COTOHA Meeting Assist
二要素認証設定マニュアル

2020.11.17 版

NTTコミュニケーションズ株式会社

目次

1．二要素認証機能の概要 4

1.1． 二要素認証機能とは 4
1.2． 認証キーの確認方法 5
1.3． 二要素認証の有効化 7
1.4． 二要素認証を利用したログイン 8

2．クライアント端末の設定 9

2.1． 推奨クライアントアプリ 9
2.1.1. Authy の提供形態 9
2.1.2. Authy の取得方法 9
2.2． iPhone で利用する場合 10
2.2.1. アプリケーションのインストール 10
2.2.2. アプリケーションの初期セットアップ 12
2.2.3. 認証キーの登録 15
2.2.4. QR コードが認識されない場合(Iphone) 19
2.3． Android で利用する場合 21
2.3.1. アプリケーションのインストール 21
2.3.2. アプリケーションの初期セットアップ 23
2.3.3. 認証キーの登録 26
2.4． PC で利用する場合 30
2.4.1. クライアントアプリのインストール(Windows) 30
2.4.2. クライアントアプリの初期セットアップ 31
2.4.3. 認証キーの登録 36
2.4.4. 二要素認証を利用したコントロールパネルへのログイン 41

本書および本書以外のマニュアルについて

ご利用の用途・目的毎に別冊のマニュアルがあります。

様々なご利用方法がありますので、ご覧いただく事をお薦めします。

マニュアル名	用途・目的	対象
セットアップマニュアル	本サービスのご利用前に必要となる設定マニュアル （セキュリティ設定/ユーザーID の準備）	管理者
管理・設定マニュアル	本サービスの詳細設定（セキュリティ設定/ユーザー管理等） ウェブサーバーおよびメールサーバーとしての利用	管理者
【別冊】二要素認証設定マニュアル（本書）	二要素認証のクライアントアプリ（Authy）の設定	管理者
利用マニュアル	サービスの利用、利用者の個人設定	利用者
【別冊】メール設定マニュアル （M&WPremiumR2 共通）	メールソフト Outlook 等の設定	利用者
【別冊】Active!mail 利用マニュアル （M&WPremiumR2 共通）	ウェブメール機能 Active!mail の利用	利用者

1.二要素認証機能の概要

二要素認証の設定をするサーバー管理者、またはドメイン管理者は COTOHA Meeting Assist のサービス画面上で認証キーを確認することができます。

1.1．二要素認証機能とは

管理者・ドメイン管理者がコントロールパネルへログインする際に、通常のパスワードだけではなく、もう一つのパスワード（ワンタイムパスワード）による二重の認証を行う仕組みです。パスワードの流出等が発生した場合に、不正にコントロールパネルへのログインを防ぐことが出来ます。

　COTOHA Meeting Assist では「時刻同期ワンタイムパスワード方式」の二要素認証機能を提供しており、30 秒ごとにワンタイムパスワードが更新されます。

1.2. 認証キーの確認方法

1. 二要素認証の設定をするサーバー管理者、またはドメイン管理者のユーザーID とパスワードを入力し、[ログイン]ボタンをクリックします。

2. 右上のユーザーID の部分をクリックし、[二要素認証]をクリックします。

3． 認証キーが「テキスト形式」と「QR コード形式」で表示されます。

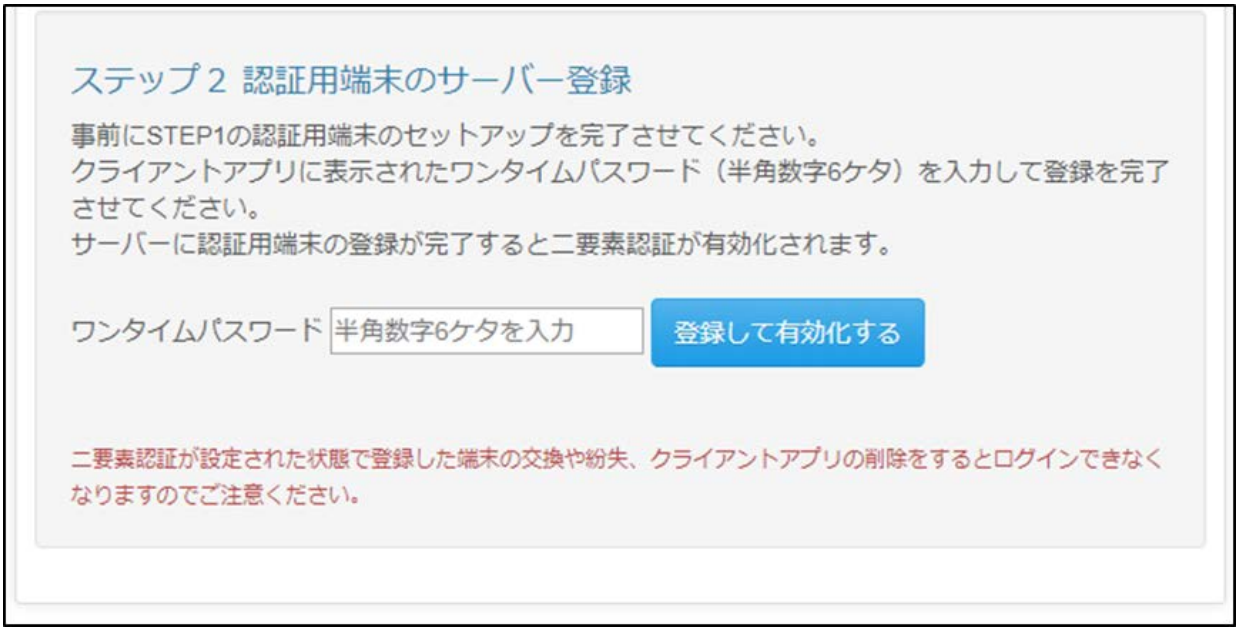
1.3. 二要素認証の有効化

二要素認証の有効化させるには以下の手順で設定が必要となります。

1. 二要素認証を有効化させるにはクライアント端末（クライアントアプリ）への認証キーを登録します。

   ※詳細は「2. クライアント端末の設定」内の「認証キーの登録」の項目を参照してください。

2. クライアントアプリ上に表示されたワンタイムパスワードをサービス画面へ登録します。

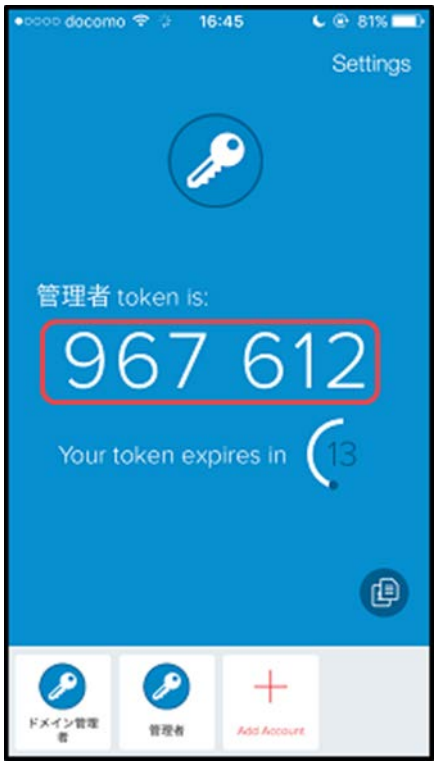


1.4．二要素認証を利用したログイン

1.コントロールパネルにアクセスし、ユーザーID、パスワードを入力し、「**※二要素認証を設定している場合はクリック**」をクリックすると[ワンタイムパスワード]欄が表示されます。

2.クライアントアプリ(Authy)に表示されている 6 桁のワンタイムパスワードを確認し、2．のワンタイムパスワード欄に入力し、[ログイン]をクリックします。

3.正常にログインできれば、二要素認証は正常に設定されています。



・サーバー管理者およびドメイン管理者以外のユーザーは、二要素認証機能はご利用いただけません。

・サーバー管理者にて二要素認証を有効化している場合、設定したクライアント端末およびアプリケーションを紛失・破損するとログインできなくなりますので十分にご注意ください。

万一、ログインできなくなった場合は管理者のパスワード再発行手続きが必要になります。

2.クライアント端末の設定

クライアント端末の設定は端末の種類ごとにご説明しております。
端末の種類をご確認の上、設定を行ってください。

2.1. 推奨クライアントアプリ

COTOHA Meeting Assist では二要素認証のクライアントアプリに「Authy」を推奨しています。

2.1.1. Authy の提供形態

Android アプリ（Android スマートフォン用）
iPhone アプリ（iPhone スマートフォン用）
Authy デスクトップアプリ (PC 用)

