Citrix Secure Internet Access

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

Contents

Citrix Secure Internet Access **2**

リリースノート **4**

新機能 **5**

解決された問題 **8**

既知の問題 **9**

はじめに **9**

ライセンス **27**

ダッシュボード **29**

構成 **32**

管理 **44**

用語集 **51**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Internet Access

February 1, 2022

Citrix Secure Internet Access とは何ですか

Citrix Secure Internet Access（CSIA）は、Web および SaaS アプリケーションへの安全なアクセスをグローバルに提供するクラウド配信サービスです。Secure Web Gateway、Cloud Access Security Broker、サンドボックスによるマルウェア対策、侵入防止および検出システム、データ損失防止など、セキュリティ機能の完全なスタックを提供します。

SD-WAN および Secure Workspace Access に加えて、Citrix Secure Internet Access は、Citrix が提供する完全に統合されたセキュアアクセスサービスエッジ（SASE）ソリューションの柱の 1 つを形成します。

Citrix Secure Internet Access は、ユーザーの場所に関係なく、Citrix Workspace 内外の Web および SaaS アプリへの安全なアクセスを提供します。Citrix Workspace ユーザーの保護を強化し、Citrix SD-WAN と統合して、完全に統合された Citrix ネットワークとセキュリティソリューションを実現します。

Citrix Secure Internet Access 機能とメリット

Citrix Secure Internet Access は、Citrix Cloud を通じて提供されるサービスを統合的に管理するのに役立ちます。次の一覧は、Citrix Secure Internet Access 主な機能と利点をまとめたものです。

- 統合管理。
  - 包括的なセキュリティ機能を包括的に把握し、きめ細かく制御できます。これは、セキュリティインシデント、異常な動作、報告されたリスク、生産性の低下、ポリシー違反を特定するための分析とともに、単一のプラットフォームで提供されます。
  - SD-WAN と Citrix Secure Internet Access 両方の資格を持つユーザーは、同じペインからこれらのサービスを管理できます。その結果、1 つのプラットフォームにネットワークとセキュリティアーキテクチャを組み合わせることで、すべてのトラフィックとユーザーが保護されます。
- 効率性。
  - Citrix SD-WAN と Citrix Secure Internet Access 間の自動構成により、シンプルで迅速な導入。
  - クラウドの速度で拡張できるハイパフォーマンスアーキテクチャ。
  - 最適なパフォーマンスを実現するシングルパスアーキテクチャ: トラフィックは一度復号化され、再暗号化される前にすべてのセキュリティ制御が適用されます。
  - SD-WAN による遅延の短縮：最も近い Citrix Secure Internet Access ゲートウェイノードを自動選択。
- 信頼性の高いパフォーマンス。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - セキュリティ脅威に対する最新の保護のための自動アップデート。
  - 二重の復元力のためにリンクをバックアップします。
  - 一元化されたビューにより、IT 担当者のトラブルシューティングが迅速化されます。

- プライバシー。Citrix Secure Internet Access サービスでは、各顧客のデータは個別のゲートウェイを介して処理され、企業ごとに分離されます。
- リモートワークでのユーザーエクスペリエンスの向上ユーザーがアクセスしたいリソースが既に存在しているクラウドにネットワークセキュリティを移行すると、セキュリティがユーザーに近づきます。Citrix Secure Internet Access サービスには、世界中に 100 を超える PoP（ポイントオブプレゼンス）があります。

主な機能とメリットの詳細については、「ソリューション概要」を参照してください。

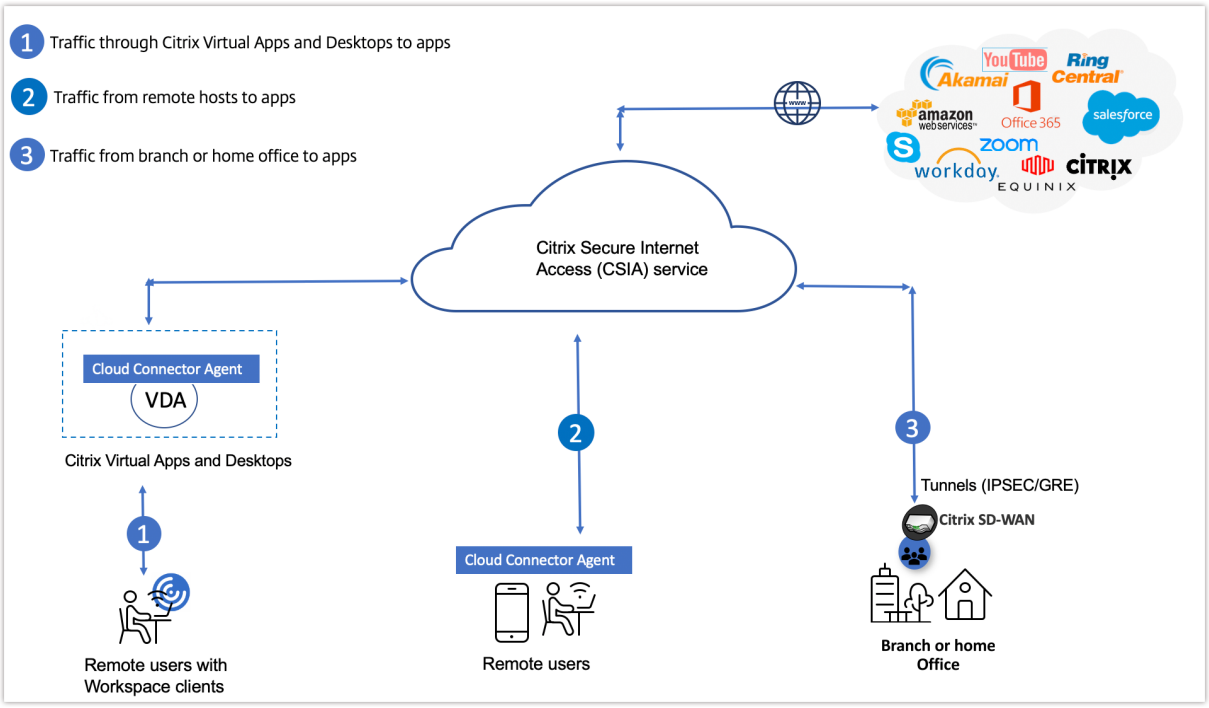
Citrix Secure Internet Access 仕組み

ユーザは、次のいずれかの方法で、認可されていない Web および SaaS アプリケーションにアクセスする可能性があります。

- Citrix Workspace を使用した仮想デスクトップ経由
- ローカルホストシステムからリモートで
- 支店やホームオフィスから

ユーザーが採用する直接インターネットアクセスの方法にかかわらず、トラフィックは Citrix Secure Internet Access 経由でリダイレクトされます。

次の図は、さまざまなユースケースを視覚的に表したものです。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

前の図に示すように、次の 3 つの主要なユースケースは、このプロセスがどのように機能するかを示しています。

1. **Citrix Virtual Apps and Desktops**。Workspace アプリを使用するリモートユーザーは、Citrix Virtual Apps and Desktops を通じて、認可されていない Web および SaaS アプリケーションに安全にアクセスできます。Virtual Delivery Agent（VDA）に CSIA Cloud Connector エージェントをインストールして、インターネットトラフィックを Citrix Secure Internet Access サービスにリダイレクトします。
2. ホストシステム上のネイティブブラウザ。リモートユーザーは、ラップトップやモバイルデバイス (管理対象または管理対象外) などのローカルシステムを使用して、認可されていないアプリに安全にアクセスできます。これらのデバイス上のトラフィックを保護するには、CSIA Cloud Connector エージェントをインストールして、すべてのインターネットトラフィックを Citrix Secure Internet Access サービスにリダイレクトします。

