



# Cisco Spaces : キャプティブポータルアプリケーション

---

この章では、Cisco Spacesを使用してキャプティブポータルを作成する方法について説明します。

- [ポータルの作成と管理 \(1 ページ\)](#)
- [キャプティブポータルルール \(42 ページ\)](#)
- [SSID, on page 49](#)
- [レポート, on page 53](#)
- [ユーザー管理, on page 57](#)
- [アクセスコード \(58 ページ\)](#)
- [信頼できるデバイス, on page 71](#)
- [設定 \(77 ページ\)](#)
- [ポータルの認定デバイス リスト \(87 ページ\)](#)
- [Cisco Spaces キャプティブポータルの動作 \(88 ページ\)](#)
- [顧客の認証手順 \(94 ページ\)](#)
- [キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#)

## ポータルの作成と管理

ポータルは、Wi-Fi ユーザーが SSID に接続したときに表示されるユーザーインターフェイスです。Cisco DNA Spaces を使用してキャプティブポータルを作成し、Cisco DNA Spaces により提供されるさまざまなポータルモジュールを使用して、ポータルを強化できます。

Cisco DNA Spaces では、独自のポータル（エンタープライズ キャプティブ ポータル）を使用して、Wi-Fi に接続するエンドユーザーをオンボードすることもできます。エンタープライズ キャプティブ ポータルの詳細については、[エンタープライズ キャプティブ ポータル](#)を参照してください。

## ポータル作成の前提条件

- ポータルを適用可能なロケーションを指定するには、ロケーション階層を定義する必要があります。ロケーション階層の定義の詳細については、[ロケーション階層の定義](#)のセクションを参照してください。
- ポータルのソーシャル認証を設定する場合は、使用するソーシャルアプリケーションで該当する設定を行い、そのソーシャルアプリケーションを Cisco Spaces に追加する必要があります。ソーシャル認証の設定の詳細については、「[ポータルのソーシャル認証](#)」のセクションを参照してください。
- ポータルに SMS ベースの認証を設定する場合は、SMS ゲートウェイを設定する必要があります。SMS ゲートウェイ設定の詳細については、[Cisco DNA Spaces での SMS ゲートウェイの設定 \(77 ページ\)](#) のセクションを参照してください。

### 帯域幅の要件

キャプティブポータルの場合、優れたエンドユーザー エクスペリエンスのために、最低 30 Mbps の帯域幅をお勧めします。

次の表は、帯域幅に基づきキャプティブポータルをロードするための応答時間を示しています。

表 1:

帯域幅	ユーザ数	応答 (秒)
1 Mbps	1	5.86
	2	5.49
	3	5.40
	4	5.63
	5	5.92

帯域幅	ユーザ数	応答 (秒)
2 Mbps	1	5.09
	2	5.10
	3	5.04
	4	5.25
	5	5.16
	6	5.23
	7	5.26
	8	5.30
	9	5.34
	10	5.40
	11	5.49
5 Mbps	5	4.92
	10	4.98
	11	5.05
	12	5.08
	13	5.11
	14	5.13
	15	5.17
	16	5.18
20	5.25	
7 Mbps	25	5.13
	30	5.20
	31	5.23
	32	5.26
	33	5.29
	34	5.33

帯域幅	ユーザ数	応答 (秒)
9 Mbps	30	4.93
	35	4.98
	40	5.05
	41	5.07
	42	5.10
	43	5.13
	44	5.15
	45	5.17
	46	5.19
	47	5.15
11 Mbps	35	4.68
	40	4.91
	50	5.05
	55	5.16
	56	5.18
	57	5.20
	58	5.24
	59	5.28
	60	5.25
	61	5.30

## サンプルのポータル

Cisco DNA Spaces は、さまざまな認証タイプのサンプルポータルを提供しています。

- データキャプチャによる電子メール認証
- パスワードの確認とデータのキャプチャを含むインライン SMS
- インラインソーシャル認証
- パスワードの確認とデータのキャプチャを含む SMS
- リンクの確認を含む SMS

- 電子メール認証
- ユーザー契約

さらに、COVID-19 の要件を満たすためのサンプルポータルが提供されています。  
サンプルポータルを確認してコピーを作成するには、次の手順を実行します。

#### 手順

- 
- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
  - ステップ 2** 表示されるウィンドウで、[Captive Portal] を選択します。
  - ステップ 3** 表示される [Captive Portal] ウィンドウで、左ペインの **Portal** を選択します。  
ポータルリストの下部に、さまざまな認証タイプのサンプルポータルが表示されます。
  - ステップ 4** 目的のサンプルポータルの右端にある [Make a Copy] アイコンをクリックします。
  - ステップ 5** 表示されるポータルウィザード画面で、キャプティブポータルの名前を指定します。
  - ステップ 6** 必要に応じて、ポータル設定に必要なカスタマイズを行います。
  - ステップ 7** ポータルを保存します。
- 

## ポータルの作成

ポータルを定義するときに、ポータルを利用可能にする必要があるロケーションを設定することもできます。

ポータルを作成するには、次の手順を実行します。

#### 手順

- 
- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
  - ステップ 2** 表示されるウィンドウで、[Captive Portal] を選択します。
  - ステップ 3** 表示される [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。
  - ステップ 4** [Create New] をクリックします。  
ポータルウィザードが表示されます。
  - ステップ 5** [Portal Name] フィールドに、ポータルの名前を入力します。
  - ステップ 6** このポータルを特定のロケーションでのみ使用できるようにする場合は、[Enable this portal for all locations] チェックボックスをオフにします。

(注)

デフォルトでは、[Enable this portal for all locations] チェックボックスがオンになっており、ロケーション階層内のすべてのロケーションでポータルを使用できるようになっています。

**ステップ 7** [Next] をクリックします。

[Authentication] ウィンドウが表示されます。

**ステップ 8** [Authentication Type] ドロップダウンリストから、ポータルに適用する認証タイプを選択します。

選択した認証タイプに基づいて、追加のフィールドが表示されます。各種認証タイプの認証手順の詳細については、[ポータルへの認証の設定 \(11 ページ\)](#) を参照してください。

**ステップ 9** 認証タイプの詳細を指定したら、[Next] をクリックします。

[Data Capture] ウィンドウが表示されます。

(注)

[Social Sign In] 認証の場合、ソーシャルサインインではデータキャプチャがないため、[User Agreements] 画面に移動します。ソーシャルサインインでは手順 10 から手順 12 をスキップします。

**ステップ 10** このポータルにデータキャプチャフォームを追加する場合は、[Enable Data Capture] チェックボックスをオンにします。

**ステップ 11** データキャプチャフォームを設定します。[+ Add Field Element] ボタンを使用して、データキャプチャフォームに必要なフィールドを追加します。データキャプチャフォームへのフィールドの追加の詳細については、[ポータルへのデータキャプチャフォームの追加 \(19 ページ\)](#) を参照してください。

**ステップ 12** [Next] をクリックします。

[User Agreements] ウィンドウが表示されます。

**ステップ 13** [Terms & Condition Message] フィールドに、ポータルの「利用規約」を入力します。

(注)

デフォルトでは、[Enable Terms & Conditions] チェックボックスはオンになっています。「利用規約」を指定しない場合は、[Enable Terms & Conditions] チェックボックスをオフにします。

**ステップ 14** 利用規約とともにプライバシーポリシーを表示する場合は、[Enable Privacy Policy] チェックボックスをオンにして、表示される [Privacy Policy] フィールドにプライバシーポリシーを入力します。

プライバシーポリシーを指定すると、顧客獲得時に「利用規約」とともにプライバシーポリシーも表示されます。

**ステップ 15** [How frequently do you want users to accept agreements] ドロップダウンリストから、顧客がインターネットにアクセスするために「利用規約」に同意する必要がある頻度を選択します。

**ステップ 16** [User Accepts Terms In] 領域で、顧客獲得時に「利用規約」をどのように表示するかを選択します。

- [1-Click] : [Terms & Conditions] リンクのみを表示する場合は、このオプションを選択します。このオプションを選択すると、顧客獲得時に、顧客は [Accept Terms and Continue] ボタンをクリックして先に進むことができます。
- [2-Click] : [Terms & Conditions] リンクとともにチェックボックスを表示する場合は、このオプションを選択します。このオプションを選択した場合、顧客獲得時に、顧客はチェックボックスを選択し、[Accept Terms and Continue] ボタンをクリックして先に進む必要があります。

(注)

[2-Click] オプションは、特定の国の法的要件を満たすために Cisco DNA Spaces で提供されています。

**ステップ 17** 特定の年齢未満の顧客によるインターネットアクセスを制限する場合は、[Enable Age gating] チェックボックスをオンにして、必要な年齢制限の方法を以下から選択します。

- [Moderate] : このオプションを選択した場合、顧客獲得時に、顧客は年齢が 16 歳以上であることを確認する必要があります。
- [Strict] : このオプションを選択すると、顧客獲得時に、顧客は生年月日を指定してインターネットにアクセスする必要があります。顧客が 16 歳未満の年齢を指定した場合、警告メッセージが表示され、顧客はそれ以上インターネットにアクセスできなくなります。ただし、必要に応じて、年齢を変更するオプションが顧客に提供されます。

**ステップ 18** [Save and Configure Portal] をクリックします。

[Portal saved successfully] メッセージが表示されて [Portal] ウィンドウが開き、左側にポータルモジュールが、右側にポータルのプレビューが表示されます。

**ステップ 19** [ポータルモジュール \(7 ページ\)](#) を使用してポータルに機能を追加します。

**ステップ 20** [Save] をクリックして、各モジュールに加えた変更を保存します。

(注)

ポータルの作成時に、ポータルの名前と場所を指定した後で、ポータルを保存できます。新しいポータルが [Portal] ウィンドウにリストされます。そのポータルの [Edit Portal] ボタンを使用して、認証タイプ、利用規約、データキャプチャフォームなどを後でいつでも構成できます。

(注)

キャプティブポータルを使用して SSID に接続する顧客の名前や電話番号などの詳細情報をキャプチャするには、「データキャプチャフォーム」をキャプティブポータルに追加していることを確認してください。顧客獲得時 (ランタイム) に、インターネットをプロビジョニングする前に、データキャプチャフォームが顧客に表示されます。キャプチャされた顧客の詳細情報は、Cisco DNA Spaces に保存されます。

(注)

ポータルをキャプティブポータルルールに関連付けると、ポータルが稼働を開始し、そのルールが公開されます。

## ポータルモジュール

次のとおり、Cisco Spaces のポータルモジュールがあります。

- **Header/Branding**—このモジュールを使用してポータルのページタイトルとブランド名を定義します。

[ページタイトル (Page Title)] フィールドを使用してキャプティブポータルのページタイトルを変更します。更新されたページタイトルが使用する Cisco Spaces : キャプティブポ

ポータルアプリケーションに表示されます。ブランド名をテキストやロゴのイメージで追加できます。

- **Welcome Message** : このモジュールを使用してポータルにウェルカムメッセージを追加します。初回ユーザーとリピーターユーザーに異なるウェルカムメッセージを表示するように構成できます。
- **Notice** : このモジュールを使用してポータルに通知を追加します。これにより、必要に応じてポータルユーザーに通知を表示できます。太字テキスト、テキスト、またはイメージ形式のテキストで通知するように設定できます。
- **Authentication** : ポータルの作成時に選択した認証タイプに基づいて、ポータルに認証モジュールが表示されます。モジュールの名前は、認証タイプに基づきます。たとえば、ポータルの認証タイプとして [SMS with link verification] を選択した場合、そのポータルの認証モジュールの名前は「SMS Authentication」になります。認証モジュールには、ポータルのランディングページ URL を構成するためのプロビジョニングが含まれます。[Data Capture] と [User Agreements] の両方が有効になっていない場合、認証タイプ [No Authentication] の認証モジュールは使用できません。
- **Venue Map** : このモジュールを使用して、施設マップのラベルとアイコンを追加します。施設マップは、ロケーションに基づいてワイヤレスネットワークからポータルにアップロードされます。
- **Videos** : このモジュールを使用してポータルに YouTube ビデオを追加します。また、ポータルのビデオセクションに適したキャプションとアイコンも追加できます。またアップロードすると、ビデオのプレビューを表示できます。
- **Feedback** : このモジュールを使用してポータルのフィードバックの質問を追加します。複数の選択肢と評価の質問を追加できます。このモジュールでは、[Submit] ボタン、[Thank You] メッセージ、および [Post Submission] ボタンのラベルもカスタマイズできます。コメントを追加するためのテキストボックスをユーザーに表示するかどうかを設定することができます。また、フィードバック用の電子メールアドレスおよび件名を指定することもできます。
- **Help** : このモジュールを使用して、顧客がサポートを求める際に連絡するヘルプの電話番号を追加します。ヘルプのキャプションおよびアイコンをカスタマイズできます。
- **Get Apps** : このモジュールを使用してポータルにアプリケーションを追加します。このモジュールを使用して、各アプリケーションに適したキャプションとアイコンを追加できます。
- **Get Internet** : 顧客がポータルの [Get Internet] セクションから移動できる外部 URL を追加します。この URL にアクセスするには、指定された利用規約を顧客が承認する必要があります。
- **Promos & Offers** : このモジュールを使用して、ポータルで表示するプロモーションおよび特典を追加します。プロモーションのタイトルを変更できます。プロモーションごとに適したキャプションとイメージを追加し、プロモーションの詳細の URL を指定できます。プロモーションは回転式で表示されます。

- **Add Module** : このモジュールを使用して、ポータルにカスタマイズしたコンテンツおよびメニューアイテムを追加します。前述のすべてのモジュールは、Cisco Spaces によって提供されるデフォルトのモジュールです。[Add Module] ボタンを使用すると、要件に応じてポータルに別のアイテムを追加できます。

## ポータルの言語の設定

Cisco DNA Spaces では、ポータル内のモジュールのキャプションや静的コンテンツを表示する言語を設定できます。英語以外の言語で静的コンテンツを表示するには、対応するテキストを Cisco DNA Spaces にアップロードする必要があります。Cisco DNA Spaces は、英語以外の言語でのコンテンツの入力をサポートしていません。デフォルトの言語は英語に設定されています。デフォルトの言語は変更できます。



- (注) Cisco DNA Spaces を使用して、ある言語で作成されたコンテンツを他の言語に翻訳することはできません。

ポータルのコンテンツを表示する言語を設定するには、次の手順を実行します。

### 手順

- ステップ 1** メッセージ、国名などの静的コンテンツを英語ではない言語で表示するには、その言語のキー値をアップロードします。任意の言語のキー値をアップロードする操作の詳細については、[任意の言語の静的コンテンツのキー値のアップロード \(10 ページ\)](#) を参照してください。
- ステップ 2** 言語を設定するポータルを開きます。
- ステップ 3** [Portal] ウィンドウの上部にある [Languages] (地球) アイコンをクリックします。  
[Add Language] ウィンドウが表示されます。
- ステップ 4** [Add Language] をクリックします。
- ステップ 5** 表示される検索フィールドに、言語を入力します。  
その言語が Cisco DNA Spaces でサポートされている場合、言語名がドロップダウンリストに表示されません。
- ステップ 6** 言語名の隣に表示される [Add] ボタンをクリックします。  
言語が [Added Languages] リストに追加されます。
- ステップ 7** [Add] をクリックします。  
ポータルで、[Languages] アイコンの隣にドロップダウンリストが表示され、新しく追加された言語がそのドロップダウンリストに表示されます。

**ステップ 8** [Languages] アイコンの隣のドロップダウンリストから、ポータルの静的コンテンツを表示する言語を選択します。

各モジュールのキャプションは、選択された言語で表示されます。

---

## デフォルト言語の設定

デフォルト言語を設定するには、次の手順を実行します。

### 手順

**ステップ 1** ポータルで、ウィンドウ右上の [Languages] アイコンをクリックします。

**ステップ 2** [Add Language] ウィンドウで、[Default Language] ドロップダウンリストからデフォルト言語を選択します。

**ステップ 3** [Add] をクリックします。

---

## 任意の言語の静的コンテンツのキー値のアップロード

静的コンテンツを英語以外の言語で表示するように設定するには、次の手順を実行します。

### 手順

**ステップ 1** ポータルで、ウィンドウ右上の [Languages] アイコンをクリックします。

**ステップ 2** [Add Language] ウィンドウで [Download] をクリックしてテンプレートをダウンロードし、保存します。

**ステップ 3** テンプレートを開きます。

テンプレートには、さまざまな静的メッセージのキー値と、言語が英語である場合に表示されるメッセージが含まれています。英語の列には、1行目に「en」と表示されています。

**ステップ 4** 英語の列の隣に、静的コンテンツを表示する言語の言語識別子を入力します。

たとえば、コンテンツをアラビア語で表示する場合は、1行目に「AR」と入力します。

**ステップ 5** 残りの行には、対応するキーに対して表示する必要があるテキストを入力します。

**ステップ 6** ファイルを保存します。

**ステップ 7** [Add Language] ウィンドウで、[Upload] ボタンを使用してウィンドウをアップロードします。

**ステップ 8** [Add] をクリックします。

## 次のタスク

静的コンテンツを任意の言語で表示する方法については、[ポータルの言語の設定 \(9 ページ\)](#)を参照してください。

さまざまな言語の言語コードを次の図に示します。

図 1: 言語コード

```
[{"Abkhaz": "ab"}, {"Afar": "aa"}, {"Afrikaans": "af"}, {"Akan": "ak"}, {"Albanian": "sq"}, {"Amharic": "am"}, {"Arabic": "ar"}, {"Aragonese": "an"}, {"Armenian": "hy"}, {"Assamese": "as"}, {"Avaric": "av"}, {"Avestan": "ae"}, {"Aymara": "ay"}, {"Azerbaijani": "az"}, {"Bambara": "bm"}, {"Bashkir": "ba"}, {"Basque": "eu"}, {"Belarusian": "be"}, {"Bengali": "bn"}, {"Bihari": "bh"}, {"Bislama": "bi"}, {"Bosnian": "bs"}, {"Breton": "br"}, {"Bulgarian": "bg"}, {"Catalan": "ca"}, {"Chamorro": "ch"}, {"Chechen": "ce"}, {"Chichewa": "ny"}, {"Chinese": "zh"}, {"Chuvash": "cv"}, {"Cornish": "kw"}, {"Corsican": "co"}, {"Cree": "cr"}, {"Croatian": "hr"}, {"Czech": "cs"}, {"Danish": "da"}, {"Divehi": "dv"}, {"Dutch": "nl"}, {"Dzongkha": "dz"}, {"English": "en"}, {"Esperanto": "eo"}, {"Estonian": "et"}, {"Ewe": "ee"}, {"Faroese": "fo"}, {"Fijian": "fj"}, {"Finnish": "fi"}, {"French": "fr"}, {"Fula": "ff"}, {"Galician": "gl"}, {"Georgian": "ka"}, {"German": "de"}, {"Greek": "el"}, {"Guaraní": "gn"}, {"Gujarati": "gu"}, {"Haitian": "ht"}, {"Hausa": "ha"}, {"Hebrew": "he"}, {"Herero": "hz"}, {"Hindi": "hi"}, {"Hungarian": "hu"}, {"Interlingua": "ia"}, {"Indonesian": "id"}, {"Interlingue": "ie"}, {"Irish": "ga"}, {"Igbo": "ig"}, {"Inupiaq": "ik"}, {"Ido": "io"}, {"Icelandic": "is"}, {"Italian": "it"}, {"Inuktitut": "iu"}, {"Japanese": "ja"}, {"Javanese": "jv"}, {"Kalaallisut": "kl"}, {"Kannada": "kn"}, {"Kannuri": "kr"}, {"Kashmiri": "ks"}, {"Kazakh": "kk"}, {"Khmer": "km"}, {"Kikuyu": "ki"}, {"Kinyarwanda": "rw"}, {"Kyrgyz": "ky"}, {"Komi": "kv"}, {"Kongo": "kg"}, {"Korean": "ko"}, {"Kurdish": "ku"}, {"Kwanyama": "kj"}, {"Latin": "la"}, {"Luxembourgish": "lb"}, {"Ganda": "lg"}, {"Limburgish": "li"}, {"Lingala": "ln"}, {"Lao": "lo"}, {"Lithuanian": "lt"}, {"Latvian": "lv"}, {"Manx": "gv"}, {"Macedonian": "mk"}, {"Malagasy": "mg"}, {"Malay": "ms"}, {"Malayalam": "ml"}, {"Maltese": "mt"}, {"Marathi": "mr"}, {"Marshallese": "mh"}, {"Mongolian": "mn"}, {"Nauru": "na"}, {"Navajo": "nv"}, {"Nepali": "ne"}, {"Ndonga": "ng"}, {"Norwegian Nynorsk": "nn"}, {"Norwegian": "no"}, {"Nuosu": "ii"}, {"Southern Ndebele": "nr"}, {"Occitan": "oc"}, {"Ojibwe": "oj"}, {"Old Church Slavonic": "cu"}, {"Oriya": "or"}, {"Ossetian": "os"}, {"Panjabi": "pa"}, {"Persian": "fa"}, {"Polish": "pl"}, {"Pashto": "ps"}, {"Portuguese": "pt"}, {"Quechua": "qu"}, {"Romanian": "ro"}, {"Kirundi": "rn"}, {"Romanian": "ro"}, {"Russian": "ru"}, {"Sanskrit": "sa"}, {"Sardinian": "sc"}, {"Sinhali": "si"}, {"Northern Sami": "se"}, {"Samoan": "sm"}, {"Sango": "sg"}, {"Serbian": "sr"}, {"Scottish Gaelic": "gd"}, {"Shona": "sn"}, {"Sinhala": "si"}, {"Slovak": "sk"}, {"Slovene": "sl"}, {"Somali": "so"}, {"Southern Sotho": "st"}, {"Spanish": "es"}, {"Sundanese": "su"}, {"Swahili": "sw"}, {"Swati": "ss"}, {"Swedish": "sv"}, {"Tamil": "ta"}, {"Telugu": "te"}, {"Tajik": "tg"}, {"Thai": "th"}, {"Tigrinya": "ti"}, {"Tibetan Standard": "bo"}, {"Turkmen": "tk"}, {"Tagalog": "tl"}, {"Tswana": "tn"}, {"Tonga": "to"}, {"Turkish": "tr"}, {"Tsonga": "ts"}, {"Tatar": "tt"}, {"Twi": "tw"}, {"Tahitian": "ty"}, {"Uyghur": "ug"}, {"Ukrainian": "uk"}, {"Urdu": "ur"}, {"Uzbek": "uz"}, {"Venda": "ve"}, {"Vietnamese": "vi"}, {"Walloon": "wa"}, {"Welsh": "cy"}, {"Wolof": "wo"}, {"Western Frisian": "fy"}, {"Xhosa": "xh"}, {"Yiddish": "yi"}, {"Yoruba": "yo"}, {"Zhuang": "za"}, {"Zulu": "zu"}]
```

## ポータルへの認証の設定

ハッキングや悪用からポータルを保護するため、ポータルには、さまざまな認証オプションを設定することができます。顧客は、認証が成功した場合のみアクセスできます。

インターネットプロビジョニングのための認証は、SMS、電子メール、アクセスコード、または Facebook、Twitter、LinkedIn などのソーシャルネットワークを介して実行できます。Cisco DNA Spaces は、SMS 認証用としてサードパーティベンダーの SMS ゲートウェイをサポートしています。「パスワードを含む SMS による確認」または「リンクを含む SMS による確認」を使用して SMS 認証を実行するように設定できます。「パスワードを含む SMS による確認」の場合、ポータル用のカスタム認証コードを定義するか、認証コードの自動生成を設定できます。

顧客の獲得中に、顧客がポータルのメニュー項目をクリックすると、認証プロセスが開始されます。ただし、認証モジュールがキャプティブポータルに表示されるようにインライン認証を設定することもできます。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#)を参照してください。

Cisco DNA Spaces は、次の認証タイプをサポートしています。

- パスワードを含む SMS による確認**：この認証タイプでは、携帯電話番号の確認が必須です。顧客が有効な携帯電話番号を入力すると、リンクと認証コードを含む SMS が携帯電話番号に送信されます。顧客は、SMS 内の認証コードを入力することで、インターネットにアクセスできます。認証コードが入力されるまで、顧客は操作を進めることができません。この認証タイプの使用例には、SMS ベースのエンゲージメントキャンペーン、インターネットに接続するユーザーを確認するための国固有の要件などがあります。顧客獲得

時の認証手順については、[SMS with Password Verification 認証の手順 \(96 ページ\)](#) を参照してください。「パスワードを含む SMS による確認」の詳細については、[ポータルでのパスワード検証付き SMS の設定 \(14 ページ\)](#) のセクションを参照してください。

**リンクを含む SMS による確認**：この認証タイプでは、携帯電話番号の確認はオプションです。顧客が有効な携帯電話番号を入力すると、認証リンクを含む SMS が携帯電話番号に送信されます。顧客は、SMS の認証リンクをクリックして確認を完了することができます。ただし、顧客は確認プロセスをスキップして先に進むことができます。この認証タイプは、携帯電話番号の確認が必須でない場合に使用できます。顧客獲得時の認証手順については、[リンク検証付き SMS による認証の手順 \(94 ページ\)](#) を参照してください。詳細については、[ポータルでのリンク検証付き SMS の設定 \(13 ページ\)](#) を参照してください。

**電子メール**：顧客がインターネットにアクセスするには、有効な電子メール ID を入力する必要があります。顧客獲得時の認証手順については、[電子メール認証の手順 \(98 ページ\)](#) を参照してください。電子メール認証の設定に関する詳細については、[Email 認証のためのポータルの設定 \(16 ページ\)](#) を参照してください。

**ソーシャルサインイン**：認証のために設定されているソーシャルサイトに顧客がログインしている場合のみ、インターネットへのアクセスが提供されます。このオプションを使用するには、少なくとも1つのソーシャルサイトを設定する必要があります。顧客獲得時の認証手順については、[ソーシャル認証の手順 \(104 ページ\)](#) を参照してください。ソーシャルサインイン認証の設定に関する詳細については、「[ソーシャルサインイン認証のためのポータル設定](#)」のセクションを参照してください。

**アクセスコード**：顧客がインターネットにアクセスするには、有効なアクセスコードを入力する必要があります。顧客獲得時の認証手順については、[アクセスコード認証の手順 \(101 ページ\)](#) を参照してください。アクセスコード認証の設定に関する詳細については、[アクセスコード認証用ポータルの設定 \(17 ページ\)](#) を参照してください。

