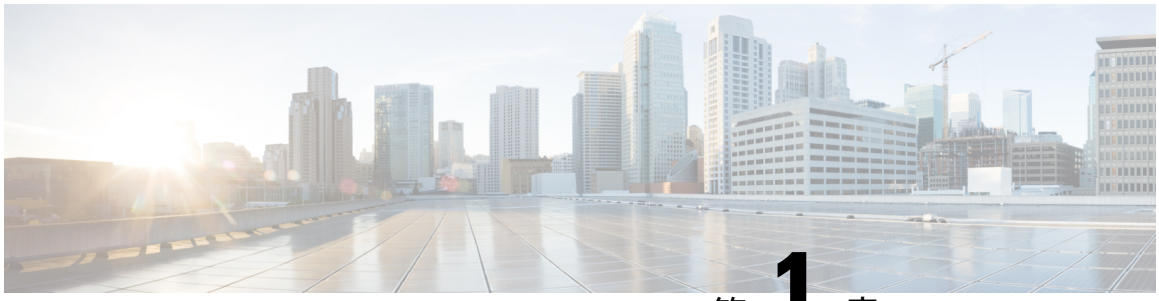
Cisco Security Cloud Sign On

初版：2019 年 10 月 1 日

最終更新：2023 年 8 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

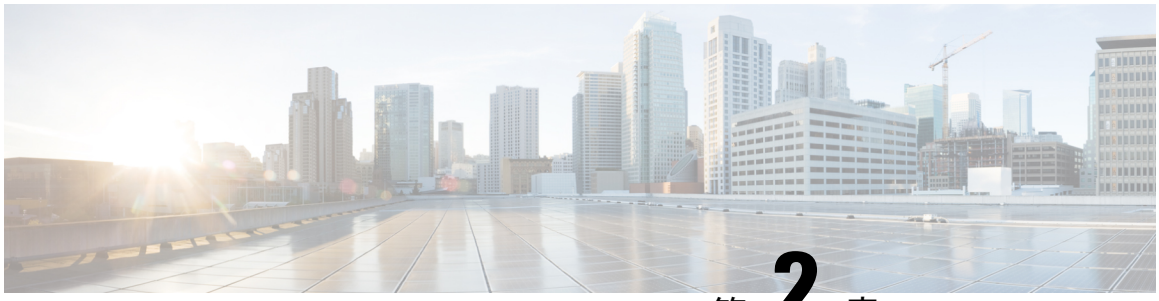
概要

概要

Cisco Security Cloud Sign On を使用すると、1 つのログイン情報で任意のデバイスからシスコのさまざまなセキュリティ製品に簡単にアクセスできます。ユーザ名とパスワードを使用してサインインすると、シスコのセキュリティ製品がすべてカスタマイズ可能なダッシュボードにアプリケーションとして表示されます。

- アプリケーションをクリックすると自動的にサインインされ、シスコのセキュリティ製品全体でシームレスなワークフローを実現します。これで、いくつものパスワードを覚える時間を削減できます。
- Duo の多要素認証（MFA）を使用した統合とは、適応型の階層化されたシンプルな認証を意味します。ワンプッシュ通知、ワンタップで簡単にアクセスできます。
- 必要に応じて、Security Cloud Control を使用して Security Cloud Sign On と独自の ID プロバイダー（IdP）を統合します。

概要



第 2 章

新機能

新規ポータル

この新しいポータルでは、Cisco SecureX Sign-on の外観と使いやすさが改善されています。お住まいの地域を選択し、拡張されたポータルから SecureX または他のシスコのセキュリティ製品を起動します。

Cisco SecureX

Cisco Security Cloud Sign On を使用した Cisco SecureX へのサインイン

Cisco Security Cloud Sign On アカウントを使用して Cisco SecureX にサインインできるようになりました。

Microsoft Azure

Microsoft Azure アカウントを使用した Cisco Secure Sign-On へのサインイン

Microsoft Azure アカウントを使用して Cisco Secure Sign-On にサインインできるようになりました。

- 使用対象者

  組織の ID プロバイダー（IdP）に Microsoft Azure を使用しているお客様。

- このメソッドを有効にする方法

お客様の Microsoft Azure の設定に応じて、組織に対して透過的に機能します。設定されていない場合は、最初のユーザがアクセスを試みたときに、管理者が Azure ポータルで承認する必要があります。設定の詳細については、Microsoft Docs Web サイトにアクセスし、次のトピックに関する Azure のドキュメントを参照してください。

