



RAS 二要素認証簡易設定ガイド

20.0

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
スイス
Tel: + 41 52 672 20 30
www.parallels.com/jp

© 2024 Parallels International GmbH. All rights reserved. Parallels および Parallels ロゴは、カナダ、米国またはその他の国における、Parallels International GmbH の商標または登録商標です。

Apple、Safari、iPad、iPhone、Mac、macOS、iPadOS は、Apple Inc.の登録商標です。Google、Chrome、Chrome OS、Chromebook は、Google LLC の登録商標です。

その他のすべての社名、製品名、サービス名、ロゴ、ブランド、またすべての登録商標または未登録商標は、識別の目的でのみ使用されているものであり、それぞれの所有者の独占的な財産となります。サードパーティに関わるブランド、名称、ロゴ、その他の情報、画像、資料の使用は、それらを推奨することを意味するものではありません。当社は、これらサードパーティに関わる情報、画像、素材、マーク、および他社の名称について所有権を主張するものではありません。特許に関するすべての通知と情報については、<https://www.parallels.com/jp/about/legal/>をご覧ください。

目次

はじめに	4
本ガイドの目的	4
注意事項	4
適用範囲	4
表記規則	4
概要	5
RAS 二要素認証とは	5
検証環境の構成	8
構築手順	8
事前準備	8
多要素認証の設定	9
利用者側の設定	17
参考情報 Web からアクセスした場合の QR コード画面	25
参考情報 iPad からアクセスした場合の QR コード画面	26

はじめに

本ガイドの目的

本ガイドは、Parallels® Remote Application Server (以降 RAS) の評価を目的に、初めて環境を構築されようとしているお客様や、販売店のエンジニア様に、シンプルなシステム構成で構築を完了し、RAS のリモート アクセスをお試しいただき体験いただくことを目的としております。

RAS 管理者ガイド (日本語) を、弊社 Web サイトに公開しておりますが、公開資料を補足する内容となっております。ぜひ、RAS 製品のシンプルで、かつ操作性の良いリモート アクセスを評価いただければ幸いです。

RAS 管理者ガイドを含むマニュアルの公開ページ
<https://www.parallels.com/jp/products/ras/resources/>

注意事項

- 本ガイドで紹介した仮想ネットワークおよび仮想サーバー等の導入に関しては自己責任での利用をお願いいたします。
- 本ガイドで示す環境構築および運用手順の実行に関しては、所属する組織等のセキュリティポリシーに必ず従ってください。
- 本ガイドに記載されている画面例、URL 等はガイド記載時のものとなるため、画面仕様が実際の画面とは異なることがありますのでご注意ください。
- 本ガイドに記載されている内容は、改善のため予告なしに変更される場合があります。あらかじめご了承ください。
- 評価の際は、是非、インストールメディアのバージョンを含め、本ガイドの最新バージョンをご使用されることを推奨いたします。

適用範囲

本ガイドは、以下バージョンを対象としています。

- RAS Ver. 20.0

表記規則

本ガイド内の表記は、以下の規則に沿って行われています。

- RAS の画面に表示されるメニュー名/タブ名/プロパティ項目名/値/ボタン名は、[] で囲んで表記しています。
- 可変の値は < > で囲んで表記しています。

概要

本ガイドでは、Parallels® RAS 二要素認証の設定方法について説明します。本資料作成時点で追加のコストが発生しない Google Authenticator を用いた簡易な二要素認証の実現方法について説明します。

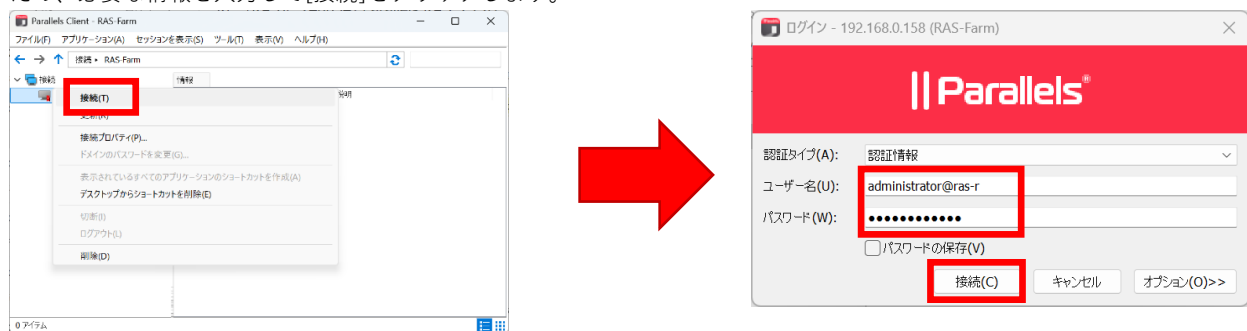
RAS 二要素認証とは

Parallels RAS では、一般的な利用方法として、RAS Client もしくはウェブブラウザから RAS に接続する際にユーザー認証を求められます。Active Directory を利用してユーザーやコンピュータを管理することを推奨しています。

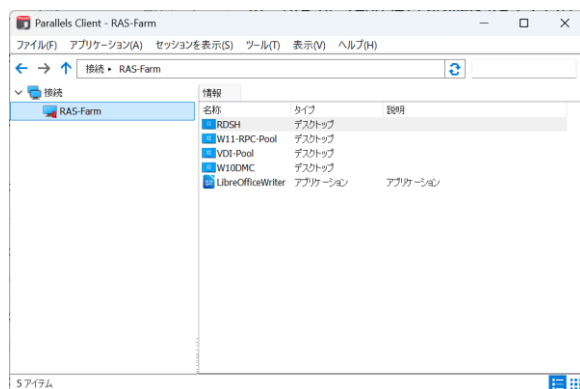
Active Directory を利用した場合、RAS Client から RAS 環境に接続する場合と、Web ブラウザから接続する場合では画面の表示が若干異なります。以下のような画面の流れで RAS 環境にログインし、認証情報を入力することにより、RAS 環境に接続してデスクトップやアプリケーションを利用することができます。