**認証なし**：認証プロセスなしでインターネットへのアクセスが提供されます。顧客獲得時の認証手順については、[利用規約による認証省略の手順 \(103 ページ\)](#) を参照してください。ポータルを認証なしに設定する手順の詳細については、[認証なしでのポータルの設定 \(18 ページ\)](#) を参照してください。



(注) [OptIn] オプションは、「ソーシャルサインイン」認証タイプでは使用できません。「ソーシャルサインイン」を除くすべての認証タイプ用にデータキャプチャフォームを設定できます。データキャプチャフォーム設定の詳細については、[ポータルへのデータキャプチャフォームの追加 \(19 ページ\)](#) を参照してください。オプトイン機能の詳細については、「ユーザーのオプトインオプション」のセクションを参照してください。



- (注) リンクを含む SMS による確認またはパスワードを含む SMS による確認の場合、SMS ゲートウェイに渡す必要のある追加情報を含めることができます。たとえば、英語以外の言語で SMS を顧客に送信する場合、SMS ゲートウェイに送信される SMS にその情報を含めることができますようになりました。

## ポータルでのリンク検証付き SMS の設定

ポータルで「リンク検証付き SMS」を設定するには、次の手順を実行します。

### 手順

- ステップ 1** ポータルを作成するときに、[Active Access Codes] ドロップダウンリストから [SMS with Link verification] を選択します。
- ステップ 2** このポータルでインライン認証を構成し、ホームページに「データキャプチャフォーム」と「ユーザーの同意」を表示する場合は、[Display Authentication, Data Capture, and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。
- ステップ 3** 通知を受け取るかどうかを選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。
- ステップ 4** [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。
- [Opt in Message] : オプトインメッセージを入力します。
  - [Default Opt-In Check Box Behavior]
    - [Checked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックしま
    - [Unchecked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。
- ステップ 5** [SMS Text] フィールドに、ユーザーに送信する SMS に表示されるテキストメッセージを入力します。
- (注)  
顧客がキャプティブポータルにアクセスできるリンクを表示する際は、テキストメッセージを編集する際に「{Link}」が削除されていないことを確認します。
- ステップ 6** [Default Country] ドロップダウンリストから、この設定が適用される国を選択します。
- ステップ 7** [SMS Gateway] ドロップダウンリストから、SMS ゲートウェイを選択します。
- [Settings] オプションで設定された SMS ゲートウェイが選択可能になっています。シスコが提供する有料の [Demo Gateway] も使用できます。

(注)

SMS ゲートウェイを設定するときの詳細については、[Cisco DNA Spaces](#) での [SMS ゲートウェイの設定 \(77 ページ\)](#) を参照してください。

ステップ 8 変更内容を保存します。

#### 次のタスク



(注) 認証タイプが [SMS with link verification] のポータルには、[SMS Authentication] という名前の認証モジュールがあります。この認証モジュールの詳細については、[認証モジュール \(19 ページ\)](#) を参照してください。



(注) ポータルの作成時に認証タイプを設定していない場合は、[Portals] ウィンドウでそのポータルの [Edit Portal] ボタンを使用していつでも指定できます。

## ポータルでのパスワード検証付き SMS の設定

ポータルを「パスワード検証付き SMS」に設定するには、次の手順を実行します。

### 手順

- ステップ 1 ポータルを作成するときに、[Authentication Type] ドロップダウンリストから [SMS with password verification] を選択します。
- ステップ 2 このポータルでのインライン認証を設定し、ポータルホームページにユーザー契約を表示する場合は、[Display Authentication and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。
- ステップ 3 通知を受け取るかどうかを選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。
- ステップ 4 [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。
- [Opt in Message] : オプトインメッセージを入力します。
  - [Default Opt-In Check Box Behavior]
    - [Checked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックしま
    - [Unchecked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

ステップ 5 [Password Type] で必要なオプションをクリックします。

- [Auto Generated password] : 認証要求ごとに、パスワードを自動的に生成します。自動生成されたパスワードが顧客に送信されます。
- [Fixed Password] : 認証用のパスワードを定義します。このパスワードは、すべての顧客に対して、認証要求があるたびに送信されます。[Fixed Password] オプションをクリックすると表示される [Password] フィールドに、顧客に送信するパスワードを入力します。

ステップ 6 [SMS field] フィールドに、ユーザーに送信する SMS に表示されるテキストを入力します。

(注)

顧客がキャプティブポータルにアクセスできるリンクを表示する際は、テキストメッセージを編集する際に「{Link}」が削除されていないことを確認します。同様に、メッセージ内にパスワードを表示する際は、「{Password}」が削除されていないことを確認します。

ステップ 7 [Default Country] ドロップダウンリストから、この設定が適用される国を選択します。

ステップ 8 [SMS Gateway] ドロップダウンリストから、SMS ゲートウェイを選択します。

[Settings] オプションで設定された SMS ゲートウェイが選択可能になっています。シスコが提供する有料の [Demo Gateway] も使用できます。

(注)

[SMS Gateway] ウィンドウが表示され、必要な SMS ゲートウェイ を設定できます。SMS ゲートウェイを設定するときの詳細については、[Cisco DNA Spaces](#) での [SMS ゲートウェイの設定 \(77 ページ\)](#) を参照してください。

ステップ 9 変更内容を保存します。

#### 次のタスク



- (注) 認証タイプが [SMS with password verification] のポータルには、[SMS Authentication] という名前の認証モジュールがあります。この認証モジュールの詳細については、[認証モジュール \(19 ページ\)](#) を参照してください。



- (注) ポータルの作成時に認証タイプを設定していない場合は、[Portals] ウィンドウでそのポータルの [Edit Portal] ボタンを使用していつでも指定できます。

## Social Sign In 認証のためのポータル設定

Cisco Spaces は、次のソーシャルネットワークを介した認証をサポートしています。

- Facebook
- Twitter

- LinkedIn



(注) ソーシャルネットワークを介してインターネットへのアクセスを認証するには、そのソーシャルネットワークのアプリケーションを Cisco Spaces で設定する必要があります。[設定 (Settings) ] オプションを使用して、Cisco Spaces でソーシャルアプリケーションを設定できます。詳細については、[ソーシャル認証のためのソーシャルアプリケーションの追加 \(86 ページ\)](#) を参照してください。

ポータルへのアクセスを Social Sign In で認証するには、次の手順を実行します。

### 手順

**ステップ 1** ポータルを作成する際、[Authentication Type] ドロップダウンリストから [Social Sign In] を選択します。

Cisco Spaces での認証用にサポートされているソーシャルネットワークが、設定済みのソーシャルアプリケーションと一緒に表示されます。

**ステップ 2** このポータルでのインライン認証を設定し、ポータルホームページにユーザー契約を表示する場合は、[Display Authentication and Users Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。

**ステップ 3** インターネットへのアクセスの認証に使用するソーシャルネットワークの隣にあるチェックボックスをオンにします。

[Settings] セクションの [Social Apps] オプションで設定されたソーシャルネットワークを選択できます。ソーシャルアプリケーションの設定の詳細については、[ソーシャル認証のためのソーシャルアプリケーションの追加 \(86 ページ\)](#) を参照してください。

**ステップ 4** 変更内容を保存します。

### 次のタスク

- 認証タイプが [Social Sign In] のポータルには、[Social Authentication] という名前の認証モジュールがあります。この認証モジュールの詳細については、[認証モジュール \(19 ページ\)](#) を参照してください。
- [+Add] ボタンをクリックすると [Social Apps] ウィンドウが表示されます。このウィンドウで、カスタマイズされたアプリケーションを設定できます。
- ポータルの作成時に認証タイプを設定していない場合は、[Portals] ウィンドウでそのポータルの [Edit Portal] ボタンを使用していつでも指定できます。

## Email 認証のためのポータルの設定

ポータルを Email 認証に設定するには、次の手順を実行します。

## 手順

- 
- ステップ 1** ポータルを作成する際、[Authentication Type] ドロップダウンリストから [Email] を選択します。
- ステップ 2** このポータルでのインライン認証を設定する場合は、[Display Authentication and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。
- ステップ 3** 通知を受け取るかどうかを選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。
- ステップ 4** [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。
- [Opt in Message] : オプトインメッセージを入力します。
  - [Default Opt-In Check Box Behavior]
    - [Checked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックします。
    - [Unchecked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。
- ステップ 5** 変更内容を保存します。

## 次のタスク



- 
- (注) 認証タイプが [Email] のポータルには、[Email] という名前の認証モジュールがあります。この認証モジュールの詳細については、[認証モジュール \(19 ページ\)](#) を参照してください。
- 

## アクセスコード認証用ポータルの設定

アクセスコード認証用のポータルを設定するには、次の手順を実行します。

## 手順

- 
- ステップ 1** ポータルを作成する際、[Authentication Type] ドロップダウンリストから [Access Code] を選択します。
- ステップ 2** このポータルでのインライン認証を設定し、ポータルホームページにユーザー契約を表示する場合は、[Display Authentication and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。

- ステップ 3** 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。
- ステップ 4** [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。
- [Opt in Message] : オプトインメッセージを入力します。
  - [Default Opt-In Check Box Behavior]
    - [Checked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックします。
    - [Unchecked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

- ステップ 5** 変更内容を保存します。

キャプティブポータルアプリの左ペインに表示される [Access Code] オプションを使用して、アクセスコードを作成し、顧客と共有することができます。アクセスコードの作成と共有の詳細については、[アクセスコード \(58 ページ\)](#) を参照してください。

#### 次のタスク



- (注) [Data Capture] または [User Agreements] が有効になっている場合の [Access Code] 認証タイプのポータル。この認証モジュールの詳細については、[認証モジュール \(19 ページ\)](#) を参照してください。

## 認証なしでのポータルの設定

ポータルを認証なしで設定するには、次の手順を実行します。

### 手順

- ステップ 1** ポータルを作成するときに、[Authentication Type] ドロップダウンリストから [No Authentication] を選択します。
- ステップ 2** ポータルホームページにデータキャプチャとユーザーの同意を表示する場合は、[Display Data Capture and User Agreements on portal home page] チェックボックスをオンにします。
- ステップ 3** 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。
- ステップ 4** [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。

- [Opt in Message] : オプトインメッセージを入力します。
- [Default Opt-In Check Box Behavior]
  - [Checked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態に表示されるようにする場合は、このオプションをクリックします。
  - [Unchecked] : 顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態に表示されるようにする場合は、このオプションをクリックします。

ステップ5 変更内容を保存します。

## インライン認証

キャプティブポータルでは、認証を他のモジュールとともにインラインモジュールとして追加できます。つまり、顧客がキャプティブポータル内のリンクをクリックする前に認証オプションが表示されるため、認証プロセスを開始するために必要なクリック数が削減されます。

インライン認証を設定するには、[Authentication] 画面で、インライン認証を設定するためのチェックボックスをオンにします。

[SMS with Link verification] 認証タイプと [SMS with password verification] 認証タイプの場合、認証セクションには、携帯電話番号を入力するフィールドと [Connect] ボタンがあります。電子メール認証の場合、認証セクションには電子メールIDを入力するフィールドがあります。ソーシャル認証の場合、認証セクションには、ポータル用に設定されたソーシャルネットワークごとに関連するボタンがあり、顧客はこのボタンを使用してソーシャルネットワーク経由で認証を完了することができます。

## 認証モジュール

ポータルの認証タイプを選択すると、選択した認証タイプに基づいて、ポータルの認証モジュールが作成されます。

ポータルの認証タイプとして [No Authentication] または [Access Code] を選択したときに、[Data Capture] または [User Agreements] のいずれかが有効になっていない場合、そのポータルの認証モジュールは作成されません。

認証モジュールには、ポータルの代替ランディングページを指定するフィールドがあります。

## ポータルへのデータキャプチャフォームの追加

ポータルで [Social Sign In] 以外の認証タイプを選択した場合、キャプティブポータルにデータキャプチャフォームを追加できます。ポータルの作成時に、データキャプチャフォームにフィールドを追加できます。顧客の名、姓、携帯電話番号などの詳細をキャプチャするように、フィールドを設定できます。顧客のフィルタリング基準となるビジネス タグの追加もできます。



(注) データキャプチャフォームで定義されたビジネスタグは、キャプティブポータルルール、エンゲージメントルール、プロフィールルールなどのルールで使用可能な [Add Tags] オプションで使用できます。

キャプティブポータルでデータキャプチャフォームを設定するには、次の手順を実行します。

## 手順

**ステップ 1** ポータルを作成する場合は、利用規約を指定した後、[Next] をクリックします。

データキャプチャの画面が表示されます。

**ステップ 2** [Data Capture] チェックボックスを有効にします。

**ステップ 3** [Add Field Element] をクリックします。

データキャプチャフォームには、次のフィールド要素を追加できます。

- [Title] : 顧客の敬称を指定します。たとえば、Mr、Ms などです。このフィールドを設定すると、顧客獲得（ランタイム）中に、この Title、Mr および Ms が顧客のデータキャプチャフォームで選択できるようになります。
- [Email] : 顧客の電子メール ID を指定します。
- [Mobile Number] : 顧客の携帯電話の番号を指定します。携帯電話の番号のデフォルトの国を指定すると、顧客獲得の際にデフォルトの国のコードがデータキャプチャフォームに表示されるようになります。
- [First Name] : 顧客の名を指定します。
- [Last Name] : 顧客の姓を指定します。
- [Gender] : 顧客の性別を指定します。
- [Date of Birth] : 顧客の生年月日を指定します。[Date of Birth] フィールドを追加すると、[User Agreements] ウィンドウの [Enable Age Gating] エリアで [Moderate] オプションを選択できなくなります。
- [Business Tags] : ビジネスタグ質問に対して顧客が選択する回答を提供します。このビジネスタグは、顧客の分類に役立ちます。
- 国固有のフィールド
  - 郵便番号 : 住所の郵便番号を提供します。
  - CPF : CPF を提供します（これはブラジルにのみ適用されます）。

(注)

[Email] フィールド要素は、**Email**認証の場合、電子メール情報は認証時にすでに収集されているため、使用できません。[Mobile Number] フィールド要素は、顧客が認証時に携帯電話番号を入力する必要があるため、**SMS with password verification** 認証では使用できません。

**ステップ 4** 対応するオプションをクリックして、フィールドを追加します。

#### 一般のフィールド

- [Place Holder] フィールドには、フィールドのプレースホルダとして表示する必要があるテキストを入力します。
- フィールドを必須にするには、[Make this field mandatory] チェックボックスをオンにします。

#### 要素固有のフィールド

- [Mobile Number] フィールド要素では、デフォルトの国を選択し、顧客獲得時にその国の国コードがデータキャプチャフォームに表示されるようにします。
- [Zip/Postal Code] フィールド要素では、[Country] ドロップダウンリストから国を選択します。これにより、顧客はデータキャプチャフォームで特定の国の郵便番号を追加できます。複数の国の郵便番号をサポートするには、[Add Country] をクリックして、別の国を追加します。
- [Business Tag] フィールド要素には、次の追加フィールドを設定する必要があります。
  - [Name] フィールドには、ビジネスタグの名前を入力します。
  - [Field Label] フィールドには、顧客に尋ねる質問を入力します。
  - [+Add Option] をクリックします。
  - 表示されるフィールドに、顧客が選択するために提供する回答を入力します。
  - その他の回答用選択肢も、同様に、[+ Add Option] を使用して追加します。

(注)

追加した選択肢を削除するには、対応する [Delete] アイコンを使用します。

(注)

顧客が認証プロセス中に [Data Capture] フォームにアクセスすると、指定した回答がドロップダウンリストで使用できるようになります。顧客は必要な値を選択できます。この値は、プロキシミティールールで顧客をフィルタリングするのに使用できます。

**ステップ 5** 変更内容を保存します。

(注)

顧客獲得時に、**データキャプチャ**フォームの [CPF] フィールドに入力された値は、「000.000.000-00」形式に変換されます。ユーザーが CPF の数値を入力すると、数値は自動的にフォーマットされます。したがって、キャプティブポータルのユーザーは、必要な形式を維持するためにドットやハイフンを手動で追加する必要はありません。

## ポータルのブランド名の定義

Cisco Spaces では **Header/Branding** モジュールを使用してポータルにブランド名とページタイトルを追加できます。ブランド名は、テキストまたはイメージとして追加できます。たとえば、会社ロゴをブランド名として使用することができます。

ポータルのブランド名とページタイトルを定義するには、次の手順を実行します。

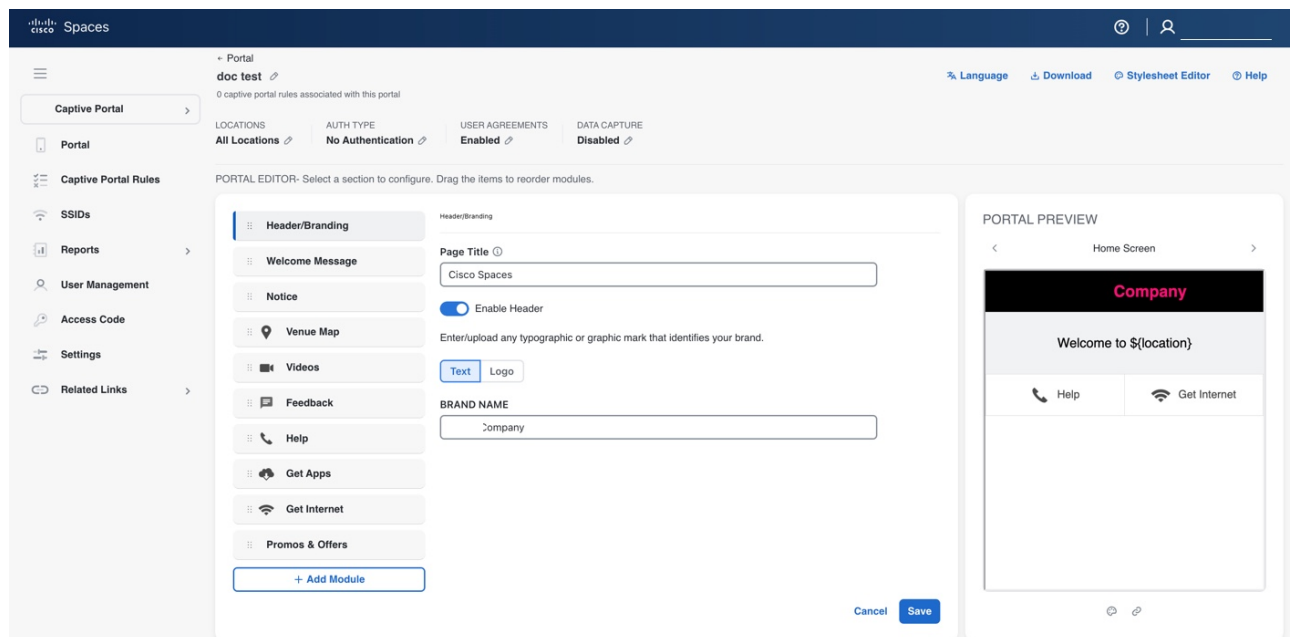
### 手順

**ステップ 1** ブランド名を定義するポータルを開きます。

**ステップ 2** [ヘッダー/ブランディング (Header/Branding) ]モジュールをクリックします。

**ステップ 3** [ページタイトル (Page Title) ]フィールドで、ページタイトルを編集します。

図 2: Header/Branding モジュール



### (注)

- 既存のポータルのページタイトルは、デフォルトで **Cisco Spaces** になります。新規作成されたポータルでは、アカウント名がデフォルトのページタイトルとなります。ページタイトルは編集できます。
- この機能は、Cisco Spaces のベータ版 UI でのみ使用できます。

**ステップ 4** [ヘッダーの有効化 (Enable Header) ]をクリックして、ポータルプレビューを表示します。

**ステップ 5** ブランドのタイプを選択します。

- [Text only] を選択する場合は、表示される [Brand Name] フィールドにブランド名を入力します。

- b) [Logo] を選択する場合は、表示される [Upload] ボタンをクリックし、ロゴイメージをアップロードします。

**ステップ 6** [Save] をクリックします。

ポータルにブランド名とページタイトルが正常に定義されます。

### 次のタスク



- (注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save & Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルへのウェルカムメッセージの追加

[Welcome] モジュールを使用すると、ポータルにウェルカムメッセージを追加することができます。追加されたウェルカムメッセージは、顧客がポータルにアクセスした際に表示されます。初回ユーザーとリピーターユーザーに異なるウェルカムメッセージを表示するように設定できます。

ポータルにウェルカムメッセージを追加するには、次の手順を実行します。

### 手順

**ステップ 1** ウェルカムメッセージの追加が必要なポータルを開きます。

**ステップ 2** [Welcome Message] モジュールをクリックします。

[Welcome Message] ウィンドウが表示されます。

**ステップ 3** [First time visitor welcome text] フィールドで、顧客が初めてポータルにアクセスした際に表示する必要があるウェルカムメッセージを入力します。Smart Link 変数を使用して、ロケーションの詳細を含めることができます。Smart Link の詳細については、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。

**ステップ 4** リピーターユーザーには別のウェルカムメッセージを表示する場合は、[Add a custom message for Repeat Visitors] チェックボックスがオンになっていることを確認し、その隣のテキストボックスに、再訪ユーザーのためのウェルカムメッセージを入力します。Smart Link 変数を使用して、名前とロケーションの詳細を含めることができます。変数「firstName」および「lastName」は、ポータルで [Data Capture] モジュールを [First Name] および [Last Name] フィールドを使用して構成した場合にのみ選択できます。変数「firstName」およ

び「lastName」は、「Social Sign In」以外の認証タイプで使用できます。Smart Link の詳細については、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。

**ステップ 5** [Save] をクリックします。

ポータルにウェルカム メッセージが定義されます。

### 次のタスク



- (注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルへの通知の追加

[Notice] モジュールでは、ポータル内に通知を表示することができます。このモジュールは、顧客に重要な情報を伝える際に便利です。ティックャーおよびテキストの通知を追加できます。テキストの通知とともにイメージを追加することもできます。

通知をいつまでポータル内に表示するかの日付を設定できます。

ポータル内の通知をダッシュボードから追加するには、次の手順を実行します。

### 手順

**ステップ 1** 通知を追加するポータルを開きます。

**ステップ 2** [Notice] モジュールをクリックします。

[Notice] ウィンドウが表示されます。

**ステップ 3** 必要な通知の種類をクリックします。次のオプションを使用できます。

- [Ticker Text Only] : 通知は、動くテキストの形式で表示されます。[Ticker Text Only] の場合、表示される [Notice] フィールドに通知のテキストを入力します。
- [Text Only] : 通知は、テキスト形式で表示されます。[Text Only] の場合、表示される [Notice] フィールドに通知のテキストを入力します。
- [Text with Image] : 通知は、アップロードされたイメージを伴うテキストとして表示されます。[Text with Image] の場合、以下の手順を実行します。
  - [Notice] フィールドに、通知のテキストを入力します。

- [Notice image] エリアで、[Upload] ボタンをクリックし、通知と一緒に表示する必要があるイメージをアップロードします。

**ステップ 4** [Hide After] フィールドで、通知をいつまでポータル内に表示するかの日付を選択します。

**ステップ 5** [Save] をクリックします。

ポータルに通知が追加されます。

---

### 次のタスク



- (注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルール作成の詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。
- 

## ポータルでの施設詳細の表示

[Venue Map] モジュールを使用すると、ポータル内に施設の詳細を表示することができます。このモジュールを使用すると、施設に対し、ラベル名の定義、アイコンイメージのアップロード、およびマップの表示をすることができます。

このモジュールのデフォルト名は、[Venue Map] です。モジュール名は、[Label] フィールドで加える変更に応じて変更されます。

ポータルに施設の詳細を追加するには、次の手順を実行します。

### 手順

---

**ステップ 1** 施設の詳細を追加するポータルを開きます。

**ステップ 2** [Venue Map] モジュールをクリックします。

[VENUE MAP] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、ポータルに表示される施設マップのラベル名を入力します。

(注)

[Venue Map] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

**ステップ 4** [Icon] 領域で、マップラベルの隣に表示されるマップアイコンを、[Upload] ボタンを使用してアップロードします。

(注)

アイコンを削除するには、[Delete] アイコンを使用します。

**ステップ 5** [Store Map] 領域に、この施設のマップが、ワイヤレスネットワークと同様に表示されます。

(注)

マップは、ワイヤレスネットワーク (CUWN、Meraki) でマップが定義されているロケーションにポータルが関連付けられている場合のみ、表示されます。顧客が現在いるロケーションのマップが表示されます。

**ステップ 6** [Save] をクリックします。

ポータルに施設マップが設定されます。

---

### 次のタスク



(注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

---

## ポータルへのビデオのアップロード

[Videos] モジュールを使用して、Cisco DNA Spaces のポータルにビデオをアップロードできます。このモジュールでは、ポータル内のビデオが表示される領域にラベルとイメージを追加することと、ビデオの YouTube URL を指定することができます。

このモジュールのデフォルト名は、[Videos] です。モジュール名は、[Label] フィールドで加える変更に応じて変更されます。



(注) ポータルに表示できるのは、YouTube のビデオのみです。

---

ポータルにビデオをアップロードするには、次の手順を実行します。

### 手順

---

**ステップ 1** ビデオをアップロードするポータルを開きます。

**ステップ 2** [Videos] モジュールをクリックします。

[VIDEOS] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、ポータル内のビデオが表示される領域のために表示が必要なラベルを入力します。

(注)

[Videos] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

**ステップ 4** [Icon] 領域で、ビデオラベルの隣に表示が必要なビデオアイコンを、[Upload] ボタンを使用してアップロードします。

(注)

アイコンを削除するには、[Delete] アイコンを使用します。

**ステップ 5** [Add a Video] をクリックします。

**ステップ 6** 表示される [YouTube URL] フィールドに、ポータルに表示するビデオの YouTube URL を入力します。

**ステップ 7** [Save] をクリックします。

ポータルにビデオがアップロードされます。

---

### 次のタスク



- (注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。
- 

## ポータルでの [Feedback] セクションの提供

Cisco DNA Spaces の [Feedback] モジュールを使用すると、ポータルの顧客からフィードバックを収集することができます。このモジュールでは、[Feedback] セクションに複数の質問を追加することができます。これらの質問には、選択肢による回答または評価による回答を付加できます。顧客がコメントを追加できるテキストボックスを提供することもできます。

