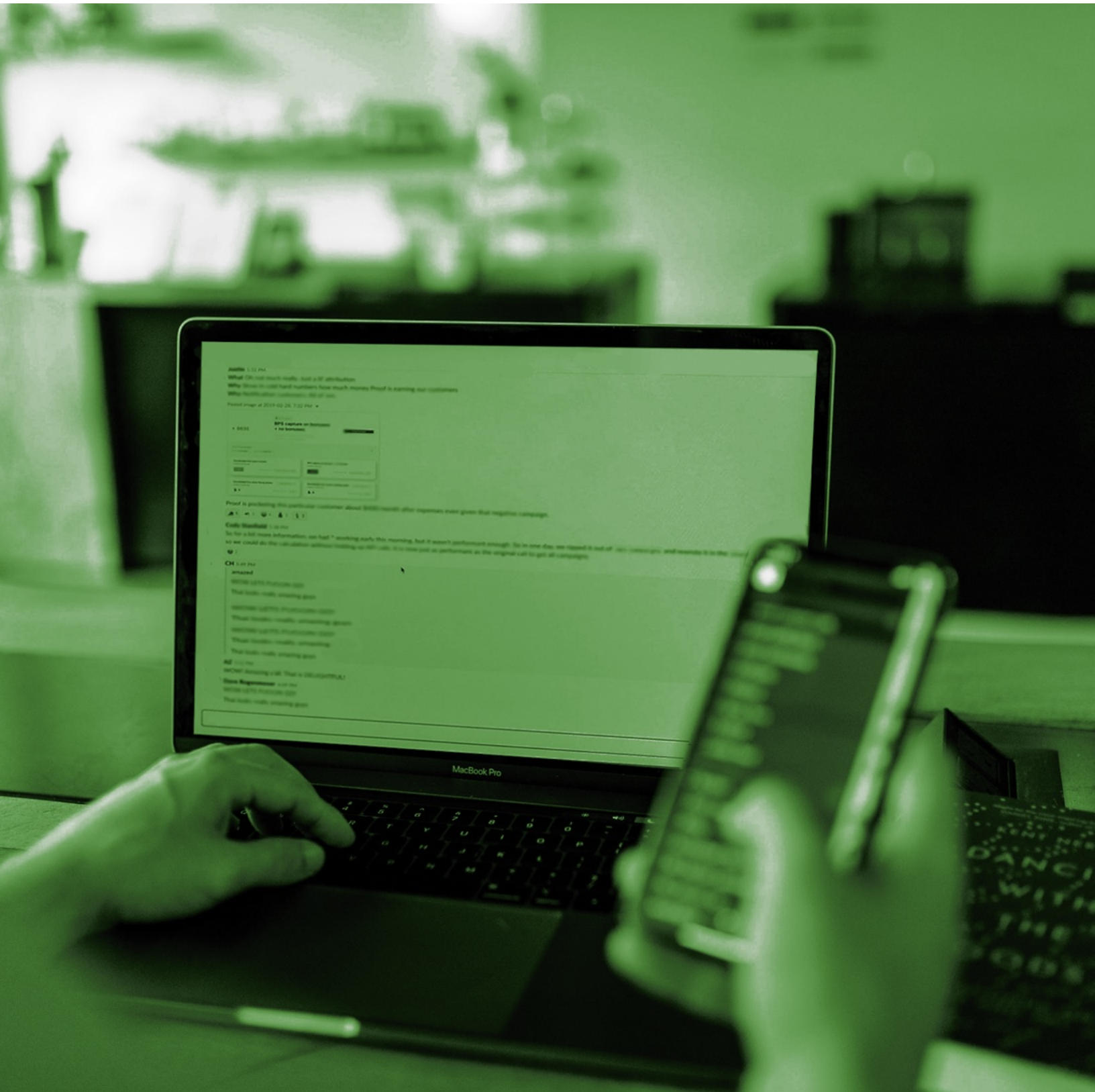
Duo Security
は、シスコ傘下企業です。

ヘルプデスクガイド

初版リリース 2016 年 6 月 22 日
バージョン 4.0 リリース:2020 年 1 月 15 日



目次

一般用語

Duo ドキュメント、社内の *IT* チーム間、またはエンドユーザにより使用される可能性のある用語は次のとお りです。

2FA(二要素認証): ユーザ名/パスワードに加えて別の要素を追加した認証方法。2FA では、ユーザが知っている情報情報 (パスワード)とユーザが持っているデバイス(スマートフォン上の Duo Mobile など)が求められ、ユーザのパスワードだけで他者がユーザのデータにアクセスすることはできません。Duo 2FAでは、ユーザ名とパスワードは変わらず入力されます。Duoが提供する2つ目の認証要素は、既存のクレデンシャルに追加されたセキュリティレイヤです。詳細については、こちらのビデオを確 認してください。