RAS Client の場合

既に RAS の接続先が登録されている RASClient から RAS 環境に接続します、認証情報を尋ねるポップアップが表示されるため、必要な情報を入力して[接続]をクリックします。



接続に使用したユーザーアカウントに使用が許可されているデスクトップやアプリケーションの一覧が表示されるため、利用したいアイコンをダブルクリックして接続、利用します。

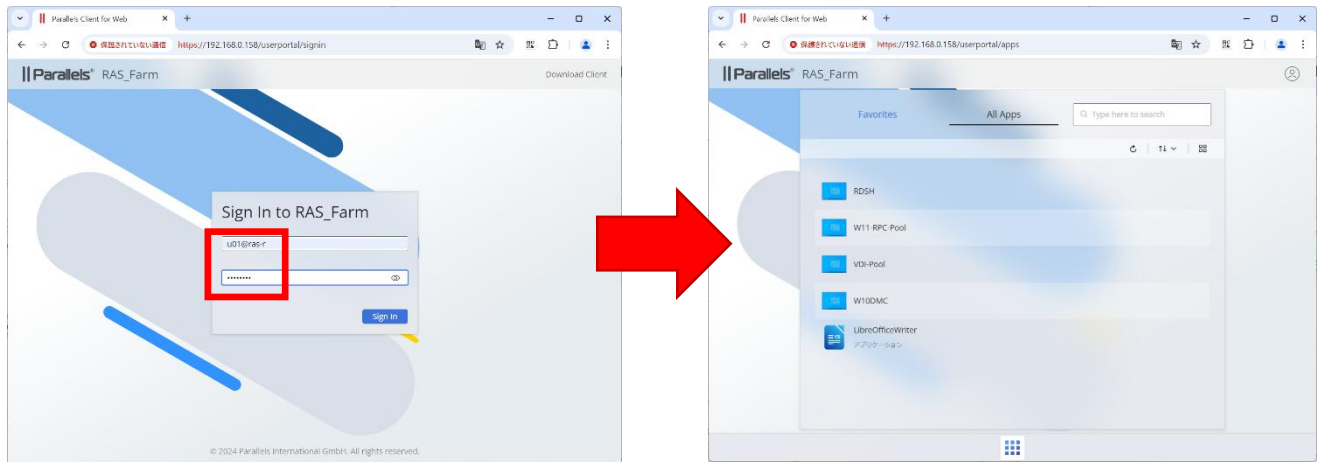


※RAS Client の設定手順は以下をご参照ください

<https://jp.learn.corel.com/business/parallels-ras-client-handbook/>

Web からの接続の場合

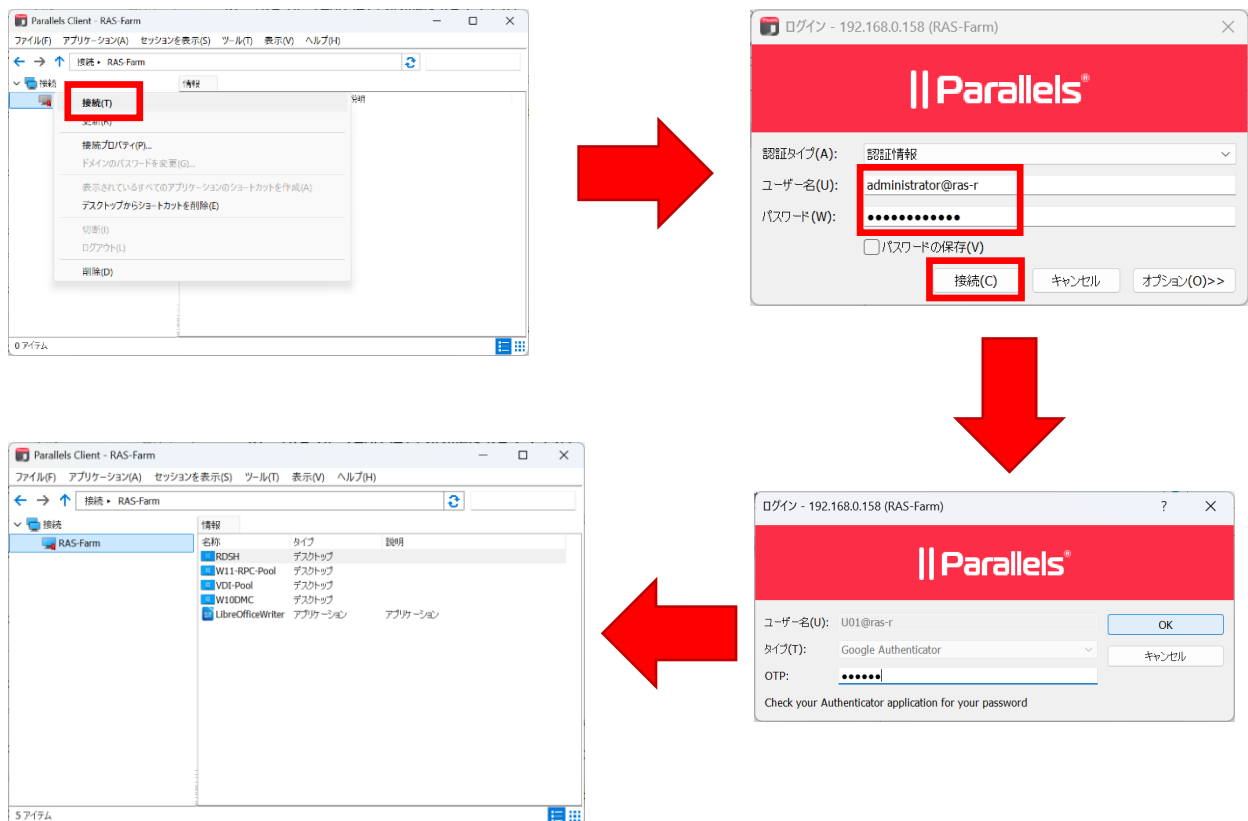
ウェブブラウザで RAS 接続先の URL を入力して接続すると、認証情報を尋ねる画面が表示されるため、必要な情報を入力して[Sign In]をクリックします。ポップアップが表示されるため、必要な情報を入力して[接続]をクリックします。接続に使用したユーザーアカウントに使用が許可されているデスクトップやアプリケーションの一覧が表示されるため、利用したいアイコンをクリックして接続、利用します。