ポータルに [Feedback] セクションを追加するには、次の手順を実行します。

### 手順

**ステップ 1** フィードバックセクションを追加する必要があるポータルを開きます。

**ステップ 2** [Feedback] モジュールをクリックします。  
[FEEDBACK] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、[Feedback] セクションに表示する必要がある名前を入力します。

- ステップ 4** [Icon] エリアで、フィードバックラベルの隣に表示する必要があるアイコンイメージを、[Upload] ボタンを使用してアップロードします。
- ステップ 5** [Question] フィールドに、顧客に回答してほしい質問を入力します。
- ステップ 6** [Image] エリアで、質問の隣に表示する必要があるイメージを、[Upload] ボタンを使用してアップロードします。
- ステップ 7** [Question Type] エリアで、次のいずれかを選択します。
- [Rating] : 顧客は、評価で質問に回答できます。
  - [Multiple Choice] : 顧客は、提供される複数の選択肢から回答できます。このオプションを選択した場合、[Option 1] および [Option 2] フィールドに回答の選択肢を入力します。提供する選択肢の数を増やす場合は、[Add option] ボタンを使って選択肢を追加します。
- (注)  
[feedback] セクションに質問を追加するには、[Add question] ボタンを使用します。
- ステップ 8** [Submit Button Label] フィールドに、顧客が回答の提出に使用する送信ボタンの名前を入力します。
- ステップ 9** [Thank You/Success message] フィールドに、顧客が回答を提出した後に顧客に表示されるメッセージを入力します。
- ステップ 10** [Post Submission button label] フィールドに、顧客の回答が提出された後に表示されるボタンの名前を入力します。顧客がこのボタンをクリックすると、Cisco DNA Spaces ダッシュボードが表示されます。
- ステップ 11** 顧客がコメントを入力するためのテキストボックスを提供するには、[Add a text box for additional comments from end user?] チェックボックスをオンにします。
- ステップ 12** [Email to] フィールドに、フィードバックを送信する宛先の電子メールアドレスを入力します。
- ステップ 13** [Email from] フィールドに、フィードバックメールの受信者に表示する [From] 電子メールアドレスを入力します。
- ステップ 14** [Email Subject] フィールドに、フィードバックを含む電子メールの件名を入力します。
- ステップ 15** [Save] をクリックします。
- ポータルに [Feedback] セクションが作成されます。

---

### 次のタスク



- (注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。
-

## ポータルへのヘルプ オプションの追加

[Help] モジュールを使用すると、Cisco DNA Spaces のポータルにヘルプラインを追加することができます。顧客は、サポートが必要な際に、このヘルプラインを使用して連絡することができます。このモジュールでは、ポータル内のヘルプラインが表示される領域にラベルとイメージを追加することと、顧客がサポートが必要な際に連絡する番号を指定することができます。

このモジュールのデフォルト名は、[Help] です。モジュール名は、[Label] フィールドで加える変更に応じて変更されます。

ポータルにヘルプ オプションを追加するには、次の手順を実行します。

### 手順

**ステップ 1** ヘルプ オプションの追加が必要なポータルを開きます。

**ステップ 2** [Help] モジュールをクリックします。

[HELP] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、ポータル内のヘルプラインが表示される領域に表示されるラベルを入力します。

(注)

[Help] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

**ステップ 4** [Icon] 領域で、ヘルプラベルの隣に表示されるヘルプアイコンを、[Upload] ボタンを使用してアップロードします。

(注)

アイコンを削除するには、[Delete] アイコンを使用します。

**ステップ 5** [Contact] フィールドに、ヘルプラインの番号を入力します。

**ステップ 6** **Save** をクリックします。

ポータルにヘルプ オプションが定義されます。

### 次のタスク



(注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルへのアプリケーションの追加

アプリケーションモジュールを使用すると、Cisco DNA Spaces ポータルにアプリケーションを追加することができます。アプリケーションは、iOS アプリストアと Play Store の両方から追加できます。このモジュールでは、ポータル内のアプリケーションが表示される領域にラベルとイメージを追加することができます。

このモジュールのデフォルト名は、[Get Apps] です。モジュール名は、[Button Label] フィールドで加える変更に応じて変更されます。

ポータルにアプリケーションを追加するには、次の手順を実行します。

### 手順

**ステップ 1** アプリケーションの追加が必要なポータルを開きます。

**ステップ 2** [Get Apps] モジュールをクリックします。

[GET APPS] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、ポータル内のアプリケーションが表示される領域に表示されるラベルを入力します。

(注)

[Get Apps] モジュール名が、[Label] フィールドで指定した名前に変更されます。

**ステップ 4** [Icon] 領域で、アプリケーションラベルの隣に表示が必要なアプリケーションアイコンを、[Upload] ボタンを使用してアップロードします。

(注)

アイコンを削除するには、[Delete] アイコンを使用します。

**ステップ 5** [Add an App] をクリックします。

**ステップ 6** [Add App] 領域で、次の手順を実行します。

- a) [Platform] ドロップダウンリストから、アプリケーションプラットフォームを選択します。
- b) [App Store URL] フィールドに、そこからアプリケーションを追加するアプリケーションストアの URL を入力します。
- c) [App URL Scheme] フィールドに、デバイスにアプリケーションをインストールする際に受け取るアプリケーションの URL スキームを入力します。
- d) デスクトップおよびラップトップに別の URL を提供する場合は、[Show this URL for Desktops and Laptops] チェックボックスをオンにします。
- e) [Show this URL for Desktops and Laptops] チェックボックスをオンにしたら、デスクトップおよびラップトップのための URL を入力します。

(注)

アプリケーションをさらに追加するには、[Add an App] ボタンを使用します。

**ステップ 7** [Save] をクリックします。

ポータルにアプリケーションが追加されます。

### 次のタスク



- (注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルからのインターネットへのアクセスの提供

[Get Internet] モジュールを使用すると、ポータルからインターネットへのアクセスを提供することができます。[Get Internet] モジュールを使用すると、外部 URL をポータルに追加することができます。このモジュールでは、ポータル内のインターネットリンクが表示される領域にラベルとイメージを追加することができます。

このモジュールのデフォルト名は、[Get Internet] です。モジュール名は、[Button Label] フィールドで加える変更に応じて変更されます。



- (注) キャプティブポータルにインライン認証が設定されている場合、[Get Internet] モジュールは、設定されていても、顧客の獲得中に表示されません。インライン認証の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。

ポータルからインターネットへのアクセスを提供するには、次の手順を実行します。

### 手順

**ステップ 1** インターネットへのリンクの提供が必要なポータルを開きます。

**ステップ 2** [Get Internet] モジュールをクリックします。

[GET INTERNET] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、ポータル内のインターネットリンクが表示されるエリアに表示されるラベルを入力します。

(注)

[Get Internet] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

**ステップ 4** インターネットリンクの隣に表示が必要なアイコンを、[Upload] ボタンを使用してアップロードします。

(注)

[Delete] アイコンを使用して、画像を削除できます。

**ステップ 5** ランディングページを変更するには、[Change Landing page URL] チェックボックスがオンになっていることを確認します。

**ステップ 6** [Launch Page] フィールドに、ポータルからインターネットに接続するための URL を入力します。

**ステップ 7** [Save] をクリックします。

ポータルにインターネットにアクセスするためのオプションが設定されます。

### 次のタスク



(注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルへのプロモーションとオファーの追加

[Promos & Offers] モジュールでは、顧客に提供するプロモーションおよびオファーをポータルに追加することができます。さまざまなプロモーション URL にリンクできるさまざまなプロモーションアイテムをポータルに追加できます。このモジュールでは、各プロモーションにラベル、アイコン、および Web URL を追加することができます。



(注) プロモーションは回転式で表示されます。

ポータルにプロモーションとオファーを追加するには、次の手順を実行します。

### 手順

**ステップ 1** [Promos & Offers] モジュールを追加するポータルを開きます。

**ステップ 2** [Promos & Offers] モジュールをクリックします。

[Promos & Offers] ウィンドウが表示されます。

**ステップ 3** [Label] フィールドに、プロモーションとオファーが表示されるエリアに表示されるラベルを入力します。

**ステップ 4** [Add a Promotion] をクリックします。

**ステップ 5** [Promo Name] フィールドに、プロモーションリンクの名前を入力します。

**ステップ 6** [Promo Image] エリアで、プロモーションリンクの隣に表示する必要があるアイコンを、[Upload] ボタンを使用してアップロードします。

**ステップ 7** [Link Promo to URL] フィールドに、プロモーション Web ページにリンクする URL を入力します。

**ステップ 8** [Save] をクリックします。

ポータルにプロモーションおよびオファーが追加されます。

#### 次のタスク



(注) [Add a Promotion] ボタンを使用すると、ポータルに複数のプロモーションを追加できます。



(注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルからのプロモーションおよびオファーの削除

Cisco DNA Spaces では、必要な期間の後、ポータルからプロモーションを削除することができます。

ポータルからプロモーションを削除するには、次の手順を実行します。

#### 手順

**ステップ 1** プロモーションを削除するポータルを開きます。

**ステップ 2** [Promos & Offers] モジュールをクリックします。

[PROMOS and OFFERS] ウィンドウが表示され、そのポータルに追加されているプロモーションが示されます。

**ステップ 3** 削除するプロモーションの右上に表示されている [Delete] アイコンをクリックします。

## カスタムのコンテンツとメニューアイテムのポータルへの追加

[Add Module] モジュールでは、要件に応じてポータルにカスタムのコンテンツやメニューアイテムを追加することができます。さまざまな Web ページにリンクできるさまざまなメニューアイテムをポータルに追加できます。このモジュールでは、各メニューアイテムにラベル、アイコン、および Web URL を追加することができます。リンク先の Web ページに互換性がある場合、「戻る」ボタンを有効にすることもできます。

カスタマイズしたメニューアイテムをポータルに追加するには、次の手順を実行します。

### 手順

**ステップ 1** カスタム メニュー アイテムの追加が必要なポータルを開きます。

**ステップ 2** [Add Module] をクリックします。

**ステップ 3** 次のいずれかを選択します。

- [Custom Content] : カスタマイズした追加テキストをポータルに含めます。
- [Menu Item] : Web ページにリンクするメニューアイテムをポータルに含めます。

カスタムモジュールがポータルモジュールリストに追加され、そのページが開きます。カスタムモジュールに表示されるフィールドは、カスタムモジュールのタイプによって異なります。

**ステップ 4** [Custom Content] の場合、カスタムモジュールに関する以下の詳細を入力します。

- [HTML Module Name] フィールドに、モジュールの名前を入力します。
- [Rich] フィールドにコンテンツを追加します。

**ステップ 5** [Menu Item] フィールドの場合、カスタムモジュールの次の詳細を入力します。

- a) [Label] フィールドに、カスタムメニューアイテムに表示されるラベルを入力します。

(注)

[Menu Item] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

- b) [Icon] 領域で、メニュー アイテムの隣に表示が必要なアイコンを、[Upload] ボタンを使用してアップロードします。

(注)

アイコンを削除するには、[Delete] アイコンを使用します。

- c) [Link to URL] フィールドに、メニューアイテムのリンク先 URL を入力します。

(注)

Smart Link オプションを使用すると、URL を強化することができます。[Add Variable] ドロップダウンリストをクリックして追加できる変数を表示します。スマートリンクの作成についての詳細は、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。

**ステップ 6** リンク先 Web ページの「戻る」ボタンを有効にするには、[Enable Back button] チェックボックスをオンにします。

**ステップ 7** [保存 (Save)] をクリックします。

カスタマイズされたコンテンツまたはメニューアイテムがポータルに正常に追加されます。

### 次のタスク



(注) 追加されたメニューアイテムは、ポータルのプレビューではテキストとして表示されますが、実行時にはリンクとして表示されます。



(注) パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルール作成の詳細については、[キャプティブポータルを表示するためのキャプティブポータルルールの作成 \(44 ページ\)](#) を参照してください。

## ポータルのエクスポート

Cisco DNA Spaces では、各種ポータルモジュールを使用して作成したポータルをエクスポートすることができます。

ポータルをエクスポートするには、次の手順を実行します。

### 手順

**ステップ 1** エクスポートするポータルを開きます。

**ステップ 2** [Portal] ウィンドウの上部にある [Export Portal] アイコンをクリックします。

[Export Portal] ダイアログボックスが表示されます。

**ステップ 3** [Download] をクリックします。

**ステップ 4** 表示されるウィンドウで、次のいずれかを実行します。

- エクスポートされたファイルを直接開くには、[Open] を選択します。
- ポータルファイルをコンピュータに保存するには、[Save File] を選択します。

ポータルの zip ファイルがコンピュータの [ダウンロード] フォルダに保存されます。

(注)

ポータルは、zip 形式でエクスポートされます。

---

## ポータルのスタイルシートの編集

Cisco DNA Spaces の [Style Sheet Editor] オプションでは、ポータルのスタイルシートを更新することができます。これは、ポータルのフォント プロパティや外観を変更するのに役立ちます。

ポータルのスタイルシートを編集するには、次の手順を実行します。

### 手順

---

- ステップ1 スタイルシートを編集するポータルを開きます。
  - ステップ2 [Portal] ウィンドウの上部にある [Stylesheet Editor] をクリックします。
  - ステップ3 [CSS Editor] タブで、スタイルシートに必要な変更を加えます。
  - ステップ4 [Save] をクリックします。
- 

### 次のタスク

スタイルシートを外部ソースからアップロードすることができます。たとえば、別のポータルのためにデザインされた CSS などです。

また、スタイルシートをダウンロードして必要な更新を行い、編集したスタイルシートをアップロードすることもできます。たとえば、CSS デザイナーにポータルの編集を依頼する場合、[Download CSS] ボタンを使用してスタイルシートをダウンロードすることができます。スタイルシートに必要な変更を加えた後、[Upload CSS] ボタンを使用して Cisco DNA Spaces にアップロードすることができます。

## スタイルシートへのアセットの追加

ポータルの外観を強化するため、イメージやフォントなどのアセットをポータルの [Style Sheet Editor] に追加することができます。jpeg、png、tif などのイメージファイルが追加できます。スタイルシートを編集し、これらのアセットをポータルに組み込みます。

ポータルのスタイルシートにアセットを追加するには、次の手順を実行します。

### 手順

---

- ステップ1 スタイルシートを編集するポータルを開きます。
- ステップ2 [Stylesheet Editor] をクリックします。

**ステップ3** [Asset Library] タブをクリックします。

**ステップ4** アセットファイルをドラッグアンドドロップするか、[Choose File] ボタンを使用してアップロードします。

(注)

キャプティブポータルのアセットライブラリに新しいアセットをアップロードする場合、添付ファイルごとにサポートされる最大ファイルサイズは 15 MB です。

ファイルがアセット リストに追加されます。

### 次のタスク

アセット下部のアセットで表示される [Copy Asset url] ボタンを使用して、アセットの URL をコピーすることができます。このアセットをポータルに追加するには、スタイルシートの適切な場所に URL を追加します。

アセットを削除するには、アセットリスト内のそのアセットに表示された [Delete] アイコンを使用します。

## ポータルのインポート

Cisco DNA Spaces では、外部パスからポータルをインポートすることができます。たとえば、外部アプリケーションを使用してポータルを強化する場合、[Export Portal] アイコンを使用してポータルをエクスポートし、必要な強化を加え、[Import Portal] オプションを使用してポータルファイルを Cisco DNA Spaces にインポートすることができます。

ポータルをインポートするには、次の手順を実行します。

### 手順

**ステップ1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

**ステップ2** 表示されるウィンドウで、[Captive Portal] をクリックします。

**ステップ3** [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。

[Captive Portal] ウィンドウが表示されます。

**ステップ4** ウィンドウの右上にある [Import Portal] をクリックします。

**ステップ5** 表示される [Import Portal] ウィンドウで、次の手順を実行します。

- [Portal Name] フィールドに、ポータルのファイル名を入力します。
- ウィンドウにポータルをドラッグアンドドロップし、[Choose File] ボタンをクリックして、インポートするファイルを選択します。
- このポータルをすべてのロケーションで使用できるようにする場合は、[Add all locations to this portal] チェックボックスがオンになっていることを確認します。選択したロケーションでのみポータルを使用できるようにする場合は、[Add all locations to this portal] チェックボックスをオフにして、ポータルを使用できるようにする必要があるロケーションを選択します。

ウィンドウの右側に選択したロケーションが表示されます。

ステップ6 [Import] をクリックします。

#### 次のタスク



(注) ポータルは、zip 形式でアップロードされます。

## ポータルの削除

ポータルを削除するには、次の手順を実行します。

### 手順

ステップ1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ3 [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。

[Captive Portal] ウィンドウが表示され、Cisco DNA Spaces 内で使用可能なポータルのリストが表示されます。

ステップ4 削除するポータルの右端に表示される [Delete] アイコンをクリックします。

ステップ5 表示される [Delete Portals] ウィンドウで、[Yes] をクリックします。

ポータルが Cisco DNA Spaces から削除されます。

(注)

削除するポータルの隣のチェックボックスを複数選択し、ウィンドウの下部に表示される [Delete] ボタンをクリックすると、複数のポータルを同時に削除できます。

(注)

キャプティブポータルルールに関連付けられているポータルは、削除できません。

## ポータルの編集

ポータルを編集するには、次の手順を実行します。

## 手順

- 
- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
  - ステップ 2** 表示されるウィンドウで、[Captive Portal] をクリックします。
  - ステップ 3** [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。  
[Captive Portal] ウィンドウが表示され、Cisco DNA Spaces 内で使用可能なポータルのリストが表示されます。
  - ステップ 4** 編集するポータルの右端に表示される [Edit] アイコンをクリックします。
  - ステップ 5** 必要な変更を行い、各モジュールに加えた変更を保存します。
  - ステップ 6** 変更をパブリッシュするには、そのポータルの [Save and Publish] ボタンをクリックします。
- 

## ポータルのロケーションの編集

ポータルのロケーションを編集するには、次の手順を実行します。

## 手順

- 
- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
  - ステップ 2** 表示されるウィンドウで、[Captive Portal] をクリックします。
  - ステップ 3** [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。
  - ステップ 4** [Captive Portal] ウィンドウが表示されたら、ロケーションを編集するポータルのチェックボックスをオンにします。
  - ステップ 5** ウィンドウの下部に表示される [Add to Locations] をクリックします。
  - ステップ 6** 表示される [Add Locations to Portals] ウィンドウで、ポータルのロケーションを選択し、[Save Changes] をクリックします。
  - ステップ 7** 変更をパブリッシュするには、そのポータルの [Save and Publish] ボタンをクリックします。
- 

## ポータルプレビュー URL の電子メールでの送信

ポータルのプレビュー URL を電子メールで送信し、受信者がその URL を使用してポータルをプレビューできるようにすることが可能です。

ポータルのプレビュー URL を電子メールで送信するには、次の手順を実行します。

## 手順

- 
- ステップ 1** プレビュー URL を電子メールで送信するポータルを開きます。  
ポータルが表示されます。
- ステップ 2** ウィンドウの右端にある [Portal Preview] エリアの [Link] アイコンをクリックします。
- ステップ 3** [Email Portal URL] フィールドに、ポータルプレビュー URL を電子メールで送信する宛先電子メール ID を入力します。
- ステップ 4** [Send] をクリックします。  
URL が指定された電子メールアドレスに送信されたことを知らせるメッセージが表示されます。
- 

## QRコードを使用したポータルのプレビュー

Cisco DNA Spaces では、ポータルの QR コードを使用してポータルをプレビューできます。この機能を使用するには、使用するモバイルに QR コードリーダーアプリをインストールする必要があります。

ポータルの QR コードをスキャンするには、次の手順を実行します。

## 手順

- 
- ステップ 1** QR コードをスキャンするポータルを開きます。
- ステップ 2** ウィンドウの右端にある [Portal Preview] エリアの [Link] アイコンをクリックします。
- ステップ 3** モバイルデバイスで QR コードリーダー アプリケーションを開きます。
- ステップ 4** ポータルで、[Scan with QR code reader on your mobile device] というラベルのエリアに、モバイルデバイスでフォーカスします。  
モバイルデバイスは QR コードをスキャンして、URL を開くかどうか質問するメッセージを表示します。
- ステップ 5** [OK] をクリックします。  
モバイルデバイスの画面にポータルが開きます。
- 

## ポータルのプレビュー

Cisco DNA Spaces では、キャプティブポータルの外観を表示することができます。Cisco DNA Spaces を使用すると、キャプティブポータルで各モジュールを個別にプレビューできます。デフォルトのプレビューは、キャプティブポータルのホーム画面です。認証モジュールのプレ

ビューは、顧客獲得（ランタイム）フローをシミュレートします。モジュールのプレビューは回転式で表示されます。

キャプティブポータルをプレビューするには、次の手順を実行します。

#### 手順

**ステップ1** プレビューを表示するポータルを開きます。

ポータルのホーム画面のプレビューは、[Portal Preview] エリアに表示されます。

**ステップ2** 右向き矢印をクリックし、次の画面に移動します。

## さまざまなデバイスでのポータルのプレビュー

Cisco DNA Spaces では、さまざまなデバイスでキャプティブポータルの外観を表示することができます。モバイルデバイス、タブレット、およびラップトップでのポータルをプレビューすることができます。Cisco DNA Spaces を使用すると、キャプティブポータルで各モジュールを個別にプレビューできます。デフォルトのプレビューは、キャプティブポータルのホーム画面です。

デバイスのキャプティブポータルをプレビューするには、次の手順を実行します。

#### 手順

**ステップ1** さまざまなデバイスでプレビューを表示するポータルを開きます。

デバイスで表示されるポータルのホーム画面のプレビューは、ポータルの右側に表示されます。

CSS エディターウィンドウが表示され、右側のペインにデバイスのプレビューが表示されます。

**ステップ2** 次のいずれかを実行します。

- a) モバイルデバイスでのポータルのプレビューを表示するには、モバイルデバイスのタブをクリックします。
  - b) タブレットでのポータルのプレビューを表示するには、タブレットタブをクリックします。
  - c) ラップトップでのポータルのプレビューを表示するには、ラップトップのタブをクリックします。
- 選択したデバイスでのキャプティブポータル ホーム ページのプレビューが表示されます。

**ステップ3** キャプティブポータルで特定のモジュールをプレビューするには、隣にあるドロップダウンリストからモジュールを選択します。

(注)

[Preview] ウィンドウでその他のデバイスでのプレビューを表示するには、対応するタブをクリックします。[Preview] ウィンドウでは、QR コードのスキャン、ポータルの URL の電子メールでの送信、および向きの変更もできます。

## キャプティブポータル内のモジュールの表示、非表示、順序変更

ポータル管理者は、モジュールの左上にあるオン/オフのトグルスイッチを切り替えることで、ポータルに追加されたモジュールを表示または非表示にすることができます。モジュールを並び替えるには、必要な位置にモジュールをドラッグアンドドロップします。プレビューセッションに変更が反映されます。

## キャプティブポータルルール

キャプティブポータルルールにより、キャプティブポータルの表示および SSID に接続している顧客のインターネットプロビジョニングを管理できます。

キャプティブポータルルールを使用して、次の方法で、キャプティブポータルの表示およびインターネットプロビジョニングを管理できます。

- **キャプティブポータルの表示** : ルールに応じてフィルタリングされた顧客が、そのルールで設定された SSID に接続すると、キャプティブポータルが表示されます。必要な認証手順が完了したら、ポータルのメニュー項目をクリックしてインターネットにアクセスできます。顧客のロケーション、アクセス数、顧客が属するタグ、ロケーションへのアクセス数、アクセス期間などに基づき、顧客に合ったさまざまなキャプティブポータルを表示するように設定できます。セッションごとに、インターネットを提供する必要がある期間を制限することができます。また、このキャプティブポータルルールでインターネットに必要な帯域幅を定義できます。
- **直接インターネットアクセス** : ルールに応じてフィルタリングされた顧客が、ルールで設定された SSID に接続すると、認証プロセスなしで、インターネットが即座に提供されます。この場合、キャプティブポータルは表示されません。
- **インターネットアクセスの拒否** : ルールに応じてフィルタリングされた顧客が SSID に接続しようとする、インターネットが拒否されて接続を確立できません。

また、キャプティブポータルルールにより、次の操作を行うことができます。

- ルールのフィルタリングに基づいてタグを作成するか、または既存のタグを変更します。
- 外部 API へのキャプティブポータルにサインインする顧客の詳細を送信します。

キャプティブポータルルールでは、定義された条件が満たされているときに実行するアクションを設定できます。ロケーション、タグ、顧客のアクセスの数や時間、アプリケーションのステータスなど、さまざまなパラメータに基づいて、ルールに応じて顧客をフィルタリングできます。

この章では、キャプティブポータルルールを作成する方法について説明します。

## キャプティブポータルルール作成の前提条件

- キャプティブポータルルールを適用可能なロケーションを指定するには、ロケーション階層を定義する必要があります。ロケーション階層の定義の詳細については、「ロケーション階層の概要」セクションを参照してください。
- [CMX On Prem] オプションの場合、必要なすべての AP が Cisco CMX に追加されていることを確認します。
- キャプティブポータルを表示するため SSID を指定するには、ワイヤレス ネットワーク システムで作成された SSID を Cisco Spaces にインポートする必要があります。SSID のインポートの詳細については、[#unique\\_173](#)を参照してください。
- キャプティブポータルルールに基づいてキャプティブポータルを表示するには、ポータルを作成する必要があります。キャプティブポータルの作成の詳細については、[ポータルの作成と管理 \(1 ページ\)](#) を参照してください。
- ルールを適用可能なタグを指定するには、タグを定義する必要があります。タグの作成の詳細については、「ロケーションペルソナアプリを使用したタグの作成または変更」のセクションを参照してください。
- キャプティブポータルにサインインした顧客の姓名などの詳細を外部 API に送信するには、キャプティブポータルでデータキャプチャフォームを設定する必要があります。Data Capture フォームがないと、デバイスの MAC アドレスなどの情報のみが外部 API に送信されます。データキャプチャフォーム設定の詳細については、[ポータルへのデータキャプチャフォームの追加 \(19 ページ\)](#) を参照してください。
- キャプティブポータルには RADIUS 認証を使用することを強くお勧めします。RADIUS 認証は、インターネットのシームレスなプロビジョニング、インターネットの拒否、およびセッション期間と帯域幅の定義を許可するために必須です。インターネットプロビジョニングと RADIUS 認証を管理するには、ワイヤレスネットワークで必要な設定を行います。
  - 使用するワイヤレスネットワークが Meraki の場合は、[RADIUS 認証用の Cisco Meraki の設定](#)で説明されている設定を行います。
  - 使用するワイヤレスネットワークが CUWN (Cisco AireOS) の場合は、[インターネットプロビジョニングおよび RADIUS 認証のためのシスコ ワイヤレス コントローラの設定](#)で説明されている設定を行います。
  - ワイヤレスネットワークが Cisco Catalyst 9800 シリーズ コントローラの場合、「[DNA Spaces 上の RADIUS サーバーを使用したキャプティブポータル](#)」に記載されている設定を行います。