2.1.2. Authy の取得方法

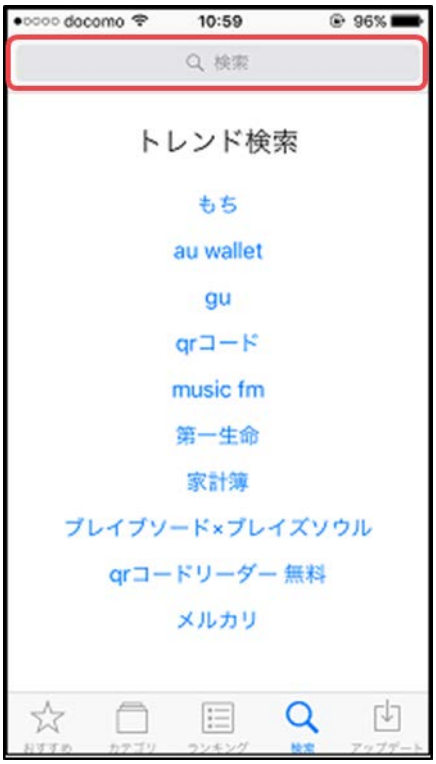
Authy のダウンロードページは各クライアントの種類により異なります。
下記のリンクから認証用端末にアプリケーションをインストールしてください。

https://authy.com/download/

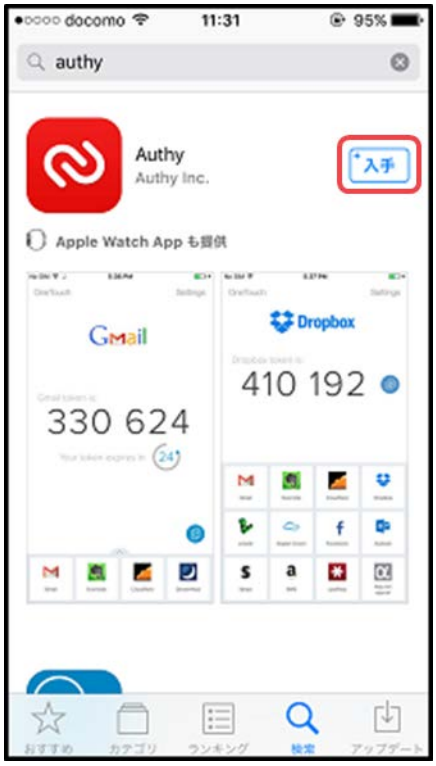
2.2. iPhone で利用する場合

2.2.1. アプリケーションのインストール

1. App Store を起動して、検索をタップします。
2. 検索欄に「authy」と入力して、右下の「Search」をタップします。



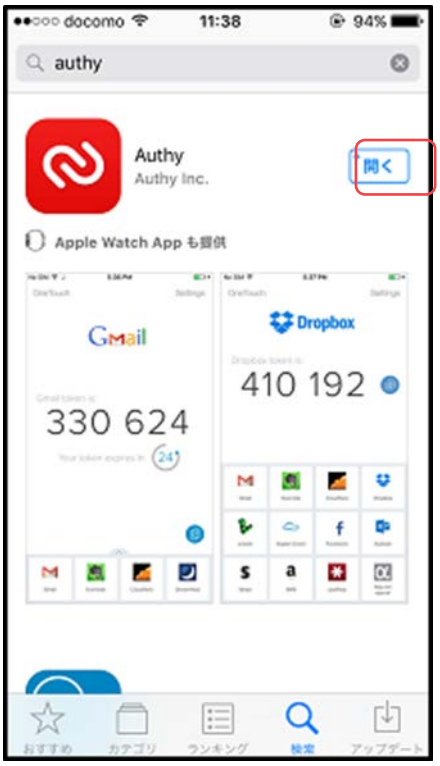
3. 検索結果が表示されたら、入手をタップします。
4. インストールをタップします。

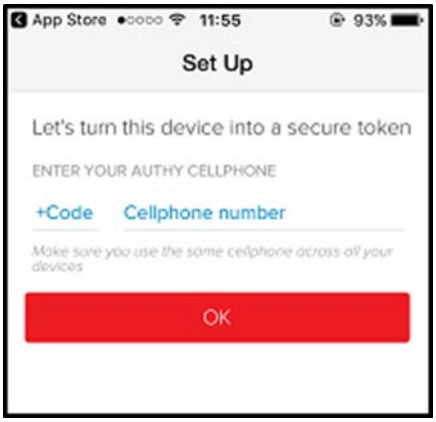


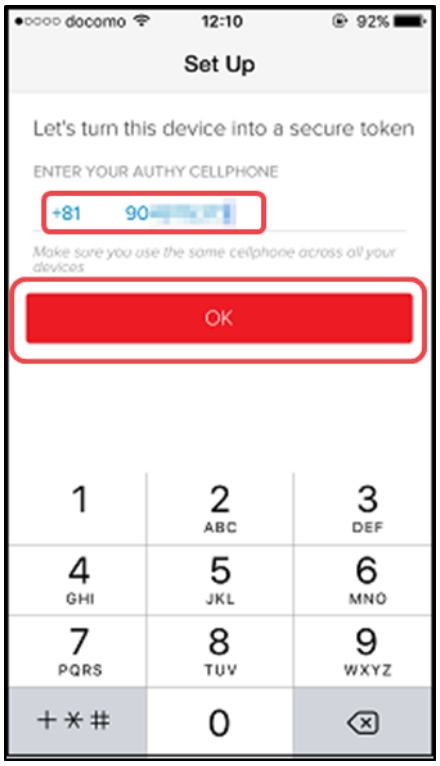
2.2.2. アプリケーションの初期セットアップ

1. インストール完了後に、開くをタップします。
2. セットアップ画面が開き、電話もしくは SMS 受信による認証を行います。
3. 電話番号の入力し、OK をタップします。

「+Code」は日本国際電話コード「+81」を選択します。
「Cellphone number」にはお客さまの電話番号を入力します。
なお、電話番号を入力する際には、先頭の「0」を省略します。
例）090-1234-5678 → 9012345678



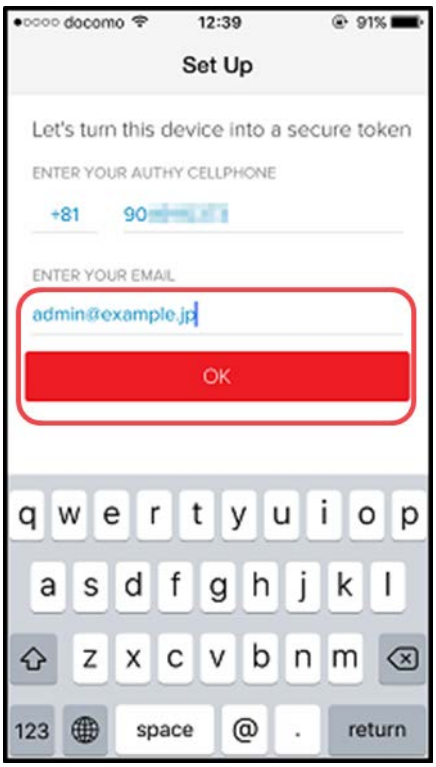


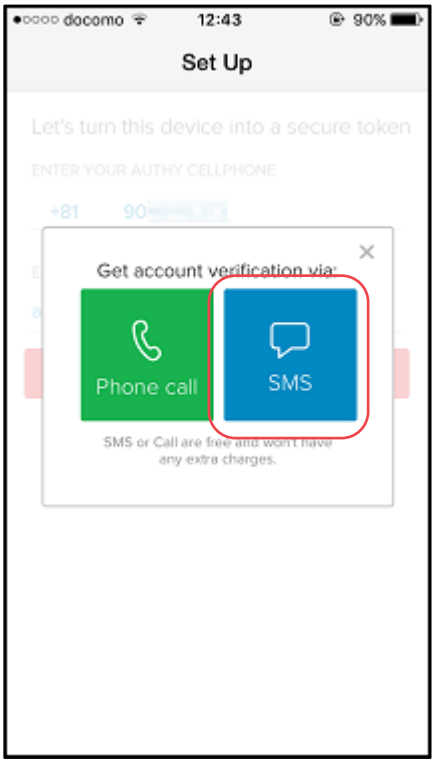


4. 「ENTER　YOUR　MAIL」と表示されますので、お客さまのメールアドレスを入力し、「OK」をタップします。

5. 電話認証か SMS(ショートメッセージ)認証を選択する画面が開くので SMS をタップします。

※ここでは SMS 認証を例に説明するため、SMS をタップします。





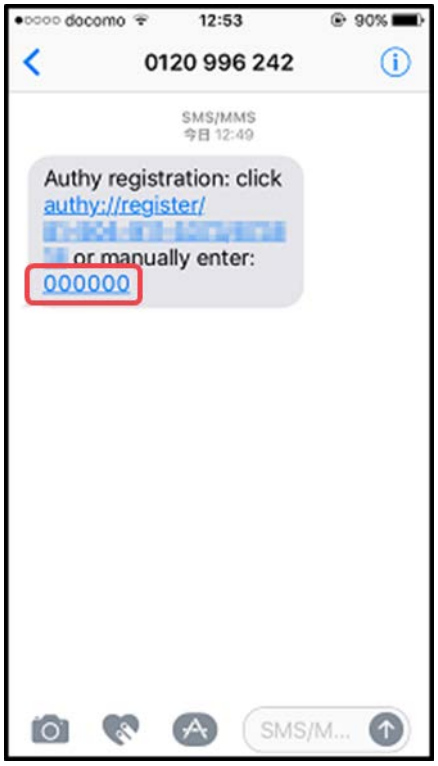
2．クライアント端末の設定

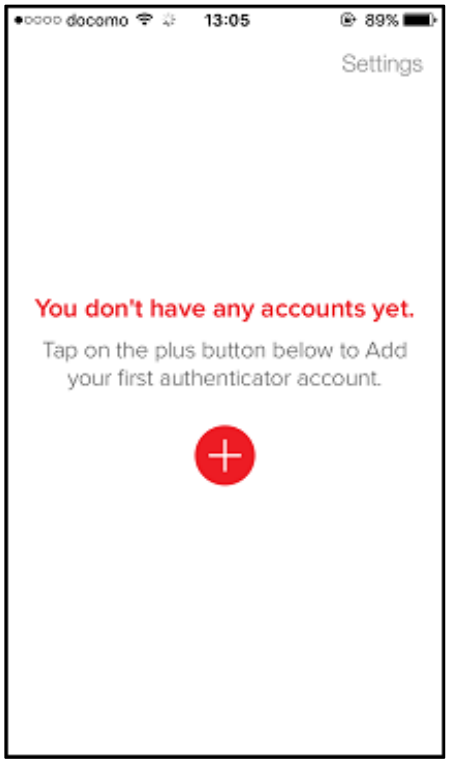
6. 「0120-996-242」の電話番号から SMS が送信されますので、末尾に記載されている 6 桁の番号をメモし、セットアップ画面に戻ります。