   また、Cloud Connector エージェントはユーザーを認証し、SSL 復号化に適した証明書をインストールします。Cloud Connector エージェントは、iOS、macOS、Android、Windows、Linux のオペレーティングシステムで使用できます。
3. 支店。オンサイトユーザーは、トラフィックを Citrix Secure Internet Access にリダイレクトすることで、Citrix SD-WAN を介して Web および SaaS アプリケーションに安全にアクセスできます。これは、Cloud Connector エージェントを必要とせずに、IPSEC または GRE トンネルを介して行われます。

   Citrix SD-WAN は、最も近い Citrix Secure Internet Access ポイント（PoP）への安全な接続を自動的に作成します。トラフィックは IPsec または GRE トンネルを介してトンネリングされます。冗長性は、トンネルレベルでも、プライマリおよびセカンダリ Citrix Secure Internet Access POP への複数のリンクを介しても実現されます。

次のステップ

- 利用可能なライセンスエディションについて理解する。ライセンシングを参照してください。
- オンボーディングを開始する前に、前提条件を確認してください。「前提条件」を参照してください。
- オンボーディングプロセスを開始します。オンボーディングを見る
- Cloud Connector エージェントを設定します。「構成」を参照

リリースノート

February 1, 2022

Citrix Secure Internet Access サービスのリリースノートでは、サービスリリースの新機能、修正された問題、既知の問題について説明しています。リリースノートには、次のセクションが含まれます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 新機能: このリリースの新機能と拡張機能。
- 修正された問題: リリースで修正された問題。
- 既知の問題: 存在する問題とその回避策 (該当する場合)。

新機能

February 1, 2022

この記事では、Citrix Secure Internet Access（CSIA）2021-Q3 リリースの最新のお客様向け機能の一覧を提供します。

2021 年 **12** 月 **2** 日

SSO に対 **Azure Active Directory** サポート

Azure Active Directory (AD) は、Citrix Secure Internet Access (CSIA) アカウントを使用したシングルサインオン (SSO) 用のアイデンティティプロバイダー (IdP) としてもサポートされています。デフォルトでは、CSIA アカウントは Citrix IdP 設定で構成されます。Citrix テナントで Azure AD が有効になっている場合、CSIA アカウントは SSO 検証用に Azure AD IdP を使用して構成されます。現在、特定の CSIA アカウントは、Azure AD IdP または Citrix IdP のいずれかの設定を持つように構成できます。

Citrix Secure Browser サービスとの統合

Citrix Secure **Browser Service** は、**Web** ブラウジングを隔離して企業ネットワークをブラウザベースの攻撃から保護することにより、リモートブラウザ隔離を提供します。Citrix Secure Internet Access では、Web フィルタリングルールを作成して適用し、Web トラフィックをセキュアブラウザインスタンスにリダイレクトできます。

2021 年 **10** 月 **28** 日

オンボーディング

Citrix Secure Internet Access オンボーディングは、クラウドアクセスを取得して初期セットアップを完了した後、ユーザーアカウントを構成するのに役立ちます。他の CSIA 設定にアクセスするには、いくつかの基本的なオンボーディング設定を行う必要があります。オンボーディングプロセスを完了しないと、構成ポリシーポータルを表示できません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

アカウント設定

アカウント設定機能は、Citrix Secure Internet Access サービスポータルに表示されるアカウント名を変更または上書きするのに役立ちます。

2021 年 10 月 14 日

オフライン・クラウド・バックアップ

Offline Cloud Backup 設定では、選択したリージョン、ロケーション、および時間に基づいて、レポートノードのバックアップ設定とログを保存/保存できます。

Swagger をサポートする Citrix Secure Internet Access API

設定関連 API のセットが swagger ドキュメントで利用可能になりました。CSIA コア Swagger API の情報は、sia-core-controller セクションにあります。

2021 年 9 月 15 日

事前定義された役割

顧客**:** 読み取り専用アクセス **(**プライバシーモード**)** ロールが、新しい定義済みロールとして導入されました。**Citrix ID** およびアクセス管理からユーザーを追加し、この役割を割り当てることができます。**Customer: Read Only Access (**プライバシーモード**)** ロールが割り当てられているユーザーは、****** ライセンスとユーザー設定を除くサービスのすべての機能を表示するための読み取り専用アクセス権を持ちます ******。

メール設定

[構成] **> [**** クラウド設定] の **[**メール設定]****** ページが拡張され、次の機能が追加されました。

- メール設定のテスト: メール設定を確認します。
- 既定の設定を設定: 既定の電子メール設定を入力します。
- **Email Recipients**: ユーザーアラートと URL 例外リクエストを受信するメール受信者を追加します。

2021 年 7 月 29 日

Citrix Secure Internet Access UI のクラウド設定

UI で、NTP サーバ、プラットフォームメンテナンス、アップデートリリース設定、および匿名ロギングの Cloud 設定がサポートされるようになりました。詳細については、「構成」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ECMP トンネル負荷分散

Citrix Secure Internet Access は、SD-WAN Orchestrator サービス ECMP 負荷分散をサポートするようになりました。詳細については、「ECMP 負荷分散」を参照してください。

2021 年 **4** 月 **29** 日

Cloud Connector トラフィックのインターネットブレークアウト

Citrix Secure Internet Access クラウドノードへのトラフィックは、サイトに展開されている IPsec トンネルと GRE トンネルではなく、インターネットサービスを介してリダイレクトされます。この直接ブレークアウトにより、トラフィックを 2 回トンネリングすることを回避できます。

通知

iboss のサブスクリプションと構成の変更に関する重要なメッセージを見逃さないように、Citrix Secure Internet Access サービスはダッシュボードにアラートを通知として表示します。

ユーザー再割り当て

特定のロケーションでのレイテンシーを最小限に抑えるために、地理的リージョン内でノードのロケーションを再構成できるようになりました。また、これらのノードに割り当てられているユーザー数を編集することもできます。

IPsec および **GRE** トンネルによるマルチリンクのサポート

複数の ISP 接続を持つ 1 つの場所から同じ Service Provider Point of Presence（POP; サービスプロバイダー Point of Presence）へのトンネルを設定することにより、ネットワークトラフィックを複数のトンネルで並行して配信します。

ノード下の **POP** のネットワークマップ

Citrix Secure Internet Access POP に接続する顧客および SD-WAN ブランチでどの POP（ポイントオブプレゼンス）が使用されているかを表示します。

ロール設定 **(**テクニカルプレビュー**)**

Citrix はロールベースのアクセス制御（RBAC）を提供しています。RBAC では、権限ベースのロールをカスタマイズしたり、これらのロールをさまざまなユーザーに追加したりすることができます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

解決された問題

February 1, 2022

以下の不具合が修正されました。

2021 年 10 月 28 日

SIAS-27: コンテンツ分析検索パターンを使用するときに、情報漏えい防止 (DLP) グラフに名前のラベルが付けられるようになりました。

SIAS-290: クラウドステータスレポートの詳細セクションが切り捨てられなくなりました。

SIAS-394: アドバイザリとインシデントのアラートには、影響を受けるデータセンター情報が含まれる。

SIAS-451: カスタム Cloud Access Security Broker（CASB）アプリケーションコントロールがユーザーインターフェイスでレンダリングされるようになりました。

2021 年 9 月 15 日

SIAS-218: 中東地域のトライアル SKU のプロビジョニングが正常に完了していない。

SIAS-302: レポートを有効にしてアラート電子メール通知を送信するには、電子メール設定の変更が必要でした。この問題は、[構成**] > [**電子メール設定**]** フィールドにデフォルト値を入力することで修正されました。