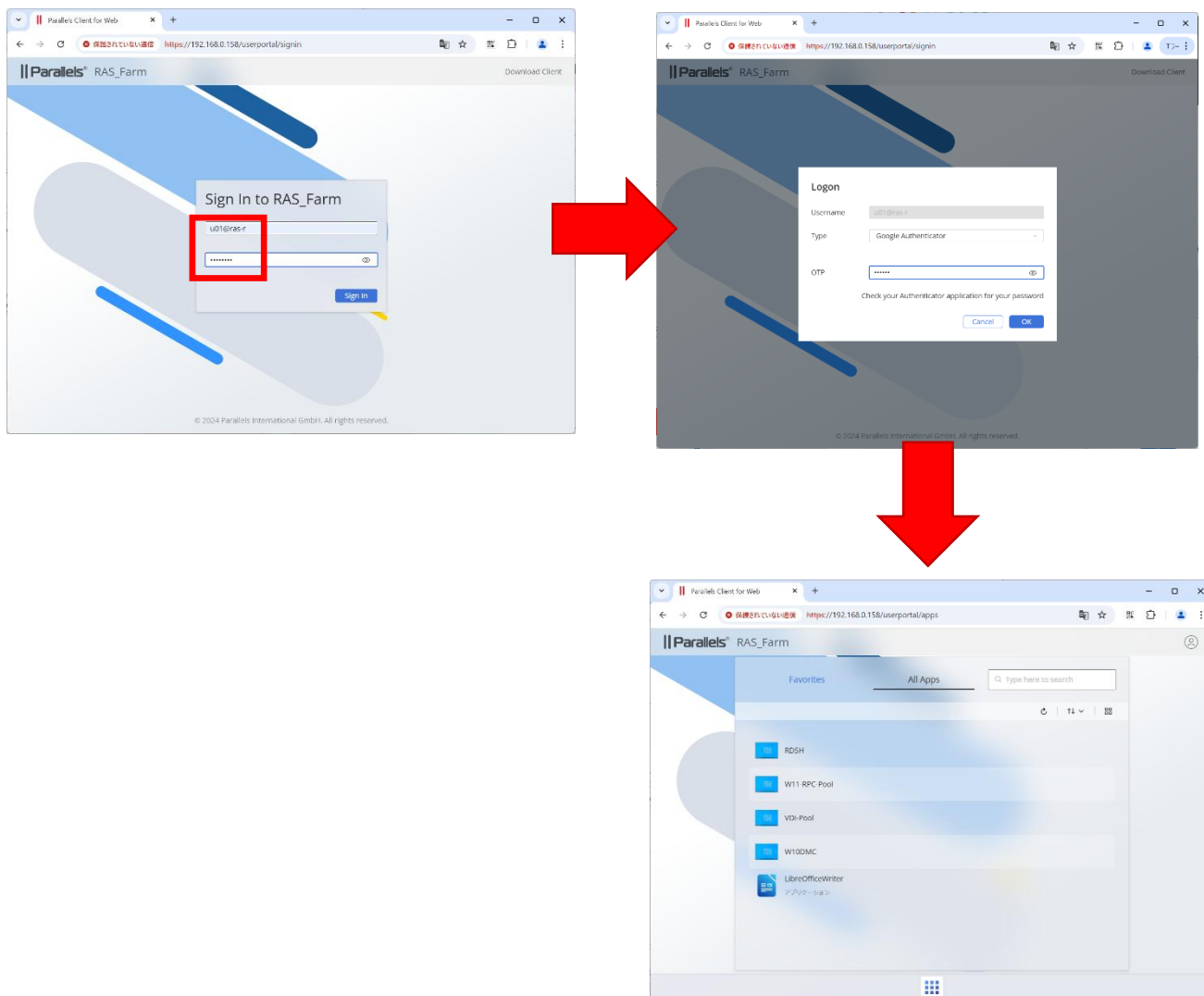
二要素認証の機能を追加することにより、ユーザー名とパスワードだけのシンプルな認証に加えてワンタイムパスワードの機能を追加することが可能です。ワンタイムパスワードの機能を追加することで、認証におけるセキュリティ強度をより高めることが可能です。

以下はワンタイムパスワードを利用した場合のログインの流れです。ここでは Google Authenticator を使用しています。

RAS Client の場合



Web から接続の場合



検証環境の構成

本ガイドであつかう検証環境について説明します。接続元であるクライアント側のコンポーネントは、Windows OS の物理マシンを使用します。

Parallels RAS 管理コンポーネントをインストールするサーバーを 1 台用意し、リモートから接続できる環境を用意しておきます。ここでは RDSH (Windows Server) のデスクトップ、Windows11 のデスクトップ、Windows 10 のデスクトップ、Windows Server 上で動作しているアプリケーションなどを事前に登録済です。

デスクトップやアプリケーションの設定方法については以下のサイトをご参照ください。

<https://jp.learn.corel.com/volume-licensing/resources/#pras>

項番	マシン	役割	OS
1	RAS Secure Gateway	RAS 環境へのログオン入り口。	Windows Server 2022
2	RAS Connection Broker 兼 RAS Console	RAS 環境への接続誘導、設定の保持。	Windows Server 2022
3	Active Directory	ユーザー認証。マシン登録。	Windows Server 2022
4	接続先リモート PC 用 物理マシン	リモート PC 接続先である物理マシン。	Windows 10
5	クライアント マシン	ユーザーが Parallels Client を使用し、VDI にリモート接続するための物理マシン。	Windows 10 *1