7. 「**Registration Code**」をタップし、上の手順でメモした、6 桁の番号を入力します。

8. 通知の許可を確認されますので、許可します。

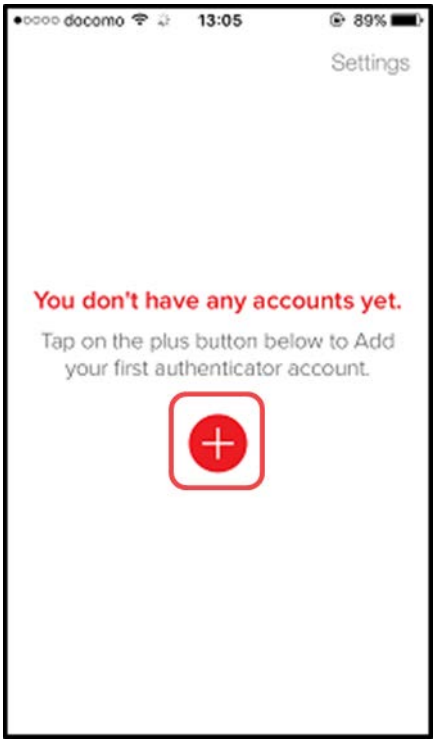
9. 右図の画面が表示されれば、初期セットアップが完了です。

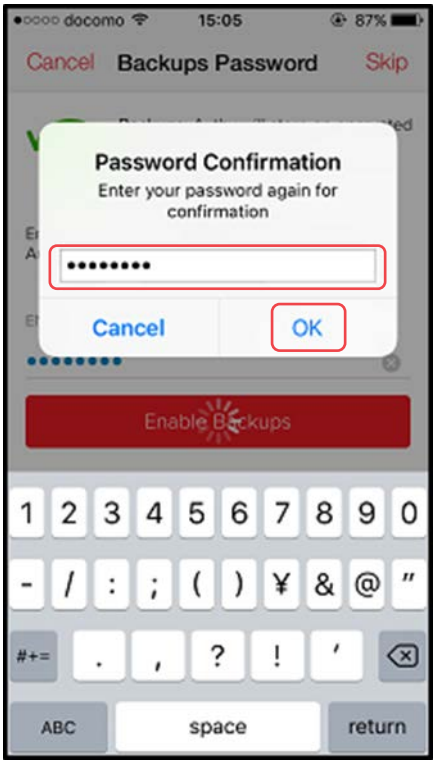




2.2.3. 認証キーの登録

1. Authy を起動して「＋」をタップします。
2. 初回起動時は、「Backups Password」設定の画面が表示されるのでパスワードを入力し、「Enable Backups」をタップします。
3. パスワードの確認画面が表示されますので、パスワードを再入力し、「**OK**」をタップします。