- エンタープライズ アプリケーションにユーザまたはグループを割り当てる
- アプリケーションにテナント全体の管理者の合意を付与する
- 管理者の合意ワークフローを設定する

- 顧客の Microsoft Azure Active Directory（AD）プロファイルからユーザ ID 属性を取得していますか。

  はい。姓、名、表示名、役職、携帯電話番号、および組織名を取得します。

- Azure グループ情報を取得して、Cisco Secure Sign-On で保護されたアプリケーションを認識および使用できますか。

  いいえ。グループの割り当てとロールの権限は、シスコのアプリケーションごとに個別に処理されます。

- Cisco Secure Sign-On を使用するアプリケーションへのアクセス方法が変わりますか。

  いいえ。同じユーザ名を使用している限り、以前と同様にアプリケーションにマッピングされます。変更されるのは認証方法のみです。

- 両方のアカウントを引き続き保持して使用できますか。

  はい、もちろんです。

- @cisco.com ユーザ名を持つシスコの従業員にはどのような影響がありますか。

  シスコでは、@cisco.com アカウントによる Microsoft サインインを有効にしていないため、この方法でサインインしようとすると、エラーメッセージが表示されます。

- [Microsoftでサインイン（Sign in with Microsoft）] オプションを使用しても、Cisco Secure Sign-On アカウントがない場合はどうなりますか。

  これは透過的に機能するため、別のアカウントを作成せずに直接サインインできます。

Cisco.com

Cisco.com アカウントを使用した Cisco Secure Sign-On へのサインイン

cisco.com アカウントを使用して Cisco Secure Sign-On にサインインできるようになりました。

- Cisco Secure Sign-On アカウントとの違いは何ですか。

  これは、標準の cisco.com アカウント（以前は CCO と呼ばれていました）で、サポートへのアクセスやソフトウェアのダウンロードなどに使用されます。

- Cisco Secure Sign-On を使用するアプリケーションへのアクセス方法が変わりますか。

  いいえ。同じユーザ名を使用している限り、以前と同様にアプリケーションにマッピングされます。変更されるのは認証方法のみです。

- 両方のアカウントを引き続き保持して使用できますか。

  はい、もちろんです。

- @cisco.com ユーザ名を持つシスコの従業員にはどのような影響がありますか。

  シスコの従業員は、[Cisco.comでサインイン（Sign in with Cisco.com）] オプションの使用が推奨されます。これにより、シスコのメトリックで従業員であると認識され、MFA プロンプトを 1 度だけ確実に受け取ることができます。

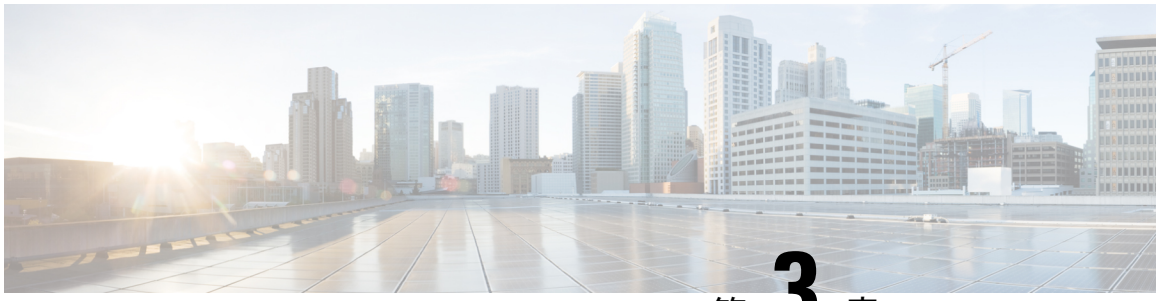
- [Cisco.comでサインイン（Sign in with Cisco.com）] オプションを使用しても、Cisco Secure Sign-On アカウントを持っていない場合はどうなりますか。

