

MFA(多要素認証)利用ガイド

はじめに

本書は、管理ポータル・チャット画面のログイン時に多要素認証を義務付けるMFA機能の利用方法について説明するガイドです。

MFA機能を利用するためには、契約時に多要素認証オプションを購入いただく必要がございます

MFA機能が有効なテナントでは、管理ポータル・チャット画面のログイン時に TOTP(Time-based One-Time Password)を利用した2要素認証が必要となり、セキュリティが強化されます。

認証に利用できるアプリケーションは以下の通りです。

- Free OTP
- Microsoft Authenticator
- Google Authenticator

MFA機能が有効なテナントでは、利用者が各画面にログインする操作、および、システム管理者のユーザ管理操作が通常のテナントと異なります。

本書は、利用者とシステム管理者それぞれに対して通常テナントとの操作が異なる部分を説明します。

画面へのログイン（利用者/システム管理者向け）

MFA機能が有効なテナントでは、利用者/システム管理者が最初に管理ポータル・チャット画面のいずれかにログインする際に、MFAデバイスの登録およびパスワードの変更を行う必要があります。

2回目以降のログインでは、登録したデバイスから発行されたワンタイムパスワードと、初回ログイン時に決定したパスワードを利用します。

MFA機能が有効なテナントの管理ポータル・チャット画面のURLは、MFA機能を利用しないテナントのURLと異なります。URLが不明な場合はシステム管理者にお問い合わせください。

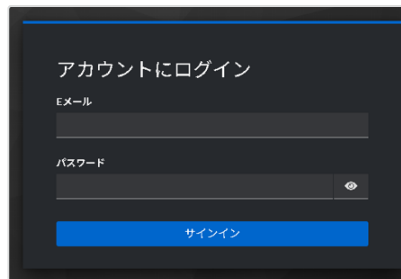
初回ログイン

MFA機能が有効なテナントで、利用者/システム管理者が初めて管理ポータル・チャット画面のいずれかにログインする場合の操作方法を示します。

システム管理者によって管理ポータルから本システムに登録されたユーザのみログイン可能です。また、ログインには登録時に指定した初期パスワードが必要です。初期パスワードが不明な場合、システム管理者にお問い合わせください。

1. メールアドレスとパスワードの入力

ユーザのメールアドレスおよび初期パスワードを用いてログインを行います。



2. MFAデバイスの登録

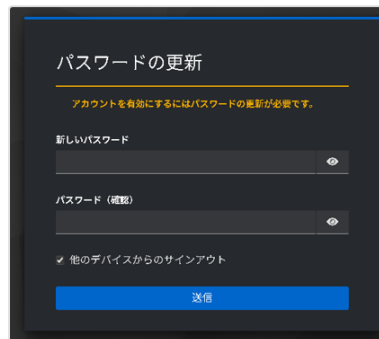
画面の表示に従い認証に利用できるアプリケーションを使用してワンタイムコードを取得し、入力して下さい。デバイス名の入力は任意です。