構築手順

RAS 環境を利用する際に、二要素認証を実施、設定するための構築手順を説明します。

事前準備

本ガイドでは、二要素認証の設定方法に限定して説明するため、事前に Active Directory を利用した環境で、RAS のデスクトップやアプリケーションの公開・設定が既に完了していることを前提としています。

RAS 環境の構築やデスクトップやアプリケーションの設定・公開方法については以下のサイトをご参照ください。

<https://jp.learn.corel.com/volume-licensing/resources/#pras>

多要素認証の設定

多要素認証は管理コンソールから設定します。ここではプライマリーのコネクションブローカーにサインインして、管理コンソール[Parallels Remote Application Server Console]を起動します。

- 1 RAS Console を起動し、左側のペインで、[接続]をクリックし、右側のペインで[多要素認証]タブをクリックします。



- 2 右側のペインの任意の場所で右クリックし、[追加]、[TOTP]をクリックし、今回は Google Authenticator を使用するため、[Google Authenticator]をクリックします。



- 3 [名前]に任意の名前を設定して、[次へ] をクリックします。



Google Authenticator MFA プロバイダーを追加

Parallels®

☒ サイト内の MFA プロバイダーを有効化(E)

名称(N):

説明(D):

タイプ: Google Authenticator

テーマ(T) + 🔍 タスク ▼

テーマ	MFA プロバイダー	説明
☐ <Default>	#0	ビルトインであること

i ゲートウェイ認証が許可されるのは、<Default>テーマが使用され、「ゲートウェイ認証接続を許可する」が設定されている場合、または [制限] タブで、Secure Gateway または Parallels Client IP が MFA から除外されている場合のみです。ご注意ください。

< 戻る(B) **次へ(N) >** キャンセル ヘルプ

- 4 次の画面では、今回はデフォルトのまま[次へ]をクリックします。



Google Authenticator MFA プロバイダーを追加 - 設定

Parallels®

表示名(N): デフォルト(E)

ユーザープロンプト(U): デフォルト(E)

認証

TOTP (Time-based One-time Password: 時間ベースのワンタイムパスワード) プロバイダーを使用する場合、Connection Broker およびクライアントデバイスの両方の時間をグローバル NTP サーバー (time.google.com など) と同期する必要があります。

TOTP の許容範囲を設定すると、セキュリティに影響する可能性があるワンタイムパスワードの有効性を高めることができます。

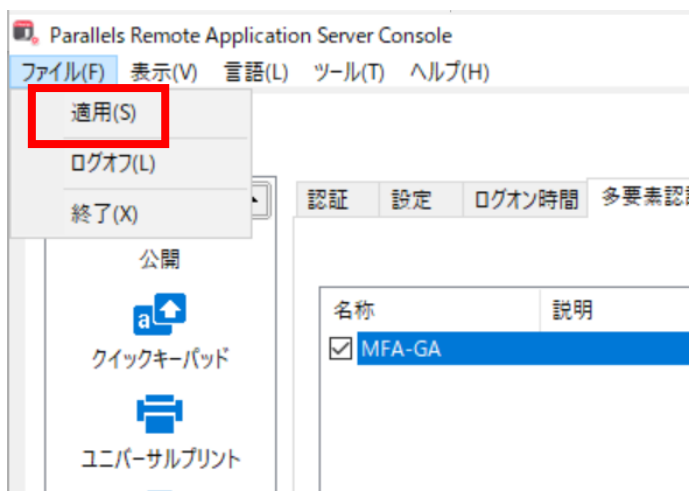
TOTP の許容範囲 (P):

< 戻る(B) **次へ(N) >** キャンセル ヘルプ

- 5 このまま利用を許可するため、デフォルトのまま[完了]をクリックします。



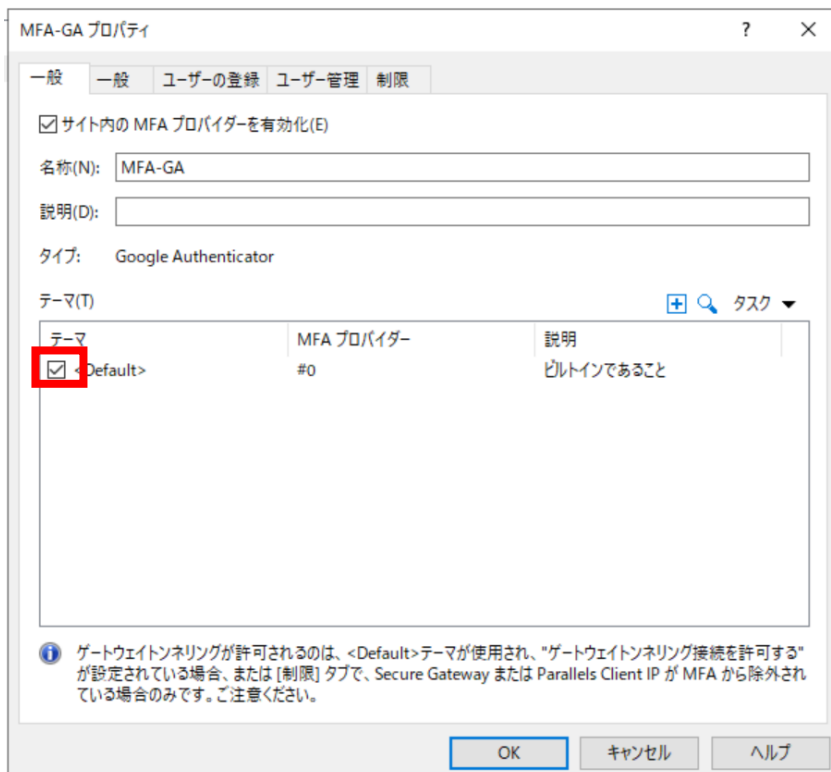
- 6 設定を保存するために[適用]を実行します。管理コンソールの右下または管理コンソール右上の[ファイル]から[適用]をクリックします。