SIAS-306: ページを表示するアクセス権を持たない管理者には、[構成**] > [**ユーザー設定**]** ページが (非表示ではなく) 表示される。アクセスしようとすると、エラーが表示される。

SIAS-307: 読み取り専用権限を持つユーザーロールを持つと、あるテナントのデータをキャッシュし、別のテナントのデータとして表示できる。

SIAS-329: クラウドステータスの電子メールアラートと通知の形式が変更され、メンテナンス、インシデント、アドバイザリメッセージの次のステータスが含まれるようになりました。

- 変更後
- 更新
- 再スケジュール済み
- 完全
- キャンセル済み

SIAS-395: URL 再分類の通知が拡張され、要求された URL のステータス、古いカテゴリ、および新しいカテゴリが含まれるようになりました。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2021 年 7 月 29 日

SIAS-1: ユーザーが write.com アプリのブロックページを受け取る

SIAS-161: Win7 32 ビットクライアントが接続しない。

SDW-18408: Citrix Secure Internet Access と SD-WAN の両方に対して同じ権限を持つユーザーが、[役割の設定の変更] に重複して表示される。

NSSDW-32478: SIA + SD-WAN カスタマーの特定のユーザーについて、カスタマースコープのユーザーロールが重複して表示される

2021 年 4 月 29 日

NSSDW-33107: Citrix SD-WAN からの GRE トンネル接続はサポートされていません。

NSSDW-33099: Android コネクタのフレームブレークアウト。

NSSDW-33530: ゲートウェイ/レポートサーバー間で Postgres クエリが暗号化されない。

NSSDW-34575: プロキシとキャッシュが読み込まれない。

既知の問題

February 1, 2022

Citrix Secure Internet Access サービスには、次の既知の問題があります。

SIAS-13: Ultrasurf ブロッキングでは、回避プロトコル設定以外にも追加の設定が必要です。

SIAS-22: 構成ポリシーポータルで、一部の設定が Citrix Secure Internet Access の展開に適用されない場合があります。

はじめに

February 1, 2022

この記事では、Citrix Secure Internet Access（CSIA）を初めて使用する方法について説明します。

初期セットアップを開始する前に、[ライセンスと前提条件に関する情報を確認してください](/ja-jp/citrix-secure-internet-access/get-started.html#pre-requisites) 。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

前提条件

次のものがあることを確認します。

- **Citrix Cloud** アカウント。Citrix Secure Internet Access を使用するには、Citrix Cloud アカウントが必要です。https://citrix.cloud.com に移動し、既存の Citrix Cloud アカウントでサインインできることを確認します。

  Citrix Cloud アカウントをお持ちでない場合は、まず Citrix Cloud アカウントを作成します。また、組織内の他のユーザーが作成した既存のアカウントに参加することもできます。詳細なプロセスと手順については、「Citrix Cloud へのサインアップ」を参照してください。
- **Citrix Workspace** からアクセスできる **Citrix Virtual Apps and Desktops** の展開環境。
- ラップトップやモバイルデバイスなどのホストシステム上の **Workspace** アプリ。
- **SD-WAN** の展開。ブランチオフィスで作業している場合は、次の展開が必要です。
  - Citrix SD-WAN 11.1 およびそれ以降
  - Citrix SD-WAN Orchestrator サービスへのサブスクリプション。SD-WAN Orchestrator でサイトの初期設定と構成が完了していることを確認します。

初期設定

このセクションでは、Citrix Secure Internet Access の初期セットアップに必要なタスクについて説明します。

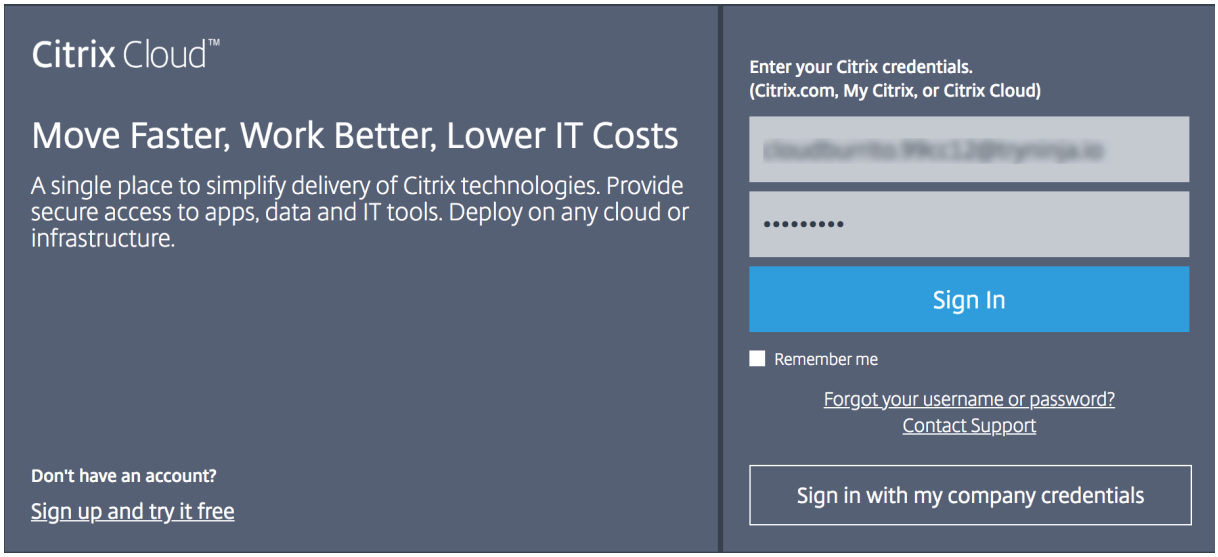
手順 **1**：**Citrix Secure Internet Access** へのアクセスを要求する

Citrix セキュアインターネットアクセスの試用版をリクエストすると、Citrix Secure Internet Access にアクセスできます。試用版は最長で 60 日間使用できます。サービストライアルの詳細については、「Citrix Cloud サービストライアル」を参照してください。