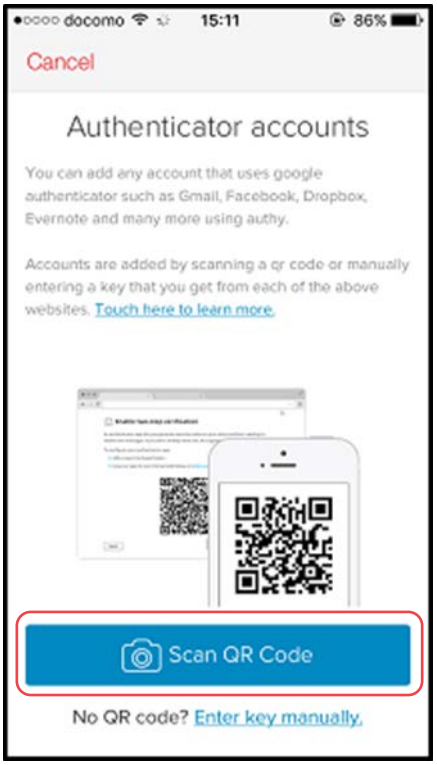
2．クライアント端末の設定

4. 「Backups Password」の設定が完了し、以下の画面が表示されます。

5. コントロールパネルに表示されている QR コードをスキャンし、設定します。

6. 「Scan QR Code」をタップします。

7. 確認画面が表示されますので、「**OK**」をタップします。



8. コントロールパネルに表示されている QR コードをスキャンします。

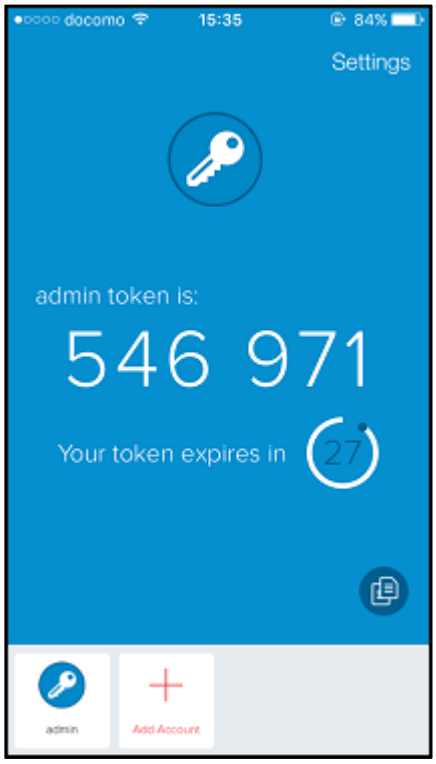
2. クライアント端末の設定

9. QR コードのスキャンに成功すると、以下の画面が表示されます。

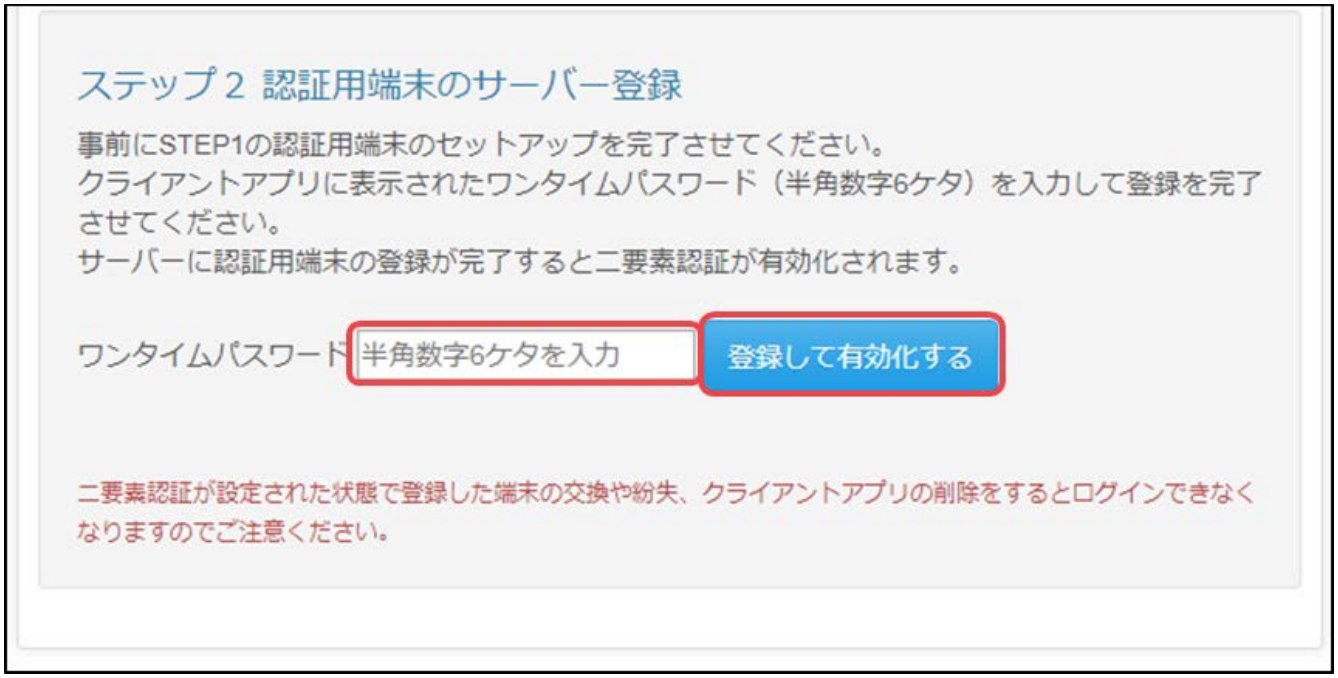
アカウント名は任意で設定してください。入力後に「Done」をタップします。

10. Twitter や Google+との連携確認画面が表示されますので、右上の「×」をタップします。

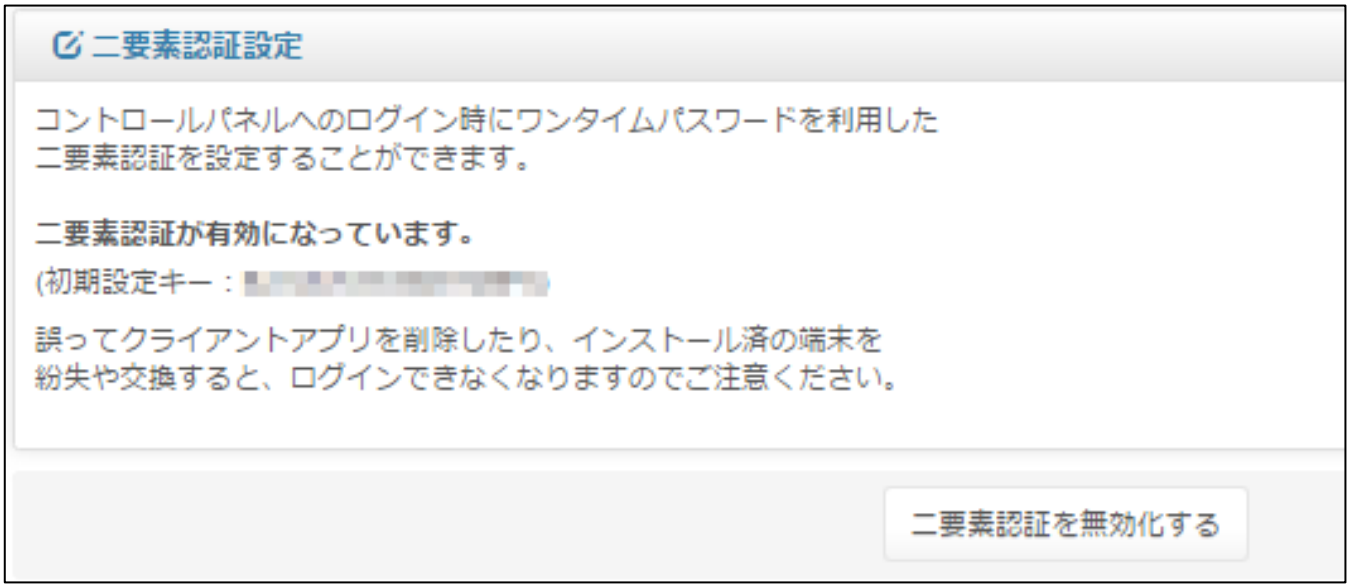
11. 初回認証に成功すると、以下のようにワンタイムパスワードが表示されます。



12. コントロールパネルに戻り、Authy に表示されているワンタイムパスワードを入力し、[二要素認証を有効化する] をクリックします。

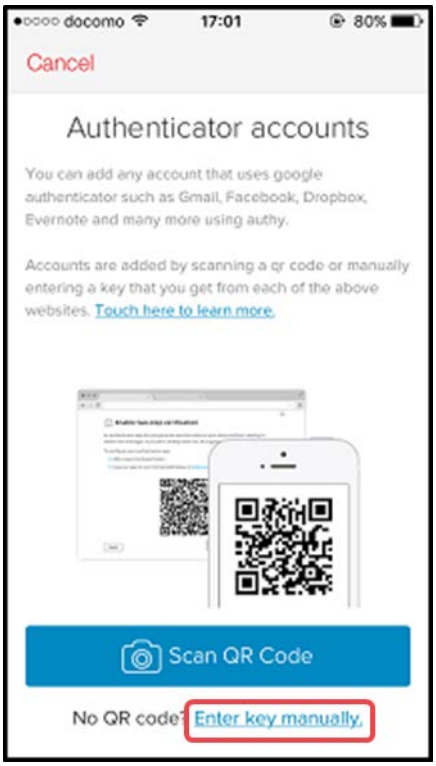


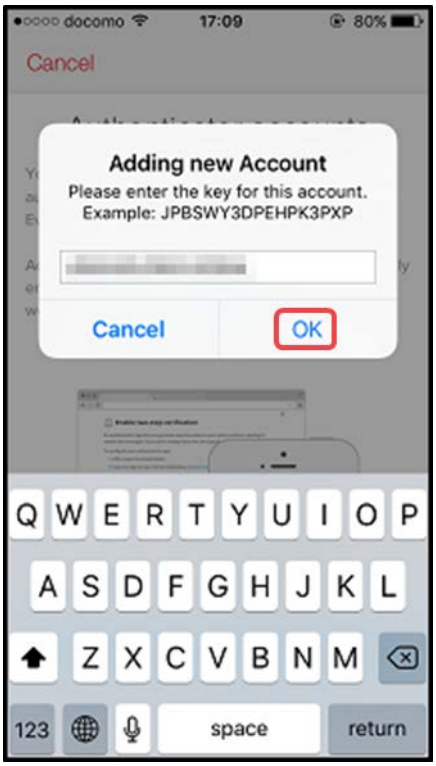
13. 下記の画面が表示されましたら、二要素認証の設定は完了となります。



2.2.4. QR コードが認識されない場合(Iphone)

1. 「Enter key manually」をタップします。
2. コントロールパネルに表示されている、認証キーを入力し、**OK** をタップします。

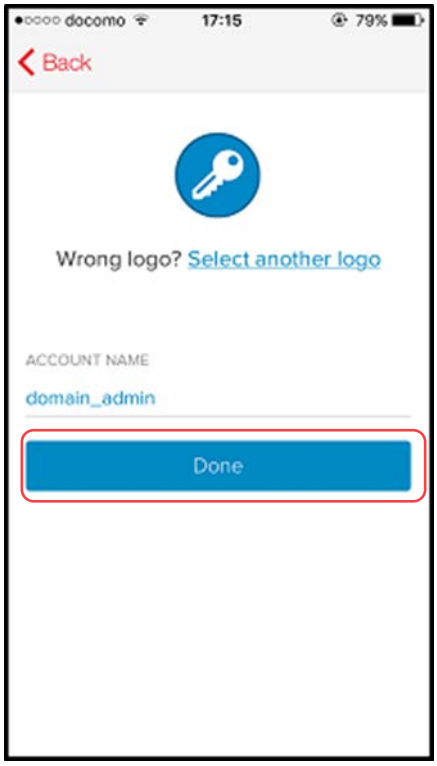


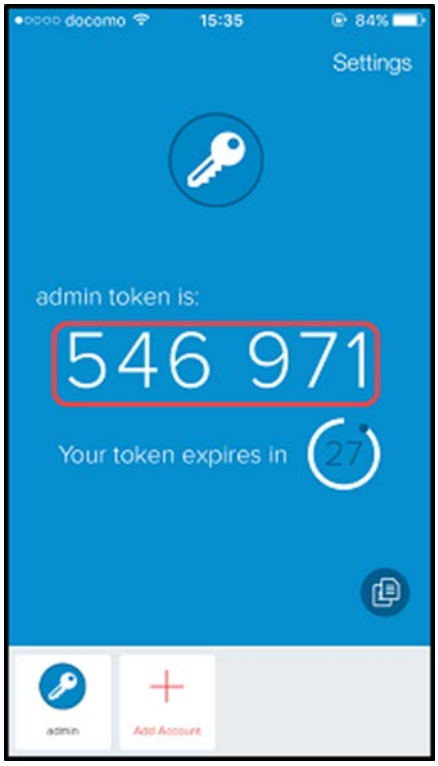


2．クライアント端末の設定

2．以下の画面が表示されますので、「**Done**」をタップします。

3．ワンタイムパスワードが表示されれば、正常に設定完了です。





2.3. Android で利用する場合

2.3.1. アプリケーションのインストール

1. Play ストア(Google Play)を起動して検索欄に「authy」と入力し、右下の「Search」をタップします。
2. 「Authy 2-Factor Authentication」を選択します。

2．クライアント端末の設定

3． 検索結果が表示されたら、「インストール」をタップします。

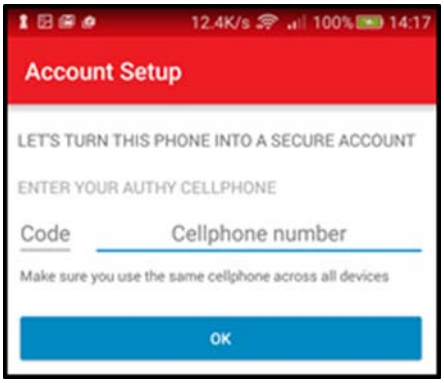
4． 確認画面が表示されますので、「同意する」をタップします。

5． インストールが完了しましたら、「開く」をタップします。

2.3.2. アプリケーションの初期セットアップ

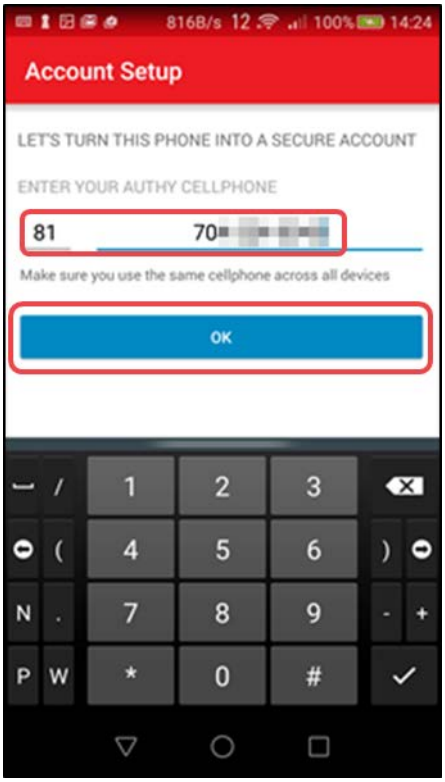
1. インストール完了後に、開くをタップします。
2. セットアップ画面が開き、電話もしくは SMS 受信による認証を行います。
3. 電話番号を入力し、OK をタップします。

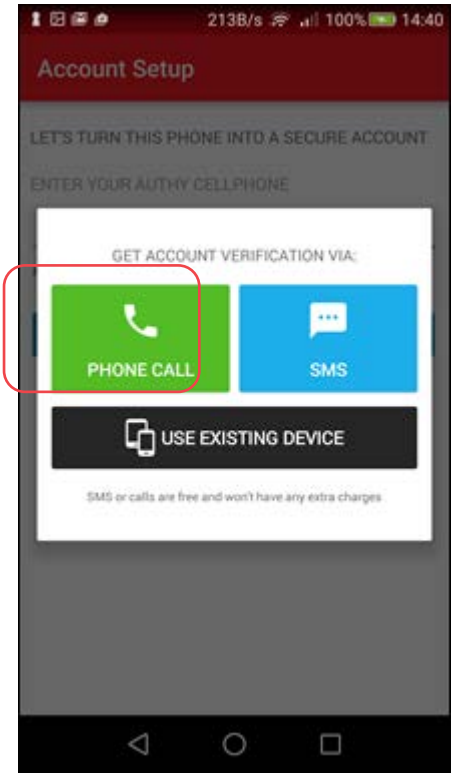
「+Code」は日本国際電話コード「+81」を選択します。
「Cellphone number」にはお客さまの電話番号を入力します。
なお、電話番号を入力する際には、先頭の「0」を省略します。
例）090-1234-5678 → 9012345678



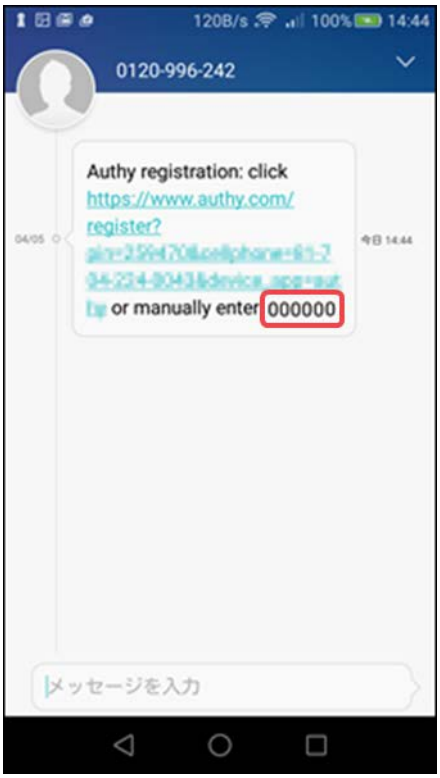
4. 「ENTER　YOUR　MAIL」と表示されますので、お客さまのメールアドレスを入力し、「OK」をタップします。
5. 電話認証か SMS(ショートメッセージ)認証を選択する画面が開くので SMS をタップします。