Duo 管理(Duo Admin) パネル: Duo 管理者がユーザ、デバイス、システム統合、ロール、ログ、課金情報などを管理できるログインによって保護されている管理インターフェイスです。

Duo プロンプト: ユーザは Web ベースのアプリケーションにログインする度に本人確認の方法(例えば、「Duo Push」または「Call」)を選択できます。Duo プロンプトでは、インライン登録と認 証を行うことができます。

パスコード: これらは、Duo モバイルアプリ、SMS(テキストメッセージ)、またはユーザのハードウェア トークンのいずれかを使用して生成できます。

プラットフォーム(Platform): ユーザの認証デバイスタイプ(iPhone、Android、固定電話電話など)です。

プッシュ通知(Duo Push): これは登録済みデバイス上の Duo Mobile アプリケーションに送信されるアウトオブバウンド方式の認証要求です。プッシュ通知には、ユーザの場所、IP アドレス、ユーザがアクセスしようとしているア プリケーションなどの情報が含まれます。

セルフサービスポータル: [Duo 管理(Duo Admin)] パネルでセルフサービスポータルが有効になっている 場合、ユーザは Duo プロンプトから直接、デバイスを追加したり、認証方法の設定を更新したりできます。Duo のすべての有料エディションで利用可能です。

パート I:概要

このガイドが必要なのはなぜですか。

二要素認証(通常は 2FA と呼ばれる)を企業に導入した場合、エンドユーザから質問が寄せられる可能性が あります。Duo のセットアップは簡単でインターフェースも使いやすいですが、二要素認証を使用したことがな いー部のユーザにとって、Duo の認証は混乱を招く可能性があります。このガイドは、エンドユーザが Duo を使用するときに生じる問題に対処できるよう、迅速な回答の助けになるよう 提供しています。

このガイドは、特定の役割の管理者が、エンドユーザの一般的な設定や問題 の解決を支援するためのものです。管理者とエンドユーザの Duo アカウントの違いについての詳細 は、こちらをご覧ください。

Duo では、1 つのアカウントに少なくとも 2 人の 所有者ロールの管理者を設定することをお勧めします。同様に、所有者が 組織に出入りする可能性があるため、管理者のリストを定期的に更新することが重要です。2 人の所有者がいることにより、Duo 管理パネルへの冗長アクセスが提供され、1 人がアクセスできない場合でも一貫 したレベルのアクセスが保証されます。複数の所有者がいることで、顧客が管理上のニーズを自分で行うことができ るため、時間を節約できます。

ここでは、[Duo 管理(Duo Admin)] パネル内での役割と、各役割に割り当てら れたアクセス権限の概要を簡単に説明します。

	所有者ロール	Administrator ロール	アプリケーション権限ロール	ユーザマネージャロール	Help Desk ロール	課金ロール	読み取り専用ロール
ログの表示とダウンロード	✅	✅	✅	✅	✅		✅
2FA デバイスとバイパスコードの管理	✅	✅		✅	✅		
ユーザとグループの管理	✅	✅		✅			
アプリケーションの管理	✅	✅	✅				
グローバル設定の変更	✅	✅					
課金の表示と管理	✅					✅	
他の管理者の管理	✅						

さらに、Duo の管理ユニット機能により、Duo の有料エディションの管理者は、Duo のユーザとアプリケーションをグループ化した り、管理権限を指定した管理者に割り当てることができます。管理ユニット機能の詳細については、次の URL を 参照して下さい。https://duo.com/docs/administrative-units
注記:制限されている管理者には、他のグループのユーザまたはアプリケーションは表示されません。

パート2: 登録とアクティベーション

エンドユーザにとって登録はどのような感じになりますか。

ユーザには 2 つのオプションがあります。ユーザが認証する予定のデバイス以外のデバイス(Duo で保護さ れたサービスにアクセスするために使用するラップトップやデスクトップなど)から、または(携帯電話など の)最終的に認証を行うデバイスから、登録プロセスを開始します。