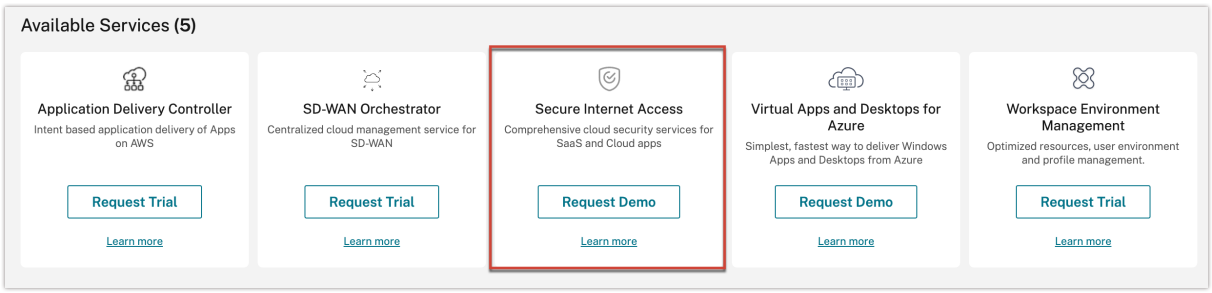
トライアルをリクエストするには、

Citrix Cloud アカウントにサインインします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



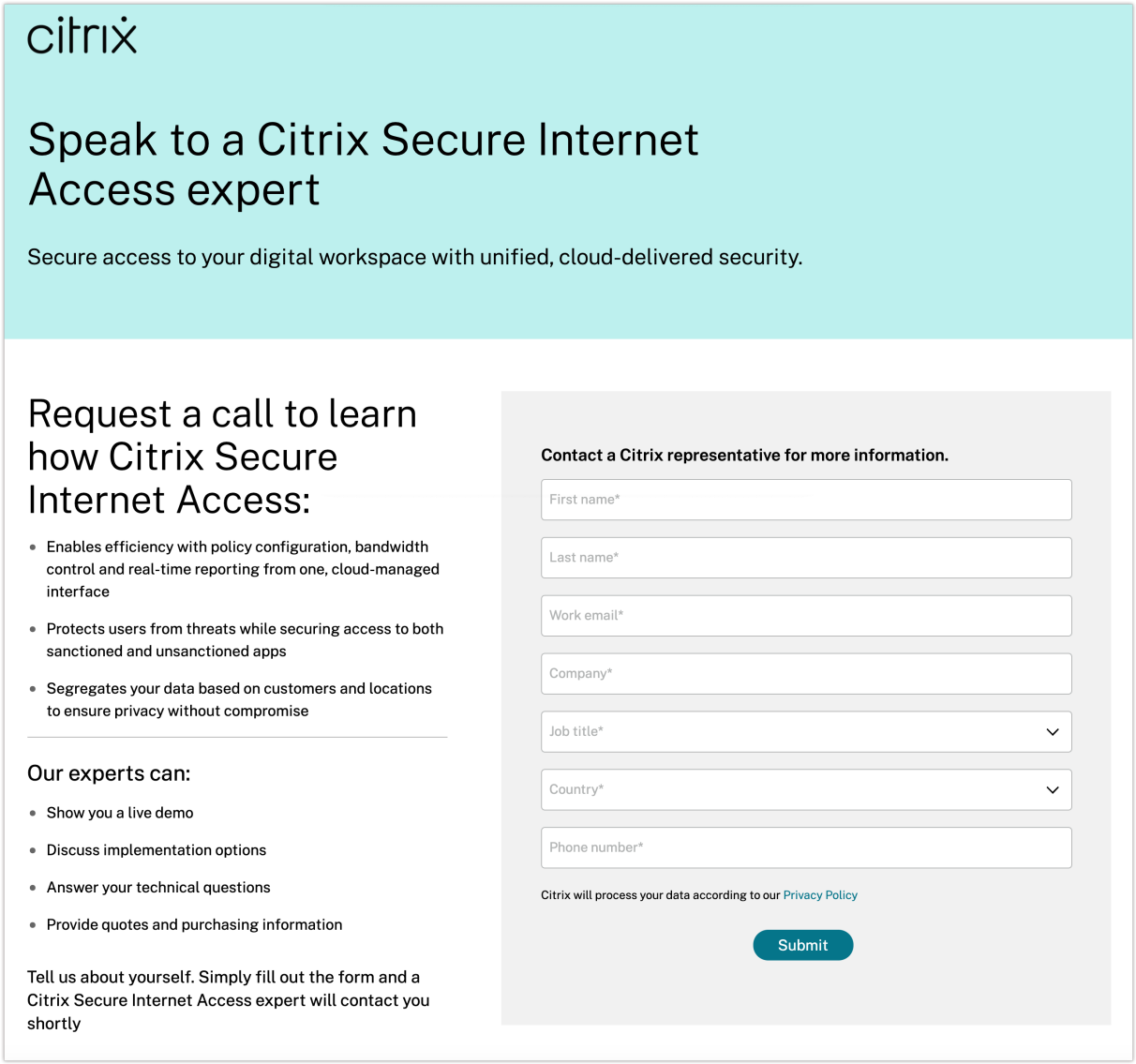
Citrix Cloud ホームページの［利用可能なサービス］の［セキュリティで保護されたインターネットアクセス］タイルで、［デモをリクエスト］をクリックします。



> 注
>
> また、https://www.citrix.com/products/citrix-secure-internet-access/form/inquiry/ にアクセスして、Citrix エキスパートに連絡することもできます。

必要な詳細を入力し、[**Submit**] を選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



トライアルが承認されると、Citrix はトライアルプロセスを開始し、選択したライセンスパッケージに基づいてカスタマーエンタイトルメントパッケージを作成します。また、確認メールが届きます。

ステップ **2:** アカウントのステータスを表示する

トライアルが承認され開始されると、確認メールが届きます。また、Citrix Cloud でアカウントのステータスを確認することもできます。

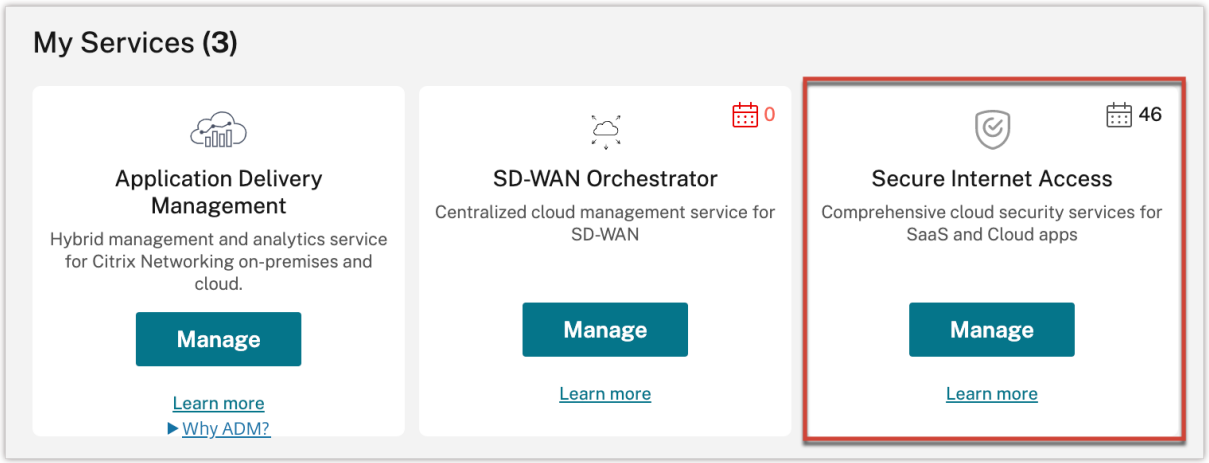
アカウントを設定するには、Citrix がゲートウェイノードを暗黙的にプロビジョニングします。これらのノードは、クラウド内のデータとトラフィックをスキャンするコンテナ化されたノードです。このノードは、Web フィルタリング、マルウェア対策、データ損失防止などのセキュリティ機能も実行します。

ノードが設定されると、アカウントが使用可能になったことを知らせる電子メール通知が届きます。ノードのプロビジョニングには数日かかる場合があります。

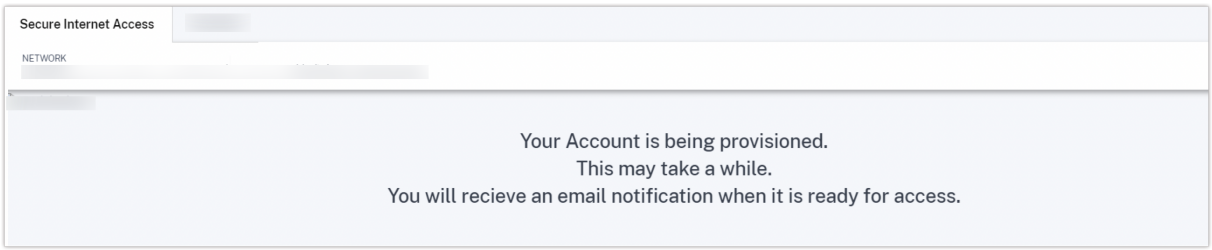
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