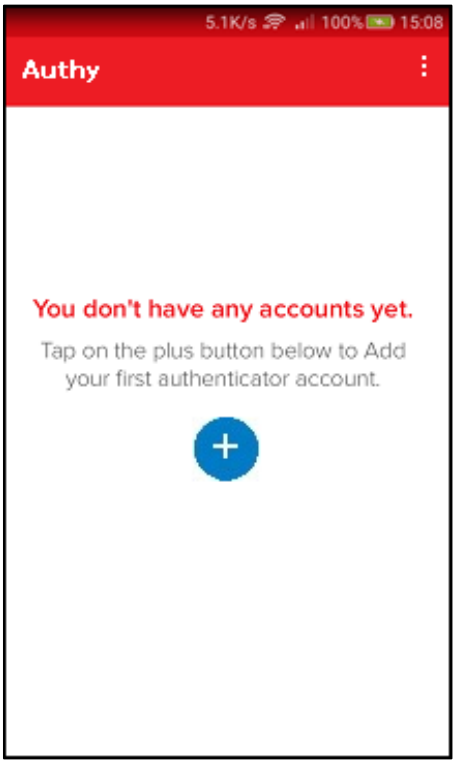
※ここでは SMS 認証を例に説明するため、SMS をタップします。





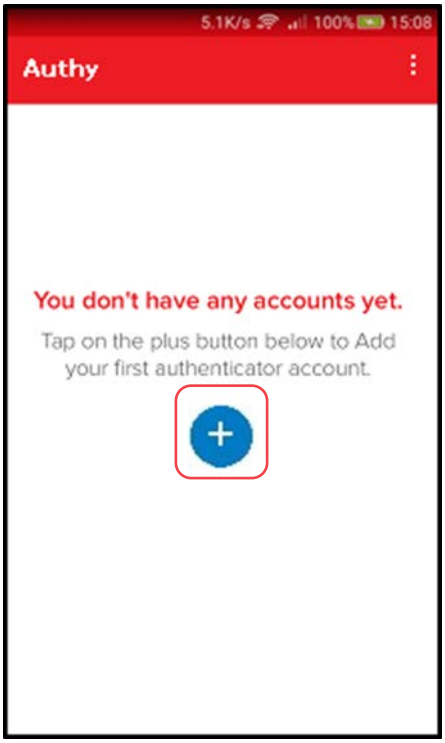
6. 「0120-996-242」の電話番号から SMS が送信されますので、末尾に記載されている 6 桁の番号をメモし、セットアップ画面に戻ります。
7. 「**Registration Code**」をタップし、上の手順でメモした、6 桁の番号を入力します。
8. 通知の許可を確認されますので、許可します。
9. 右図の画面が表示されれば、初期セットアップが完了です。

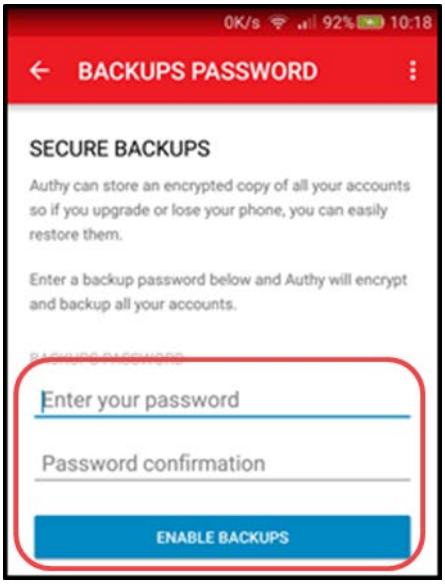




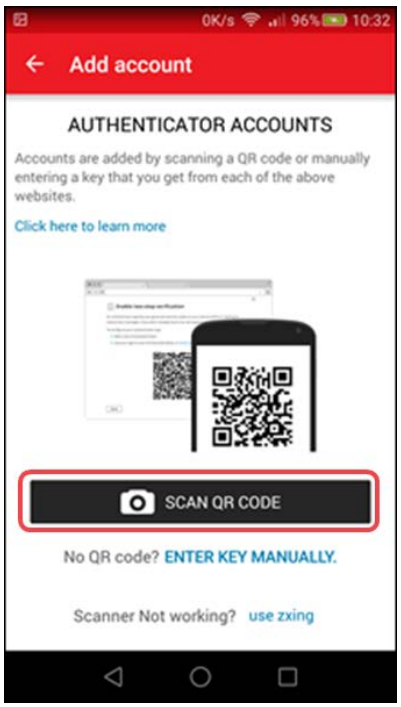
2.3.3. 認証キーの登録

1. Authy を起動して「＋」をタップします。
2. 初回起動時は、「Backups Password」設定の画面が表示されるのでパスワードを入力し、「Enable Backups」をタップします。





3. 「Backups Password」の設定が完了し、左の画面が表示されます。
4. コントロールパネルに表示されている QR コードをスキャンし、「Scan QR Code」をタップします。