ラップトップ、デスクトップ、またはその他の認証に使用されていないデバイスからの登録

ユーザは、登録電子メールに記載されているリンクから登録を開始します。登録に関するプロンプトを使用し、ユーザ は認証デバイスでこのプロンプト内のQR コードをスキャンできます。

QR コードをスキャンできないとユーザから言われた場合は、スマートフォンのカメラにアプリからのアクセスを許可したことを確認するよう依頼して下さい。そうしないと、コードをスキャンできません。この プロセスの詳細については、登録ガイド: https://guide.duo.com/enrollment を参照して下さい。

認証デバイスからの登録

この方法では、ユーザは登録電子メールに従ってスマートフォンのセットアップを開始し、登録を進め必要に 応じて最後に Duo Mobile をインストールします。詳細については、次のナレッジベースの記事を参照してく ださい:
https://help.duo.com/s/article/3890

登録電子メールを再送信するにはどうすればよいですか。

一括登録または Active Directory Sync で登録されたユーザで、まだ登録を完了していないユー ザに登録メールを再送信できます。こちらの一括自己登録のステップ 5 で説明されているプロセスに従って、登録メール を再送信します: https://duo.com/docs/enrolling_users#bulk-self-enrollment

パート 3:認証と認証方式

新しい認証デバイスを追加またはアクティブにするにはどうすればよいですか。

ユーザの新しい認証デバイス(携帯電話、固定電話、タブレット、または U2F トークン など)を追加またはアクティブにする方法について説明します。Duo プロンプト内のセルフサービスポータ ルが有効になっている場合(Duo の有料エディションでのみ使用可能)、ユーザは新しいデバイスを自分で追加 できます。セルフサービスポータルが有効になっていない場合、管理者がデバイスを追加できます。

ユーザは、事前にアクティブにした認証デバイスまたはバイパスコードがある場合に、セルフサービスポータルを介して新しいデバイスを追加できます。いずれかにアクセスできない場合は、管理 者が新しいデバイスの追加を手助けする必要があります。

セルフサービスポータルが有効になっている場合: https://guide.duo.com/add-device
手動でDuo 管理パネルから追加する場合: https://duo.com/docs/administration-devices

ユーザがデバイスを忘れた場合はどうすればよいですか。

自宅に携帯電話またはハードウェアトークンを忘れてしまったユーザがいますか。サポート可能な方法につい ては、こちらのナレッジベースの記事を参照してください: https://help.duo.com/s/article/3302

デバイスが紛失または盗難された場合はどうすればよいですか。

2FA 認証デバイスが紛失または盗難された場合、すぐに管理者に連絡する必要があることをユーザに常に強 調してください。

セルフサービスポータルが有効で、ユーザが 2 台目の認証デバイスを持っている場合、ユーザは 自分でDuo プロンプ トの [設定とデバイス(My Settings & Devices)] メニューにアクセスし、直ちに紛失または盗難にあったデバ イスを削除して下さい。セルフサービスポータルが有効でない、または 2 台目の認証デバイスを持っていない場 合、管理者はDuo からデバイスを削除し、新しい認証方法が追加されたことを確認して下さい。

セルフサービスポータルが有効になっている場合: https://guide.duo.com/common-issues#lost-phone
手動でDuo 管理パネルから削除する場合:
https://duo.com/docs/administration-devices#dealing-with-lost-or-stolen-phones

飛行機に乗っているとき、または遠隔地に旅行しているときに認証を必要とするユー ザをどのように支援できますか。

Duo Push、SMS、または電 話のコールバックが利用できない飛行機やその他の場所で、Duo モバイルアプリケーションを使用してパスコードを生成できることをユーザに案内します。Android または iOS での Duo モバイル生成パスコードを使用した認証については、エンドユーザガイド を参照してください。詳細については、『Duo Travel Guide』を参照してください。

Duo プッシュ通知を受信しないのはなぜですか。

まず、ユーザのスマートフォンが通知を許可していることを確認します。

スマートフォンと Duo サービスの間のネットワークに問題がある場合、プッシュの受信に問題が発生する可能性があります。多くのスマートフォンでは、プッシュ要求を確認するときに Wi-Fi またはモバイルデータ通信を使用するかどうかを判断するのに問題があり、インターネットに接続に問題がない場合、電話機を機内モードにして通常の動作モードに戻すだけで、この種の問題が解決することがよくあります。同様に、デバイスの Wi-Fi 接続をオフにし、モバイルデータ通信を使用して問題を解決できる可能性があります。Duo プッ シュ通知はわずか 2 KB です。