アカウントのステータスを表示するには

1. Citrix Cloud アカウントにサインインします。
2. **Citrix Cloud** ホームページの［マイサービス］の［セキュリティで保護されたインターネットアクセス］タイルで、［管理］をクリックします。



アカウントのプロビジョニングが進行中の場合は、次のメッセージが表示されます。



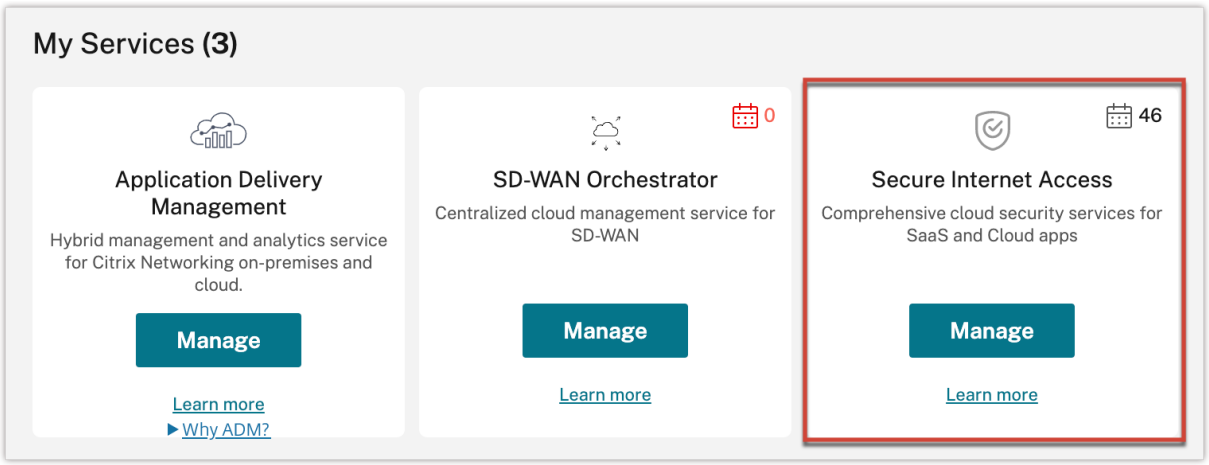
手順 **3**：**Citrix Secure Internet Access** 管理する

アカウント設定に関する確認メールを受け取ったら、Citrix Cloud にサインインして、展開の構成と管理を開始します。

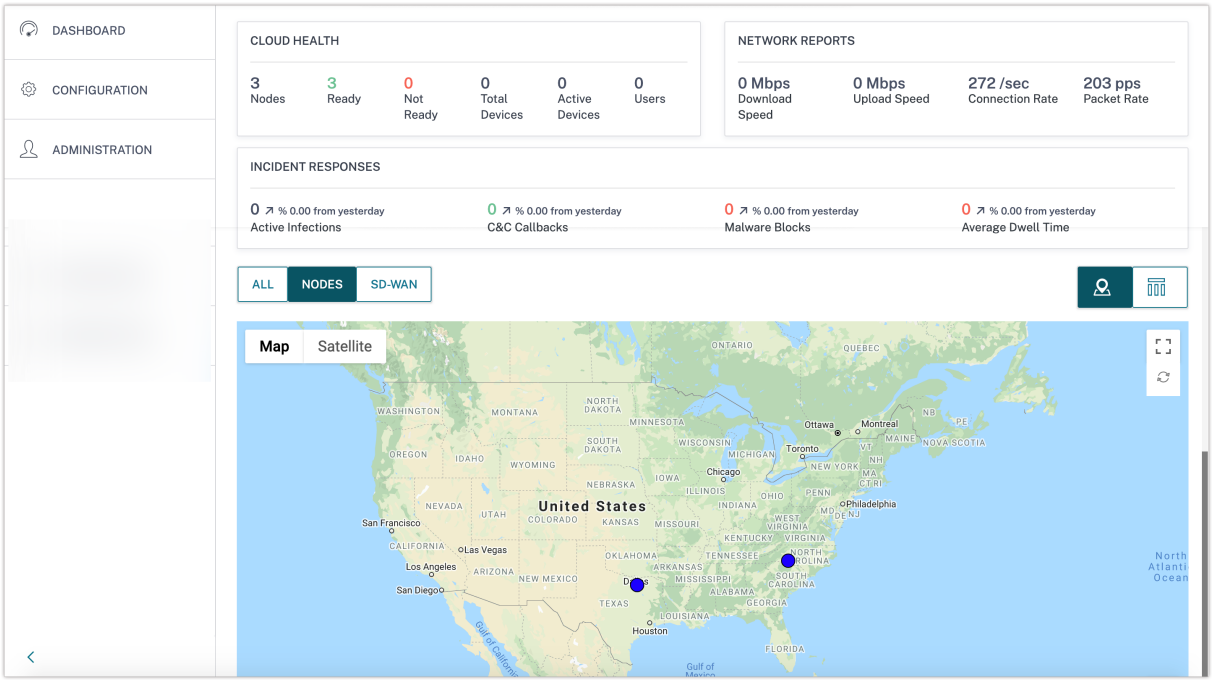
Citrix Cloud ホームページの［マイサービス］の［セキュリティで保護されたインターネットアクセス］タイルで、［管理］をクリックします。

> 注
>
> Citrix SD-WAN Orchestrator サブスクリプションをお持ちの場合は、［**SD-WAN Orchestrator**］タイルの［管理］をクリックして［**Citrix Secure** Internet Access］ダッシュボードを表示することもできます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



「ダッシュボード」**(Dashboard**) メニューでは、ノードのステータスとグラフィカルな表現を表示できます。



これで初期設定は完了です。

オンボード

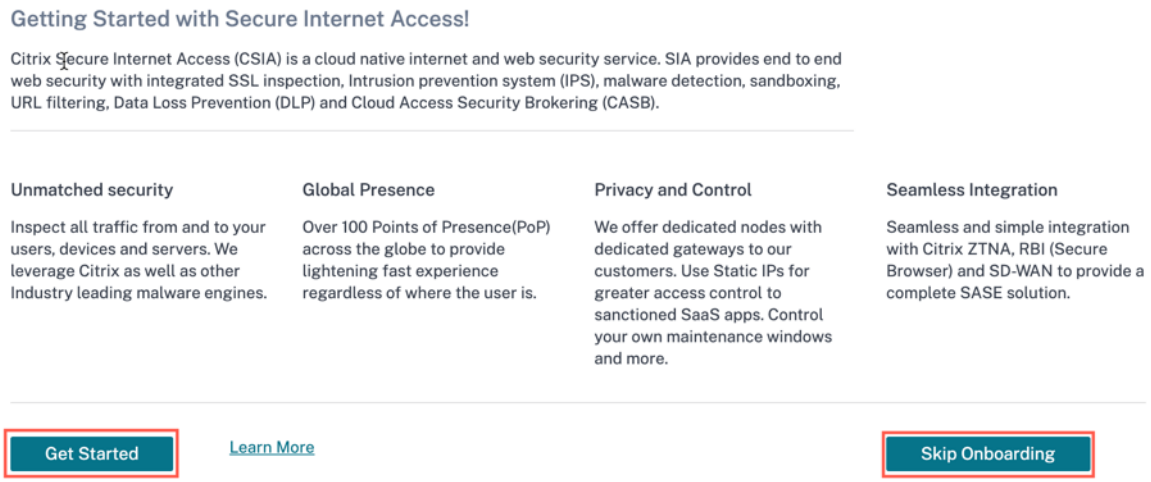
Citrix Secure Internet Access オンボーディングでは、アカウントのプロビジョニング後にユーザーアカウントを構成できます。他の CSIA 設定にアクセスするには、いくつかの基本的なオンボーディング設定を行う必要があります。