  これは透過的に機能するため、別のアカウントを作成せずに直接サインインできます。

URL の変更

URL の変更

Cisco Secure Sign-On のドメインは、2020 年 3 月 24 日に security.cisco.com から sign-on.security.cisco.com に移行し、Cisco SecureX に対応しました。ブックマークとパスワードマネージャ（LastPass、1Password、DashLane など）を更新して、新しい URL を参照します。



第 3 章

使用する前に

Security Cloud Sign On でのサインイン

始める前に

この手順を完了するには、Security Cloud Sign On アカウントが必要です。アカウントの作成については、「Security Cloud Sign On アカウントの作成 （7 ページ）」を参照してください。

ステップ 1 https://sign-on.security.cisco.com を開きます。

ステップ 2 Security Cloud Sign On アカウントを持っている場合：

a) ユーザー名を入力し、[次へ（Next）] をクリックします。

b) パスワードを入力して、[Log In（ログイン）] をクリックします。

c) Duo MFA または Google Authentication（設定されている場合）を使用して認証します。

または、**シスコ** または **Microsoft** の ID サービスでサインインするには、[その他のログインオプション（Other login options）] をクリックし、認証に使用する ID プロバイダーをクリックします。

Security Cloud Sign On アカウントの作成

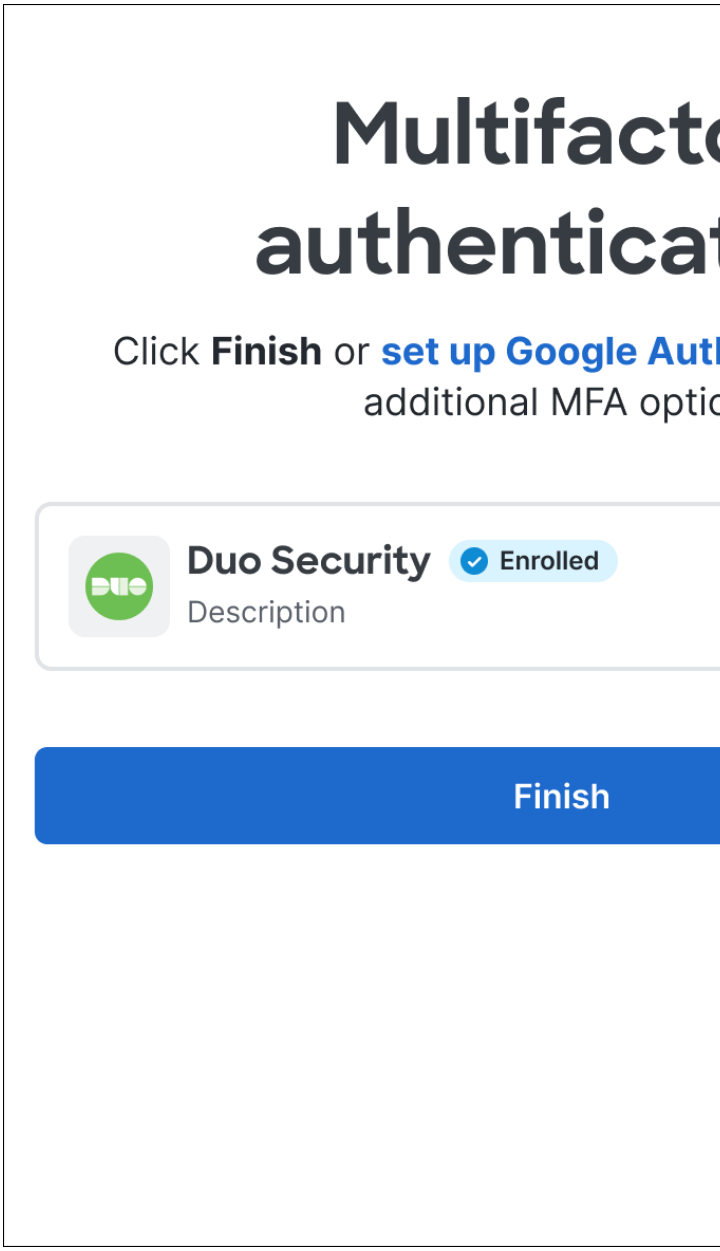
Security Cloud Sign On アカウントを作成するには、アカウント アクティベーション電子メールの送信先となる電子メールアドレスを指定する必要があります。すべての Security Cloud Sign On ユーザーアカウントは、多要素認証（MFA）を使用する必要があります。Duo MFA は Security Cloud Sign On アカウントに無料で含まれています。または、Google Authenticator アプリから時間ベースのワンタイムパスワードを使用することもできます。