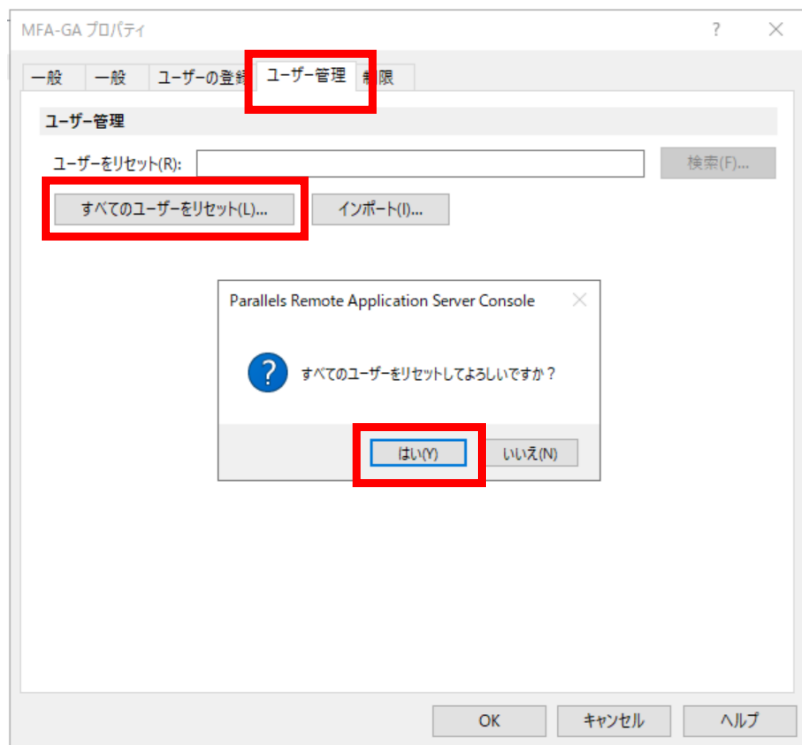
- 7 作成した多要素認証の設定を右クリックして[プロパティ]を開きます



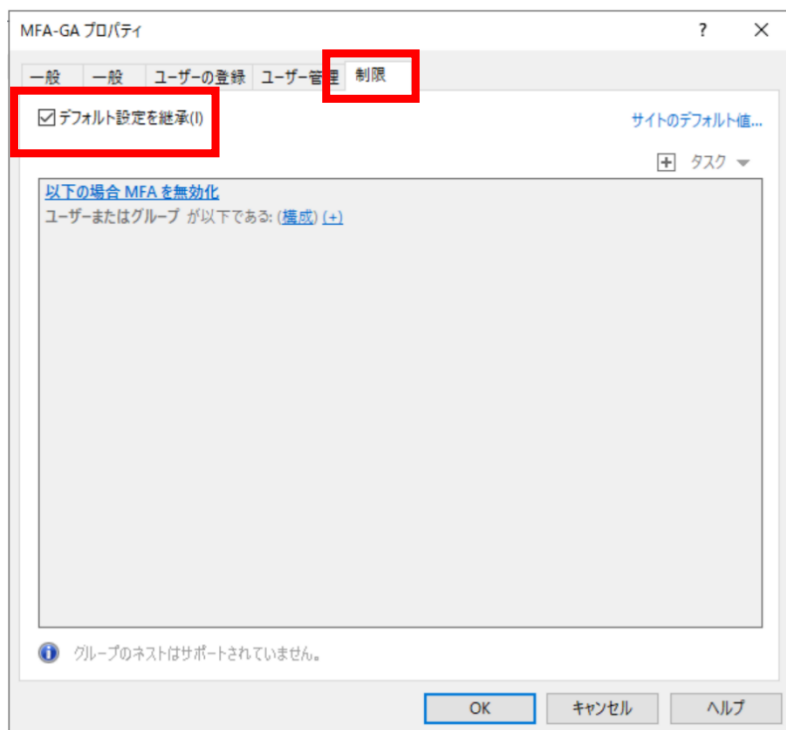
- 8 最初に表示される[一般]タブでデフォルトのテーマのチェックボックスにチェックを入れます。



- 9 [ユーザー管理]タブを選択し、一度全てのユーザーをリセットしておきます。[すべてのユーザーをリセット]をクリックして、ポップアップ画面で[はい]をクリックします。



- 10 続いて[制限]タブをクリックします。今回はサイトのデフォルト値を使わずにこの設定のための制限を設定するため[デフォルト値を継承]のチェックを外します。



- 11 [以下の場合 MFA を無効化]をクリックして[以下の場合 MFA を有効化]に変更します。

MFA-GA プロパティ

一般 一般 ユーザーの登録 ユーザー管理 制限

☐ デフォルト設定を継承(I)

以下の場合 MFA を無効化

ユーザーまたはグループ が以下である: (構成) (+)

クリック後

MFA-GA プロパティ

一般 一般 ユーザーの登録 ユーザー管理 制限

☐ デフォルト設定を継承(I)

以下の場合 MFA を有効化

ユーザーまたはグループ が以下である: (構成) (+)

- 12 [ユーザーまたはグループが以下である]の[構成]をクリックします。

MFA-GA プロパティ

一般 一般 ユーザーの登録 ユーザー管理 制限

☐ デフォルト設定を継承(I)

以下の場合 MFA を有効化

ユーザーまたはグループ が以下である: **(構成) (+)**

- 13 [ユーザーまたはグループを編集]の画面が表示されるので、[条件を有効化]にチェックを入れて、[+]ボタンをクリックします。

ユーザーまたはグループを選択

☒ 条件を有効化(E)

マッチングモード(M): 次のいずれか 1つ

グループ化 **+** タスク

名称	タイプ	SID
----	-----	-----

- 14 [ユーザーまたはグループの選択]画面がポップアップされるので適用するグループを設定します。ここでは事前に設定した RAS 利用者用のグループを入力し、[名前の確認]をクリックします。