## キャプティブポータルを表示するためのキャプティブポータルルールの作成

キャプティブポータルルールを作成する前に、すべての前提条件が満たされていることを確認してください。キャプティブポータルルールを作成するための前提条件については、[キャプティブポータルルール作成の前提条件](#) (43 ページ) を参照してください。

顧客のロケーション、顧客がオプトインユーザーかどうか、顧客が属するタグ、初回ユーザーかリピートユーザーか、顧客のアクセス回数などに基づいて、ルールを適用する顧客をフィルタリングできます。ロケーションまたはそのロケーションに関連付けられているメタデータに基づいて、ルールが適用されるロケーションをフィルタリングできます。指定された時間内に指定したロケーションに顧客がアクセスした回数に基づいて、ルールを適用することもできます。また、特定の期間内の特定の時間だけ、および特定の曜日だけにルールを適用するように設定することもできます。

キャプティブポータルルールにより、ルールに応じてフィルタリングされた顧客が SSID に接続する際に、直接インターネット接続を提供するように設定することもできます。この場合、キャプティブポータルは表示されませんが、顧客はインターネットへアクセスできるようになります。また、キャプティブポータルルールに応じてフィルタリングされた顧客にインターネットアクセスを拒否するようにも設定できます。

キャプティブポータルルールを使用して、新しいタグを作成、またはルールに応じてフィルタリングされた顧客の既存のタグを変更できます。キャプティブポータルルールはまた、ルールで設定されている SSID に接続されている顧客の詳細を外部 API へ送信します。



- (注) シスコ ワイヤレス コントローラが Cisco CMX を介して接続されている場合は、キャプティブポータルルールが機能するために必要なすべての AP が Cisco CMX に追加されていることを確認してください。ロケーション階層を定義した後、新しい AP を Cisco CMX に追加すると、新しく追加された AP はロケーション階層に自動的に表示されます。

ポータルを表示するキャプティブポータルルールを作成するには、次の手順を実行します。

### 手順

- ステップ 1 Cisco DNA Spaces ダッシュボードで、Captive Portal アプリをクリックします。
- ステップ 2 表示される [Captive Portal] ウィンドウで、ダッシュボードの左ペインにある [Captive Portal Rule] をクリックします。
- ステップ 3 ウィンドウの右端にある [Create New Rule] をクリックします。
- ステップ 4 [Rule Name] フィールドに、キャプティブポータルルールの名前を入力します。
- ステップ 5 [Sense] 領域で、次の手順を実行します。
  - a) [When a user is on WiFi] の後のドロップダウンリストから、[WiFi] を選択します。
  - b) [and connected to] の後のドロップダウンリストから、ルールを適用する SSID を選択します。

(注)

SSID は、SSID をインポート/設定した場合にのみ選択することができます。必要な SSID がインポート/設定されていない場合は、ドロップダウンリストに表示されている [Configure SSID] ボタンを使用してインポート/設定できます。[Configure SSID] ボタンを選択すると、[Import/Configure SSID] ウィンドウにリダイレクトされます。SSID のインポート/設定の詳細については、[#unique\\_173](#) を参照してください。

**ステップ 6** [Location] 領域で、ルールを適用するロケーションを指定します。

ロケーション階層全体、グループ、ロケーション、フロア、ゾーンなどの 1 つまたは複数のロケーションにルールを適用するように設定できます。キャプティブポータルルールには Meraki と CUWN の両方のロケーションを追加できます。ロケーション階層の作成に関する詳細については、「ロケーション階層の定義」のセクションを参照してください。

選択したロケーション、またはその親や子のロケーションに定義されているメタデータに基づき、ロケーションを再度フィルタリングできます。ロケーションのメタデータ設定の詳細については、「ロケーションのメタデータの定義または編集」のセクションを参照してください。特定のメタデータのロケーションにルールを適用するか、または特定のメタデータのロケーションを除外することができます。ロケーションのフィルタリングの詳細については、[ロケーションによるフィルタリング \(81 ページ\)](#) を参照してください。

**ステップ 7** [IDENTIFY] 領域で、ルールを適用する顧客のタイプを指定します。

(注)

顧客のオンボーディングステータス、顧客がオプトインユーザーかどうか、顧客が属するタグ、顧客の訪問回数などに基づいてルールを適用する顧客をフィルタリングできます。これらのフィルタをすべて適用することも、要件に応じて一部を適用することもできます。

キャプティブポータルルールを適用する顧客を指定するには、次の手順を実行します。

- 顧客のオンボーディングステータスに基づいて顧客をフィルタリングするには、[Filter by Onboarding Status] チェックボックスをオンにします。オンボーディング済みの顧客（認証プロセスを完了した顧客）をルールでフィルタリングする場合は、[Onboarded Visitor] ラジオボタンをクリックします。オンボーディング済みでない顧客（認証プロセスを完了していない顧客）をルールでフィルタリングする場合は、[Not Onboarded Visitor] ラジオボタンをクリックします。
- オプトインステータスにより顧客をフィルタリングする場合、[Filter by Opt-In Status] チェックボックスをオンにして、オプトインユーザーまたは非オプトインユーザーのどちらかをフィルタリングするかを指定します。オプトインユーザーの詳細については、ページ 6 ~ 5 の「ユーザーのオプトインオプション」を参照してください。
- タグに基づいて顧客をフィルタリングするには、[Filter by Tags] チェックボックスをオンにします。

(注)

2 つの異なる方法でタグをフィルタリングできます。ルールを適用する必要があるタグを指定することも、ルールを適用しないタグを指定することもできます。要件に基づいて、最適なフィルタリング方法を選択できます。たとえば、1 つのタグを除くすべてのタグの顧客にルールを適用する場合、除外オプションを選択し、ルールを適用しない特定のタグを指定する方法が簡単です。

- 選択したタグの顧客にルールが適用されるようにタグを含めるには、[Include] の [Add Tags] ボタンを使用します。

- 除外したタグの顧客にルールを適用しないようにするには、[Exclude] の [Add Tags] ボタンを使用します。

タグフィルタの使用の詳細については、「タグによるフィルタリング」を参照してください。

- d) 選択したロケーションにおける顧客の訪問数に基づいて顧客をフィルタリングするには、[Filter by Previous Visits] チェックボックスをオンにします。

[Add Locations] ボタンをクリックします。[Choose Locations] ウィンドウで、顧客の訪問をフィルタリングの条件にする必要があるロケーションを指定します。次のフィールドで、フィルタリング対象のアクセス数と時間を指定します。自分で設定できる訪問回数と継続時間の詳細については、「以前の訪問の条件」のセクションを参照してください。

**ステップ 8** [Schedule] 領域で、ルールを適用する期間を指定します。

- a) [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドで、キャプティブポータルルールを適用する期間の開始日と終了日を指定します。
- b) [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドに、キャプティブポータルルールを適用する時間範囲を指定します。
- c) 特定の曜日にもみルールを適用する場合、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストからルールを適用する曜日をクリックします。

**ステップ 9** [Actions] 領域で、前述の条件が満たされたときに実行する操作を設定します。

- a) ルールに応じてフィルタリングされた顧客のインターネットのプロビジョニングを管理するには、次から必要なオプションを選択してください。
- [Show Captive Portal] : キャプティブポータルルールに応じてフィルタリングされた顧客が、そのルールで設定された SSID に接続するとキャプティブポータルが表示されるようにするには、このオプションを選択します。[Select Captive Portal] ドロップダウンリストから、このルールで定義された条件を満たすときに表示するキャプティブポータルを選択します。

(注)

選択したロケーションに作成したポータルを選択することができます。必要なポータルを作成していない場合は、[Select Captive Portal] ドロップダウンリストにある [Create Portal] ボタンを使用して作成できます。[Create Portal] ボタンを選択すると、[Create Portal] ウィンドウにリダイレクトされます。ポータルの作成の詳細については、[ポータルの作成 \(5 ページ\)](#) を参照してください。

- あるセッションに対してインターネットが提供される期間を制限する場合は、[Session Duration] チェックボックスをオンにして、表示されるフィールドにセッション期間を入力します。セッション期間は分、時間、または日数で指定できます。
- このキャプティブポータルルールに基づいて顧客に提供されるインターネットの帯域幅を制限する場合は、[Bandwidth] チェックボックスをオンにして、表示される帯域幅バーで帯域幅を指定します。帯域幅は、1 kbps から 1 tbps の範囲で定義できます。

(注)

ここで定義されたセッション期間は、シスコワイヤレスコントローラや Meraki などのワイヤレスネットワークのセッション有効期限の設定を上書きします。そのため、このオプションを使用する

と、ワイヤレスネットワークで設定されているものより長いセッション期間をキャプティブポータルで定義できます。

- **[Seamlessly Provision Internet]** : 顧客が SSID に接続してすぐにインターネットを提供するには、このオプションを選択します。この場合、顧客は認証の手順を実行する必要がありません。このオプションを使用するには、[キャプティブポータルルール作成の前提条件 \(43 ページ\)](#) で説明されているように、シスコワイヤレスコントローラや Meraki などのワイヤレスネットワークで特定の設定を行う必要があります。このオプションに入力するデータは、ワイヤレスネットワークによって異なります。
- **[Rule/Policy Name]** フィールドに、ポリシーの名前を入力します。ワイヤレスネットワークで定義したものと同一名前を指定する必要があります。

(注)

このフィールドは、シスコワイヤレスコントローラまたは Cisco 9800 シリーズワイヤレスコントローラでは必須ではありません。

- セッション期間を指定するには、**[Session Duration]** チェックボックスをオンにして、**[Enter Session Duration]** フィールドに、接続ごとにインターネットアクセスを提供する期間を指定します。
- 帯域幅を指定するには、**[Bandwidth the Limit]** チェックボックスをオンにし、表示される帯域幅バーを使用して帯域幅を指定します。最大で 1 tbps の帯域幅を指定できます。

**[Show Manual Configuration]** オプションを使用して、キャプティブポータルルールで許可される帯域幅を手動で入力することもできます。このオプションを使用すると、事前定義された値ではなく、設定したい正確な帯域幅を指定できます。帯域幅は、KBPS、MBPS、GBPS、または TBPS で指定できます。

(注)

Meraki の場合、Cisco Meraki で設定された帯域幅が考慮されるため、帯域幅フィールドは必須ではありません。

- **[Deny Internet]** : 顧客が SSID に接続しようとしたときに、ルールに応じてフィルタリングされた顧客に対してインターネットを拒否するには、このオプションを選択します。この場合、顧客は SSID への接続が許可されません。
- b) このキャプティブポータルルールに基づいてフィルタリングされた顧客にタグを作成する、または、フィルタリングされた顧客を既存のルールに追加または削除するには、**[Add Tags]** ボタンをクリックします。タグフィルタの使用の詳細については、「[タグによるフィルタリング](#)」セクションを参照してください。
  - c) このルール向けに設定されたキャプティブポータルにサインアップした顧客の名、姓、携帯電話番号などの詳細情報を外部 API に送信する場合は、**[Trigger API]** チェックボックスをオンにして、必要な API 設定を行います。API 設定の詳細については、「[トリガー API の設定](#)」を参照してください。

(注)

ルールの概要がウィンドウの右側に表示されます。

**ステップ 10** **[Save and Publish]** をクリックします。

ルールがパブリッシュされ、[Captive Portal Rules] ウィンドウにリストされます。

(注)

ルールを今すぐパブリッシュしたくない場合、[Save] ボタンをクリックします。ルールを開いて [Save and Publish] ボタンをクリックすることで、後でいつでもルールをパブリッシュできます。また、[Captive Portal Rules] ウィンドウの右側にある [Make Rule Live] アイコンをクリックして、ルールをパブリッシュすることもできます。

## 使用例 : キャプティブポータルルール

XYZ は、モバイルストアからスーパーマーケットまで、さまざまな事業のストリームラインに関わっているビジネスグループです。XYZ はニューヨークの各地に 5 軒のモバイルストアと 4 軒のスーパーマーケットを展開しています。ニューヨークの XYZ の SSID 名は XYZID です。XYZ は顧客が XYZ のスーパーマーケットから XYZID に接続すると、スーパーマーケットのさまざまな品目が利用可能なオファーを表示する、キャプティブポータル C1 を表示したいと考えています。同様に、キャプティブポータル C2 は、XYZ のモバイルストアから XYZID に接続する顧客に表示される必要があります。キャプティブポータルは、オプトインではないユーザーに表示される必要があります。

スーパーマーケットのロケーション : L1、L2、L3、L4、L5

モバイルストアのロケーション : L7、L8、L9、L10

前述のシナリオを実現するには、次の手順を実行します。

### 手順

- ステップ 1 シスコワイヤレスコントローラで、アクセスポイントのモードを定義し、ACLを作成し、SSID「XYZID」を作成します。シスコワイヤレスコントローラの設定に関する詳細については、[#unique\\_178](#)を参照してください。
- ステップ 2 Cisco DNA Spaces にログインします。
- ステップ 3 [Import SSID] オプションを使用して、Cisco DNA Spaces に XYZID を追加します。
- ステップ 4 XYZ のロケーション階層を作成します。ロケーション階層では、ニューヨークの XYZ のすべてのスーパーマーケットとモバイルストアが、ロケーション [New York] に属するロケーションとして定義される必要があります。ロケーション L1、L2、L3、L4、L5 のロケーションメタデータとしてキー [StoreType]、値 [SM] を追加します。ロケーション L7、L8、L9、L10 のロケーションメタデータとしてキー [StoreType]、値 [MS] を追加します。ロケーションメタデータの定義の詳細については、「ロケーションのメタデータの定義または編集」のセクションを参照してください。
- ステップ 5 スーパーマーケットのポータル C1 と、モバイルストアのポータル C2 を作成します。ポータルの作成の詳細については、[ポータルの作成 \(5 ページ\)](#) を参照してください。
- ステップ 6 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
- ステップ 7 表示されるウィンドウで、[Captive Portal] を選択します。

- ステップ 8** [Captive Portal] ウィンドウで、左ペインの [Captive Portal Rule] を選択します。
- ステップ 9** [Create New Rule] をクリックします。
- ステップ 10** [RULE NAME] フィールドに、キャプティブポータルルールの名前「**R1**」を入力します。
- ステップ 11** [When a user is on] ドロップダウンリストから [Wi-Fi] を、[add Connected to] ドロップダウンリストから [XYZID] を選択します。
- ステップ 12** [Locations] 領域で、次の手順を実行します。
- [Add Locations] ボタンをクリックし、表示される [Choose Locations] ウィンドウで、ニューヨークのロケーションを選択し、[OK] をクリックします。
  - [Filter by metadata] チェックボックスをオンにし、フィルタの [Add Metadata] ボタンをクリックします。
  - [Choose Location Metadata] ウィンドウで、キー [StoreType] を選択し、値 [SM] を選択します。
- (注)  
ロケーションメタデータ [StoreType] は、ロケーション [New York] に属するロケーションに対して定義されているため、[Choose Location Metadata] ウィンドウで選択することができます。
- ステップ 13** [Identify] エリアで、[Filter by Opt-In Status] チェックボックスをオンにし、[Only for not opted-in Visitor] を選択します。
- ステップ 14** [Schedule] エリアで、[Set a date range for the rule] チェックボックスをオンにし、開始日に現在の日付を、終了日に今年の最終日を指定します。
- ステップ 15** [Actions] エリアで、[Show Captive Portal] を選択し、[Select Captive Portal] ドロップダウンリストから [C1] を選択します。
- ステップ 16** [Save and Publish] をクリックします。  
ルールがパブリッシュされます。
- ステップ 17** 同様に、ロケーションメタデータキーが [StoreType]、値が [MS]、キャプティブポータルが [C2] の、別のルール **R2** を、モバイルグループ用に作成します。  
これで、顧客が XYZ のスーパーマーケットにアクセスして XYZID に接続すると、**C1** が表示されます。同じ顧客が XYZ のモバイルストアから XYZID に接続すると、**C2** が表示されます。

## SSID

サービスセット識別子 (SSID) は、ワイヤレスネットワーク識別子であり、

- ユーザーが使用デバイスを特定のワイヤレスネットワークに接続できるようにします
- 企業がさまざまな場所にある複数のネットワークを区別して管理できるようにします
- Cisco Spaces 内でさまざまなキャプティブポータルを割り当てるための基礎として機能します。

SSID とは、顧客がインターネットにアクセスするために接続するワイヤレスネットワーク ID を指します。ビジネス拠点に複数の SSID を保持できます。Cisco Spaces では、要件に応じて、ビジネス拠点で同じ SSID またはさまざまな SSID を使用して、異なるキャプティブポータルを表示できます。

SSID は、Cisco Unified Wireless Network (UWN) 向けシスコ ワイヤレス コントローラなどのワイヤレス ネットワーク システムで定義されます。SSID に対してキャプティブポータルを表示するには、SSID を Cisco Spaces にインポートする必要があります。

インポートされた SSID はグリッドビューに表示されます。各 Meraki SSID には、Meraki で SSID を設定できる「Detail」リンクがあります。必要に応じて、ワイヤレスネットワーク用にインポートされた SSID をグリッドから削除できます。

SSID の [手動設定 (Configure Manually)] リンクをクリックすると、対応するワイヤレスネットワークの手動設定方法が表示されます。たとえば、Meraki SSID の [手動設定 (Configure Manually)] リンクは、Cisco Meraki の設定手順につながります。

Cisco Spaces では、SSID が Cisco Meraki などのワイヤレスネットワークから削除されていない場合でも、SSID を削除できます。この機能により、ネットワーク同期に遅延があるときに不要な SSID を削除できます。

## SSID のインポートまたは設定の前提条件

SSID を Cisco Spaces にインポートまたは設定するには、次の手順を実行します。

- ロケーション階層を作成します。このプロセスの詳細については、「[ロケーション階層の概要](#)」を参照してください。
- ワイヤレス ネットワーク システムで SSID を作成します。
  - CUWN 用の SSID を作成するには、「[Cisco DNA Space におけるシスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ コントローラの設定](#)」の章を参照してください。
  - Meraki 用に SSID を作成するには、「[Cisco Meraki での SSID の有効化](#)」セクションを参照してください。
- Meraki の SSID をインポートするには、Cisco Spaces と Meraki が接続されていることを確認してください。通常、この接続は、ロケーション階層を定義するときに確立されます。または、Cisco Spaces ダッシュボードの右上にある [Wi-Fi] アイコンを使用して Meraki に接続することもできます。
- 既存の SSID の場合、ACL リストに現在のドメインとそれぞれの IP を保持することを推奨します。

## ワイヤレスネットワークからの SSID のインポート

SSID をインポートする前に、前提条件が満たされていることを確認してください。SSID をインポートするための前提条件の詳細については、「[SSID のインポートまたは設定の前提条件 \(50 ページ\)](#)」を参照してください。



(注) SSID のキャプティブポータルルールを作成するには、その SSID を CUWN または Meraki からインポートする必要があります。

## シスコワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレスコントローラの SSID のインポート



### Note

- Cisco AireOS シリーズ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、Cisco Spaces に SSID を手動で追加する必要があります。
- Cisco CMX と Cisco AireOS シリーズ ワイヤレス コントローラや Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを使用する場合、SSID は CMX ではなく、シスコワイヤレスコントローラで設定します。
- Cisco Spaces で指定した SSID 名は、コントローラで設定されている SSID 名と一致する必要があります。コントローラダッシュボードで SSID 名を確認します。
- Cisco Spaces クラウド RADIUS サーバーは、Web RADIUS 認証で PAP のみをサポートします。CHAP はサポートされていません。クライアント認証の失敗を回避するには、シスコワイヤレスコントローラで Web RADIUS 認証方式として PAP を設定する必要があります。

SSID を Cisco Spaces に手動でインポートするには、次の手順を実行します。

### Procedure

- ステップ 1 Cisco Spaces ダッシュボードで、[Home] を選択します。
- ステップ 2 [Spaces アプリケーション (Spaces App)] タブの [訪問者オンボーディングおよびエクスペリエンス (Visitor Onboarding & Experiences)] エリアで、[キャプティブポータル (Captive Portal)] をクリックします。
- ステップ 3 表示される [キャプティブポータル (Captive Portal)] ウィンドウで、左ペインの [SSIDs] を選択します。
- ステップ 4 [Import/Configure SSID] をクリックします。
- ステップ 5 表示される [SSID のインポート/設定 (Import/Configure SSID)] ウィンドウで、[ワイヤレスネットワーク (Wireless Network)] ドロップダウンリストから [CUWN (CMX/WLC)] を選択します。
- ステップ 6 [SSID] フィールドに、インポートする SSID の名前を入力し、[Add] をクリックします。

インポートされた SSID が [SSIDs] ウィンドウに表示されます。

#### What to do next



**Note** Cisco Spaces は、インポートされた SSID をロードするにはコントローラと同期させる必要があるため、インポートされた SSID を表示するためにウィンドウを更新する必要があります。

## Cisco Meraki 用の SSID のインポート (GUI)

Cisco Meraki ネットワークから Cisco Spaces に SSID をインポートし、キャプティブポータル機能を有効にして、さらに設定できるようにします。

Meraki の SSID のキャプティブポータルルールを作成するには、Meraki ネットワークからその SSID をインポートする必要があります。SSID をインポートした後、Meraki ダッシュボードで、Cisco Spaces と連携できるように SSID を設定する必要があります。



**Note** ロケーション階層にインポートされるロケーションの SSID のみをインポートできます。

SSID をインポートするには、次の手順を実行します。

### Procedure

- ステップ 1 Cisco Spaces ダッシュボードで、[ホーム (Home)] を選択します。
- ステップ 2 [Spaces アプリケーション (Spaces App)] タブの [訪問者オンボーディングおよびエクスペリエンス (Visitor Onboarding & Experiences)] エリアで、[キャプティブポータル (Captive Portal)] をクリックします。
- ステップ 3 表示される [キャプティブポータル (Captive Portal)] ウィンドウで、左ペインの [SSIDs] を選択します。[Import/Configure SSID] をクリックします。
- ステップ 4 表示される [インポート/設定 (Import/Configure)] ウィンドウで、[ワイヤレスネットワーク (Wireless Network)] ドロップダウンリストから [Meraki] を選択します。
- ステップ 5 [組織 (Organization)] ドロップダウンリストから、SSID をインポートする組織を選択します。  
選択した組織の Meraki で有効になっている SSID を選択できます。
- ステップ 6 インポートする SSID のチェックボックスをオンにして、[Import] をクリックします。  
インポートされた SSID が [SSIDs] ウィンドウに表示されます。
- ステップ 7 その SSID のグリッドで、[Detail] リンクをクリックします。
- ステップ 8 表示されるウィンドウで、[アクティブ化 (Activate)] をクリックして、Meraki の SSID に関する Cisco Spaces の設定を更新します。

[SSID Configuration Sync] ウィンドウに、Meraki で設定する必要がある SSID の更新が表示されます。

ステップ 9 [更新 (Update) ] をクリックします。

**Note**

Meraki で SSID を手動設定することもできます。Meraki で SSID を手動設定する方法については、「Cisco Meraki 用 SSID の手動設定」のセクションを参照してください。

**What to do next**

**Note** インポートされた SSID をロードするために Cisco Spaces を Meraki ネットワークと同期させる必要があるため、SSID を表示するには、ウィンドウの更新が必要になる場合があります。

## レポート

レポートは、データ要約のために次の機能を実行します。

- カスタマイズ可能な期間におけるキャプティブポータルの使用状況に関する洞察を提供
- 複数の場所にまたがる情報の表示
- 特定の場所とタイムフレームに注目してフィルタ処理可能。

Cisco Spaces には、次のキャプティブポータルレポートが用意されています。

デフォルトでは、レポートには過去 1 年間の全ロケーションのデータが含まれます。ロケーションおよび期間でレポートをフィルタ処理できます。

レポートを表示するには、[レポート (Reports) ] を [キャプティブポータル (Captive Portal) ] ウィンドウの左ペインでクリックします。

## デバイスのオンボーディング

デバイスのオンボーディングには、次のレポート機能があります。

- 使用する SSID に接続している各デバイスを識別して記録します。
- 同じ顧客が複数のデバイスで接続した場合でも、顧客固有のデバイス数を提供します。
- オンボーディングレポート内のプロモーションとオファーのエンゲージメントを追跡できます。

デバイスオンボーディングレポートの [プロモーションとオファーのパフォーマンス (Promos & Offers Performance) ] セクションにプロモーションのビュー数が含まれるようになりました。この機能を使用すると、特定のプロモーションのビュー数とクリック数を追跡できます。

## オンボーディングジャーニー

このセクションには、選択したロケーションと期間における一意のデバイスの数が表示されます。

- **SSIDに接続 (Connected to SSID)** : 指定された期間に選択されたロケーションから SSID に接続した一意のデバイスの総数。
- **表示されたキャプティブポータル (Shown Captive Portal)** : 指定された期間に選択されたロケーションから SSID に接続し、キャプティブポータルが正常にロードされた一意のデバイスの総数。
- **プロビジョニングされたインターネット (Provisioned Internet)** : 指定された期間中に、選択されたロケーションからインターネットがプロビジョニングされた一意のデバイスの総数。Cisco Spaces の展開日以降、全ロケーションにおけるこのメトリクスが、[インターネットにプロビジョニングされた一意のデバイスの総数 (Total Unique Devices Provisioned Internet) ] のレポートの上部に表示されます。

## SSID 別の新規および再アクセスデバイスの日次傾向

このセクションには、指定された期間に選択ロケーションから SSID に接続した、新規および再アクセスした一意のデバイスの日次の傾向が表示されます。

- [New Devices] : 指定された期間に選択されたロケーションから SSID に接続した一意の新規デバイスの総数。デバイスの総数に対する一意の新規デバイスの割合も表示されます。
- **再アクセスデバイス (Returning Devices)** : 指定された期間中に、選択したロケーションから SSID に複数回接続した一意のデバイスの総数。接続されている一意のデバイスの総数に対する一意の復帰デバイスの割合も表示されます。