5. コントロールパネルに表示されている QR コードをスキャンします。

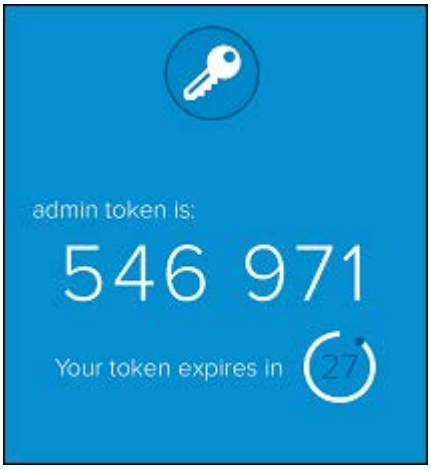
2．クライアント端末の設定

6． QR コードのスキャンに成功すると、以下の画面が表示されます。

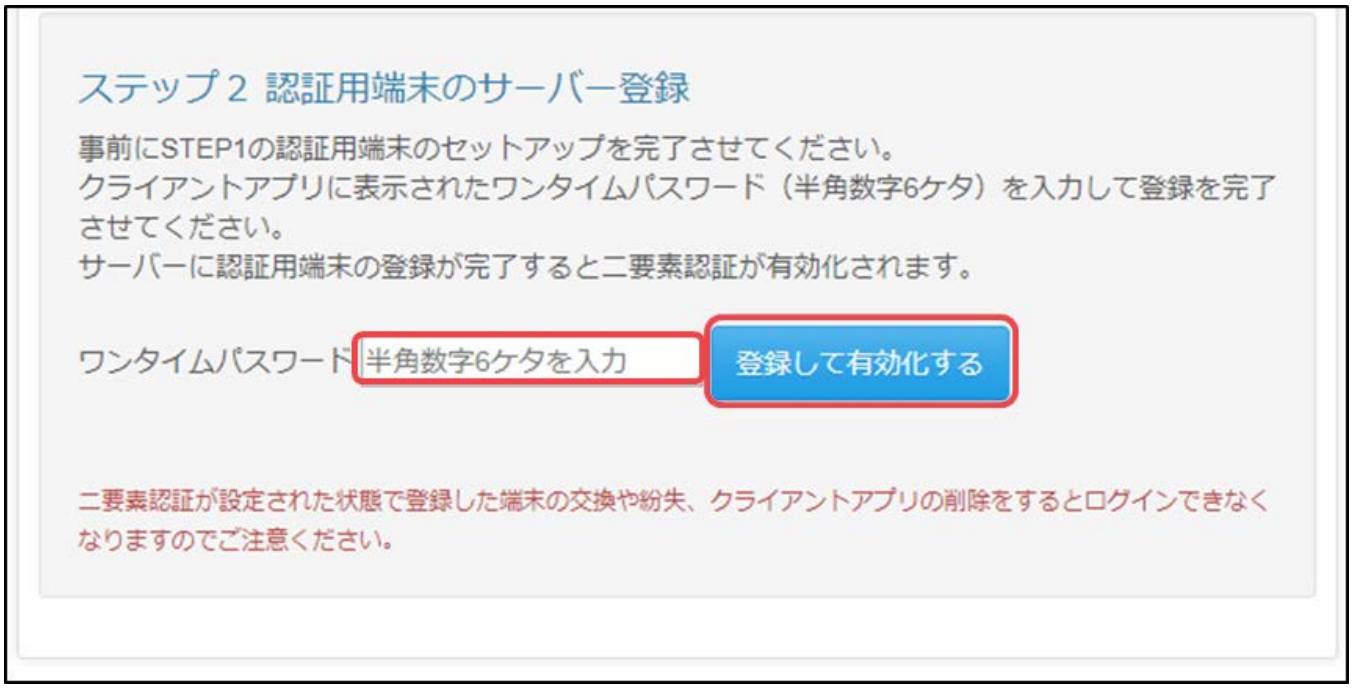
アカウント名は任意で設定してください。入力後に「Done」をタップします。

7． Twitter や Google+との連携確認画面が表示されますので、右上の「×」をタップします。

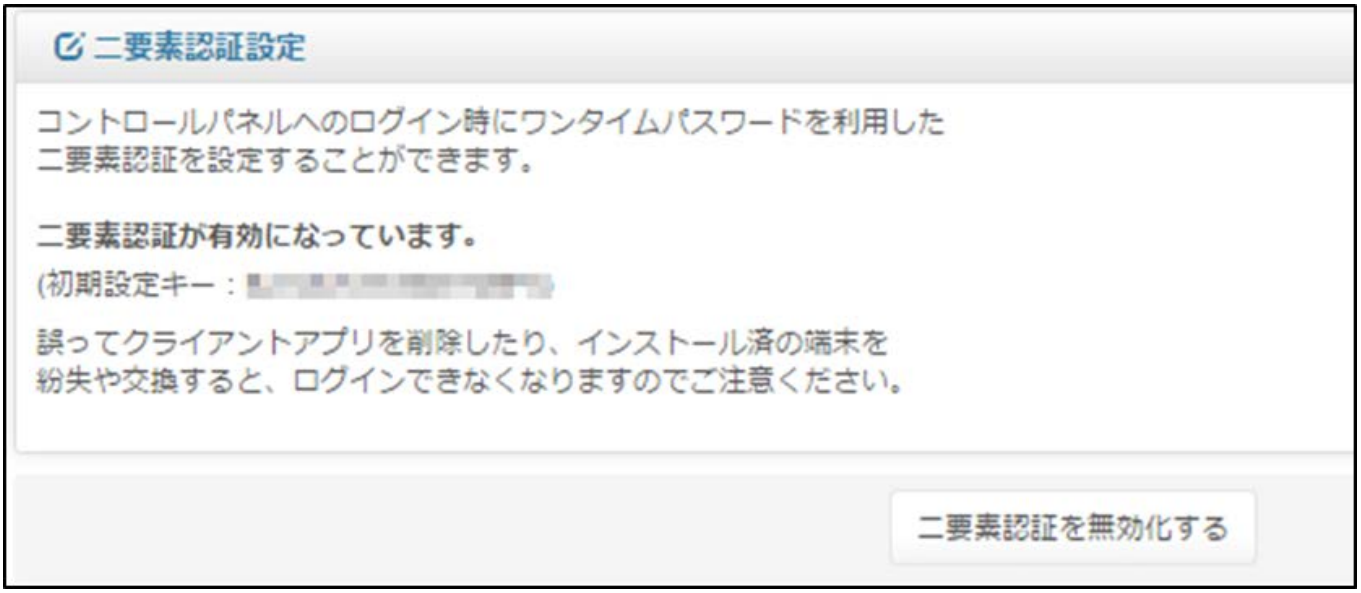
8． 初回認証に成功すると、以下のようにワンタイムパスワードが表示されます。



9． コントロールパネルに戻り、Authy に表示されているワンタイムパスワードを入力し、[二要素認証を有効化する] をクリックします。



10. 下記の画面が表示されましたら、二要素認証の設定は完了となります。



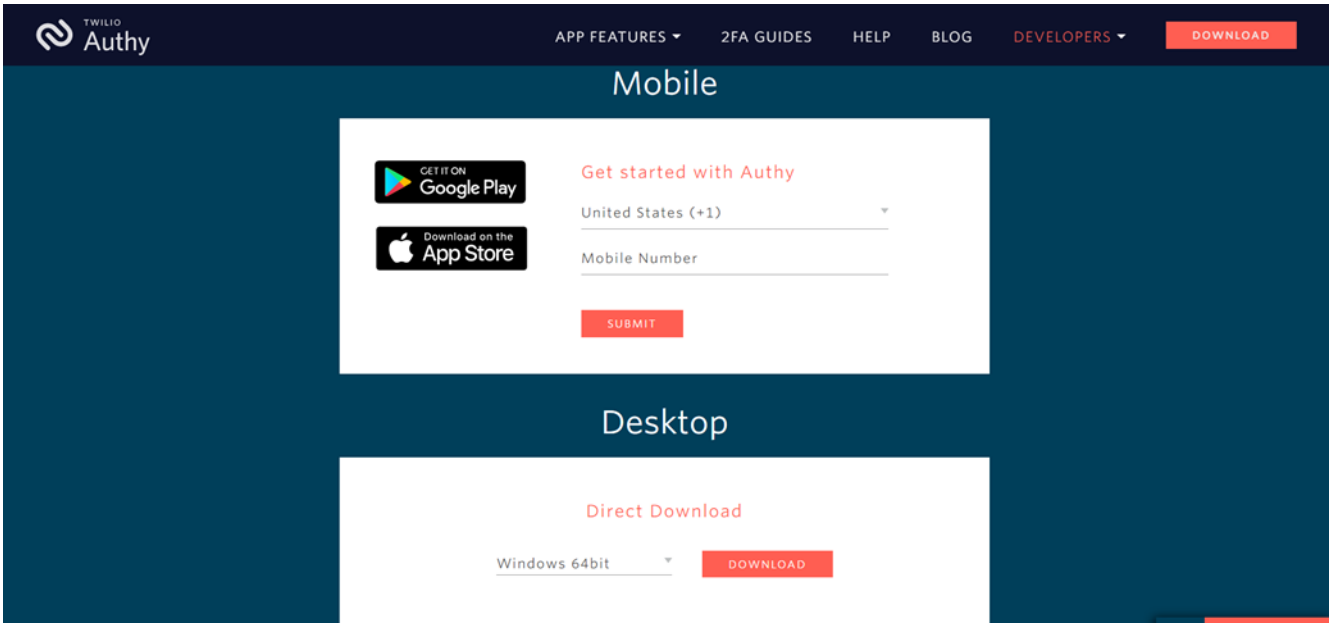
2.4．PC で利用する場合

PC をクライアント端末として利用する場合は Authy のデスクトップ版アプリのインストールが必要です。

※本書では Windows のイメージ画像で説明いたします。

2.4.1. クライアントアプリのインストール(Windows)

1. Windows 用のクライアントアプリは Authy の公式ページから提供されております。
2. ブラウザーから Authy のダウンロードページにアクセスします。
（リンク先：https://authy.com/download/）
3. 「Desktop - Direct Download」から Windows 版を選択し、DOWNLOAD をクリックします。

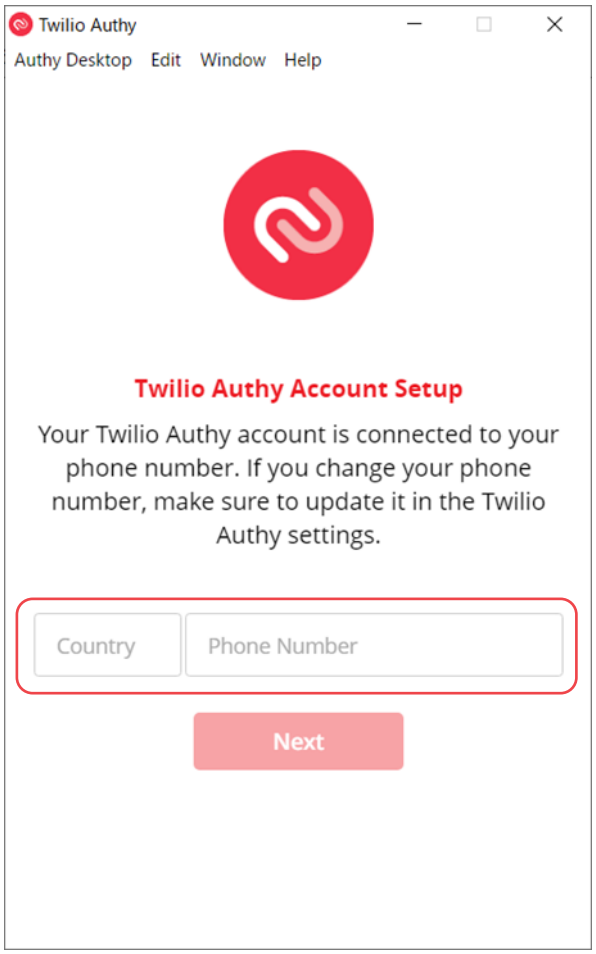


4. ダウンロードしたファイルを実行し、Authy をインストールします。
5. 初回の認証には電話による認証、もしくは SMS 受信が必要になりますので認証の手続きを行います。

2.4.2. クライアントアプリの初期セットアップ

初回の認証には電話による認証、もしくは SMS 受信が必要になります。
以下で認証の手続きを行ってください。

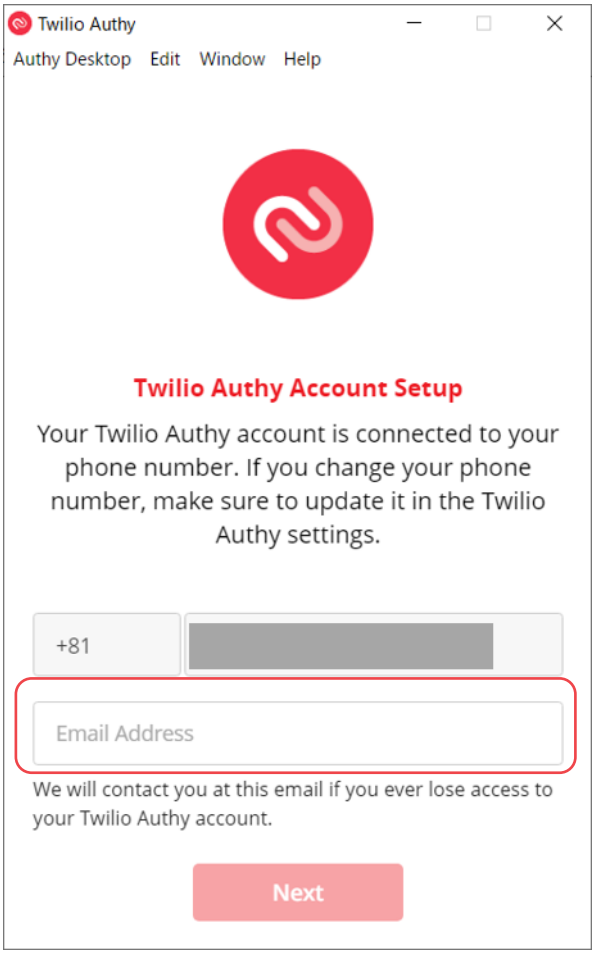
1. 「Country」には、日本国際電話コード「+81」を「Phone Number」には、
   お客さまの電話番号を入力します。
   なお、電話番号を入力する際には、先頭の「0」を省略します。
   例として、「090-1234-5678」の場合は「9012345678」と入力します。
2. 電話番号の入力が終わったら、NEXT をクリックします。