ユーザーまたはグループの選択

オブジェクトの種類(S):
ユーザー、グループまたはビルトイン セキュリティ プリンシパル

場所の指定(F):
ras-r.com

選択するオブジェクト名を入力してください (例)(E):
RAS-Users

名前の確認(C)

詳細設定(A)... OK キャンセル

- 15 オブジェクト名の下にアンダーラインが表示されて、名前の確認が完了したら、[OK]をクリックします。

ユーザーまたはグループの選択

オブジェクトの種類(S):
ユーザー、グループまたはビルトイン セキュリティ プリンシパル

場所の指定(F):
ras-r.com

選択するオブジェクト名を入力してください (例)(E):
RAS-Users

名前の確認(C)

詳細設定(A)... OK キャンセル

- 16 前の画面に戻るので[OK]をクリックして閉じます。

ユーザーまたはグループを選択

☒ 条件を有効化(E)

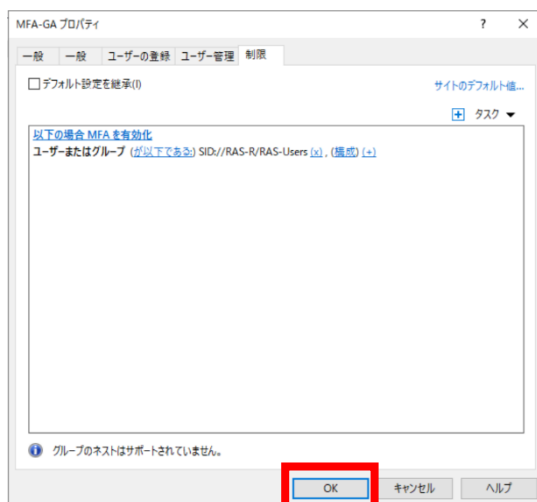
マッチングモード(M): 次のいずれか 1 つ

グループ化 + - 回転 タスク

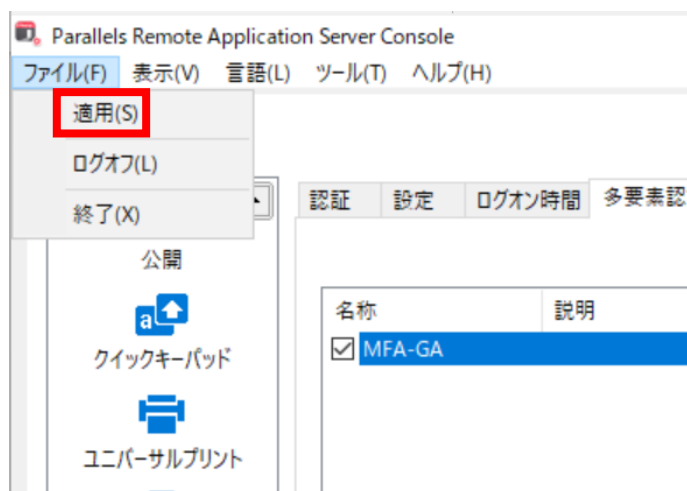
名称	タイプ	SID
SID: //RAS-R/RAS-Users	group	S-1-5-21-363206111...

OK キャンセル

- 17 再度前の画面に戻るので、[OK]をクリックして閉じます。



- 18 再度設定を保存するために[適用]を実行します。管理コンソールの右下または管理コンソール右上の[ファイル]から[適用]をクリックします。

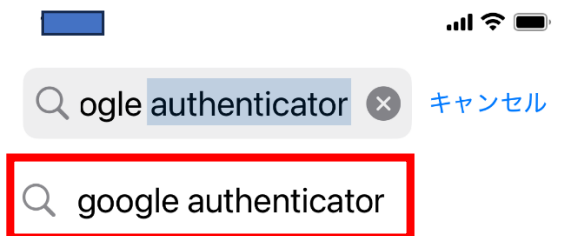


- 19 サーバー側の設定はこれで終了です。

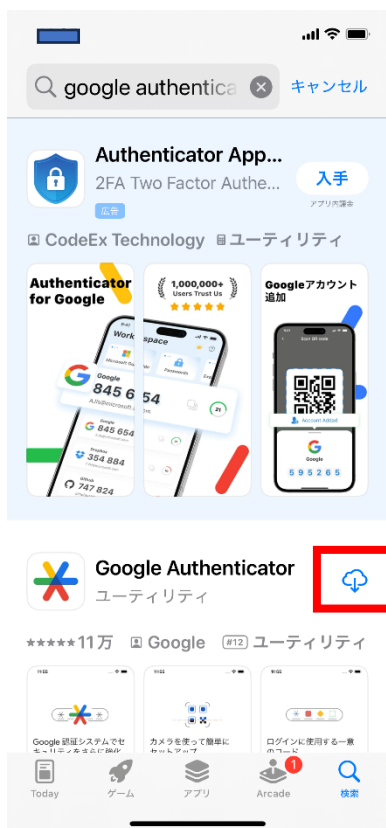
利用者側の設定

Google Authenticator を利用するためには、スマートフォンへの Google Authenticator アプリのインストールと設定が必要です。（ブラウザでの利用も可能ですが、セキュリティ強度が落ちるため推奨しません）

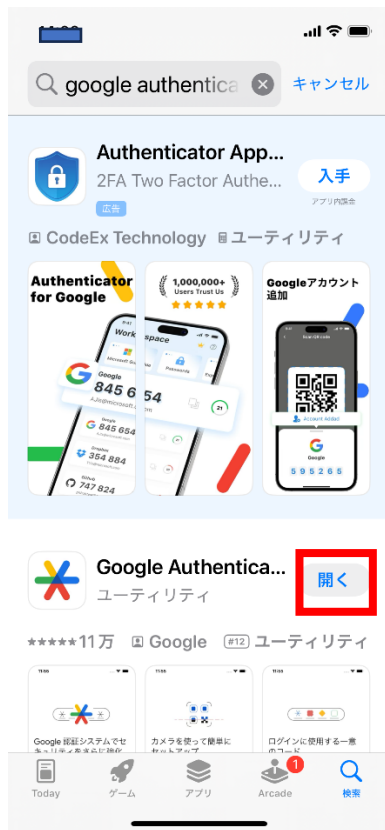
- 1 スマートフォンに Google Authenticator のアプリをインストールします。ここでは iPhone を例に説明します。
- 2 iPhone の App Store で検索を開き、検索ボックスに Google Authenticator と入力します。google authenticator がリストされるので、タップします。