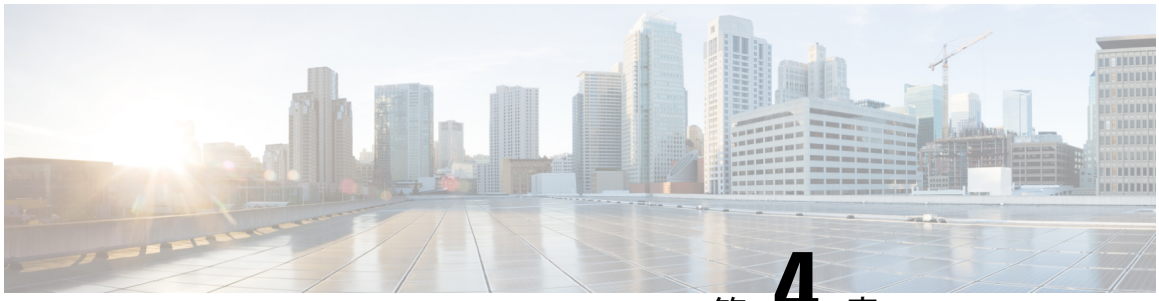
手順の概要

1. [アカウントのサインアップ（Account Sign Up）] ページを開きます。
2. 要求された情報を入力し、エンドユーザーライセンス契約に同意して、[サインアップ（Sign up）] をクリックします。
3. シスコから送信された「アカウントを有効化（Activate Account）」という件名の電子メールから、[アカウントを有効化（Activate Account）] をクリックします。
4. Duo 多要素認証オプション（Touch、Duo Mobile、セキュリティキー、または電話番号）を選択し、検証プロセスを完了します。ヘルプについては、『Duo Guide to MFA and Device Enrollment』を参照してください。
5. 必要に応じて追加の認証要素を追加するか、[今はスキップ（Skip for now）] をクリックします。
6. [Duo でログイン（Log in with Duo ）] をクリックし、任意の認証オプションを使用してサインインします。
7. [完了（Finish）] をクリックしてサインインを終了するか、必要に応じてリンクをクリックして、追加の MFA オプションとして Google Authenticator を追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	[アカウントのサインアップ（Account Sign Up）] ページを開きます。	
ステップ 2	要求された情報を入力し、エンドユーザーライセンス契約に同意して、[サインアップ（Sign up）] をクリックします。	指定したアドレスにアクティベーション電子メールが送信されます。
ステップ 3	シスコから送信された「アカウントを有効化（Activate Account）」という件名の電子メールから、[アカウントを有効化（Activate Account）] をクリックします。	（注） アクティベーションリンクの有効期限は 7 日です。
ステップ 4	Duo 多要素認証オプション（Touch、Duo Mobile、セキュリティキー、または電話番号）を選択し、検証プロセスを完了します。ヘルプについては、『Duo Guide to MFA and Device Enrollment』を参照してください。	
ステップ 5	必要に応じて追加の認証要素を追加するか、[今はスキップ（Skip for now）] をクリックします。	
ステップ 6	[Duo でログイン（Log in with Duo）] をクリックし、任意の認証オプションを使用してサインインします。	

	コマンドまたはアクション	目的
ステップ 7	[完了（Finish）]をクリックしてサインインを終了するか、必要に応じてリンクをクリックして、追加の MFA オプションとして Google Authenticator を追加します。	