Citrix SIA 構成を開く］オプションは、［ネットワーク構成］ホームページにあります。オンボーディングプロセスを完了しないと、構成ポリシーポータルを表示できません。

アカウントがプロビジョニングされると、デフォルトで［Citrix Secure Internet Access オンボーディング］ペー

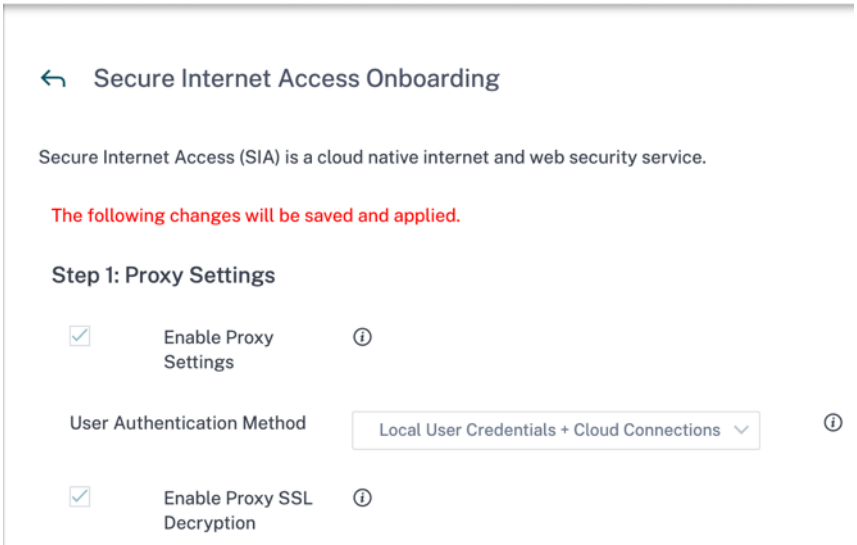
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ジが表示されます。[**Get Started**] をクリックしてオンボーディングプロセスを続行するか、[**Skip Onboarding**] をクリックしてこのステップをスキップし、後でオンボーディングを実行します。［オンボーディングをスキップ］をクリックすると、［Citrix Secure Internet Access］ダッシュボードページが表示されます。



1. プロキシ設定を構成する

   ドロップダウンリストからユーザー認証方法を選択します。デフォルト値は [ローカルユーザー資格情報 **+** クラウド接続] に設定されています。



   次の 4 つの認証方式があります。

   - ローカルユーザー資格情報 **+** クラウド接続: ローカルの安全なインターネットアクセスアカウントでログインします。この方法では、リクエストにプロキシ認証を注入することで、セキュアなインターネットアクセスエージェント/エンドポイントがゲートウェイに自動的に登録されるエージェントモードもサポートされます。
   - ローカルユーザー資格情報: ローカルの安全なインターネットアクセスアカウントでログインします。

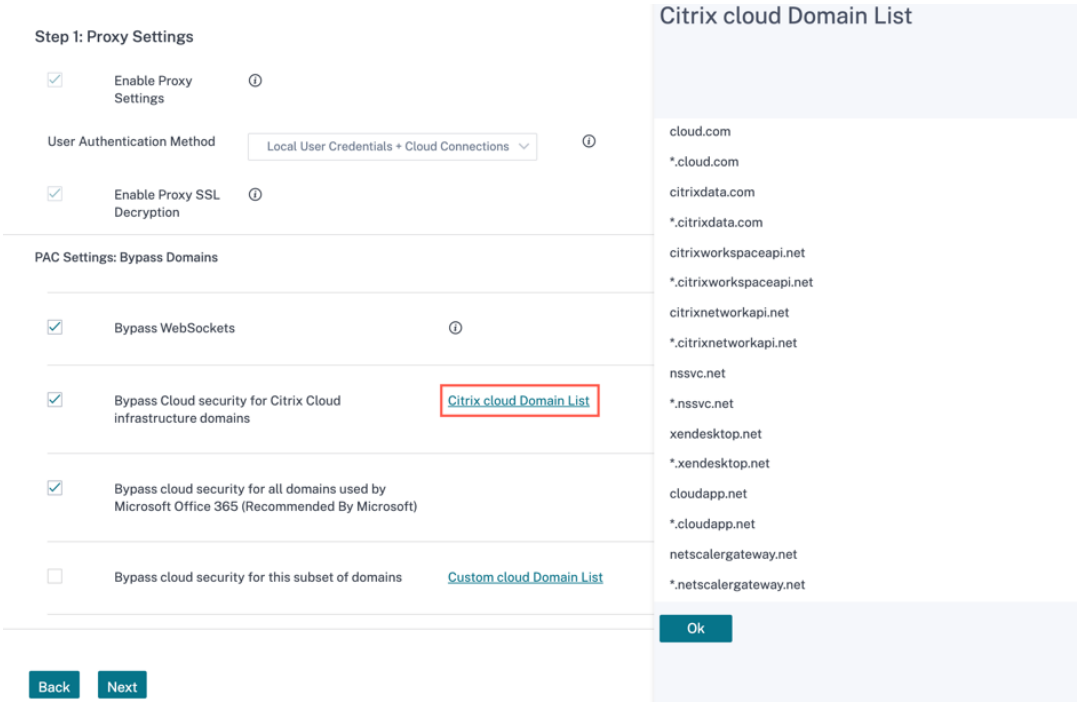
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Cloud Connector Only**: エージェントモードを使用します。エージェントモードを使用すると、リクエストにプロキシ認証を注入することで、セキュアなインターネットアクセスエージェント/エンドポイントがゲートウェイに自動的に登録されます。
- ブラウザベースの **SMAL**: ブラウザでの認証で、同じパブリック IP をソースとするブランチオフィスユーザに最適です。

[プロキシ設定を有効にする**]** と **[**プロキシ **SSL** 復号化を有効にする] の設定はデフォルトで有効になっており、編集不可のチェックボックスです

プロキシ自動構成設定の [**PAC** 設定**:** ドメインのバイパス] セクションで、必要に応じて次のチェックボックスをオンにします。

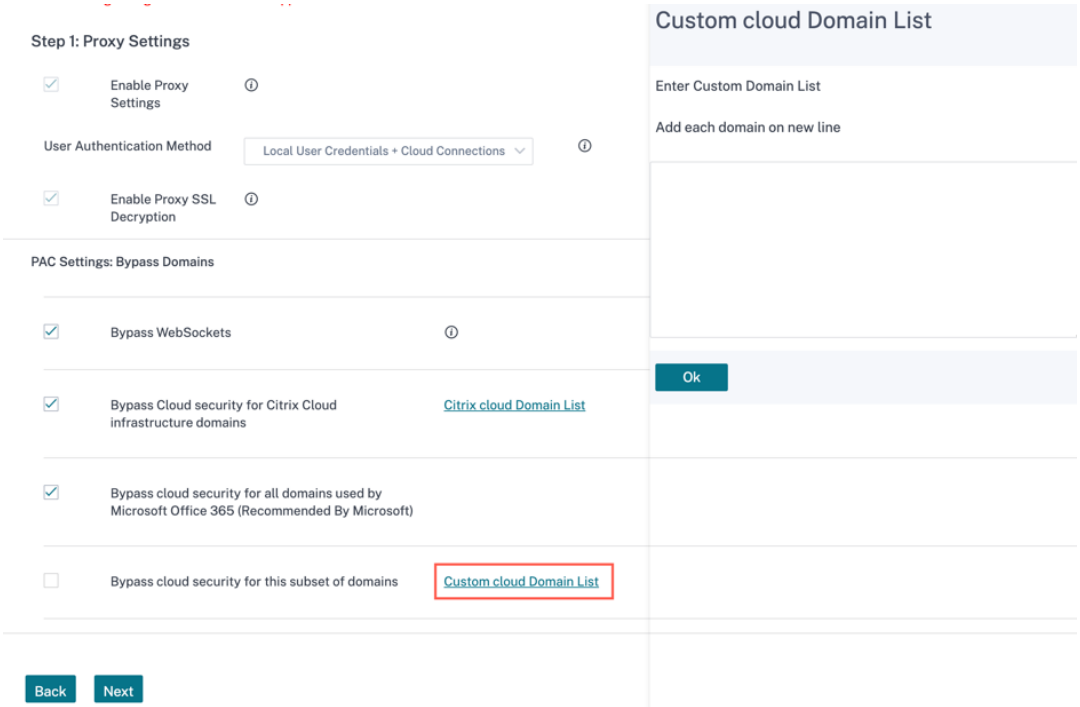
- **WebSockets** のバイパス: セキュアソケットレイヤー (SSL) /トランスポート層セキュリティ (TLS) 経由で WebSocket トラフィックと WebSocket トラフィックのドメインをバイパスします。[**WebSockets** をバイパスする] チェックボックスはデフォルトで有効になっています。
- **Citrix Cloud** インフラストラクチャドメインのクラウドセキュリティをバイパスする: Citrix サイトのリクエストをバイパスします。このオプションは、デフォルトで有効になっています。**Citrix Cloud** ドメインリストは、検査からバイパスする必要がある Citrix Cloud インフラストラクチャドメインの編集不可能なリストです。