グラフは、指定された期間の各日に選択したロケーションから接続された一意の新規デバイスと再アクセスデバイスの対比を表します。グラフの X 軸は選択した期間の日数を表し、Y 軸は一意のデバイスの数を表します。新規および復帰した一意のデバイスのカラーインジケータは、グラフの上部に表示されます。

## キャプティブポータルでのメニューボタンのクリック回数

このセクションには、プロモーションやオファーによる顧客のエンゲージメント詳細が日次で表示されます。プロモーションやオファーによる毎日のエンゲージメントは、指定された期間中に顧客がメニューボタンをクリックした回数で計算されます。

- **メニューボタン数 (Menu buttons)** : 指定した期間中に選択したロケーションから少なくとも 1 回クリックされたメニューボタンの総数。
- **クリック数 (Clicks)** : 指定した期間中に選択したロケーションからキャプティブポータルでクリックされた合計回数。

## 顧客獲得

このレポートには、特定の期間に選択したロケーションから最近獲得した一意の顧客に関する洞察が表示されます。また、これらの顧客から収集される個人データおよびデモグラフィックデータについても説明します。



- (注) 新しい顧客が複数のデバイスを使用してお客様のロケーションに接続し、同じ個人 ID（携帯電話番号、電子メール、ソーシャル ID など）を使用した場合、顧客は 1 回だけカウントされます。

## 顧客獲得

顧客獲得は、次の特徴を備えたメトリックです。

- 個人識別子によって特定された一意の新規顧客の総数を追跡する
- 「認証なし」または「アクセスコード」で認証された顧客を除外する
- 新しいデバイス接続に対する取得率を示すパーセンテージを提供する。
- SSID に接続された新規デバイス (New Devices Connected to SSID)** : 指定された期間に選択されたロケーションから対象 SSID に接続した一意の新規デバイスの総数。デバイスの総数に対する一意の新規デバイスの割合も表示されます。
- 特定された新規顧客 (News Customers Identified)** : 指定された期間に、選択した場所から携帯電話番号、電子メール、ソーシャル ID などの個人識別情報を介して獲得した、一意の新規顧客の総数。デバイスの総数に対する一意の新規デバイスの割合も表示されます。Cisco Spaces のインストール日以降で全ロケーションに関するこれらのメトリックは、このレポートの上部にある [特定された顧客 (Customers Identified) ] の下に表示されます。
- [Customers Opted In]** : 指定されて期間に、選択したロケーションからサブスクリプションにオプトインした、一意の新規獲得顧客の総数。一意の新規顧客獲得の総数のうち、オプトインした一意の新規獲得顧客の割合も表示されます。オプトインユーザーの詳細については、「ユーザーのオプトインオプション」を参照してください。
- 完了したデータキャプチャ (Completed Data Capture)** : 携帯電話番号、電子メール、ソーシャル ID などの個人識別情報を通じて獲得され、指定された期間中に、指定されたロケーションからデータキャプチャフォームを完了した一意の新規獲得顧客の総数。一意の新規獲得顧客の総数のうち、データキャプチャを完了した一意の新規獲得顧客の割合も表示されます。

## 日次顧客獲得

このセクションには、指定された期間における選択したロケーションの、「SSID に接続された一意の新規デバイス」と「携帯電話番号、電子メール、ソーシャル ID などの個人識別情報を通じて獲得された一意の新規顧客」の数を示す棒グラフが表示されます。また、サブスクリ

プッシュにオプトインしてデータキャプチャを完了した、「一意の新規顧客獲得」の数も日次で示しています。X軸は選択した期間の日数を示し、Y軸はカウントを示します。カラーインジケータが、グラフの上部に表示されます。グラフにカーソルを合わせると、特定の日のカウントが表示されます。



(注) このレポートでは、認証タイプ「認証なし」および「アクセスコード」で獲得された顧客はカウントされません。

## キャプチャされたデータ

このセクションには、指定した期間に選択したロケーションからキャプチャされた電子メールアドレス、電話番号、名前、性別の詳細などが表示されます。

- 電話番号：指定した期間に指定したロケーションからキャプチャされた、一意の電話番号の総数。
- 電子メール：指定した期間に指定したロケーションからキャプチャされた、一意の電子メールアドレスの総数。
- ソーシャルID：ソーシャル認証を介して、指定した期間に指定したロケーションからキャプチャされた、一意のソーシャルIDの総数。
- 名前：指定した期間に指定したロケーションから名前（姓/名）がキャプチャされた、顧客/デバイスの総数。
- 性別：指定した期間に指定したロケーションから性別が収集された顧客/デバイスの総数。

## 顧客のデモグラフィック プロファイル属性

このセクションには、指定された期間に選択したロケーションから新たにキャプチャされた国、性別、言語などのプロフィールの詳細が表示されます。

**国数 (Countries)** : 国データが収集された顧客総数のうち、さまざまな国からの顧客の割合を円グラフでこのパネルに表示します。国の合計数は円グラフの中央に表示されます。顧客数が最も多い国は、顧客数とともに表示されます。[すべて表示 (Show All)] ボタンをクリックすると、少なくとも1人の顧客がいる国をすべて表示できます。国名は、認証プロセス中に指定された電話番号の国番号に基づいて決定されます。

**言語 (Languages)** : 言語データが収集された顧客総数のうち、さまざまな言語を使用する顧客の割合を円グラフで表示します。最も多くの顧客が使用する言語は、顧客数とともに円グラフの下に表示されます。[すべて表示 (Show All)] ボタンをクリックすると、少なくとも1人の顧客がいる言語をすべて表示できます。言語数は、キャプティブポータルで顧客が選択した言語に基づいて算出されます。

**性別 (Gender)** : 顧客総数に対する男性、女性、「性別指定なし」の顧客の割合を円グラフで表示します。性別の詳細を入力した顧客の割合の合計が円グラフの中央に表示されます。男性、女性、および性別不明の顧客の数は、円グラフの下部に表示されます。

## ユーザー管理

新しいユーザーに関連するロールとロケーションアクセスを割り当て、適切なポータルアクセスと管理権限を付与します。

[User Management] オプションを使用して、ユーザーロール、[Creative User] または [AccessCodeManager] を持つキャプティブポータルユーザーを招待できます。キャプティブポータルアプリケーションの読み取りと書き込み権限を持つユーザーのみが、[ユーザー管理 (User Management)] オプションを使用して他のユーザーを招待できます。

- **クリエイティブユーザー (Creative User)** : このユーザーは、アクセス権が付与されているロケーションでキャプティブポータルを作成、表示、および編集できます。このユーザーは、Cisco Spaces の他の機能にアクセスできません。このロールは、キャプティブポータルデザイナー向けです。
- **[AccessCodeManager]** : このユーザーは、アクセス権が提供されているロケーションのアクセスコードを作成し、管理できます。このユーザーは、**キャプティブポータルアプリ**にのみアクセスできます。このロールは、アクセスコードマネージャ向けです。

このロールは [Roles] タブに一覧表示されます。[Roles] タブからロールを編集することはできません。

アクセスコードマネージャまたはクリエイティブユーザーを定義するには、次の手順を実行します。

### Procedure

**ステップ 1** Cisco Spaces ダッシュボードで、[ホーム (Home)] を選択します。

**ステップ 2** [Captive Portals] をクリックします。

**ステップ 3** 表示されるウィンドウで、左ペインの [User Management] をクリックします。

#### Note

[ユーザー管理 (User Management)] オプションは、キャプティブポータルアプリケーションで読み取りと書き込み権限を持つユーザーのみが Cisco Spaces ダッシュボードで使用できます。

**ステップ 4** [Invite User] をクリックします。

**ステップ 5** [ユーザーを招待 (Invite User)] ウィンドウで、招待するユーザーの電子メールアドレスを入力し、[次へ (Next)] をクリックします。

**ステップ 6** [ロール (Role)] ドロップダウンリストから、[クリエイティブユーザー (Creative User)] または [アクセスコードマネージャ (AccessCodeManager)] を選択します。

**ステップ 7** [Location] をクリックします。

**ステップ 8** [ロケーション階層 (Location Hierarchy)] エリアで、このユーザーにアクセスを許可するロケーションのチェックボックスをオンにします。[Done] をクリックします。

**ステップ 9** [Send Invitation] をクリックします。

ユーザーに招待状が送信されます。ユーザー名は[ユーザー (Users)] タブに表示されます。[ユーザーの検索 (Find Users)] フィールドを使用して、ユーザーを検索できます。

## アクセスコード

### アクセスコードの作成

Cisco Spaces により、アクセスコードを使用して事業の場所のインターネットプロビジョニングを制御できます。さまざまなロケーション用にアクセスコードを作成し、これらのコードを使用してそれぞれの場所のインターネットアクセスを制御できます。つまり、顧客は、そのロケーション用に設定されたアクセスコードを入力した後でのみインターネットにアクセスできます。このセクションでは、Cisco Spaces を使用してアクセスコードを作成および管理する方法について説明します。

この機能を使用するには、使用するキャプティブポータルのアクセスコード認証を設定します。キャプティブポータルのアクセスコード認証の設定に関する詳細は、「[アクセスコード認証用ポータルの設定 \(17 ページ\)](#)」を参照してください。

使い捨てアクセスコードを作成することもできます。 >[**アクセスコード (Access Code)**] > [**アクセスコードの作成 (Create Access Code)**] を選択して、新しい一回限りのアクセスコードを作成します。詳細については、[使い捨てアクセスコードを作成する \(61 ページ\)](#) を参照してください。

### アクセスコードの設定要件

- アクセスコードを作成または管理できるのは、アカウント管理者またはアクセスコードマネージャの権限を持つ Cisco Spaces ユーザーのみです。
- アクセスコードマネージャとしてユーザーを招待できるのは Cisco Spaces アカウント管理者ユーザーのみです。アクセスコードオプションは、Cisco Spaces ダッシュボードのアカウント管理者またはアクセスコードマネージャアカウントのみが使用できます。
- アクセスコードレベルで設定された**セッション期間**と**帯域幅制限**が、キャプティブポータルによって考慮されます。認証中に、値はコントローラに渡され、セッションの継続時間と帯域幅についてコントローラで行われたデフォルト設定を上書きします。

### アクセスコードとインターネットプロビジョニング

Cisco Spaces では、アクセスコードを顧客と共有できます。アクセスコードの有効期間を指定できます。アクセスコードに単一のコード値を持たせる、またはコード値を毎週や毎月変更するように設定できます。アクセスコードに手動でコード値を指定するか、または自動生成することができます。アクセスコードを使用して、顧客がインターネットにアクセスできる時間を定義できます。

Cisco Spaces では、特定のアクセスコードを使用してインターネットにアクセスするときに、アクセスコードのダウンロードおよびアップロードの帯域幅制限を設定することもできます。

1つのロケーションに複数のアクセスコードを定義できます。たとえば、プラチナメンバーにのみ高速インターネットを提供する場合、最大帯域幅を持つアクセスコードを作成し、限られた帯域幅を持つアクセスコードを別に作成できます。その後、顧客のタイプに基づいてアクセスコードを共有できます。

アクセスコード認証の手順については、「[アクセスコード認証の手順 \(101ページ\)](#)」を参照してください。

### 効果的なアクセスコード管理

インターネットプロビジョニングのセキュリティと機能を維持するには、次のガイドラインに従ってください。

- アカウント管理者またはアクセスコードマネージャロールを持つユーザーにのみ、アクセスコードの作成および管理権限を付与します。
- Cisco Spaces アカウント管理者ユーザーのみを介してアクセスコードマネージャになるようにユーザーを招待します。
- アクセスコードレベルで設定されたセッション期間および帯域幅の制限は、認証プロセス中、デフォルトのコントローラ設定よりも優先されることに留意してください。

## 共有アクセスコードの作成

アクセスコードを作成するには、次の手順を実行します。

### 手順

**ステップ 1** Cisco Spaces ダッシュボードで、[キャプティブポータル (Captive Portals)] をクリックします。

**ステップ 2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[アクセスコード (Access Code)] オプションは、Cisco Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco Spaces ダッシュボードで使用できます。Cisco Spaces ユーザーの作成の詳細については、「[Cisco Spaces ユーザーの招待](#)」を参照してください。

**ステップ 3** [Location] ドロップダウンリストから、アクセスコードを定義するロケーションを選択します。

**ステップ 4** [Create Access Code] をクリックします。

**ステップ 5** [Create Access Code] ウィンドウで、[Shared Access Code] タブをクリックします。

**ステップ 6** [Shared Access Code] タブで、作成するアクセスコードのタイプを選択します。次のオプションがあります。

- [Fixed] : コード値はアクセスコードが有効である限り変わりません。
- [Weekly] : アクセスコードのコード値は毎週変更されます。
- [Monthly] : アクセスコードのコード値は毎月変更されます。

表示される残りのフィールドは、選択したアクセスコードタイプによって異なります。

アクセスコードタイプに [Fixed] を選択したら、次の詳細を入力します。

- a) [Access Code Name] フィールドにアクセスコードの名前を入力します。
- b) アクセスコードに独自コード値を定義するには、[Set your own access code?] チェックボックスをオンにします。
- c) 表示される [Access Code] フィールドに、コード値を入力します。
- d) [Limit session by time] バーを調整して、アクセスコードを使用して顧客がインターネットにアクセスできる時間を指定します。この時間は、1回のセッションの値です。
- e) アクセスコードの有効期間を定義するには、[Define a validity period for this access code] チェックボックスをオンにします。それぞれのボタンをクリックして、開始日と終了日を指定します。
- f) 顧客がこのアクセスコードを使用してインターネットにアクセスするときに帯域幅を制限する場合、[Limit bandwidth] チェックボックスをオンにします。
- g) [Bandwidth Limit] バーを調整して、このアクセスコードを使用してインターネットにアクセスするときに、顧客に提供する必要がある最大帯域幅を指定します。
- h) [Show More] リンクをクリックして、アップロードおよびダウンロードの制限を指定します。
- i) [Number of times access code can be used] ドロップダウンリストから、顧客がこのアクセスコードを使用してインターネットにアクセスできる最大回数を選択します。

アクセスコードタイプに [Weekly] を選択したら、次の詳細を入力します。

- a) [Access Code Name] フィールドにアクセスコードの名前を入力します。
- b) アクセスコードを生成する方法を指定します。
  - すべての週に独自のコード値を指定する場合は、[Upload access codes from the csv file] チェックボックスをオンにします。メッセージボックス内のリンクをクリックすると、アクセスコードのテンプレートをダウンロードできます。テンプレートで必要なすべての週にすべてのコード値を入力した後、[Upload] ボタンを使用してテンプレートを CSV ファイルとしてアップロードできます。
  - すべての週のコード値を自動的に生成するには、[Access Code Validity time period] バーを調整して、このアクセスコードが有効な期間を週単位で指定します。

(注)

[Access Code Validity time period] バーは [Upload access codes from the csv file] チェックボックスを選択しなかった場合のみ使用できます。[Upload access codes from csv File] チェックボックスを選択した場合、有効期間は CSV ファイルに入力したコード値の数に基づいて判断されます。たとえば、CSV ファイルに3つのコード値を定義した場合、アクセスコードは3週間有効です。CSV ファイルに指定されたコード値は、それぞれの週に順次対応していると見なされます。

- c) [Limit session by time] バーを調整して、アクセスコードを使用して顧客がインターネットにアクセスできる時間を指定します。この時間は、1回のセッションの値です。
- d) [Start Date] ボタンをクリックして、アクセスコードが有効になる開始日を指定します。
- e) 顧客がこのアクセスコードを使用してインターネットにアクセスするときに帯域幅を制限する場合、[Limit bandwidth] チェックボックスをオンにします。
- f) 表示される [Bandwidth limit] バーで、このアクセスコードを使用してインターネットにアクセスするときに、顧客に提供する必要がある最大帯域幅を、バーを調節して指定します。

- g) [Show More] リンクをクリックして、アップロードおよびダウンロードの制限を指定します。
- h) [Number of times access code can be used] ドロップダウンリストから、顧客がこのアクセスコードを使用してインターネットにアクセスできる最大回数を選択します。

[Monthly] を選択した場合、次の詳細を入力します。

- a) [Access Code Name] フィールドにアクセスコードの名前を入力します。
- b) アクセスコードを生成する方法を指定します。
  - すべての月に独自のコード値を指定する場合、[Upload access codes from the csv file] チェックボックスをオンにします。メッセージボックスのリンクをクリックすると、アクセスコードのテンプレートをダウンロードできます。テンプレートで必要なすべての月のすべてのコード値を入力した後、[Upload] ボタンを使用してテンプレートを CSV ファイルとしてアップロードできます。
  - すべての月のコード値を自動的に生成するには、[Access Code Validity time period] バーを調整して、このアクセスコードが有効な期間を月単位で指定します。

(注)

[Access Code Validity time period] バーは [Upload access codes from the csv file] チェックボックスをオンにしなかった場合のみ使用できます。[Upload access codes from the csv file] チェックボックスをオンにした場合、有効期間は CSV ファイルに入力したコード値の数に基づいて判断されます。たとえば、CSV ファイルに 3 つのコード値を定義した場合、アクセスコードは 3 か月間有効です。CSV ファイルに指定されたコード値は、それぞれの月に順次対応していると見なされます。

- c) [Limit session by time] バーを調整して、アクセスコードを使用して顧客がインターネットにアクセスできる時間を指定します。この時間は、1 回のセッションの値です。
- d) [Start Date] ボタンをクリックして、アクセスコードが有効になる開始日を指定します。
- e) 顧客がこのアクセスコードを使用してインターネットにアクセスするときに帯域幅を制限する場合、[Limit bandwidth] チェックボックスをオンにします。
- f) 表示される [Bandwidth limit] バーで、このアクセスコードを使用してインターネットにアクセスするときに、顧客に提供する必要がある最大帯域幅を、バーを調節して指定します。
- g) [Show More] リンクをクリックして、アップロードおよびダウンロードの制限を指定します。
- h) [Number of times access code can be used] ドロップダウンリストから、顧客がこのアクセスコードを使用してインターネットにアクセスできる最大回数を選択します。

ステップ 7 [作成 (Create) ] をクリックします。

## 使い捨てアクセスコードを作成する

[アクセスコードの作成 (Create Access Code) ] ウィンドウで、[一回限りのアクセスコード (Single Use Access Code) ] オプションを選択して、ワンタイムのアクセスコードを作成します。

選択したロケーションの定義済みテンプレートを作成するには、[設定 (Settings) ] > [アクセスコードテンプレート (Access Code Template) ] にある [アクセスコードテンプレートの有効化 (Enable Access Code Template) ] チェックボックスをオンにします。

このオプションが有効になっている場合は、最初にテンプレート（ロケーションで使用可能）を選択してから、使い捨てアクセスコードを作成します。



(注) Cisco Spaces : キャプティブポータル アプリケーションの [設定 (Settings)] > [アクセスコードテンプレート (Access Code Templates)] で [アクセスコードテンプレートの有効化 (Enable Access Code Template)] チェックボックスがオフになっている場合、現在のアクセスコード作成プロセスに変更はありません。

使い捨てのアクセスコードを作成するには、次の手順を実行します。

## 手順

**ステップ 1** Cisco Spaces ダッシュボードで、[キャプティブポータル (Captive Portals)] をクリックします。

**ステップ 2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[アクセスコード (Access Code)] オプションは、Cisco Spaces アカウント管理者またはアクセスコードマネージャのユーザーのみが、Cisco Spaces ダッシュボードで使用できます。Cisco Spaces ユーザーの作成に関する詳細は、「[Cisco Spaces ユーザーの招待](#)」を参照してください。

**ステップ 3** [Location] ドロップダウンリストから、アクセスコードを定義するロケーションを選択します。

**ステップ 4** [Create Access Code] をクリックします。

**ステップ 5** 選択したロケーションでアクセスコードテンプレートを使用できる場合は、テンプレートを選択する必要があります。

- a) [テンプレートの選択 (Choose a template)] エリアで、アクセスコードテンプレートを選択して、新しいアクセスコードのセットを作成します。
- b) [Next] をクリックします。
- c) [アクセスコードの生成 (Generate Access Code)] エリアで、次の手順を実行します。

- [Access code name] : 新しい使い捨てアクセスコードの名前を入力します。
- **ロケーションの選択 (Choose Location)** : テンプレートを作成するネットワークのロケーションをドロップダウンリストから選択します。
- **アクセスコード数 (# of Access Code)** : 作成するアクセスコードの数を入力します。
- **このアクセスコードの有効期間を定義 (Define a validity period for this access code)** : チェックボックスをオンにして、カレンダーを使用して次の日付を入力し、アクセスコードの有効期間を設定します。
  - **Start Date**
  - **End Date**

**ステップ 6** 選択したロケーションで **アクセスコードテンプレート** を使用できない場合は、次の手順を実行します。

- a) [アクセスコードの作成 (Create Access Code) ] ウィンドウで、[一回限りのアクセスコード (Single Use Access Code) ] タブをクリックします。
- b) [Single Use Access Code] タブで、次の手順を実行します。
  - [Access code name] : 新しい使い捨てアクセスコードの名前を入力します。
  - [Access code type] : アクセスコードタイプを選択するには、[Numeric] または [Alphanumeric] ラジオボタンをクリックします。
  - [# of Access Code] : 作成するアクセスコードの数を入力します。デフォルト値は 1 です。
  - [#of Characters] : アクセスコードに必要な文字数を入力します。使い捨てのアクセスコードには、3 文字以上を含める必要があります。
  - [Limit session by time] : スライダーを使用して、セッションの制限時間を設定します。有効な範囲は 30 分～3 ヶ月です。
  - [Define a validity period for this access code] : カレンダーを使用して次の日付を入力し、アクセスコードの有効期間を設定します。
    - **Start Date**
    - **End Date**
  - [Limit bandwidth] : チェックボックスをオンにして、帯域幅を 1 Mbps に制限します。

**ステップ 7** [Create] をクリックします。

- 生成されたアクセスコードは 1 回限りの使用です。アクセスコードが以前に使用されている場合は、次のエラーメッセージが表示されます。

```
invalid access code
```
- 新しいアクセスコードのステータスは、[View Access Codes] ウィンドウに [Available] と表示されます。アクセスコードを使用すると、ステータスが [Used] に変わります。
- [編集 (Edit) ] をクリックして開始日と終了日を編集し、[更新 (Update) ] をクリックして変更を保存します。詳細については、[アクセスコードの編集 \(66 ページ\)](#) を参照してください。

---

## アクセスコードテンプレートの作成

アクセスコードテンプレートを使用すると、ネットワークまたは建物の場所に合わせてカスタマイズされたアクセスコードを簡単かつ迅速に生成できます。

選択したネットワークまたは建物の場所のアクセスコードテンプレート機能を有効にするには、[設定 (Settings) ] > [アクセスコードテンプレート (Access Code Templates) ] タブで [アクセスコードテンプレートの有効化 (Enable Access Code Template) ] チェックボックスをオンにします。

アクセスコードテンプレート機能を有効にすると、新しいアクセスコードテンプレートを作成した後、選択したテンプレートに基づいて一回限りのアクセスコードを作成できます。



- (注) この機能は一回限りのアクセスコードにのみ適用され、最大制限数に基づいて設定できます。特定のロケーションに対してテンプレートが作成されていない場合は、アクセスコードを作成する従来の方法が使用されます。

## 手順

**ステップ 1** Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコンをクリックし、[ホーム (Home)] > [SMART VENUES] > [キャプティブポータル (Captive Portals)] アプリケーションタイトルを選択します。

オプションで、[ダッシュボード (Dashboard)] ドロップダウンリスト (Cisco Spaces [ホーム (Home)] ウィンドウの左側のナビゲーションペイン) から [キャプティブポータル (Captive Portals)] を選択します。

[ポータル (Portal)] ウィンドウが表示されます。左側のナビゲーションペインでは、**キャプティブポータル** アプリケーションの使用可能なタブを表示できます。

**ステップ 2** 左側のナビゲーションペインで [設定 (Settings)] をクリックします。

[設定 (SETTINGS)] ウィンドウには、[SMSゲートウェイ (SMS Gateway)]、[ソーシャルアプリケーション (Social Apps)]、[アクセスコードテンプレート (Access Code Templates)]、および [信頼できるデバイステンプレート (Trusted Devices Templates)] の 4 つのタブが表示されます。

**ステップ 3** [アクセスコードテンプレート (Access Code Templates)] をクリックします。

**ステップ 4** アクセスコードテンプレートを作成する設定を有効にするには、[アクセスコードテンプレートの有効化 (Enable Access Code Template)] チェックボックスをオンにします。

[テンプレートの作成 (Create Template)] オプションが表示されます。有効にすると、アクセスコードは事前定義されたテンプレートを使用した場合のみ生成できるようになるため、標準化された安全なプロセスが保証されます。これは、一回限りのアクセスコードを作成するときのみ適用されます。

**ステップ 5** 選択したロケーションの定義済みテンプレートを作成するには、[テンプレートの作成 (Create Template)] をクリックします。

[アクセスコードテンプレートの作成 (Create Access Code Template)] ウィンドウが表示されます。

**ステップ 6** 一回限りのアクセスコードを生成するための新しいテンプレートを作成するには、次の手順を実行します。

- **テンプレート名 (Template Name)** : 一回限りの新しいアクセスコードテンプレートの名前を入力します。
- **ロケーションの選択 (Choose Location)** : テンプレートを作成するネットワークのロケーションをドロップダウンリストから選択します。
- **アクセスコードタイプ ([Access code type])** : アクセスコードタイプを選択するには、[数字 (Numeric)] または [英数字 (Alphanumeric)] ラジオボタンをクリックします。

- **文字数 (# of Characters)** : 作成するアクセスコードの文字数を入力します。
- **[Limit session by time]** : スライダーバーを使用して、セッションの制限時間を設定します。有効な範囲は30分～3ヵ月です。
- **[Limit bandwidth]** : チェックボックスをオンにして、帯域幅を1 Mbps に制限します。
- **このアクセスコードの有効期間を定義 (Define a validity period for this access code)** : チェックボックスをオンにして、カレンダーを使用して次の日付を入力し、アクセスコードの有効期間を設定します。
  - **Start Date**
  - **End Date**
- **このアクセスコードの有効期間を定義 (Define a validity period for this access code)** :
- **アクセスコードの一括作成を許可 (Allow bulk access code creation)** : チェックボックスをオンにして、一括作成を許可するアクセスコードの制限を入力します。