第 4 章

サポート対象製品

サポートされている製品

このガイドでは、Security Cloud Sign On をサポートするシスコのセキュリティ製品をリストしています。一部の製品はデフォルトで Security Cloud Sign On をサポートしており、構成を変更する必要はありません。それ以外のシスコのセキュリティ製品では、Security Cloud Sign On にオプトインするかユーザーを移行する必要があります。

以下にリストされている各製品について、Security Cloud Sign On がデフォルトで有効になっているかオプトインまたはユーザーの移行が必要かを示します。オプトインまたはユーザーの移行が必要な製品については、関連するドキュメントへのリンクを示してあります。

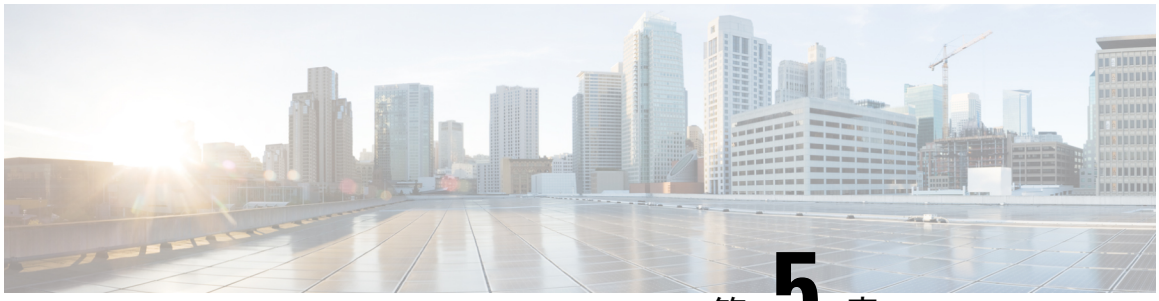
製品	オプトインが必要	資料
Cisco Cloudlock	対応	オプトインガイド
Cisco Defense Orchestrator	対応	オプトインガイド
Cisco Meraki	対応	オプトインガイド
Cisco Secure Access	なし	Secure Access のシングルサインオン認証
Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）	対応	移行ガイド
Cisco Secure Email Threat Defense（旧 Cloud Mailbox）	なし	該当なし
Cisco Secure Endpoint（旧 Advanced Malware Protection for Endpoints）	対応	オプトインガイド

製品	オプトインが必要	資料
Cisco Secure Malware Analytics（旧 Threat Grid）	対応	オプトインガイド（サインインが必要）
Cisco SecureX	なし	該当なし
Cisco Umbrella	対応	オプトインガイド
Cisco XDR	なし	該当なし

サポートされている新興テクノロジーおよびインキュベーションの製品

Security Cloud Sign On をサポートする新興テクノロジーおよびインキュベーションの製品を次に示します。

製品	オプトインが必要	資料
Cisco Panoptica	なし	該当なし



第 5 章

FAQ

FAQ

現在、OneLogin を使用しています。Security Cloud Sign On に移行するには何が必要ですか。

Security Cloud Sign On ページに移動し、[今すぐ登録（Sign up now）] をクリックして自己登録プロセスを開始します。

アカウント有効化メールの有効期間はどのくらいですか。

アカウント有効化メールは、受信してから 7 日間有効です。

アカウントパスワードを変更するにはどうすればよいですか。

（注） 組織の SSO プロバイダーで Security Cloud Sign On にサインインしている場合、以下の方法でパスワードを変更することはできません。SSO プロバイダーでパスワードを変更する必要があります。

Security Cloud Sign On アカウントのパスワードを変更するには、SecureX アプリダッシュボードのトップメニューでプロファイルアイコンをクリックし、[ユーザーアイデンティティ設定（User Identity Settings）] を選択します。[セキュリティ（Security）] セクションで [パスワードの変更（Change Password）] をクリックします。現在のパスワードと新しいパスワードを入力し、[パスワードの変更（Change Password）] をクリックしてから [保存（Save）] をクリックします。

