは、固有のコードを含むバウチャーを作成する方法を説明します。バウチャーはプリントしてゲストに渡すことができます。作成したバウチャーのリストには、各バウチャーの利用法の概要が表示されており、管理するのに役立ちます。

9 OTP トークン

このページでは、ワンタイムパスワードを使用してログインする方法を説明します。

ワンタイムパスワード（OTP）は、1回限りのログインセッションに対して有効なパスワードです。ワンタイムパスワードはスタティックコンポーネント (プライマリパスワード) から構成されている、時間制限のある一時的なパスコードです。

1. ご利用のデバイスに Sophos Authenticator をインストールします。
   Sophos Authenticator は App Store からダウンロードできます。
2. ご利用の電話の　Sophos Authenticator を使用して、画面に表示される QR コードをスキャンします。
   アプリはパスコードを生成します。このパスコードは一定間隔で更新されます (「タイムステップ」の説明を参照)。
3. **「ログインに進む」**をクリックします。
4. ログインのために生成されたばかりのパスコードに続き、ユーザー名とユーザーポータルパスワードを入力します。
5. **「ログイン」**をクリックします。
   これで、ユーザーポータルにアクセスできるようになります。