**ステップ 7** [作成 (Create) ] をクリックします。

作成された新しいテンプレートは、[アクティブテンプレート (Active Template) ] エリアに表示されます。

---

### 次のタスク

[アクセスコード (Access Code) ] ウィンドウに移動し、テンプレートを選択して、一回限りのアクセスコードを作成できます。

## アクセスコードの表示

有効期間がまだ切れていないロケーションのすべてのアクセスコードを表示できます。

ロケーションに定義されているアクセスコードを Cisco DNA Spaces で表示するには、次の手順を実行します。

### 手順

---

**ステップ 1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ 2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ 3** 表示された [Access Code] ウィンドウのドロップダウンリストから、アクセスコードを表示するロケーションを選択します。

ロケーションに対して定義されたアクセスコードが表示されます。

選択したロケーションについて、利用可能なアクセスコードの総数、期限切れのアクセスコードの総数、およびそれらのうちのアクティブおよび非アクティブなアクセスコードの数が表示されます。

さらに、ロケーションに対して定義されたアクセスコードの次のような詳細が表示されます。

- [Status] : アクセスコード名がアクティブであるかどうか。
- [Name] : アクセスコードの名前。
- [Code] : アクセスコードを表示した時点のアクセスコード名のコード値。コードの値は毎週または毎月変更するように設定した場合、変更されます。
- [Type] : アクセスコードのタイプ。アクセスコードタイプは固定することも、毎週または毎月変更することもできます。
- [Expiry Date] : アクセスコードが有効である期間。
- [Actions] : 編集、共有、削除など、アクセスコードに対して実行できる操作。

---

## アクセスコードの編集

アクセスコードを編集するには、次の手順を実行します。

### 手順

---

**ステップ 1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ 2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ 3** 表示される [Access Code] ウィンドウで、アクセスコードを編集するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

**ステップ 4** 編集するアクセスコードの [Active Access Codes] 領域で、[Edit] ボタンをクリックします。

**ステップ 5** 必要な変更を行って、[Update] をクリックします。

---

## アクセスコードの共有

Cisco DNA Spaces では、顧客とアクセスコードを共有できます。

アクセスコードを共有するには、次の手順を実行します。

### 手順

**ステップ 1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ 2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ 3** 表示される [Access Code] ウィンドウで、アクセスコードを共有するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

**ステップ 4** 共有するアクセスコードの [Active Access Codes] 領域で、[Share] ボタンをクリックします。

**ステップ 5** 表示される [Share Access Code] ウィンドウに、アクセスコードを共有する人の電子メール ID を入力し、[Invite] をクリックします。

## アクセスコードの削除

アクセスコードを削除するには、次の手順を実行します。

### 手順

**ステップ 1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ 2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ 3** 表示される [Access Code] ウィンドウで、アクセスコードを削除するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

**ステップ 4** [Active Access Codes] エリアで、削除するアクセスコードの [Delete] ボタンをクリックします。

**ステップ5** 表示される [Delete] ウィンドウで [Yes] をクリックし、削除を確定します。

(注)

複数のアクセスコードを同時に削除できます。アクセスコードごとにチェックボックスが表示され、一度に複数のアクセスコードを選択して同時に削除することができます。また、期限切れのアクセスコードを削除することもできます。

---

## アクセスコードの非アクティブ化

アクセスコードを非アクティブ化するには、次の手順を実行します。

### 手順

---

**ステップ1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ3** 表示される [Access Code] ウィンドウで、アクセスコードを非アクティブ化するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

**ステップ4** 非アクティブ化するアクセスコードの [Status] トグルスイッチを切り替えます。

非アクティブ化すると、ステータス ボタンはグレーに変わります。

---

## アクセスコードの再アクティブ化

デフォルトでは、アクセスコードは作成されたときはアクティブモードになっています。これを非アクティブ化した後は、アクセスコードの有効期限内であれば、必要に応じてアクティブ化できます。

アクセスコードを再アクティブ化するには、次の手順を実行します。

### 手順

---

**ステップ1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ3** 表示される [Access Code] ウィンドウで、アクセスコードをアクティブ化するロケーションを選択します。そのロケーションに対して定義されたアクセスコードが表示されます。

**ステップ4** アクティブ化するアクセスコードの [Status] トグルスイッチを切り替えます。アクティブ化すると、ステータス ボタンは緑に変わります。

---

## アクセスコードのエクスポート

Cisco DNA Spaces では、ロケーション用に作成したアクセスコードを .csv ファイルまたは PDF としてエクスポートできます。

Cisco DNA Spaces でロケーション用に定義されているアクセスコードを表示するには、次の手順を実行します。

### 手順

---

**ステップ1** Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

**ステップ2** 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

(注)

[Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセスコードマネージャユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、[#unique\\_202](#)を参照してください。

**ステップ3** 表示された [Access Code] ウィンドウのドロップダウンリストから、アクセスコードをエクスポートするロケーションを選択します。

選択したロケーションについて、利用可能なアクセスコードの総数、期限切れのアクセスコードの総数、およびそれらのうちのアクティブおよび非アクティブなアクセスコードの数が表示されます。

**ステップ4** 必要な形式に基づいて、次のいずれかを実行します。

- アクセスコードを PDF ファイルとしてエクスポートするには、[Export] > [Export as PDF] を選択します。
- アクセスコードを .csv ファイルとしてエクスポートするには、[Export] > [Export as CSV] を選択します。

**ステップ5** 表示されるウィンドウで、[OK] をクリックしてファイルを保存します。

アクセスコードは、指定された形式でコンピュータの [ダウンロード] フォルダにダウンロードされます。

(注)

アクティブなアクセスコードのみがエクスポートされます。

---

### 次のタスク

期限切れのアクセスコードをエクスポートする場合、または特定の期間内に有効なアクセスコードをエクスポートする場合は、[Filter] オプションを使用して実行できます。

## エクスポートするアクセスコードのフィルタリング

エクスポートするアクセスコードをフィルタリングするには、次の手順を実行します。

### 手順

---

**ステップ1** [Access Code] ウィンドウのドロップダウンリストから、アクセスコードをエクスポートするロケーションを選択します。

**ステップ2** [Filter] をクリックします。

- [All Access Codes] : 選択した場所に対して作成されたすべてのアクセスコードをエクスポートします。アクティブなアクセスコードと期限切れのアクセスコードが含まれます。
- [Filter by] : 適用されたフィルタに基づいてアクセスコードをエクスポートします。今週、今月、または特定の日付範囲で期限切れになるアクセスコードをフィルタリングするように選択できます。同様に、今週、今月、または特定の日付範囲に期限切れになったアクセスコードをフィルタリングすることもできます。[Expires in] および [Expired] オプションを使用して、期限切れのアクセスコードとアクティブなアクセスコードの両方を同時に含めることができます。

**ステップ3** [Apply] をクリックします。

フィルタリングされたアクセスコードは、[Filtered Access Codes] ウィンドウに表示されます。

**ステップ4** 必要な形式に基づいて、次のいずれかを実行します。

- アクセスコードを PDF ファイルとしてエクスポートするには、[Export] > [Export as PDF] を選択します。
- アクセスコードを .csv ファイルとしてエクスポートするには、[Export] > [Export as CSV] を選択します。

**ステップ5** 表示されるウィンドウで、[OK] をクリックしてファイルを保存します。

アクセスコードは、指定された形式でコンピュータの [ダウンロード] フォルダにダウンロードされます。

## 信頼できるデバイス

アクセスコードマネージャには次の機能があります。

- 管理者は、リストを信頼し、ダッシュボードを使用して、デバイスを直接導入準備できません。
- Cisco Spaces RADIUS エンジンを紹介したオンボーディングテンプレートと認証プロファイルの適用を自動化します
- 大規模なデバイスアクセスのプロビジョニング、モニタリング、管理を合理化します。

Cisco Spaces ダッシュボードでは、アクセスコードマネージャ機能により、信頼できるデバイスのオンボーディングと管理が改善されました。管理者は、ダッシュボードから直接デバイスを信頼できるようになり、コントローラを手動で設定したり、複数のシステムにログインしたりする必要がなくなりました。ダッシュボードでは、キャプティブポータルブラウザを使用しないデバイスがサポートされているため、安全なオンボーディングが可能になり、管理者は設定可能なテンプレートを使用してセッション期間と帯域幅制限を設定できます。

ダッシュボードで作成されたオンボーディングテンプレートと認証プロファイルが、Cisco Spaces RADIUS エンジンによって自動的に解釈および適用されるようになり、環境全体での一貫性が維持されます。デバイスのオンボーディングステータスとポリシー適用がリアルタイムで監視できるため、必要に応じて迅速な検証とトラブルシューティングが可能です。

### テンプレート管理

管理者が再利用可能なテンプレートを作成、更新、廃止し、ロケーションまたは SSID によりテンプレートを割り当て、組み込みの予防対策とデバイスの関連付けを維持することで、テンプレート管理が合理化されます。ゲストの滞在や運用ポリシーに合わせて、必要に応じてデバイスのアクセスをプロビジョニングまたは取り消すことができます。MAC アドレス検証機能と集中監査機能の向上により、ネットワークセキュリティが強化されています。

これらの更新により、デバイスのオンボーディングと管理がより効率的かつ安全になり、Cisco Spaces の展開全体で大規模な運用ニーズがサポートされるようになりました。

### サマリーセクション

[信頼できるデバイス (Trusted Devices)] ウィンドウには、追加されたデバイス数、アクティブなデバイス数、期限切れのデバイス数など、デバイスの要約が表示されます。

## デバイスセクション

デバイスを信頼できるものとして追加するには、テンプレートが必要です。作成されたテンプレートがない場合は、[設定 (Settings)] > [信頼できるデバイスのテンプレート (Trusted Devices Templates)] に移動し、新しいテンプレートを作成します。

テンプレートがすでに使用可能な場合は、[+新しいデバイス (+New Devices)] をクリックして新しいデバイスを信頼できるデバイスとして追加します。

[デバイス (Devices)] セクションには、[期限切れのデバイス (Expired Devices)] と [アクティブなデバイス (Active Devices)] の2つのオプションがあります。すべてのデバイスが期限切れステータスの場合、[アクティブなデバイス (Active Devices)] オプションは [+新しいデバイス (+New Devices)] に切り替わります。[検索 (Search)] フィールドを使用して、デバイスの詳細を検索します。

Figure 3: 信頼できるデバイス

The screenshot shows the 'Trusted Devices' section in the Cisco Spaces interface. It features a summary card with three metrics: '2 Devices added', '2 Active Devices', and '0 Expired Devices'. Below this is a table of devices. The table has columns for Label, Template, Mac Address, Last Connected, Valid Till, Added By, and Actions. There are two rows of data: 'Test' and 'Device 2'. The 'Test' row shows a Mac Address of 01:23:45:67:89:AB and a Valid Till of 21/10/2025, 13:00:13. The 'Device 2' row shows a Mac Address of 00:1A:2B:3C:4D:5E and a Valid Till of 21/10/2025, 13:00:58. The interface also includes a search bar, an 'Export' button, and a '+ New Device' button.

Label	Template	Mac Address	Last Connected	Valid Till	Added By	Actions
Test	doc	01:23:45:67:89:AB	Never	21/10/2025, 13:00:13	j@cisico.com	<a href="#">Edit</a> <a href="#">Delete</a>
Device 2	doc	00:1A:2B:3C:4D:5E	Never	21/10/2025, 13:00:58	ico.com	<a href="#">Edit</a> <a href="#">Delete</a>

[期限切れのデバイス (Expired Devices)] をクリックして、[期限切れのデバイス (Expired Devices)] セクションと期限切れデバイスの詳細を表示します。次の情報を表示できます。

- ラベル
- テンプレート
- MAC アドレス (MAC Address)
- 有効期限の終了
- 追加者
- アクション

[エクスポート (Export)] をクリックして、デバイスの詳細を CSV 形式でエクスポートします。



**Note** この機能を使用するには、レイヤ2 キャプティブポータルを設定し、RADIUS をコントローラと統合します。

## テンプレートの作成

デバイスがキャプティブポータルワークフローをバイパスできるようにします。これは、キャプティブポータルをサポートしていないデバイスで役立ちます。

信頼できるデバイステンプレートを作成して、キャプティブポータルの制限から除外するデバイスを定義します。

### Procedure

**ステップ 1** Cisco Spaces ダッシュボードで、[メニュー (Menu) ]アイコンをクリックし、[ホーム (Home) ]>[SMART VENUES]>[キャプティブポータル (Captive Portals) ]アプリケーションタイトルを選択します。

オプションで、[ダッシュボード (Dashboard) ]ドロップダウンリスト (Cisco Spaces [ホーム (Home) ]ウィンドウの左側のナビゲーションペイン) から [キャプティブポータル (Captive Portals) ]を選択します。

[ポータル (Portal) ]ウィンドウが表示されます。左側のナビゲーションペインでは、**キャプティブポータル** アプリケーションの使用可能なタブを表示できます。

**ステップ 2** 左側のナビゲーションペインで [設定 (Settings) ] をクリックします。

[設定 (SETTINGS) ]ウィンドウには、[SMSゲートウェイ (SMS Gateway) ]、[ソーシャルアプリケーション (Social Apps) ]、[アクセスコードテンプレート (Access Code Templates) ]、および [信頼できるデバイステンプレート (Trusted Devices Templates) ] の3つのタブが表示されます。

**ステップ 3** [信頼できるデバイステンプレート (Trusted Devices Templates) ] をクリックします。

**ステップ 4** テンプレートを作成するには、[テンプレートの作成 (Create Template) ] をクリックします。

[テンプレートの作成 (Create Template) ]ウィンドウが表示されます。

Figure 4: テンプレートの作成

**Create Template** ×

Enable devices to bypass the Captive portal workflow. Useful for devices not supporting Captive portals

---

**Template Name**

Template Name

**Choose Location**

Select Any Location ▾

**Choose SSID**

Choose ssid ▾

Limit Validity

Limit Bandwidth

Cancel Create

**ステップ 5** [テンプレートの作成 (Create Template)] ウィンドウで、次のパラメータを入力します。

- [テンプレート名 (Template Name)] : テンプレートの名前を入力します。
- [ロケーションの選択 (Choose Location)] : [ロケーションの選択 (Choose Location)] ドロップダウンリストからロケーションを選択します。
- [SSIDの選択 (Choose SSID)] : [SSIDの選択 (Choose SSID)] ドロップダウンリストから SSID を選択します。
- [有効期限 (Limit Validity)] : 有効性を制限するには、[有効期限 (Limit Validity)] チェックボックスをオンにして、スライダーで期限を設定します。有効な範囲は 30 分～2 ヶ月 (約 60 日間) です。
- [帯域幅の制限 (Limit Bandwidth)] : 帯域幅を制限するには、[帯域幅の制限 (Limit Bandwidth)] チェックボックスをオンにして、スライダーで帯域幅を設定します。帯域幅は 50 KB/秒 (kbps) ～無制限です。

ステップ 6 [作成 (Create) ] をクリックします。

---

新しいテンプレートが正常に作成され、[設定 (Settings) ] > [信頼できるデバイステンプレート (Trusted Device Templates) ] タブに表示されました。

#### What to do next

テンプレートを選択して、デバイスを追加できます。

## デバイスの追加

デバイス管理用に信頼できるデバイスをキャプティブポータルに追加します。

このタスクで、MAC アドレスを使用してキャプティブポータルに新しいデバイスを追加します。

#### Before you begin

追加するすべてのデバイスの MAC アドレスを持っていることを確認します。

#### Procedure

---

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu) ] アイコンをクリックし、[ホーム (Home) ] > [SMART VENUES] > [キャプティブポータル (Captive Portals) ] アプリケーションタイトルを選択します。

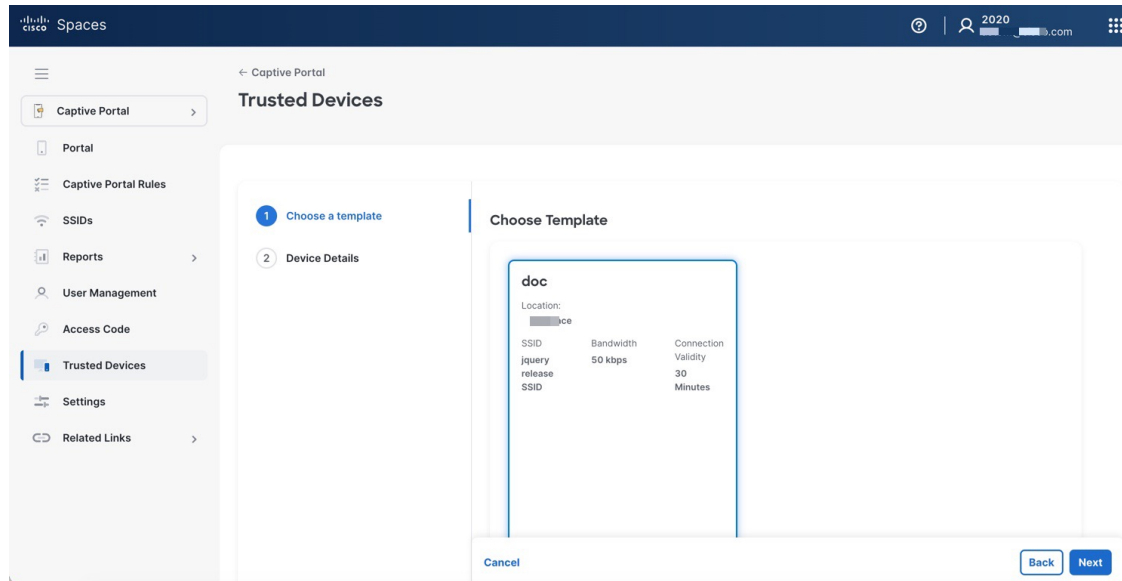
オプションで、[ダッシュボード (Dashboard) ] ドロップダウンリスト (Cisco Spaces [ホーム (Home) ] ウィンドウの左側のナビゲーションペイン) から [キャプティブポータル (Captive Portals) ] を選択します。

[ポータル (Portal) ] ウィンドウが表示されます。左側のナビゲーションペインでは、キャプティブポータル アプリケーションの使用可能なタブを表示できます。

ステップ 2 左側のナビゲーションペインで、[信頼できるデバイス (Trusted Devices) ] をクリックします。

ステップ 3 [信頼できるデバイス (Trusted Devices) ] ウィンドウで、[+新しいデバイス (+New Devices) ] をクリックします。

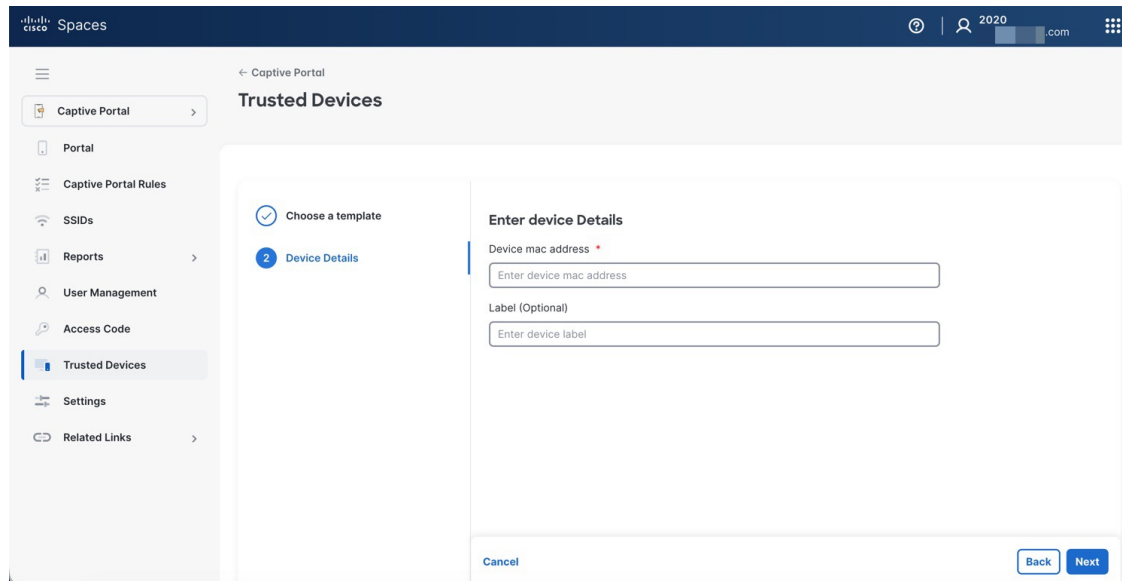
Figure 5: デバイスを追加する。



**ステップ 4** テンプレートを選択し、[次へ (Next)] をクリックします。

**ステップ 5** [デバイスの詳細 (Device Details)] セクションでは、デバイスの MAC アドレスを入力し、ラベルの説明を入力します。デバイスの MAC アドレスは必須です。

Figure 6: デバイスの詳細の追加



**ステップ 6** [次へ (Next)] をクリックして、新しい信頼できるデバイスを追加します。新しく信頼できるデバイスが正常に保存されたことを示す成功メッセージが表示されます。

新しい信頼できるデバイスの詳細が、[デバイス (Device)] セクションの下にある[信頼できるデバイス (Trusted Devices)] ウィンドウに表示されます。

#### What to do next

続行して複数の信頼できるデバイスを追加したり、既存のデバイスの詳細を編集したりできます。[編集 (Edit)] (鉛筆アイコン) を使用してデバイスの詳細を更新するか、[削除 (Delete)] (ゴミ箱アイコン) を使用してデバイスを削除します。

## 設定

Cisco Spaces : キャプティブポータルアプリケーションの [設定 (Settings)] ウィンドウには、次のタブが含まれます。

- **SMSゲートウェイ (SMS Gateway)** : SMS を介してユーザーに關与するための SMS ゲートウェイを設定します。SMS 認証を使用する場合に必須です。  
デフォルトゲートウェイは有料で利用できます。ただし、SMSゲートウェイをすでに導入している場合は、Cisco Spaces : キャプティブポータル と統合できます。
- **ソーシャルアプリケーション (Social Apps)** : ソーシャルメディアアプリケーションを追加します。
- **アクセスコードテンプレート (Access Code Template)** : テンプレートを有効にして作成し、デバイスを関連付けます。
- **信頼できるデバイス (Trusted Devices)** : アクセスコードマネージャ機能により、信頼できるデバイスのオンボーディングと管理を行います。

## Cisco DNA Spaces での SMS ゲートウェイの設定

SMS 通知を送信し、SMS を介してポータル認証を管理するには、SMS ゲートウェイを設定する必要があります。Cisco DNA Spaces では、サードパーティベンダーの SMS ゲートウェイを使用できます。Cisco DNA Spaces で SMS ゲートウェイを設定するには、次の手順を実行します。

### 手順

- ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
- ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。
- ステップ 3 表示される [Captive Portal] ウィンドウの左ペインで [Settings] をクリックします。
- ステップ 4 [Settings] ウィンドウで、[SMS] を選択します。
- ステップ 5 [Add SMS gateway] をクリックします。

**ステップ 6** [SMS Gateway Type] ドロップダウンリストから、使用する SMS ゲートウェイタイプを選択します。選択した SMS ゲートウェイタイプに基づいて、追加のフィールドが表示されます。

Cisco DNA Spaces では、次の SMS ゲートウェイタイプがサポートされます。

- REASON8
- SMPP
- WATERFALL
- MGAGE
- TWILIO
- PANACEA MOBILE
- DATAMETRIX
- TROPO
- NYY
- TRU
- PHIZZLE
- AWS\_SNS
- PROXIMUS
- TELENOR

**ステップ 7** 選択した SMS ゲートウェイタイプに基づいて表示される追加フィールドで、必要な値を指定します。

**ステップ 8** [保存 (Save) ] をクリックします。

(注)

作成された SMS ゲートウェイは、ポータルの [SMS with password verification] および [SMS with link verification] 認証オプションの [SMS Gateway] ドロップダウンリストで選択肢として表示されます。これらの SMS ゲートウェイは、エンゲージメントルールで SMS 通知を構成するときにも選択できます。

---

## キャプティブポータルルールの管理

要求されるたびに、キャプティブポータルルールを一時停止したり、再度有効にしたりできます。必要に応じて、キャプティブポータルルールを変更したり、削除したりできます。ロケーションに設定されているキャプティブポータルルールを表示することもできます。

### キャプティブポータルルールの一時停止

キャプティブポータルルールを一時停止するには、次の手順を実行します。

## 手順

- 
- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
- ステップ 2** [My Apps] エリアで、[Captive Portal] を選択します。
- ステップ 3** [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。  
作成されたキャプティブポータルルールがリストされます。
- ステップ 4** 一時停止するキャプティブポータルルールのチェックボックスをオンにします。
- ステップ 5** ウィンドウ下部に表示される [Pause] ボタンをクリックします。
- ステップ 6** 表示されるウィンドウで [Pause Rule] をクリックし、一時停止することを確認します。  
キャプティブポータルルールが一時停止します。
- 

## 次のタスク



- (注) 複数のキャプティブポータルルールを一時停止するには、一時停止するキャプティブポータルルールのチェックボックスをオンにし、ページの下部に表示される [Pause] ボタンをクリックします。
- 

## キャプティブポータルルールの再起動

一時停止中のキャプティブポータルルールを再起動するには、次の手順を実行します。

## 手順

- 
- ステップ 1** Cisco DNA Spaces ダッシュボードで、**Home** を選択します。
- ステップ 2** [My Apps] エリアで、[Captive Portal] を選択します。
- ステップ 3** [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。  
作成されたキャプティブポータルルールがリストされます。
- ステップ 4** 再起動するキャプティブポータルルールのチェックボックスをオンにします。  
ウィンドウ下部に表示される [Make Live] ボタンをクリックします。
-

### 次のタスク



- (注) 複数のキャプティブポータルルールを再起動するには、再起動するキャプティブポータルルールのチェックボックスをオンにして、ウィンドウの下部に表示される [Make Live] ボタンをクリックします。