- **Microsoft Office 365** で使用されるすべてのドメインでクラウドセキュリティをバイパスする **(Microsoft** が推奨**)**: Microsoft Office 365 で使用されているドメインをバイパスします。[**Microsoft Office 365** で使用されるすべてのドメインでクラウドセキュリティを使用しない **(Microsoft** 推奨**)**] チェックボックスは、既定で有効になっています。

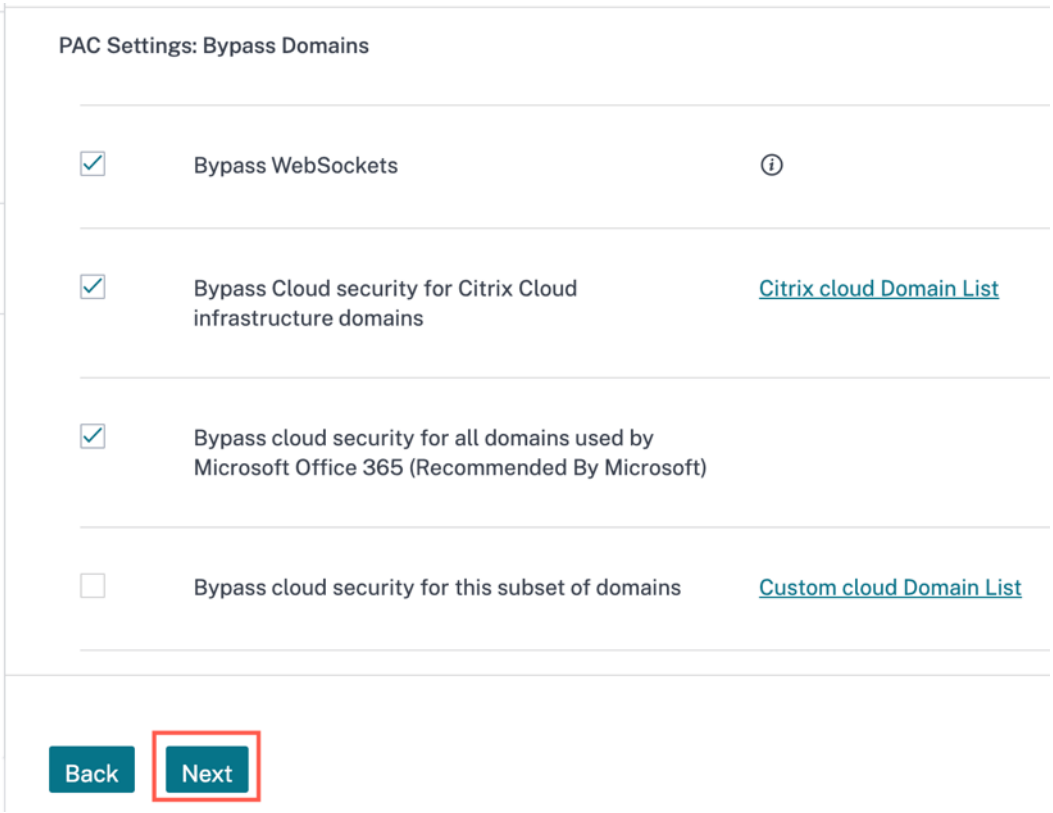
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- このドメインのサブセットに対してクラウドセキュリティをバイパスする: カスタムドメインをすべてバイパスします。[**Custom Cloud Domain List**] オプションを使用して、独自のドメインを作成できます。



［次へ］をクリックします。

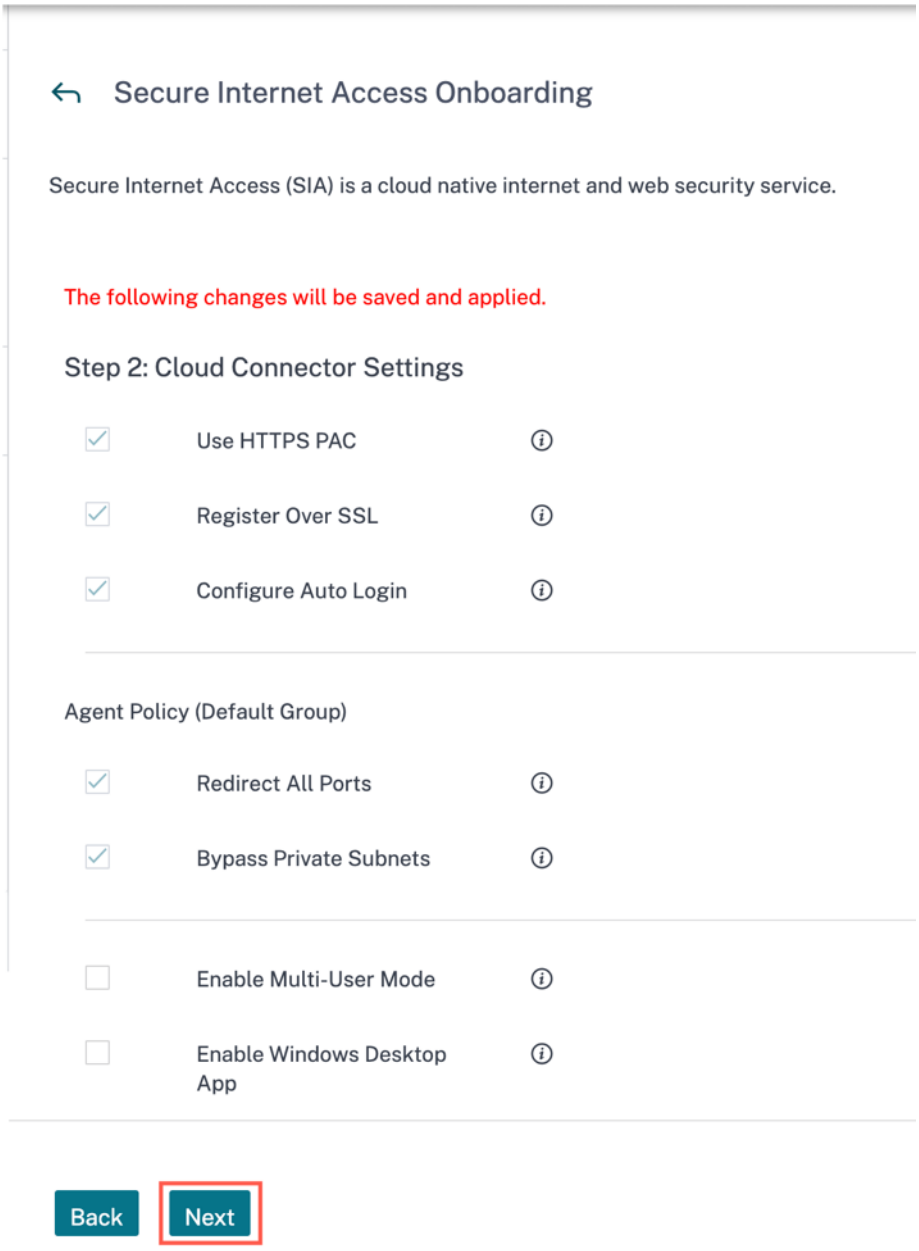
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Cloud Connector の設定を構成する