現在、多要素認証に Google Authenticator を使用しています。ID は移行されますか。

いいえ。Google Authenticator の MFA は移行されません。すべての Security Cloud Sign On アカウントで Duo の MFA を使用する必要があります。これにより、ハードウェアおよびソフトウェアソリューションへの通話とテキストメッセージの送信が可能になります。Google Authenticator を引き続き使用する場合は、アカウントのバックアップ要素として追加できます。

FAQ

アカウントの有効化中に、DuoでMFAを設定します（プライマリ）。次に、Google Authenticatorで追加のMFAを設定します（バックアップ）。

（注） Security Cloud Sign Onに独自のIDプロバイダーを統合している組織は、Duo MFAをオプトアウトして独自のMFAソリューションを代わりに使用できます。

組織のDuoポリシーと設定を自分のDuo MFAに使用できますか。

はい。Security Cloud Sign Onに独自のIDプロバイダーを統合している場合、シスコが提供するDuo MFAをオプトアウトして組織のDuoポリシーと設定を代わりに使用できます。

パスワードを忘れた場合はどうすればよいですか。

Security Cloud Sign Onページで、[サインインのお手伝いが必要ですか？（Need help signing in?）] の [パスワードを忘れた場合（Forgot Password?）] をクリックします。パスワードをリセットするには、次の3つのオプションがあります（推奨順に記載）。

- [Duo経由でリセット（Reset via Duo）] をクリックし、IDを確認して認証後、新しいパスワードを入力します。
- アカウント設定に追加した携帯電話番号を入力し、[SMS経由でリセット（Reset via SMS）] をクリックします。SMSメッセージを探し、プロンプトに従います。
- 電子メールまたはユーザ名を入力し、[電子メール経由でリセット（Reset via Email）] をクリックします。電子メールを探し、プロンプトに従います。

これらのオプションを使用できない場合は、サポートされている製品チームにお問い合わせください。

私のパスワードは安全ですか。

はい。お客様の情報を保護するための厳格なセキュリティ対策と制御を行っています。これらの制御は監査され、SOC2レポートで保証されます。

ユーザー名とパスワードはどこにどのように保存されているのですか。

強力な暗号化を使用してデータを保護するのと同様に、ユーザー名とパスワードのクレデンシャルにも強力な（256ビットAES）暗号化を使用しています。

Duoで本人確認を行うために使用していた電話機を紛失した場合はどうすればよいですか。

電話機を紛失しても、ユーザー名とパスワードでサインインできる場合は、Duoの検証ページで [設定（Settings）] をクリックします。[新しいデバイスの追加（Add a new device）] を選択し、プロンプトに従って新しい交換用電話機を登録します。詳細については、『Duo Guide to Adding a New Device』[英語] を参照してください。

パスワードの入力が必要なアプリと必要でないアプリがあるのはなぜですか。

Security Cloud Sign On を使用すると、単一の統合ダッシュボードからアプリケーションにアクセスできます。これらのアプリケーションへのアクセスは、セキュリティ アサーション マークアップ言語（SAML）を使用したシングルサインオン（SSO）テクノロジーによって提供されます。SAML により、Security Cloud Sign On が自動的にトークンを介してアクセスを渡すため、アプリケーションで更新が必要な場合も手動で変更する必要はありません。

既存のアプリケーションのユーザー名とパスワードを変更するにはどうすればよいですか。

既存のパスワードを変更するには、アプリケーションのタイルにマウスポインタを合わせます。タイルの右上隅に歯車のアイコンがあります。歯車アイコンをクリックして設定を開き、現在のユーザー名とパスワードを入力して本人確認を行います。確認後、新しいパスワードを入力できるようになります。

管理者は私のサインイン情報を確認できますか。

管理者はユーザ名を確認することはできますが、パスワードにはアクセスできません。

アカウントがロックアウトされた場合はどうすればよいですか。

アカウントがロックされた場合は、[サインインのお手伝いが必要ですか？（Need help signing in?）] をクリックし、Security Cloud Sign On ページで [アカウントのロック解除（Unlock Account）] を選択します。これらのオプションを使用できない場合は、サポートされている製品チームにお問い合わせください。

セキュリティイメージが表示されないことがあるのはなぜですか。

セキュリティイメージは、サインイン時に設定される Cookie です。ブラウザの Cookie がクリアされている場合は、次にサインインするまでセキュリティイメージが表示されないことがあります。