スマートフォンの時刻と日付が正しいことを確認してください。スマートフォンの日付と時刻が手動で設定されている場合は、設定を変更して、日付と時刻がネットワークと自動的に同期するようにしてください。

また、iOS: https://help.duo.com/s/article/2051 および Android: https://help.duo.com/s/article/2050. の Duo プッシュ配信について、詳細なトラブルシューティングガイドを作成しました。発生している特定の問 題によっては、ポートアクセスを変更できる IT 管理者が必要になる場合があります。

トークンをユーザに割り当てるにはどうすればよいですか。

Duo から購入したトークンは、アカウントに自動的にインポートされます。管理者は、サードパーティの OTP トークン情報を手動で Duo にインポートする必要があります。トークンをインポートする場合は、トー クンを Duo アカウント間で一意にする必要があることに注意してください。

Duo は FIDO U2F トークンをサポートしていますが、U2F トークンは管理パネルからインポートしたりユー ザに割り当てたりすることはできません。代わりに、ユーザは、U2F トークンを Duo 登録プロンプトまたは セルフサービスポータルを使用して自分で登録します。詳細については、エンドユーザの U2F 認証と U2F 登録 プロセスの有効化に関するドキュメントを参照してください。

トークンをエンドユーザに割り当てるには、https://duo.com/docs/administration-devices#assigning-a-token-to-an-end-user を参照してください。

バイパスコードを作成するにはどうすればよいですか。

バイパスコードは、特定のユーザを対象に管理者によって作成された一時的なパスコードです。これらは通常「バックアップコード」として使用されるため、モバイルデバイスに問題が発生しているユーザ(たとえば、モバイルサービスが中断された場合、デバイスを紛失/盗難された場合など)は、引き続き Duoで保護されたシステム にアクセスできます。バイパスコードは、自分でデバイスを登録できないアプリケー ションに一時的なユーザがデバイスを登録せずにアクセスを許可することもできます。バイパスコードは、許可された回数を使用し た後、または管理者が定義した時

間が経過した後に期限切れになります。デフォルトでは、バイパスコード は、1 回の使用または 1 時間後のどちらかで期限切れになります。

バイパスコードの作成方法は以下をご参照下さい:
https://duo.com/docs/administration-users#generating-a-bypass-code

ロックアウトされたユーザを支援するにはどうすればよいですか。

認証試行時の指定されたしきい値を超えたため、ステータスが「ロックアウト」になっているユーザは、ス テータスを「アクティブ」に戻す必要があります。ユーザステータスの詳細と、ここでの変更方法について は、https://duo.com/docs/administration-users#changing-user-status を参照してください。

パート 4:役立つヒント

ユーザがフィッシングに関するアラートに敏感になっている場合

Duoを社内で導入したばかりの場合、ユーザは Duo の登録やアクティベーションメールなどの通知を疑わしいと思うかもしれません。これらのメールをフィッシングメールだとユーザから報告される場合があります。送信された通知を確認する場合、Duo 管理パネルから送られた電子メールまたは SMS のコ ピーと同じか確認します。もしくは受信したメッセージのコピーを転送するようにユーザに依頼し、ユーザが登録/認証を続行で きるようにそのメッセージの安全性を確認します。

ユーザに **Duo Push** を利用するように推奨する

可能なかぎり、ユーザに Duo Push の使用を推奨します。Duo Push は最適なオプションです。便利 で、安全で、最も安価です(プッシュ認証には電話料金は発生しません)。携帯電話の電波 が届かない場合でも、またどの国でもユーザはプッシュを使えます。

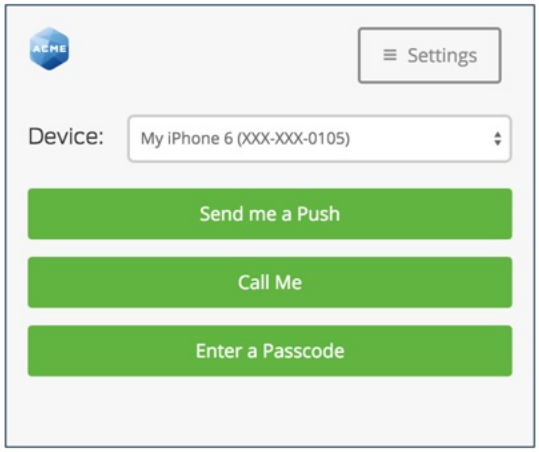
また、Duo Push をユーザに勧める上で役立つガイドも作成しました:
https://help.duo.com/s/article/promoting-push