3. 初期パスワードの変更

ユーザ登録時にシステム管理者が指定した初期パスワードの変更を求められます。

画面の表示に従い新しいパスワードを登録してください。以降のログインでは更新後のパスワードを利用します。

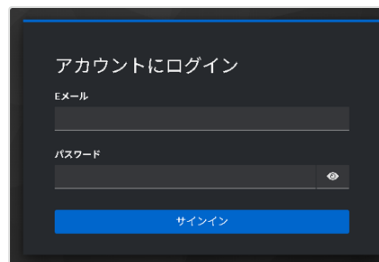


2回目以降のログイン

MFA機能が有効なテナントで、管理ポータル・チャット画面のいずれかへの2回目以降ログインする際の操作方法を示します。

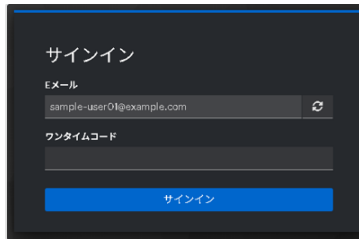
1. メールアドレスとパスワードを入力

ユーザのメールアドレスと初回ログイン時に変更したパスワードを用いてログインを行います



2. ワンタイムコード入力

パスワードによる認証に成功した場合、ワンタイムパスワードが求められます。初回ログイン時に登録したMFAデバイスを使用してワンタイムパスワードを入力してください。



① 登録したMFAデバイスを変更する場合、システム管理者にご連絡ください。システム管理者にMFAデバイスのリセット操作を実施いただく必要があります。

ユーザの管理（システム管理者向け）

ユーザの登録、編集、パスワードの初期化

ユーザの登録/編集についての詳細は「管理ポータル操作ガイド（ユーザ登録編）」をご参照下さい。

ここでは、MFA機能利用時のみ設定が必要な内容を記載します。

ユーザ登録時においては、初期パスワードの指定が必要です。またユーザ編集画面でパスワードの初期化を行う事が出来ます。

⚠ ユーザ登録後、以下の情報を対象ユーザに通知してください。

- 管理ポータルの基本情報画面で確認できるチャットサービスのURL
- 登録時に指定したユーザの初期パスワード

・ユーザ追加

・ユーザ編集

目	内容
パスワード	画面にログインする際のパスワードです。 <ul style="list-style-type: none"> • 新規登録時 <ul style="list-style-type: none"> ◦ 画面に初回ログインする際の初期パスワードを指定します。登録されたユーザは、初回ログイン時にパスワードの変更が求められます。 • 編集時 <ul style="list-style-type: none"> ◦ パスワードを初期化するにはトグルスイッチをONにします。 パスワードが初期化されたユーザは、パスワード初期化後の初回ログイン時にパスワードの変更が求められます。

ユーザの一括更新

MFA機能が有効なテナントでは、ユーザーの一括更新で新規登録するユーザーに対して、初期パスワードを指定する必要があります。

パスワード以外の項目は、「管理ポータル操作ガイド（ユーザ登録編）」の「ユーザー一括更新」をご参照ください。

CSVファイルの形式

- CSVファイルの内容について
以下の表に従ってカラムを設定してください。

項目	値	入力制限
----	---	------

user_name	「管理ポータル操作ガイド（ユーザ登録編）」の「ユーザー一括更新」をご参照ください。	
email	「管理ポータル操作ガイド（ユーザ登録編）」の「ユーザー一括更新」をご参照ください。	
pwd	登録を行うユーザの初回ログイン時に使用するパスワードを指定します。 登録されたユーザは指定されたパスワードでログインを行った後、パスワードの変更が求められます。	空白禁止
authority	「管理ポータル操作ガイド（ユーザ登録編）」の「ユーザー一括更新」をご参照ください。	
group_name	「管理ポータル操作ガイド（ユーザ登録編）」の「ユーザー一括更新」をご参照ください。	
group_id	「管理ポータル操作ガイド（ユーザ登録編）」の「ユーザー一括更新」をご参照ください。	

CSVの例

```
1 user_name,email,pwd,authority,group_name
2 日電太郎,taro@example.com,invalid,dummy_password,admin,group_name
```

ユーザの削除

ユーザの削除方法は、通常テナントと同一です。管理ポータル操作ガイド(基本操作編)を参照ください。

ユーザの一括削除

ユーザの削除方法は、通常テナントと同一です。管理ポータル操作ガイド(基本操作編)を参照ください。

MFAデバイスのリセット

本サービスに登録したMFAデバイスの変更が必要な場合、対象ユーザのMFAデバイスのリセット操作を実施してください。

登録が解除されたMFAデバイスは本サービスのログインには利用できなくなります。また、MFAデバイスの登録が解除されたユーザは、次回ログイン時に新しいデバイスの登録が求められます。

MFAデバイスをリセットする場合、管理ポータルのユーザー一覧画面の対象ユーザの列で「MFA端末解除」ボタンを押下してください。ボタン押下時に確認ダイアログが表示されます。確認ダイアログでOK ボタンを押下することで、登録したMFAデバイスが解除されます。

MFAデバイスが解除されたユーザでログインした場合、初回ログインと同様にMFAデバイスの登録画面が表示されます。

MFAデバイスのリセットを行うには、組織管理者またはユーザ管理者の役割が必要です。

ユーザー一覧 更新 追加 一括追加

ユーザー システムユーザー

Q sample ×

<input type="checkbox"/>	名前	email ↑	役割	MFA...	編集	削除
<input type="checkbox"/>	サンプルユーザ1	sample-user01@example.com	ユーザ管理者	🔄	✎	🗑️

ページあたりの行数: 10 1 ~ 1 / 1 < >

一括削除