セッションの期限が切れているのに、一部のアプリケーションがまだ開けるのはなぜですか。

Security Cloud Sign On セッションからログアウトしても、アプリケーションの Security Cloud Sign On からログアウトしたことにはなりません。

SecureX セッショントークンの有効期限はどれくらいで切れますか？

SecureX セッショントークン（JWT）は 24 時間後に期限切れになります。

Security Cloud Sign On がダウンした場合はどうなりますか。

Security Cloud Sign On は、「常時稼働」するアーキテクチャとして構築されています。サービスがダウンした場合、シングルサインオンを使用したサインインやアプリケーションへのアクセスはできなくなります。ただし、一部のアプリには直接リンクからアクセスできる場合があります。Security Cloud Sign On にアクセスできず、サービスの停止が原因であるかどうかを確認するには、サポートされている製品チームにお問い合わせください。

FAQ

既存の Cisco SecureX Sign-on アカウントを削除するにはどうすればよいですか。

製品管理者によってアカウントを削除し、個々の製品アプリケーションへのアクセス権を削除することができますが、サポートされている製品から Cisco TAC に連絡し、Cisco SecureX Sign-on のエンジニアリングチームにアカウントを削除してもらう必要があります。

私の組織では、すでにシングルサインオンに IdP を使用しています。SecureX Sign-on と統合するにはどうすればよいですか。

「独自の IdP を使用」して SecureX Sign-on と統合できる場合があります。これにより、すべてのユーザアカウントを手動で再作成することなくシスコのセキュリティアプリケーションにアクセスできます。詳細については、『Cisco SecureX Sign-On Third-Party IdP Integration Guide』[英語] を参照してください。

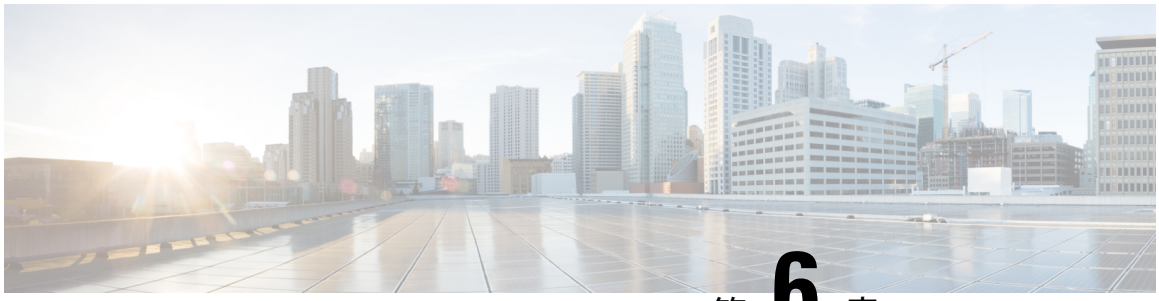
関連リソース

詳細については、次のリソースを参照してください。

- Cisco SecureX Sign-on の製品ページ
- Cisco SecureX Sign-on のプライバシーデータシート
- Cisco SecureX Sign-on のステータスページ

第 I 部

付録



第 6 章

アプリケーションのエクスポート

概要

[アプリケーションのエクスポート（Export Applications）]ページ（SecureXアプリダッシュボードのユーザー プロファイル メニューからアクセス）に、Security Cloud Sign On からアクセスできるシスコのセキュリティ製品アプリケーションがリストされます。各アプリケーションの横には、次を行うためのリンクがあります。

- アプリケーションの名前をクリップボードにコピーする
- アプリケーションの URL をクリップボードにコピーする
- アプリケーションのロゴをコンピュータにダウンロードする

ここから、シスコのセキュリティ製品アプリケーションをシングルサインオン（SSO）アプリケーションポータルにエクスポートできます。これは、共通のシングルサインオンでアクセスできる一連のアプリケーションを表示するランディングページです。一般的なSSOアプリケーションには、Duo Access Gateway、Microsoft Azure、Okta SSO などがあり、いずれも一度サインインすれば、同じユーザ ID とクレデンシャルでアクセスできます。[アプリケーションのエクスポート（Export Applications）]ページのリンクとその情報を使用して、SSOアプリケーションにアプリケーションを追加して設定します。この章では、一般的なプロセスを2つの例を使用して説明します。