- 3 Google Authenticator が表示されるのでダウンロードボタンをタップしてインストールします。



- 4 インストールが完了したら[開く]をタップして Google Authenticator を起動します。



- 5 Google Authenticator の初期画面が表示されるので、[開始]をタップします。



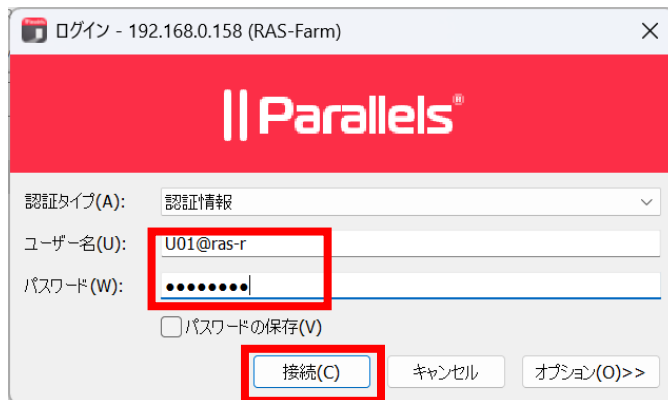
- 6 既に iPhone で Google アカウントにサインインしている場合は、そのアカウントを利用するか聞いてきます。ここではサインインすることなく利用するため、[アカウントなしで Authenticator を使用]をタップします。



- 7 認証システムのコードがない旨表示されます。このタイミングで一度、iPhone の作業は中断して、RAS Client の作業を行います。



- 8 既にログインしている場合は一度ログアウトして、ログインします。認証情報を求められるため、必要な情報を入力して[接続]をクリックします。



- 9 以下のような画面が表示されるため、QRコードを読み取るため、iPhoneでの操作に戻ります。



- 10 iPhone の Google Authenticator の停止していた画面で[コードを追加]をタップします。



- 11 認証システムのコードの追加は2通りあります。一つは QR コードをスキャンする方法、もう一つは認証コードを入力する方法です。ここでは QR コードを利用する方法で進めます。[QR コードをスキャン]をタップします。



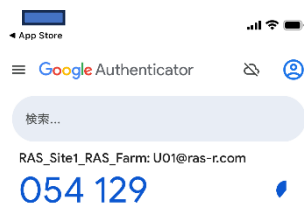
- 12 アプリケーションのカメラへのアクセス許可を求められるため、許可をタップします。



- 13 QR コードをスキャンする画面が表示されるため、緑色の四角の中に 9 のステップで表示された QR コードを投影します。



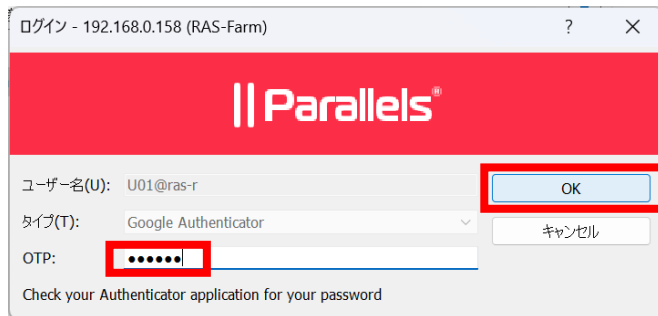
- 14 QR コードが認識されると、以下のようなワンタイムパスワードの画面が表示されます。数字の右側の円グラフは表示されているパスワードの有効期限です。デフォルトでは 30 秒毎にリフレッシュされます。