## キャプティブポータルルールの変更

キャプティブポータルルールを変更するには、次の手順を実行します。

### 手順

- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
- ステップ 2** [My Apps] エリアで、[Captive Portal] を選択します。
- ステップ 3** [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。  
作成されたキャプティブポータルルールがリストされます。
- ステップ 4** 変更するキャプティブポータルルールの [Edit Rule] アイコンをクリックします。
- ステップ 5** 必要な変更を加えます。
- ステップ 6** 変更を保存するには、[Save] をクリックします。または変更をパブリッシュするには、[Save and Publish] をクリックします。  
(注) ライブルールに表示されるのは [Save and Publish] オプションのみです。[Save and Publish] ボタンをクリックすると、変更を反映したルールがパブリッシュされます。

## キャプティブポータルルールの削除

キャプティブポータルルールを削除するには、次の手順を実行します。

### 手順

- ステップ 1** Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
- ステップ 2** [My Apps] エリアで、[Captive Portal] を選択します。
- ステップ 3** [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。  
作成されたキャプティブポータルルールがリストされます。
- ステップ 4** 削除するキャプティブポータルルールの右端に表示される [Delete Rule] アイコンをクリックします。

### 次のタスク



- (注) 複数のキャプティブポータルルールを削除するには、削除するキャプティブポータルルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Delete] ボタンをクリックします。

### ロケーションのキャプティブポータルルールの表示

グループ、ビルディング、フロアなどのロケーションのキャプティブポータルルールを表示するには、次の手順を実行します。

#### 手順

**ステップ 1** Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

**ステップ 2** キャプティブポータルルールを表示するロケーションをクリックします。

**ステップ 3** [Proximity Rules] タブをクリックします。

**ステップ 4** [Captive Portal Rule] タブをクリックします。

ロケーションのキャプティブポータルルールがリストされます。

### 次のタスク



- (注) ロケーションの [Proximity Rules] リンクは、そのロケーションに少なくとも 1 つのプロキシミティールールが存在する場合にのみ有効になります。

### ロケーションによるフィルタリング

キャプティブポータルルール、エンゲージメントルール、ロケーションパーソナルルール、密度ルールなどの Cisco DNA Spaces ルールでは、ルールを適用するロケーションをフィルタリングできます。ロケーションに定義されているメタデータにより、ロケーションをフィルタリングすることも可能です。

ルールを適用するロケーションを指定するには、次の手順を実行します。

#### 手順

**ステップ 1** [Add Locations] ボタンをクリックします。

**特定のメタデータのロケーションにルールを適用する**

**ステップ 2** 表示される [Choose Locations] ウィンドウで、ルールを適用するロケーションを選択します。

**ステップ 3** [Done] をクリックします。

ロケーションに定義されているメタデータを使用して、ロケーションを再度フィルタリングできます。選択したロケーション、その親および子のロケーションに定義されているメタデータのみを選択できます。

---

**特定のメタデータのロケーションにルールを適用する**

特定のメタデータのロケーションにルールを適用するには、次の手順を実行します。

**手順**

**ステップ 1** [Filter by Metadata] チェックボックスをオンにします。

**ステップ 2** [Filter] 領域で、[Add Metadata] ボタンをクリックします。  
[Choose Location Metadata] ウィンドウが表示されます。

**ステップ 3** ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

**ステップ 4** [Done] をクリックします。

---

**特定のメタデータのロケーションを除外する**

特定のメタデータのロケーションを除外するには、次の手順を実行します。

**手順**

**ステップ 1** [Filter by Metadata] チェックボックスをオンにします。

**ステップ 2** [Exclude] 領域で、[Add Metadata] ボタンをクリックします。  
[Choose Location Metadata] ウィンドウが表示されます。

**ステップ 3** ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

**ステップ 4** [Done] をクリックします。

---

**トリガー API の設定**

Cisco DNA Spaces ルールを使用して通知または顧客の詳細を外部 API に送信するように設定するには、次の手順を実行します。

- [Method] ドロップダウン リストから、API をトリガーするメソッドを選択します。



(注) API URI にスマートリンク変数を追加するか、メソッドパラメータに変数を追加することにより、API に送信される通知メッセージまたは顧客の詳細に顧客の姓名などのデータを含めることができます。

- **GET** : GET メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、要求パラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を含めることができます。API で定義された要求パラメータのキーを追加し、変数を使用してこれらの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が一覧表示されます。変数の詳細については、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。[Add] ボタンを使用して、さらに「get パラメータ」を追加できます。
- **POST FORM** : POST FORM メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、フォームパラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を含めることができます。API で定義されたフォームパラメータのキーを追加して、これらの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が一覧表示されます。変数の詳細については、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。[Add] ボタンを使用して、さらに「フォームパラメータ」を追加できます。
- **POST JSON** : POST JSON メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、API に送信する JSON データを指定できるテキストボックスが表示されます。API で定義されるさまざまな JSON フィールドの JSON 値を指定できます。値はハードコード値または変数のどちらでもかまいません。変数を JSON として追加するには、[JSON Data] テキストボックスをクリックします。変数がリストされます。追加する変数を選択します。変数の詳細については、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。
- **POST BODY** : POST BODY メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、API に送信する内容を指定できる追加のフィールドが表示されます。内容には変数を追加できます。変数を BODY として追加するには、[Post Body Data] テキストボックスをクリックします。変数がリストされます。
  - [URI] フィールドに、API の URI を入力します。スマートリンクを使用して、API に送信する通知または顧客データに追加の顧客情報を含めることができます。[URI] フィールドをクリックして追加できる変数を表示します。変数についての詳細は、[キャプティブポータルのスマートリンクとテキスト変数 \(105 ページ\)](#) を参照してください。



(注) GET、POST FORM、POST BODY、およびPOST JSON の各メソッドのカスタム変数を定義できます。メソッドの変数フィールドをクリックすると、事前定義された変数とともに [Add Custom Variable] ボタンが表示されます。POST BODY メソッドの場合、現在、POST BODY DATA フィールドに対するカスタム変数のサポートはありません。一方、URI フィールドにはカスタム変数のサポートがありません。



(注) ポータルの [Data Capture] モジュールを使用してキャプチャするように設定されたこれらのデータだけが通知に含まれます。

## ポータルへのソーシャル認証

ポータルへのソーシャル認証を有効にするには、次の手順を実行します。

- [Social Sign In 認証のためのポータル設定 \(15 ページ\)](#)

### ソーシャル認証に向けたワイヤレスネットワークの設定

ソーシャル認証の場合、Meraki や CUWN などのワイヤレスネットワークでいくつかの設定を行う必要があります。詳細については、次のリンクを参照してください。

- [ソーシャル認証のための Cisco Meraki の設定](#)
- [ソーシャル認証のためのシスコ ワイヤレス コントローラの設定](#)

### ソーシャル認証のためのアプリケーションの設定

このセクションでは、さまざまなネットワーキングサイトを介したソーシャル認証のためのアプリケーションに必要な設定について説明します。

#### Facebook

ソーシャル認証のために Facebook アプリケーションを設定するには、次の手順を実行します。

##### 手順

**ステップ 1** [developers.facebook.com](https://developers.facebook.com) に移動します。

**ステップ 2** [My Apps] ドロップダウンリストから、ソーシャル認証のために Cisco Spaces で設定するアプリケーションを選択します。

ステップ3 [設定 (Settings)] をクリックします。

ステップ4 [App Domains] フィールドに、リージョンに基づいて、以下のリストから適切な値を入力します。

- 米国の場合、**splash.dnaspaces.io** と入力します。
- EU の場合、**splash.dnaspaces.eu** と入力します。

ステップ5 [User Data Deletion] フィールドに、リージョンに基づいて、以下のリストから適切なデータ削除コールバック URL を入力します。

- 米国の場合、**https://splash.dnaspaces.io/p/<CustomerAccountName>/fb\_revoke** と入力します。
- EU の場合、**https://splash.dnaspaces.eu/p/<CustomerAccountName>/fb\_revoke** と入力します。

ステップ6 [Facebook Login Settings] タブの [Valid OAuth Redirect URIs] フィールドに、リージョンに基づいて、以下のリストから適切な値を入力します。

- 米国の場合、[https://splash.dnaspaces.io/p/facebook\\_auth](https://splash.dnaspaces.io/p/facebook_auth) と入力します。
- EU の場合、[https://splash.dnaspaces.eu/p/facebook\\_auth](https://splash.dnaspaces.eu/p/facebook_auth) と入力します。

---

## Twitter

ソーシャル認証のために Twitter アプリケーションを設定するには、次の手順を実行します。

### 手順

---

ステップ1 <https://developer.twitter.com/en/apps> にログインします。

ステップ2 ソーシャル認証のために Cisco DNA Spaces で設定するアプリケーションをクリックします。

ステップ3 [Settings] タブをクリックします。

ステップ4 [Callback URL] フィールドに、コールバック URL を入力します。

- グローバルリダイレクト URL : **https://splash.dnaspaces.io/p/twitter\_auth**
- EU のリダイレクト URL : **https://splash.dnaspaces.eu/p/twitter\_auth**

ステップ5 [Enable Callback Locking] チェックボックスをオフにします。

ステップ6 [Allow this application to be used to Sign in with Twitter] チェックボックスをオンにします。

ステップ7 Twitter から情報を取得するには、[Permissions] タブで次の操作を行います。

- [Access Permissions] エリアで、[Read and write] オプションボタンを選択します。

- [Additional Permissions] エリアで、[Request email address from users] をオンにします。

---

## LinkedIn アプリケーション

### 手順

- 
- ステップ 1 <https://www.linkedin.com/developers/> にログインします。
  - ステップ 2 [My Apps] をクリックします。
  - ステップ 3 ソーシャル認証のために設定するアプリケーションをクリックします。
  - ステップ 4 [Authentication] をクリックします。
  - ステップ 5 [Default Application Permissions] エリアで、[r\_basicprofile] および [r-emailaddress] チェックボックスをオンにします。
  - ステップ 6 [Authorized Redirect URLs] フィールドにリダイレクト URL を入力し、[Add] をクリックします。
    - グローバルリダイレクト URL : [https://splash.dnaspaces.io/p/linkedin\\_auth](https://splash.dnaspaces.io/p/linkedin_auth)
    - EU のリダイレクト URL : [https:// splash.dnaspaces.eu/p/linkedin\\_auth](https://splash.dnaspaces.eu/p/linkedin_auth)
  - ステップ 7 [Settings] タブで、ドメインの [splash.dnaspaces.io](https://splash.dnaspaces.io) を設定します。  
EU リージョンの場合、ドメインは [splash.dnaspaces.eu](https://splash.dnaspaces.eu) です。

---

## ソーシャル認証のためのソーシャル アプリケーションの追加

ソーシャルネットワークサイトを介したポータルへの認証を管理するには、対応するソーシャルアプリを Cisco DNA Spaces で設定する必要があります。たとえば、Facebook にサインイン中の顧客に対してポータルへのアクセスを認証する必要がある場合、Cisco DNA Spaces で Facebook アプリを設定する必要があります。Cisco DNA Spaces に追加できるソーシャルネットワーク サイトのアプリは次のとおりです。

- Facebook
- Twitter
- LinkedIn

Cisco DNA Spaces でソーシャルアプリを設定するには、次の手順を実行します。

### 手順

- 
- ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

**ステップ2** 表示されるウィンドウで、[Captive Portal] をクリックします。

**ステップ3** 表示される [Captive Portal] ウィンドウの左ペインで [Settings] をクリックします。

**ステップ4** [Settings] ウィンドウで [Social Apps] を選択します

**ステップ5** アプリを設定するソーシャル ネットワーク サイトに対応する [Add] ボタンをクリックします。

アプリケーションを設定するためのフィールドが表示されます。

**ステップ6** アプリケーションの名前、アプリケーションID、およびアプリケーションの秘密鍵を、それぞれのフィールドに入力します。

**ステップ7** [Save] をクリックします。

## ポータルの認定デバイス リスト

ポータルのためにテストされ、認定されているデバイスおよびオペレーティングシステムは、次の表のとおりです。

表 2:

デバイス	OS バージョン	ブラウザ/キャプティブネットワーク アシスタント (CNA) (サイトが正常に読み込まれ、動作する)
モバイルデバイス		
Moto G2	6.0	CNA、Google Chrome
Sony Xperia SP	4.3	Google Chrome
Samsung S2	4.1.2	Google Chrome
Samsung Galaxy S5	6.0.1	Google Chrome
Samsung S6	6.0.1	Google Chrome
Micromax	5.0 および 4.4.4	Google Chrome
Google Nexus 6	6.0.1	CNA、Google Chrome
Moto X Play	6.0.1	Google Chrome
iPhone 4s	7.1.2	CNA Safari
iPhone 5s	9.3.5 および 9.3.4	CNA、Safari
iPhone 6	9.3.4	CNA、Safari
iPhone 6s	9.3.4	CNA、Safari

デバイス	OS バージョン	ブラウザ/キャプティブネットワーク アシスタント (CNA) (サイトが正常に読み込まれ、動作する)
iPhone 6 Plus	9.3.2	CNA、Safari
Huawei Honor	6.0.1 および 6.0	Google Chrome
Huawei P8	5.0.1	Google Chrome
Microsoft Lumia 950	Windows 10	CNA およびネイティブブラウザ
Nokia Lumia 1320	Windows 8.1	CNA およびネイティブブラウザ
<b>iPad またはタブレット</b>		
Samsung Galaxy Tab 2	4.1.2	Google Chrome
Samsung Galaxy Tab 3 Neo	4.2.2	Google Chrome
iPad mini	8.3	CNA、Safari
iPad 2	9.3.2	CNA、Safari
<b>ラップトップまたはデスクトップ</b>		
Windows Lap HP ProBook	Windows 7	Chrome/Firefox/IE
Windows Lap Lenovo	Windows 10	Chrome/Firefox/IE
Macbook Pro 13-inch	Mac OS X El Capitan 10.11.6	CNA
Macbook Pro 13-inch Retina display	Mac OS X El Capitan 10.11.6	CNA

## Cisco Spaces キャプティブポータルの動作

さまざまなデバイスでのキャプティブポータルの動作は、次のとおりです。

### Apple iOS 7.x ~ 11.x

顧客がキャプティブポータル URL で設定されている SSID に接続すると、Captive Network Assistant (CNA) ウィンドウが表示されます。CNA によってポータルのコンテンツがロードされ、表示されます。

顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、「[ポータルへの認証の設定 \(11 ページ\)](#)」を参照してください。顧客は、利用規約への同意、SMS による検証、電子メールによる検証、またはソーシャル認証の使用を含む認証手順を実行する必要があります。各種認証タイプの認証手順の詳細については、「[顧客の認証手順 \(94 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク (CUWN, Meraki) に要求を送信します。インターネットプロビジョニングが正常に行われると、CNA ウィンドウは終了して、Mobile Safari が開きます。Mobile Safari では、顧客が先にクリックしていたメニューまたはリンクの Web ページが開きます。



- (注) iOS 11.0 ~ 11.3 の場合、インターネットプロビジョニング後、CNA ウィンドウは自動的に閉じられません。[Complete] ボタンをクリックして CNA ウィンドウを閉じるよう顧客に求めるメッセージが表示されます。

CNA が無視され、Mobile Safari または Chrome を使用して許可リストにない (アクセス制御リストまたはウォールガーデン範囲にない) URL にアクセスした場合、設定されているキャプティブポータルの URL にリダイレクトされます。ブラウザによってキャプティブポータルのコンテンツがロードされ、表示されます。顧客がポータルのメニューまたはリンクをクリックすると、[ログイン (Login)] 画面が表示されます。顧客は認証手順を完了して、インターネットをプロビジョニングする必要があります。



- (注) インターネットプロビジョニングの後、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。



- (注) インターネットプロビジョニング中にエラーが生じると、キャプティブポータルが再表示されます。



- (注) キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、リンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。

## Android 5.x 以降 (CNA を使用)

顧客がキャプティブポータル URL で設定されている SSID に接続すると、[Sign in to {SSID name}] オプションが通知領域に表示されます。この通知をクリックすると、Android 5.x 以降を搭載したデバイスでは、CNA ウィンドウが立ち上がります。CNA によってポータル URL が

らコンテンツがロードされ、ポータルが表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、[ポータルへの認証の設定 \(11 ページ\)](#) を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認、SMS 認証、Eメール認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、[顧客の認証手順 \(94 ページ\)](#) を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク (CUWN, Meraki) に要求を送信します。インターネットが正常にプロビジョニングされると、CNA ウィンドウが閉じます。

あるいは、顧客は通知を無視してネイティブブラウザまたは Chrome ブラウザの使用に進むこともできます。顧客が、許可リストにない (アクセス制御リストやウォールガーデンの範囲にない) URL にアクセスした場合、顧客は、設定済みのキャプティブポータル URL にリダイレクトされます。ブラウザによってキャプティブポータルのコンテンツがロードされ、表示されます。顧客がポータルのメニューまたはリンクをクリックすると、[ログイン (Log in)] 画面が表示されます。インターネットアクセスをプロビジョニングするには、顧客が前述の認証手順を完了する必要があります。インターネットプロビジョニングが行われると、顧客がクリックしていたメニューまたはリンクの Web ページが表示されます。



(注) インターネットプロビジョニングの後は、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。



(注) インターネットプロビジョニング中にエラーが生じると、キャプティブポータルが再表示されます。



(注) キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、リンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。

## Android 4.x 以前

顧客がキャプティブポータル URL で設定されている SSID に接続すると、[Sign in to {SSID name}] オプションが通知領域に表示されます。この通知をクリックすると、Android 4.x 以前を搭載したデバイスでは、デフォルトのブラウザが立ち上がります。ブラウザは、デバイスで生成される URL をロードしようとしています。この URL は許可リストにない (アクセス制御リストまたはウォールガーデンの範囲にない) ため、顧客はキャプティブポータルにリダイレクトされます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、[ポータルへの認証の設定 \(11 ページ\)](#) を参照してください。

顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認、SMS 認証、Email 認証、またはソーシャル認証を含む場合があります。各種認証タイプの認証手順の詳細については、[顧客の認証手順 \(94 ページ\)](#) を参照してください。顧客が認証を完了すると、Cisco Spacesがワイヤレスネットワーク (CUWN、Meraki) に対してこのデバイスのインターネットアクセスを提供するように要求を送信します。インターネットアクセスが正常に提供されると、顧客が以前にクリックしたメニューまたはリンクの Web ページが同じブラウザに表示されます。



- (注) インターネットアクセスがプロビジョニングされた後、顧客はそれ以上の認証なしでポータル内のメニューやリンクを移動できます。



- (注) インターネットプロビジョニング中にエラーが生じると、キャプティブポータルが再表示されます。



- (注) キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに認証を開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、[インライン認証 \(19 ページ\)](#) を参照してください。

## Windows Phone

顧客がキャプティブポータル URL で設定されている SSID に接続すると、Captive Network Assistant (CNA) が表示されます。CNA によってキャプティブポータル URL のコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、「[ポータルへの認証の設定 \(11 ページ\)](#)」を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Eメール認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、[顧客の認証手順 \(94 ページ\)](#) を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットアクセスをプロビジョニングするように、ワイヤレスネットワーク (CUWN、Meraki) に要求を送信します。インターネットが正常にプロビジョニングされると、CNA ウィンドウが閉じます。



- (注) インターネットプロビジョニング中にエラーが生じると、キャプティブポータルが再表示されます。



- 
- (注) キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、「[インライン認証 \(19 ページ\)](#)」を参照してください。
- 

## Windows PC とラップトップ

顧客が、キャプティブポータル URL で設定されている SSID に接続した後で、許可リストにならない（アクセス制御リストやウォールドガーデンの範囲にない）URL を参照した場合、顧客は、その SSID に対するキャプティブポータルページにリダイレクトされます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、「[ポータルへの認証の設定 \(11 ページ\)](#)」を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、E メール 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、「[顧客の認証手順 \(94 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク（CUWN, Meraki）に要求を送信します。インターネットプロビジョニングが行われると、顧客が先にクリックしていたメニューまたはリンクの Web ページが同じブラウザに表示されます。

Windows 10 の場合、顧客がキャプティブポータル URL で設定されている SSID に接続すると、Captive Network Assistant（CNA）が表示されます。CNA によってキャプティブポータル URL のコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、「[ポータルへの認証の設定 \(11 ページ\)](#)」を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、E メール 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、「[顧客の認証手順 \(94 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク（CUWN, Meraki）に要求を送信します。インターネットアクセスがプロビジョニングされると、CNA ウィンドウは閉じます。



- 
- (注) インターネットアクセスがプロビジョニングされた後、顧客はそれ以上の認証なしでポータル内のメニューやリンクを移動できます。
- 



- 
- (注) インターネットプロビジョニング中にエラーが発生すると、キャプティブポータルが再表示されます。
-



- (注) キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、「[インライン認証 \(19 ページ\)](#)」を参照してください。

## Macbook

顧客がキャプティブポータル URL で設定されている SSID に接続すると、Captive Network Assistant (CNA) ウィンドウが表示されます。CNA によってキャプティブポータルのコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、「[ポータルへの認証の設定 \(11 ページ\)](#)」を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認、SMS 認証、Eメール認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、「[顧客の認証手順 \(94 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該デバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク (CUWN、Meraki) にリクエストを送信します。インターネットプロビジョニングが正常に行われると、顧客のデフォルトのブラウザに、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。顧客が選択したページに加えて、ブラウザで CNA のホームページを含む別のタブが開きます。

あるいは、顧客は、キャプティブポータルのウィンドウを終了して、そのままブラウザを使用することもできます。顧客が、許可リストにない (アクセス制御リストやウォールドガーデンの範囲にない) URL にアクセスした場合、顧客は、設定済みのキャプティブポータル URL にリダイレクトされます。ブラウザによってキャプティブポータル URL のコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ログイン画面が表示されます。インターネットを利用するには、顧客はここで、前述した認証手順を完了する必要があります。インターネットプロビジョニングが正常に行われると、同じブラウザに、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。



- (注) インターネットプロビジョニングの後には、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。



- (注) インターネットプロビジョニング中にエラーが生じると、キャプティブポータルが再表示されます。



- (注) キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、「[インライン認証 \(19 ページ\)](#)」を参照してください。

## 顧客の認証手順

さまざまな認証タイプで、インターネットを利用できるようにするために顧客が完了する必要がある認証手順は、次のとおりです。

### リンク検証付き SMS による認証の手順

「リンク検証付き SMS」による認証を完了するには、次の手順を実行します。

#### 手順

**ステップ 1** キャプティブポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

**ステップ 2** 表示されるログイン画面で、携帯電話の番号を入力します。

(注)

[Data Capture] モジュールが設定されている場合、携帯電話番号フィールドを含むデータキャプチャフォームが表示されます。

**ステップ 3** データキャプチャフォームに携帯電話番号とすべての必須フィールドを入力し、[Accept Terms and Continue] を押します。

インターネット接続が提供され、ポータルにアクセスするためのリンクが含まれた SMS が、入力した携帯電話の番号に送信されます。

**ステップ 4** SMS 内のリンクをクリックして、フィンガープリント検証を行います。

フィンガープリント検証の詳細については、[フィンガープリントの検証 \(96 ページ\)](#) を参照してください。

(注)

顧客が一定時間内に SMS 内のリンクをクリックしなかった場合、[Skip] ボタンが表示されます。顧客は、フィンガープリント検証を行わずに [Skip] ボタンをクリックして先に進むことができます。顧客が次回インターネットにアクセスしようとする時、空白の携帯電話番号フィールドが表示され、携帯電話番号の再入力が必要とされます。これは、顧客がフィンガープリント検証を完了するまで、すべてのインターネットアクセスに対して発生します。

## リンク検証付き SMS でのレポートユーザーの認証手順

さまざまなシナリオでのレポートユーザーの認証手順は、次のとおりです。

- 指紋認証を完了している（[Data Capture] モジュールが設定されていない）：顧客がメニュー項目をクリック/タップすると、インターネットが提供されます。
- 指紋認証を完了している（[Data Capture] モジュールが設定され、[Data Capture] フォームに入力されている）：顧客がメニュー項目をクリック/タップすると、インターネットが提供されます。
- 指紋認証を完了しているが、[Data Capture] フォームに入力されてない、または一部が入力されている（必須フィールド以外）：顧客がメニュー項目をクリック/タップすると、インターネットが提供されます。ただし、[Data Capture] フォームに変更がある場合は、[Data Capture] フォームが表示されます。
- 指紋認証は完了していないが [Data Capture] フォームに入力されている：顧客がメニュー項目をクリックまたはタップすると、事前に入力された [Data Capture] フォームとともに携帯電話番号フィールドが表示されます。インターネットにアクセスするには携帯電話番号を再度入力する必要があります。これは、顧客が指紋認証を完了するまで、すべてのインターネットアクセス試行に対して継続されます。
- 前回のインターネットアクセス中に携帯電話番号の検証プロセスが完了していなかった：所定の時間内に検証プロセスが完了しなかった場合、無効な携帯電話番号に対してもインターネットが提供されます。このようなレポートユーザーの場合、キャプティブポータルが読み込まれ、顧客がポータル内のメニュー項目またはリンクをクリックすると、ログイン画面に携帯電話番号フィールドが表示されます。有効な携帯電話番号を入力する必要があります。
- [Data Capture] モジュールが設定されており、登録情報が無効化している：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前に入力されたデータを含む登録フォームが表示されます。顧客は、フォームを更新して [Connect] を押すと、インターネットにアクセスできます。

以下は、登録情報が無効化するシナリオの一部です。

- **新規必須フィールドを追加**：[Data Capture] モジュールに新規必須フィールドを追加した場合。たとえば、次のような場合です。[Gender] フィールドなしで [Data Capture] モジュールを設定。顧客が登録を完了。その後、[Data Capture] モジュールに [Gender] フィールドを必須フィールドとして追加。
- **オプションのフィールドが必須になった場合**：[Data Capture] モジュールが変更され、顧客が登録時に入力しなかった任意フィールドを必須フィールドとした場合。たとえば、次のような場合です。[Last Name] を任意にして [Data Capture] モジュールを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、[Data Capture] モジュールを変更し、[Last Name] を登録のために必須とする。
- **選択肢を変更した場合**：選択可能だった選択肢が削除または置き換えられた場合。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須の

ビジネス タグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。



(注) 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。インターネットにアクセスしたり、次の認証手順に進んだりするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