Duo Access Gateway へのアプリケーションのエクスポート

次の手順に従って、Duo Access Gateway ランチャーのブックマークをシスコのセキュリティ製品アプリケーションに追加します。

始める前に

- Cisco SecureX Sign-on でアプリケーションにアクセスできる必要があります。
- Duo Access Gateway の管理者権限が必要です。
- Duo Access Gateway ランチャーを設定して有効にします（https://guide.duo.com/dag-launcher）。

ステップ 1 Duo Access Gateway 管理コンソールで、[ランチャー（Launcher）] をクリックします。

ステップ 2 [ブックマーク（Bookmarks）] をクリックします。

ステップ 3 [ブックマークの追加（Add a Bookmark）] をクリックします。

ステップ 4 [名前（Name）] にアプリケーションの名前を入力します（[アプリケーションのエクスポート（Export Applications）] ページからアプリケーションの**名前をコピー**します）。

ステップ 5 [URL] にユーザがアプリケーションにアクセスするために使用する URL を入力します（[アプリケーションのエクスポート（Export Applications）] ページからアプリケーションの **URL をコピー**します）。

ステップ 6 （オプション）アプリケーションの**ロゴ**イメージをアップロードします（[アプリケーションのエクスポート（Export Applications）] ページでアプリケーションの**ロゴをダウンロード**します）。

ステップ 7 デフォルトでは、すべてのユーザに新しいブックマークが表示されます。Duo グループを使用して、ブックマークを表示するユーザを制御できます。[特定のグループのユーザのみアクセスを許可する（Only allow access from users in certain groups）] または [このブックマークを特定のユーザグループにのみ表示する（Show this bookmark to only certain groups of users）] ボックスをオンにし、グループ選択フィールドに入力を開始して Duo グループのリストを取得します。ランチャーで、新しいブックマークを表示するユーザを含む各グループをクリックします。

ステップ 8 [追加（Add）] または [保存（Save）] をクリックします。

Microsoft Azure へのアプリケーションのエクスポート

シスコのセキュリティ製品アプリケーションを Microsoft Azure ポータルに追加するには、次の手順を実行します。

始める前に

- Cisco SecureX Sign-on でアプリケーションにアクセスできる必要があります。
- Microsoft Azure のネットワーク管理者権限が必要です。

ステップ 1 ネットワーク管理者権限で、https://portal.azure.com にサインインします。

ステップ 2 [Azure Active Directory] をクリックします。

ステップ 3 左側のメニューで、[エンタープライズアプリケーション（Enterprise applications）] を選択します。

ステップ 4 [新規アプリケーション（New Application）]→[非ギャラリーアプリケーション（Non-gallery application）]をクリックします。

ステップ 5 [名前（Name）] にアプリケーションの名前を入力します（[アプリケーションのエクスポート（Export Applications）] ページからアプリケーションの**名前をコピー**します）。

ステップ 6 （オプション）アプリケーションのロゴイメージをアップロードします（[アプリケーションのエクスポート（Export Applications）] ページでアプリケーションの**ロゴをダウンロード**します）。

ステップ 7 [シングルサインオンの設定（Set up single sign on）] をクリックします。

ステップ 8 [リンク済み（Linked）] を選択します。

ステップ 9 [サインオンURL（Sign on URL）] を、ユーザがアプリケーションにアクセスするために使用する URL に設定して（[アプリケーションのエクスポート（Export Applications）] ページでアプリケーションの **URL をコピー**）、[保存（Save）] をクリックします。

ステップ 10 アプリケーションの左側にあるメニューで、[ユーザーとグループ（Users and groups）] をクリックします。

ステップ 11 アプリケーションにユーザまたはグループを割り当てます。https://myapplications.microsoft.com にアクセスすると、割り当てられたユーザーにのみアプリケーションが表示されます。

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。