- 15 RAS Client に戻り、以下の画面で[次へ]をクリックします。



- 16 ワンタイムパスワードの入力を求められるため、[OTP]欄に iPhone に表示されているワンタイムパスワードを入力して[OK]をクリックします。

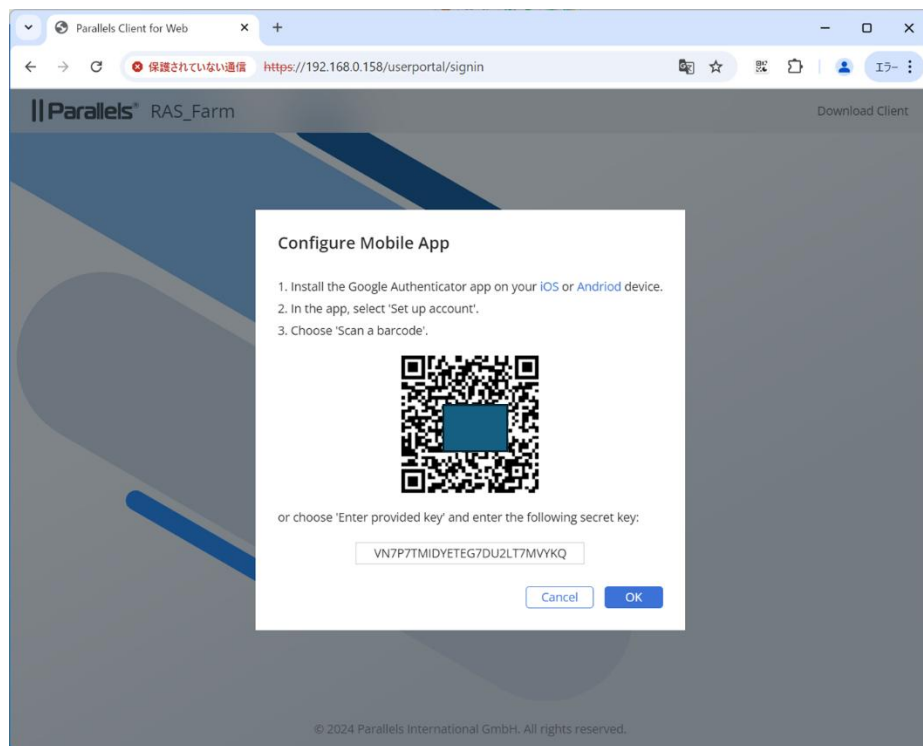


- 17 成功した旨のポップアップが表示されるため、[OK]をクリックして、デスクトップやアプリケーションの利用を開始します。



参考情報 Web からアクセスした場合の QR コード画面

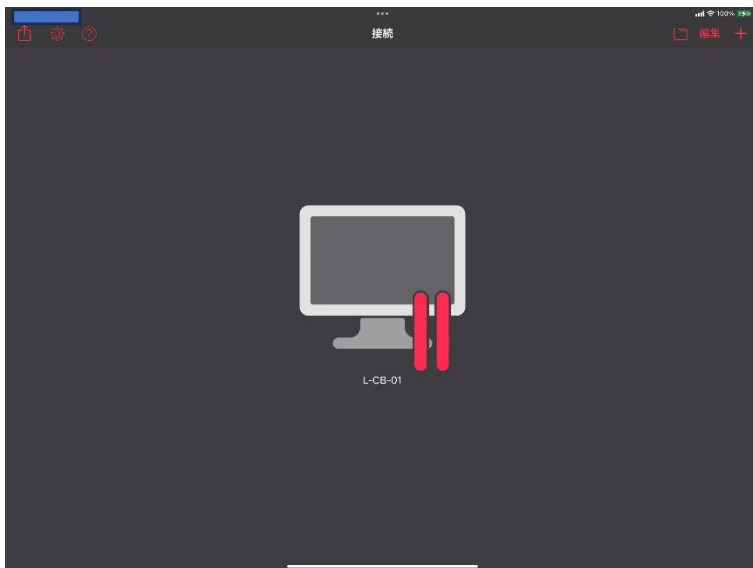
Web からアクセスした場合、Google Authenticator の QR コード設定画面は下記のイメージです。



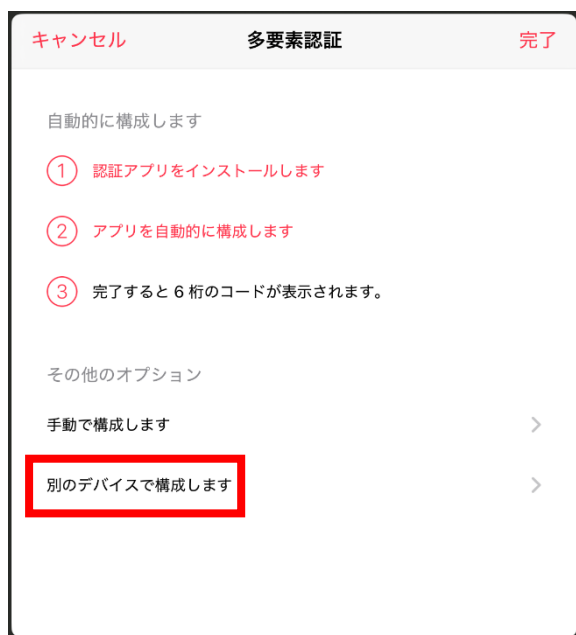
参考情報 iPad からアクセスした場合の QR コード画面

iPad からアクセスした場合の画面遷移は以下のようになります。

- 1 iPad の RAS Client から設定済の RAS へ接続するため、アイコンをタップします。



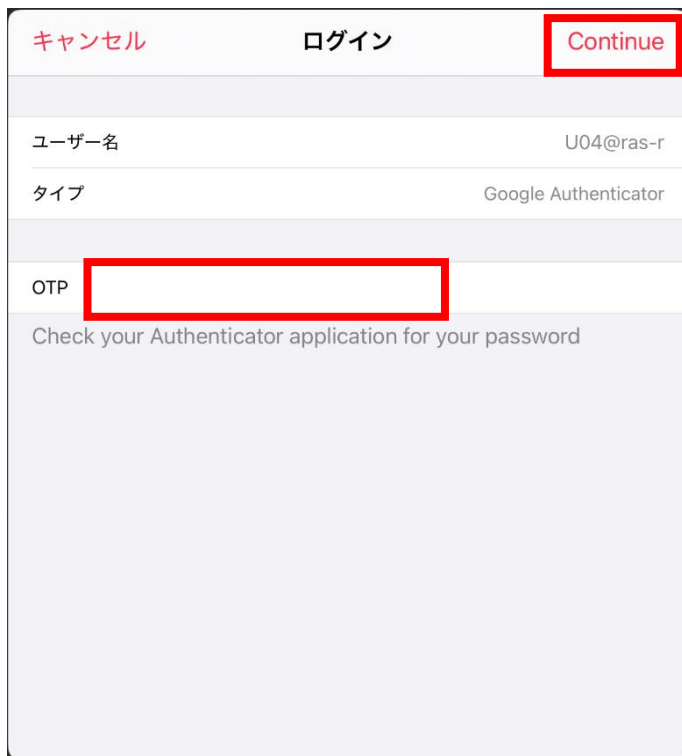
- 2 初めて多要素認証を利用する場合は以下の画面が表示されます。ここでは iPhone を使って多要素認証を実現するため、[別のデバイスで構成します]をタップします。



- 3 QRコードが表示されるため、前述の手順と同じように iPhone にインストールした Google Authenticator アプリで QRコードを読み取ります。



- 4 ワンタイムパスワードの入力画面が表示されるため、iPhone に表示されているワンタイムパスワードを入力して[Continue]をタップします。



- 5 初回のみ以下のメッセージが表示されます。[OK]をタップして、RAS をご利用ください。