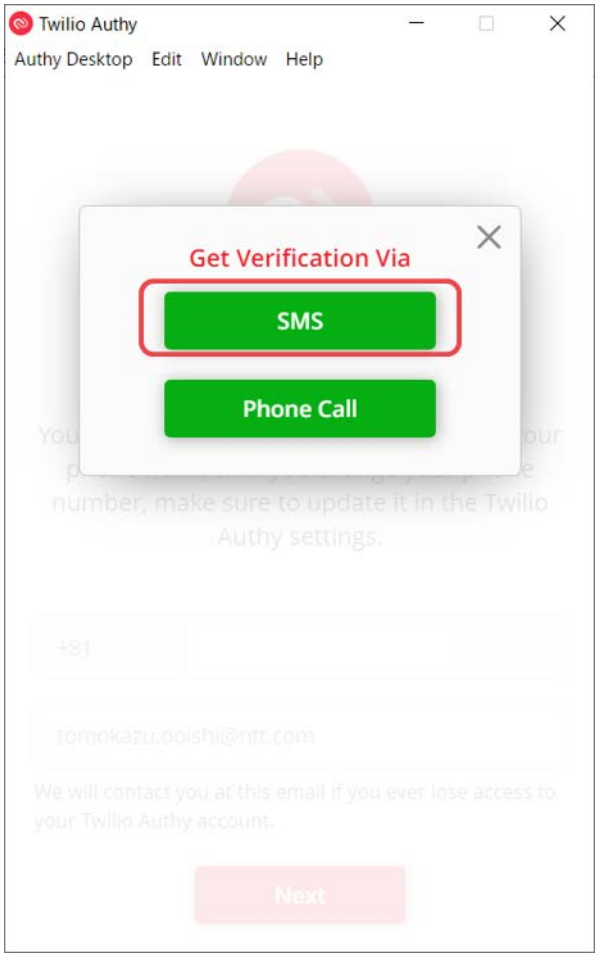
2．クライアント端末の設定

3． メールアドレスの入力を求められた場合は、お客さまのメールアドレスを入力します。

4． 電話番号の入力が終わったら、Next をクリックします

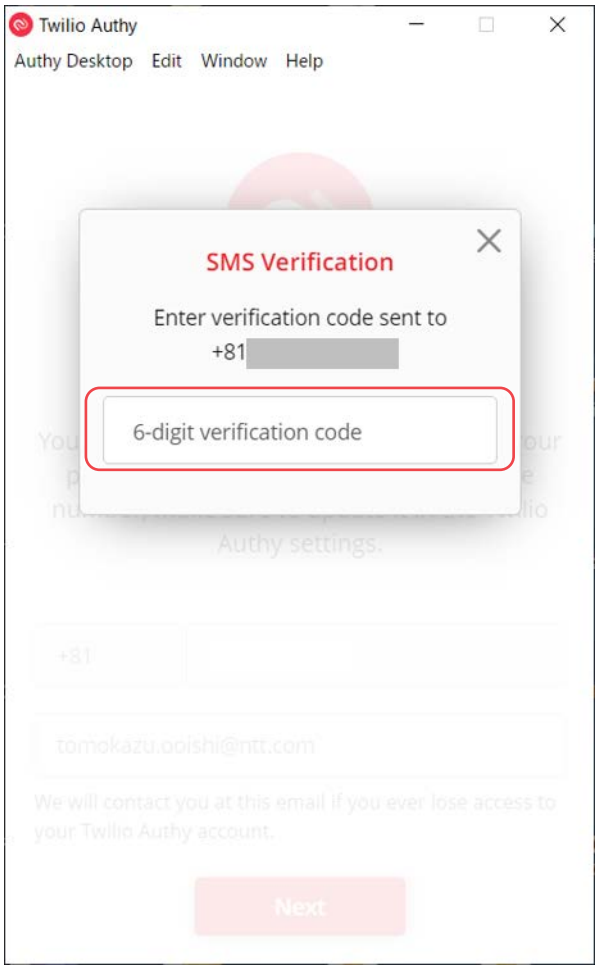


5. 電話認証か SMS(ショートメッセージ)認証を選択する画面が開きます。
ここでは SMS 認証を例に説明いたします。SMS をクリックします。

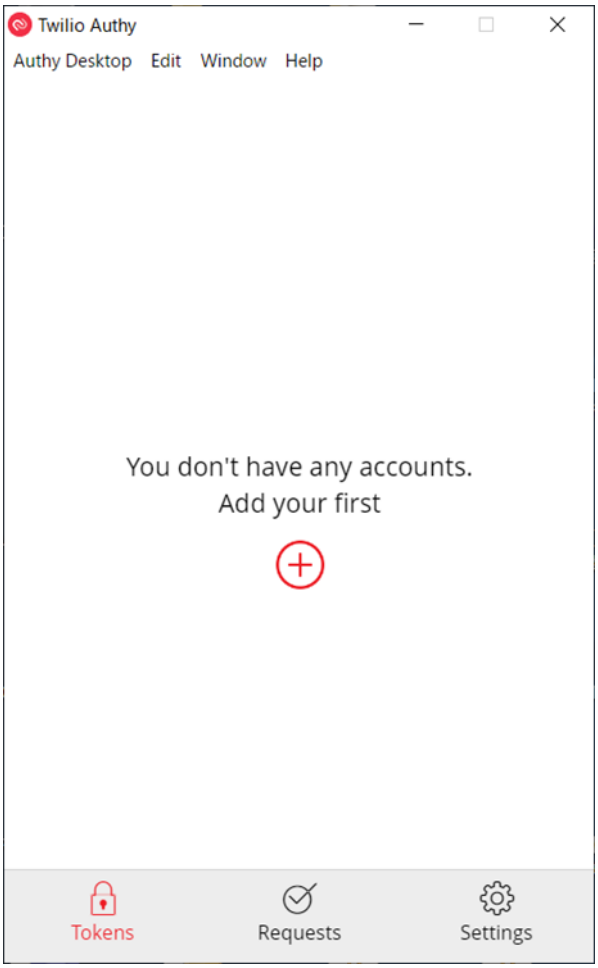


6. 「お客さまが入力した電話番号に SMS を受信しますので、メッセージを確認し、末尾(manually enter)に記載されている 6 桁の番号を確認します。