## フィンガープリントの検証

顧客が「リンク検証付き SMS」認証用の携帯電話番号を提供すると、提供された携帯電話番号にリンク付きのメッセージが送信され、インターネットのプロビジョニングが行われます。フィンガープリント検証は、顧客がメッセージ内のリンクをクリックすると実行されます。事前に定義された時間内に顧客がリンクをクリックしない場合、[SKIP] オプションを含む一時ページが顧客に表示されます。顧客が [Skip] オプションをクリックすると、フィンガープリント検証なしでインターネットにアクセスできます。

さまざまなシナリオのフィンガープリント検証ステータスを次に示します。

- 顧客がメッセージ内のリンクをクリックすると、フィンガープリントが一致した場合は顧客獲得が行われ、顧客はポータルページにリダイレクトされます。顧客は、次の訪問時にはリピートユーザーと見なされます。
- 顧客がメッセージ内のリンクをクリックしたときにフィンガープリント検証に失敗すると（たとえば、顧客が SMS 認証の開始に使用したものは別のブラウザでリンクを開いた場合、フィンガープリント検証は失敗します）、確認ページが顧客に表示されます。顧客が [Confirm] をクリックすると、顧客獲得が行われ、顧客はポータルページにリダイレクトされます。顧客は、次の訪問時にはリピートユーザーと見なされます。
- 顧客がメッセージ内のリンクをクリックしたときにフィンガープリント検証に失敗すると、顧客に確認ページが表示されます。顧客が [Cancel] をクリックすると、顧客は次の訪問時に初回ユーザーと見なされ、ログイン画面に空白の携帯電話番号フィールドが表示されます。
- 表示された一時ページで顧客が [Skip] をクリックすると、顧客は次の訪問時に初回ユーザーと見なされ、ログイン画面に空白の携帯電話番号フィールドが表示されます。

## SMS with Password Verification 認証の手順

SMS with password verification 認証を完了するには、次の手順を実行します。

### 手順

**ステップ 1** キャプティブポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

**ステップ 2** 表示されるログイン画面で、携帯電話の番号を入力します。

(注)

同じ携帯電話番号を使用して複数のデバイスを接続できますが、新しいデバイスを接続するたびに、以前のユーザーアイデンティティが添付されます。

ただし、OTP を入力できるのは 1 分間に 3 回までです。3 回試行すると、それ以上のログイン試行は一時的に制限されます。

**ステップ 3** 顧客が通知の受け取りを停止するには、[Opt In to Receive notification] チェックボックスをオフにします。

(注)

[Opt In to receive notification] チェックボックスがログイン画面に表示されるのは、ポータルの認証の詳細を設定する際、[Authentication] 画面で [Allow users to Opt in to receive message] チェックボックスをオンにしていた場合のみです。

**ステップ 4** [Accept Terms and Continue] を押します。

**ステップ 5** 表示される画面で、SMS を通じて受け取った認証コードを入力します。

**ステップ 6** [Verify] を押します。

データキャプチャフォームが設定されている場合、認証コードの検証が成功すると、データキャプチャフォームが表示されます。

**ステップ 7** データキャプチャフォームのすべての必須フィールドに入力し、[Connect] を押します。

(注)

すべてのフィールドが任意である場合、[Skip] と [Connect] という 2 つのボタンが表示されます。[Skip] ボタンをクリックすると、顧客はデータを入力せずに続行することができます。フォームに変更がある場合のみ、顧客が [Skip] をクリックした際に、顧客に対して登録フォームが表示されます。

登録が成功すると、インターネットプロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

(注)

[Data Capture] モジュールが有効でない場合、認証コードの検証後、インターネットはすぐにプロビジョニングされます。

---

## パスワード検証付き SMS によるレポートユーザーの認証手順

さまざまなシナリオでのレポートユーザーの認証手順は、次のとおりです。

- **データキャプチャが設定されていない** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。
- **データキャプチャが設定されており、顧客が登録を完了している** : キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。

- **データキャプチャが設定されていない、登録詳細が古い** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前入力したデータが入ったデータキャプチャフォームが表示されます。顧客はフォームを更新して [Connect] ボタンを押すと、インターネットにアクセスできます。

以下は、登録情報が無効化するシナリオの一部です。

- **新規必須フィールドを追加** : データキャプチャフォームに新規必須フィールドを追加した場合。たとえば、次のような場合です。[Gender] フィールドなしでデータキャプチャフォームを設定。顧客が登録を完了。その後、データキャプチャフォームに [Gender] フィールドを必須フィールドとして追加。
- **オプションのフィールドが必須になった場合** : データキャプチャフォームが変更され、顧客が登録時に入力しなかった任意フィールドが必須フィールドになっています。たとえば、次のような場合です。[LastName] を任意にしてデータキャプチャフォームを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、データキャプチャフォームを変更し、フォームの [Last Name] を必須とした場合などです。
- **選択肢を変更した場合** : 選択可能だった選択肢が削除または置き換えられています。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須のビジネス タグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。
- **前回のログイン時に無効な電子メール ID を入力した場合** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、前回ログイン時に入力された無効な電子メール ID を含むデータキャプチャフォームが表示されます。続行するには、顧客は有効な電子メール ID を入力する必要があります。



- (注) 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。顧客がインターネットにアクセス、または次の認証手順に進むには、[Accept Terms and Continue] ボタンを押す必要があります。

## 電子メール認証の手順

Email 認証を完了するには、次の手順を実行します。

### 手順

- ステップ 1** キャプティブポータルで、いずれかのメニューアイテムをクリックまたはタップします。
- ステップ 2** 表示されるログイン画面で、電子メール ID を入力します。
- ステップ 3** 顧客が通知の受け取りを停止するには、[Opt In to Receive notification] チェックボックスをオフにします。

(注)

[Opt In to Receive notification] チェックボックスがログイン画面に表示されるのは、ポータルの認証の詳細を設定する際に、認証タイプ [Email] について [Allowed users to Opt in to receive message] チェックボックスをオンにしていた場合のみです。

**ステップ 4** [Accept Terms and Continue] を押します。

入力された電子メール ID が有効であれば、インターネットが利用できるようになります。

**ステップ 5** キャプティブポータルの認証画面でデータキャプチャが有効になっている場合、顧客が [Accept Terms and Continue] を押すと、データキャプチャフォームが表示されます。

**ステップ 6** データキャプチャフォームのすべての必須フィールドに入力し、[Connect] を押します。

(注)

すべてのフィールドが任意である場合、[Skip] と [Connect] という 2 つのボタンが表示されます。[Skip] ボタンをクリックすると、顧客はデータを入力せずに続行することができます。顧客が [Skip] をクリックした際、フォームに変更がある場合のみ、リピーターユーザーに対してデータキャプチャフォームが表示されます。

インターネットプロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

---

## Email 認証によるリピーターユーザの認証手順

Cisco Spaces では、新しいユーザーの認証ワークフローの一環として、電子メールアドレスを一度だけ入力する必要があります。ドメイン関連のすべての検証と MX レコードのチェックは特定の期間キャッシュされ、キャッシュされている期間内の同じドメインの他のユーザーに対して同じチェックが繰り返されることはありません。

たとえば、10 人のユーザーがキャプティブポータルに同時に接続し、同じドメイン

(xyz@abc.com) に属する電子メールアドレスを入力した場合、ドメイン検証と MX レコードチェックは、指定されたキャッシング期間中に一度だけ実行されます。ただし、ユーザー ID が有効かどうかを検証するために、10 人のユーザーすべてに対して SMTP 接続とメールボックスのチェックが実行されます。

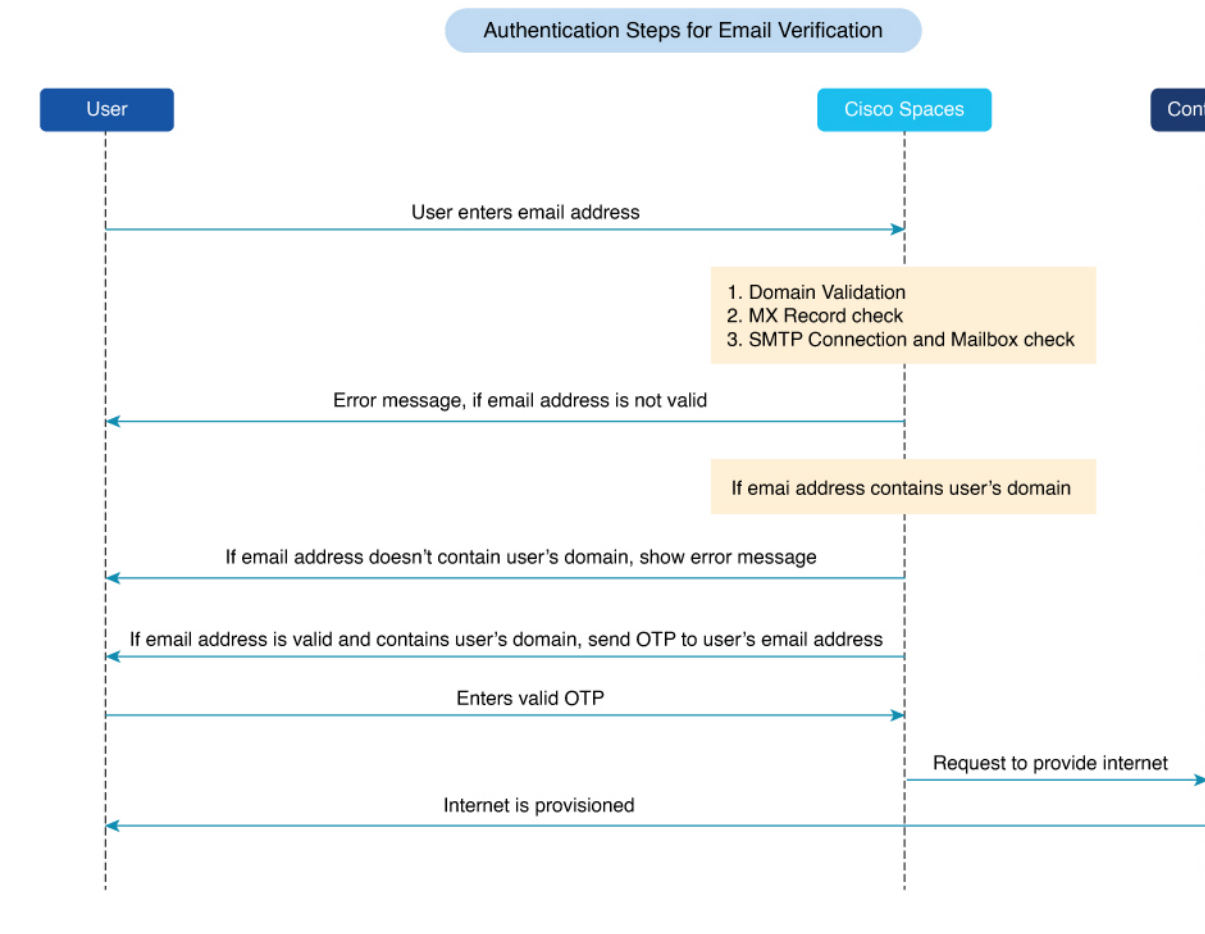
SMTP 接続を確立するには、次の手順を実行します。

1. SMTP サーバーへのソケット接続を確立し、応答を確認します。
2. **ELHO** コマンドを実行し、応答を確認します。
3. **MAIL FROM** コマンドを実行し、応答を確認します。
4. **RCPT TO** コマンドを実行し、応答を確認します。



(注) キャプティブポータルの新規ユーザーオンボーディングワークフローの一環として、ユーザーの電子メールアドレスが一度だけ記録されます。Cisco Spaces がメールボックスチェックから応答を受信しなかった場合でも、Cisco Spaces への認証が許可されます。ただし、次のアクセス時に電子メールアドレスを再度入力する必要があります。メールボックスチェックプロセスの一環として、Cisco Spaces では、ユーザーが指定した電子メールアドレスに電子メール要求が送信されることはありません。

図 7: 認証ワークフロー



### 認証シナリオ

さまざまなシナリオでのリピーターユーザーの認証手順は、次のとおりです。

- **前回ログイン時に無効な電子メール ID を入力した場合**：キャプティブポータルがロードされ、ポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、前回ログイン時に入力された無効な電子メール ID を含むログイン画面が表示されます。続行するには、有効な電子メール ID を入力する必要があります。

- **データキャプチャが有効でない場合** : キャプティブポータルがロードされ、ポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットが利用できるようになります。
- **データキャプチャが有効で、顧客が登録を完了した場合** : キャプティブポータルがロードされ、ポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットが利用できるようになります。
- **データキャプチャが有効で、登録情報が古くなっている場合** : キャプティブポータルがロードされ、ポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前に入力されたデータを含むデータキャプチャフォームが表示されます。フォームを更新し、[接続 (Connect)] をクリックすると、インターネットにアクセスできます。

### 登録情報

以下は、登録情報が無効化するシナリオの一部です。

- **新規必須フィールドを追加** : データキャプチャフォームに新規必須フィールドを追加した場合。たとえば、データキャプチャフォームを[性別 (Gender)] フィールドなしで設定した場合です。登録プロセスを完了します。その後、データキャプチャフォームに[性別 (Gender)] フィールドを必須フィールドとして追加しました。
- **オプションのフィールドが必須になった場合** : データキャプチャフォームが変更され、顧客が登録時に入力しなかった任意フィールドが必須フィールドになっています。たとえば、<Last Name> を任意にしてデータキャプチャフォームを設定した場合です。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、データキャプチャフォームを変更し、フォームで姓を必須としました。
- **選択肢を変更した場合** : 選択可能だった選択肢が削除または置き換えられた場合。たとえば、**Age Criteria (年齢基準)** という必須のビジネスタグを **Child** および **Adult** という選択肢で設定した場合です。顧客は **Age Criteria** に **Child** を選択して登録を完了しました。その後、選択肢の表示を **Kids** と **Adult** に変更しました。



- (注) 上記のすべてのシナリオで、定義済みの**利用規約**が変更された場合は、[規約を承認し続行 (Accept Terms and Continue)] オプションが表示されます。インターネットにアクセスするか、次の認証手順に進むには、[規約を承認し続行 (Accept Terms and Continue)] オプションをクリックする必要があります。

## アクセスコード認証の手順

アクセスコード認証を完了するには、次の手順を実行します。

## 手順

**ステップ 1** キャプティブポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

**ステップ 2** [ログイン (Log In) ] ウィンドウで、アクセスコードを入力します。

**ステップ 3** 顧客が通知の受け取りを停止するには、[Opt In to Receive notification] チェックボックスをオフにします。

(注)

[Opt In to receive notification] チェックボックスがログイン画面に表示されるのは、ポータルの認証の詳細を設定する際、[Authentication] 画面で [Allow users to Opt in to receive message] チェックボックスをオンにしていた場合のみです。

**ステップ 4** [Accept Terms and Continue] を押します。

**ステップ 5** [Verify] を押します。

[Data Capture] が有効である場合、アクセスコードの検証が成功すると、データキャプチャフォームが表示されます。

**ステップ 6** データキャプチャフォームのすべての必須フィールドに入力し、[Connect] を押します。

(注)

- すべてのフィールドが任意である場合、[Skip] と [Connect] という 2 つのボタンが表示されます。[Skip] ボタンをクリックすると、顧客はデータを入力せずに続行することができます。フォームに変更がある場合のみ、顧客が [Skip] をクリックした際に、顧客に対して登録フォームが表示されます。

登録が成功すると、インターネットプロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

- **Data Capture** モジュールが有効でない場合、認証コードが検証されると、すぐにインターネット接続が提供されます。
- **時間によるセッションの制限** または **帯域幅の制限** を設定する必要がある場合は、ネットワーク用に Cisco Spaces Radius サーバーを設定していることを確認してください。Cisco Spaces RADIUS サーバーをセットアップするには、「[RADIUS 認証用の Cisco Meraki の設定](#)」および「[インターネットプロビジョニングおよび RADIUS 認証用のシスコワイヤレスコントローラの設定](#)」を参照してください。

## アクセスコード認証によるリピートユーザーの認証手順

さまざまなシナリオでのリピートユーザーの認証手順は、次のとおりです。

- **データキャプチャが設定されていない** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。

- **データキャプチャが設定されていない、顧客が登録を完了している** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。
- **データキャプチャが設定されていない、登録詳細が古い** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前入力したデータが入ったデータキャプチャフォームが表示されます。顧客はフォームを更新して [Connect] ボタンを押すと、インターネットにアクセスできます。

以下は、登録情報が無効化するシナリオの一部です。

- **新規必須フィールドを追加** : データキャプチャフォームに新規必須フィールドを追加した場合。たとえば、次のような場合です。[Gender] フィールドなしでデータキャプチャフォームを設定。顧客が登録を完了。その後、データキャプチャフォームに [Gender] フィールドを必須フィールドとして追加。
- **オプションのフィールドが必須になった場合** : データキャプチャフォームが変更され、顧客が登録時に入力しなかった任意フィールドが必須フィールドになっています。たとえば、次のような場合です。[LastName] を任意にしてデータキャプチャフォームを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、データキャプチャフォームを変更し、フォームの [Last Name] を必須とした場合などです。
- **選択肢を変更した場合** : 選択可能だった選択肢が削除または置き換えられています。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須のビジネスタグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。
- **前回のログイン時に無効な電子メール ID を入力した場合** : キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、前回ログイン時に入力された無効な電子メール ID を含むデータキャプチャフォームが表示されます。続行するには、顧客は有効な電子メール ID を入力する必要があります。



(注) 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。顧客がインターネットにアクセス、または次の認証手順に進むには、[Accept Terms and Continue] ボタンを押す必要があります。

## 利用規約による認証省略の手順

顧客へのインターネットプロビジョニングを、顧客が利用規約を承認することのみを条件として行うように設定することができます。

利用規約の承認のみが必要な認証を完了するには、次の手順を実行します。

## 手順

**ステップ 1** キャプティブポータルで、いずれかのメニューアイテムをクリックまたはタップします。

**ステップ 2** 表示されるログイン画面で、[Accept Terms and Continue] を押します。

インターネットプロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

## 利用規約の承認によるリピート ユーザの認証手順

キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットが利用できるようになります。



(注) 定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。インターネットにアクセスしたり、次の認証手順に進んだりするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

## ソーシャル認証の手順

ポータルへのソーシャル認証を完了するには、次の手順を実行します。

## 手順

**ステップ 1** 顧客がキャプティブポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、ポータルへのすべての Social Sign In オプションが使用できる画面が表示されます。

(注)

サインインオプションは、ポータルに設定されているソーシャルネットワークのみに表示されます。ポータルに対してソーシャルネットワークを設定する方法の詳細については、[Social Sign In 認証のためのポータル設定 \(15 ページ\)](#) を参照してください。

**ステップ 2** 認証を完了するために使用するソーシャルネットワークのサインインオプションをクリックします。ソーシャルネットワークのログインページが表示されます。

たとえば、LinkedIn のサインインオプションをクリックすると、LinkedIn のログイン画面が表示されます。

**ステップ 3** ソーシャルネットワークのログイン クレデンシャルを入力して、ログイン ボタンを押します。

**ステップ 4** 表示される画面で、[Allow] を押します。

リダイレクト URI がロードされ、[Terms and Conditions] 画面が表示されます。

**ステップ 5** [Accept Terms and Continue] を押します。

(注)

Facebook および Twitter には、リダイレクト URI の設定は不要です。リダイレクト URI は、Linked In の場合に設定が必要です。Linked In のリダイレクト URI を設定するときの詳細については、[ソーシャル認証のためのアプリケーションの設定 \(84 ページ\)](#) を参照してください。

**ステップ 6** インターネットプロビジョニングが行われると、[Continue] ウィンドウが表示されます。

**ステップ 7** 先にクリックしていたリンクのページを表示するには、[Continue] を押します。

## ソーシャル認証によるリピーターユーザの認証手順

キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、設定されているすべてのソーシャルネットワークについて、接続のためのオプションが表示されます。顧客が以前に認証のために使用したソーシャルネットワークは、「Continue with [social network]」というラベルで表示されます。たとえば、顧客が以前、キャプティブポータルを通じたインターネットへのアクセスに Facebook 認証を使用していた場合、Facebook のオプションが、[Continue with Facebook] というラベルで表示されます。これまで認証に使用されていないソーシャルネットワークについては、サインインオプションが表示されます。たとえば、[Signin with LinkedIn] です。

- 顧客が以前に認証のために使用したソーシャルネットワークを継続して使用する場合、インターネットは、認証プロセスなしで利用できます。ただし、利用規約に変更がある場合は、[Terms and Conditions] 画面が表示されます。このとき、インターネットにアクセスするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。
- 顧客がこれまで認証に使用されていないソーシャルネットワークを使用してサインインする場合、顧客は、そのソーシャルネットワークの認証プロセスの全体を完了する必要があります。顧客がいずれかのソーシャルネットワークを介したソーシャル認証を使用してインターネットにアクセスした場合、認証プロセス中に [Terms and Conditions] 画面は表示されません。ただし、利用規約に変更がある場合は、認証プロセス中に [Terms and Conditions] 画面が表示されます。このとき、インターネットにアクセスするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

## キャプティブポータルのスマートリンクとテキスト変数

### スマートリンク

スマートリンクオプションにより、パーソナライズされた Web ページやメッセージを顧客に提供することができます。[Smart Link] オプションを使用して、キャプティブポータル内のカスタムメニューリンクへの URL をカスタマイズし、パーソナライズされたビューを提供することができます。サイトのページをユーザ別またはユーザのグループ別にパーソナライズすることができます。

たとえば、ポータル内のカスタムメニューアイテムに「optedinstatus」パラメータを設定することができます。これにより、このカスタムメニューアイテムの Web ページで「オプトイン」ユーザーと「非オプトイン」ユーザーに対して異なるコンテンツを表示するよう設定すること

ができます。オプトインユーザーがキャプティブポータルでカスタムメニューリンクをクリックすると、オプトインユーザー用のコンテンツが表示されます。非オプトインユーザーが同じカスタムメニューリンクをクリックすると、非オプトインユーザー用のコンテンツが表示されます。



(注) これらのパラメータを使用して顧客にパーソナライズされたビューを表示するためには、Web ページをそれに応じて設定する必要があります。

キャプティブポータルアプリケーションで、スマートリンクを以下のオプションに含めることができます。

- ポータルのカスタムメニューアイテムに追加されたリンク。
- トリガー API の **URI** フィールドに追加された URL。

### テキスト変数

テキスト変数を使用することで、**Trigger API** を使用して API エンドポイントに送信されるメッセージに、名前、携帯電話番号、性別などの顧客の個人情報を追加できます。デフォルトでは、メッセージに顧客の姓名が記載されます。この変数を使用して、さらに顧客の詳細を追加できます。

たとえば、Trigger API 通知を作成し、SMS 通知の [メッセージ (message) ] テキストボックスに変数「mobile」および「gender」を設定していたとします。この場合、顧客がこのエンゲージメントルールに基づく SMS メッセージを受信すると、メッセージには、顧客の携帯電話の番号と性別の詳細も表示されます。

次のオプションで変数を追加できます。

- **Trigger API** を使用して API エンドポイントに送信されるメッセージ。
- 初めてのユーザーとリピーターのユーザーへのウェルカムメッセージ。
- ポータルに追加された通知 (バックエンドサポートのみ)。

Cisco Spaces は、データキャプチャフォームを使用して顧客の個人情報を取得します。スマートリンクまたはテキスト変数に名、姓、性別などの個人に関する詳細を含めるためには、ポータルにデータキャプチャフォームを設定する必要があります。キャプティブポータルへのデータキャプチャフォームの追加の詳細については、「[ポータルへのデータキャプチャフォームの追加](#)」セクションを参照してください。



(注) 「SMS with link verification」と「SMS with password verification」メッセージに含まれるキャプティブポータルの URL は、スマートリンク機能ではサポートされません。

Cisco Spaces は特定の定義済み変数を提供します。Web ページのパーソナライズされたビューの提供と、通知メッセージへの顧客の詳細の追加には、これらの変数を使用する必要があります。

スマートリンクには、静的変数と動変数を含めることができます。

スマートリンクまたはテキストに含めることができる静的パラメータは、次のとおりです。

表 3: 静的変数一覧

静的変数名	説明
<b>\$location</b> または <b>\$locationName</b>	ルールがトリガーされるロケーションの名前。
<b>\$Address</b>	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定されたアドレス。
<b>\$State</b>	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定されたステート。
<b>\$Country</b>	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定された国。
<b>\$City</b>	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定された市区町村。
<b>\$TotalAreaValue</b>	[Location Hierarchy] の [Location Info] ウィンドウのロケーションに設定されたエリア合計。
<b>\$firstName</b> (ウェルカムモジュールの初回訪問者には適用されません)。	顧客の名前。
<b>\$lastName</b> (ウェルカムモジュールの初回訪問者には適用されません)。	顧客の姓。
これらの変数は <b>Welcome</b> モジュールには適用されませんが、カスタムモジュールとトリガー API にのみ適用されます。	
<b>\$email</b>	顧客の電子メールアドレス。
<b>\$mobile</b>	顧客の携帯電話番号。
<b>\$gender</b>	顧客の性別。
<b>\$URL</b>	URL リンク値。
<b>\$macaddress</b>	デバイスの MAC アドレス。
<b>\$encryptedMacAddress</b>	暗号化された、デバイスの MAC アドレス。
<b>\$deviceSubscriberId</b>	データベース内のデバイスのサブスクライバ ID。
<b>\$optinStatus</b>	顧客のオプトインステータス。

さらに、スマートリンクまたはテキストには、次の動的変数を含めることができます。

表 4: 動的変数一覧

動的変数名	説明
<b>Business Tags</b>	顧客が属するビジネスタグ。データキャプチャフォームで設定されるビジネスタグは、変数としてリストされます。ビジネスタグの作成の詳細については、「 <a href="#">ポータルへのデータキャプチャフォームの追加</a> 」セクションを参照してください。
<b>Location Metadata</b>	顧客のロケーションのロケーションメタデータ。ロケーション階層で定義されたロケーションメタデータキーは、変数としてリストされます。ロケーションメタデータの定義の詳細については、「 <a href="#">ロケーションのメタデータの定義または編集</a> 」セクションを参照してください。

URL にスマートリンクを、またはテキストに変数を挿入するには、次の手順を実行します。

## 手順

---

**ステップ 1** URL フィールドまたはテキストボックスの任意の場所をクリックするか、対応する [変数の追加 (Add Variable) ] ドロップダウンリストをクリックします。

追加できる変数がリストされています。

**ステップ 2** 追加する変数を選択します。

---

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。