Help Desk プッシュを使用してユーザの本人確認を行う

ユーザのヘルプやリクエストに応じて変更を実施する前にDuo Pushを使ってユーザの本人確認を行うことができます。Help Desk のプッシュを利用する方法の詳細は、次のマニュアルを参照してください。
https://duo.com/docs/administration-users#verifying-users-with-duo-push

ユーザの **Duo** プロンプトが、想定されているものとは異なる形式で表示される

ユーザが(タブレットなどの)小さなデバイスまたは小さなブラウザウィンドウからログインしている場 合、Duo プロンプトがエンドユーザマニュアルに表示されているものと若干異なる場合があります。これら の機能は、同じ権限を持つ他のユーザと同じ機能です。



no-reply@duosecurity.com を受信許可リストに登録する

組織で電子メールフィルタリングを使用している場合、このアドレスを受信許可リストに登録しないと、登録メールやアクティベーション電子メールを受信できないことがあります。

アクティベーションリンクと登録リンクの有効期限が異なる

登録リンクは 30 日後に期限切れになります。登録メールを再送信しても、登録期限はリセットされません。

アクティベーションリンクは ディフォルトで24 時間後に期限切れになります。[Duo 管理(Duo Admin)] パネルからアクティベーションリンクを最近送信したユーザに対しては、既存のリンクが期限切れになるまで 新しいリンクを送信することはできません。

アクティベーション & 登録メッセージの詳細については、https://duo.com/docs/enrolling_users をご参照下さい。

パート 5:トラブルシューティングとサポート

トラブルシューティング リソース

Duo 管理パネルのプロセスおよびアプリケーション設定の推奨事項は、duo.com/docs にある Duo の包括的なドキュメンテーションページからお探し頂けます。

help.duo.com では Duo のナレッジベースを提供しており、トラブルシューティング リソースとセルフサー ビスコンテンツを検索できます。

Duo コミュニティcommunity.duo.com で、お探しの回答が過去の投稿にあるかどうか確認したり、新たにご自身で質問を投稿することができます。

[Duo 管理(Duo Admin)] パネルへの認証またはアクセスに問題がありますか。当社のサポートチームは、https://status.duo.com の Duo ステータスページをリアルタイムで更新し、サービス上の問題をお知らせしています。管理者ロールと所有者ロールの Duo 管理者は自動的に登録され、自身のデプロイメントに関連した StatusPageの更新 を受信します。

是非ご登録下さい。[ステータス(Status)] ページの登録の詳細については、を参照してください。

認証ログレポートは、ユーザログインの問題のトラブルシューティングに役立ちます。具体的に は、認証が拒否された理由を理解することで役立ちます。こちらの詳細についてはナレッジベース記事、https://help.duo.com/s/article/1023 を参照してください。

Duo からの最適なサポートを得る

必要な情報が見つからなかった場合、Duo サポートに連絡の際に必要な事項を以下にご案内します。

- サポートへ連絡の際、担当者が[Duo 管理(Duo Admin)] パネルの管理者として登録されていることを確 認してください。
    - 所有者以外の管理者の場合、Duo サポートは管理者の権限レベルに応じてサポートすることができます。
- Duo以外のアプライアンスまたはアプリケーション(例:Active Directory)が関係している場合は、それらにアクセスできる管理者がいることを確認してください。
- 可能な限り、スクリーンショットとログファイルを提供してください。
- アカウントID
- ● Duo 認証を通じて本人確認を行う機能。スマートフォンでの管理者の認証に Duo プッシュを有効 にする手順は、次の URL から入手できます:https://duo.com/docs/administration-admins#use-duo-push-for-administrator-authentication
    - Duo Push で管理者の本人確認を行うことができない場合、別の方法にて本人確認を行うため、サポートにお電話頂いた際、確認にお時間がかかることがあります。
- 認証プロキシ .cfg またはその他の機密ファイルを送る場合は、プレーンテキストで秘密鍵(SKEY) を共有しないでください。GPG 暗号化を推奨します。
- すでに同じ問題についてDuoサポートに連絡している場合は、既存のチケット番号を併せてご案内下さい。

お使いのエディションと緊急性に基づいて、Duo サポートにご連絡下さい。: https://help.duo.com/s/article/1441