7. SMS で受け取った 6 桁の認証コードを「6-digit verification code」に入力します



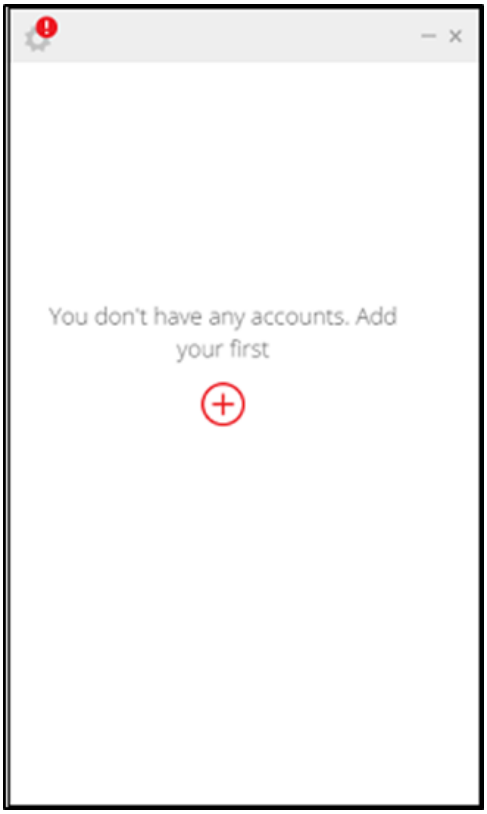
8．以下の画面が表示されれば、インストール完了です。



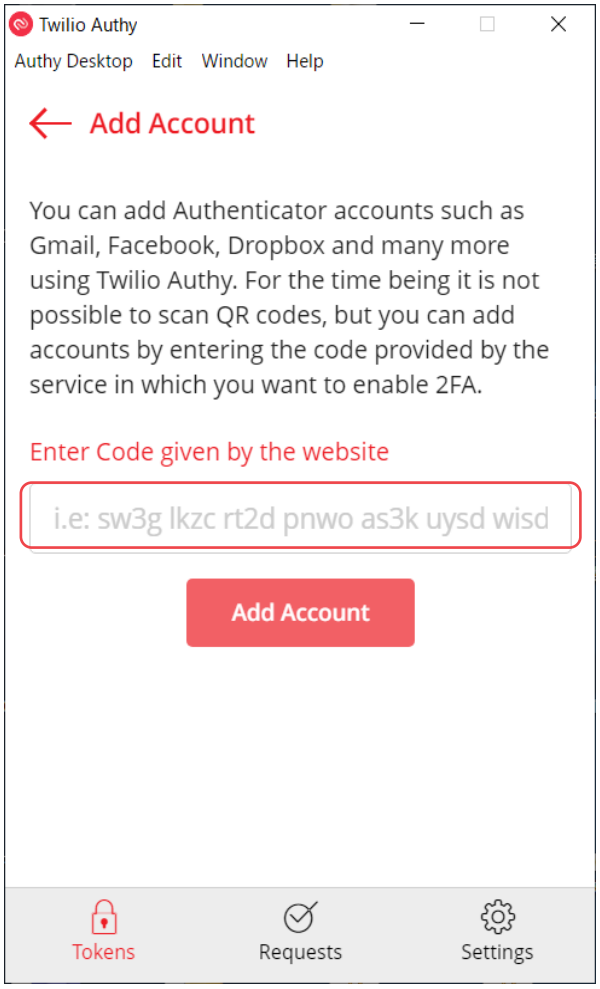
2.4.3. 認証キーの登録

1. Windows では、QR コードによる認証ができませんので、コントロールパネルに表示されている、「初期設定キー」を手動で入力する必要があります。

2. Authy を起動し「＋」をクリックします

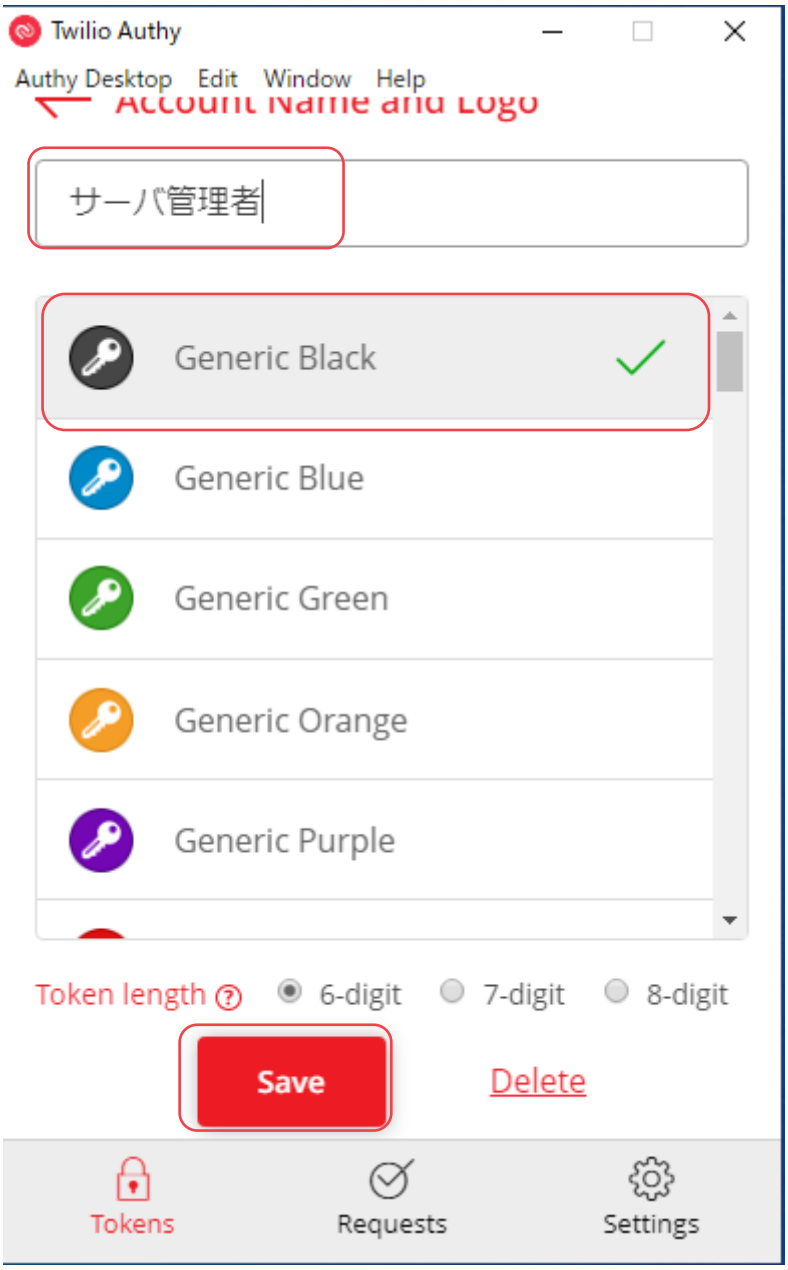


3. 認証キーを入力する画面が開きますので、「Enter　Code given by the website」へ認証キーを入力して「Add Account」をクリックします。

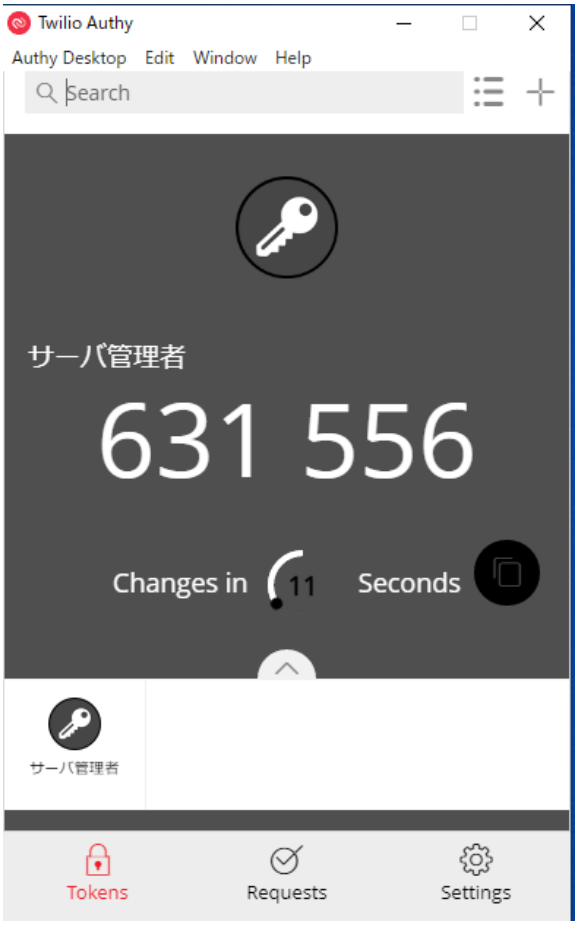


2．クライアント端末の設定

4． アカウントのアイコンとアカウント名を決定する選択する画面が表示されますので、任意のアイコンとアカウント名を入力し、「Done」をクリックします。

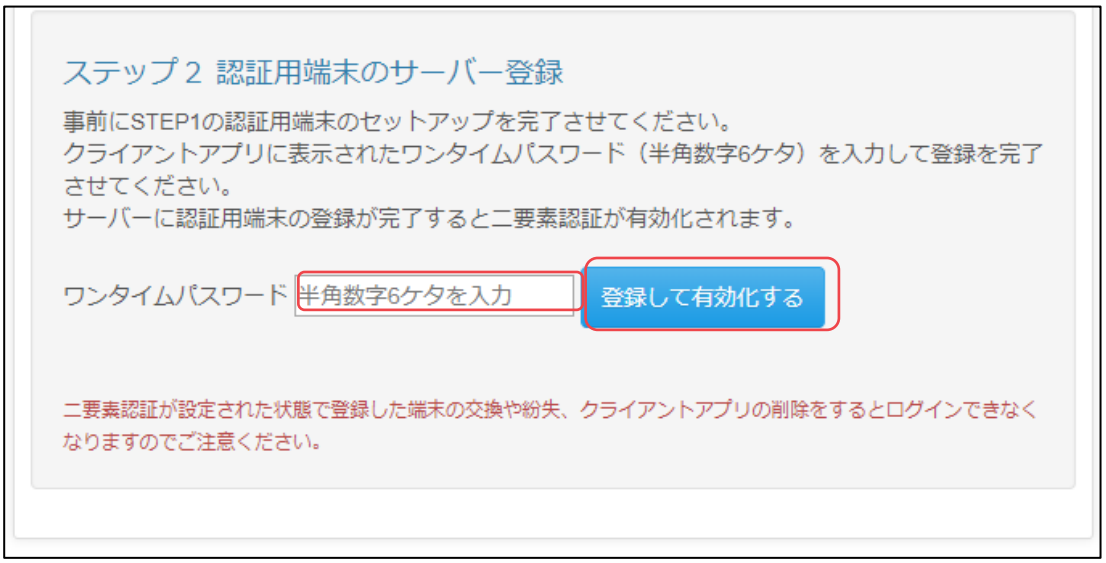


5. ワンタイムパスワードが表示されます。

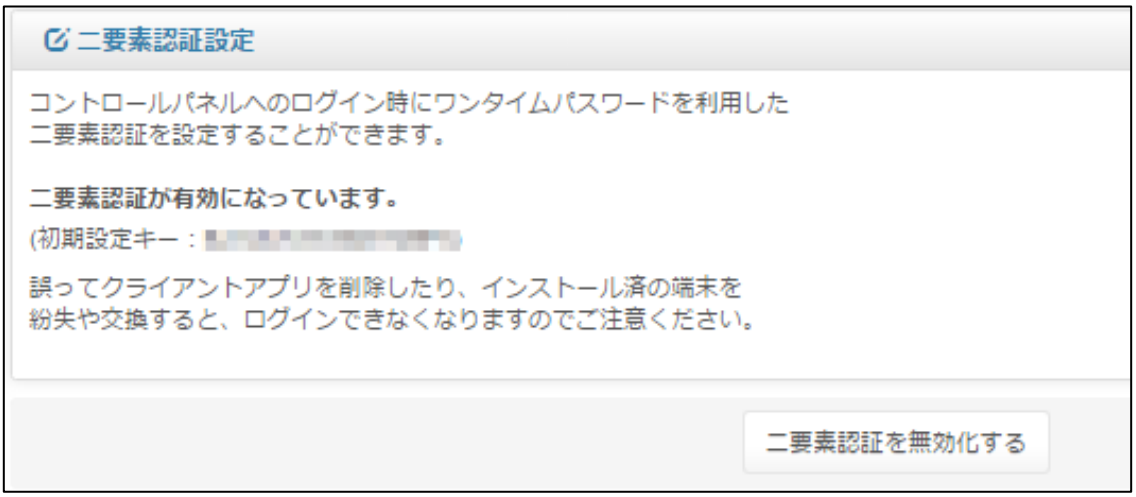


2．クライアント端末の設定

6． コントロールパネルに戻り、Authy に表示されているワンタイムパスワードを入力し、
入力し、[登録して有効化する] をクリックします



7． 下記の画面が表示されましたら、二要素認証の設定は完了となります



2.4.4. 二要素認証を利用したコントロールパネルへのログイン

1. コントロールパネルにアクセスします。

2. ユーザーID、パスワードを入力し、「**※二要素認証を設定している場合はクリック**」をクリックすると[ワンタイムパスワード]欄が表示されます。

3. クライアントアプリ(Authy)に表示されている 6 桁のワンタイムパスワードを確認し 2. のワンタイムパスワード欄に入力し、[ログイン]をクリックします。

2．クライアント端末の設定

４．　正常にログインできれば、二要素認証は正常に設定されています

COTOHA Meeting Assist
二要素認証設定マニュアル

発行　ＮＴＴコミュニケーションズ株式会社
〒100-8019　東京都千代田区大手町2-3-1