   Cloud Connector は、Windows、Linux、macOS などのさまざまな OS で利用できるダウンロード可能なエージェントです。これらの設定により、デバイスにインストールされている Cloud Connector の動作が構成されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



[**HTTPS PAC** の使用]、**[SSL** 経由の登録**]**、**[**自動ログインの構成**]**、**[**すべてのポートのリダイレクト]、[プライベートサブネットのバイパス] の設定はデフォルトで有効になっており、

- マルチユーザーモードを有効にする: 必要に応じて [マルチユーザーモードを有効にする**]** をオンまたはオフにします。[マルチユーザーモードを有効にする] を選択すると、仮想デスクトップまたはターミナルサーバーを実行しているときに複数のユーザーセッションをサポートできます。
- **Windows** デスクトップアプリを有効にする: 必要に応じて [**Windows** デスクトップアプリを有効にする**]** をオンまたはオフにします。**[Windows** デスクトップアプリケーションを有効にする**]** を選択すると、対話型デスクトップアプリケーションが Windows デバイスにインストールされます。

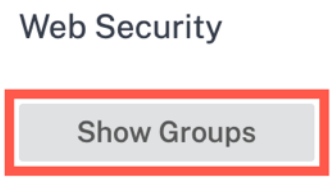
［次へ］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

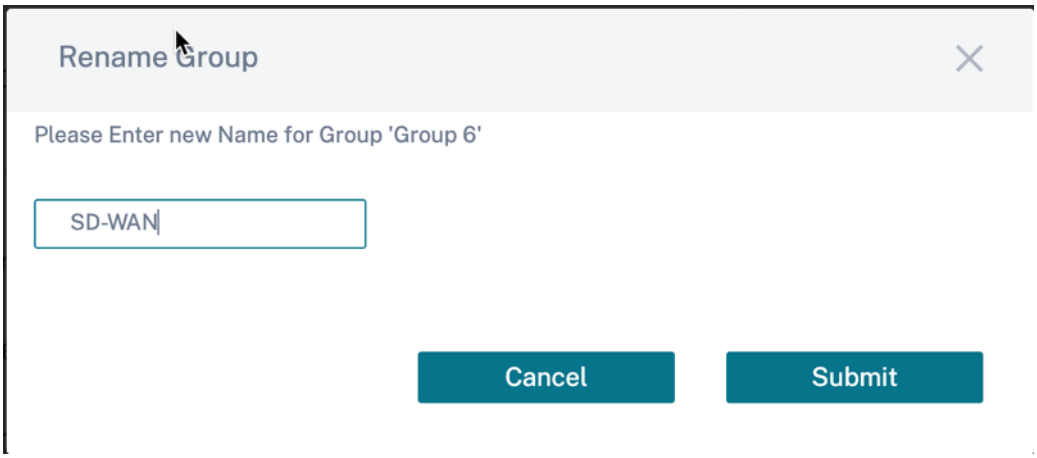
3. セキュリティ設定を構成する

   [セキュリティの設定] ページで、[Web セキュリティ]、[クラウドアクセスセキュリティブローカ]、[マルウェア防御と侵入防御] の設定 (Advanced SKU および Premium SKU で利用可能)、および情報漏えい対策 (プレミアム SKU で利用可能) を設定します

   - **Web** セキュリティ
     - グループを表示: 最初の 20 個のグループリストを表示します。

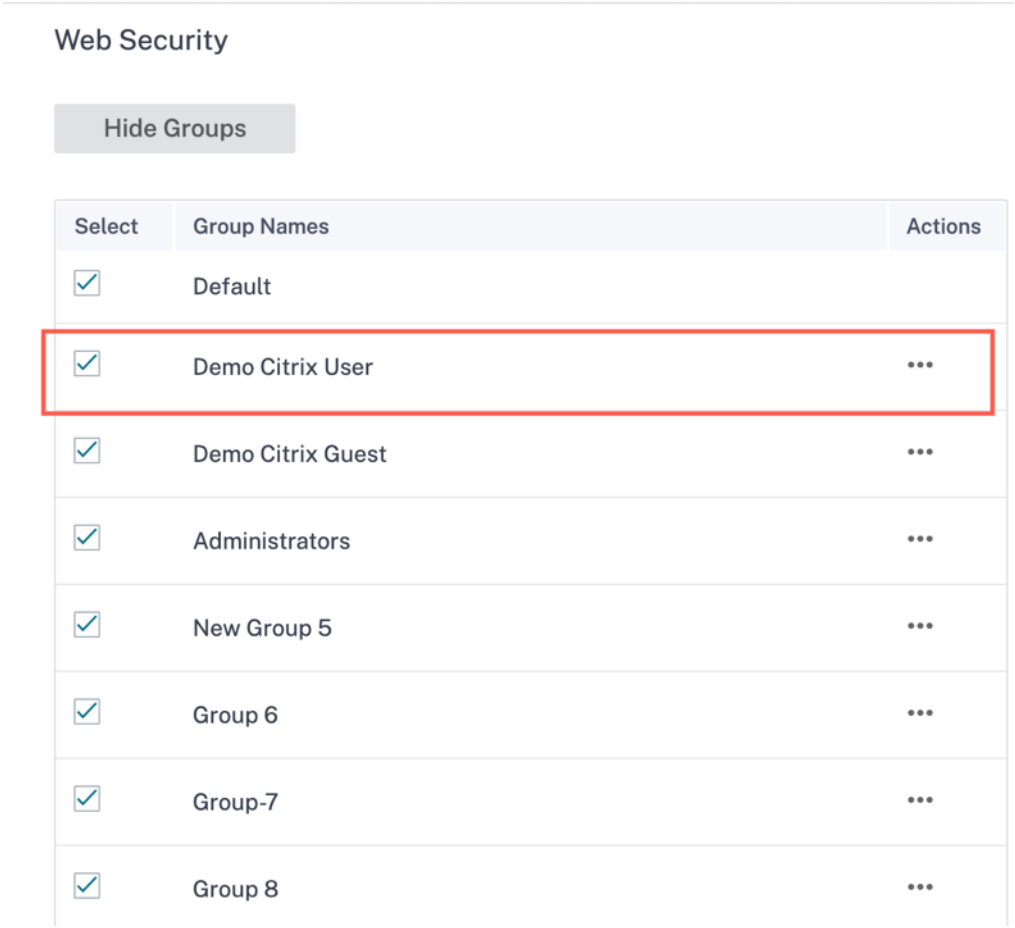


   部署、ドメイン、製品など、グループの名前を編集できます。グループ名の横にある編集オプションをクリックし、グループ名を入力し、[**Submit**] をクリックします。



   グループを選択すると、定義済みのグループポリシーがユーザーに適用されます。[既定] (**Default**) グループは編集不可能なグループです。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



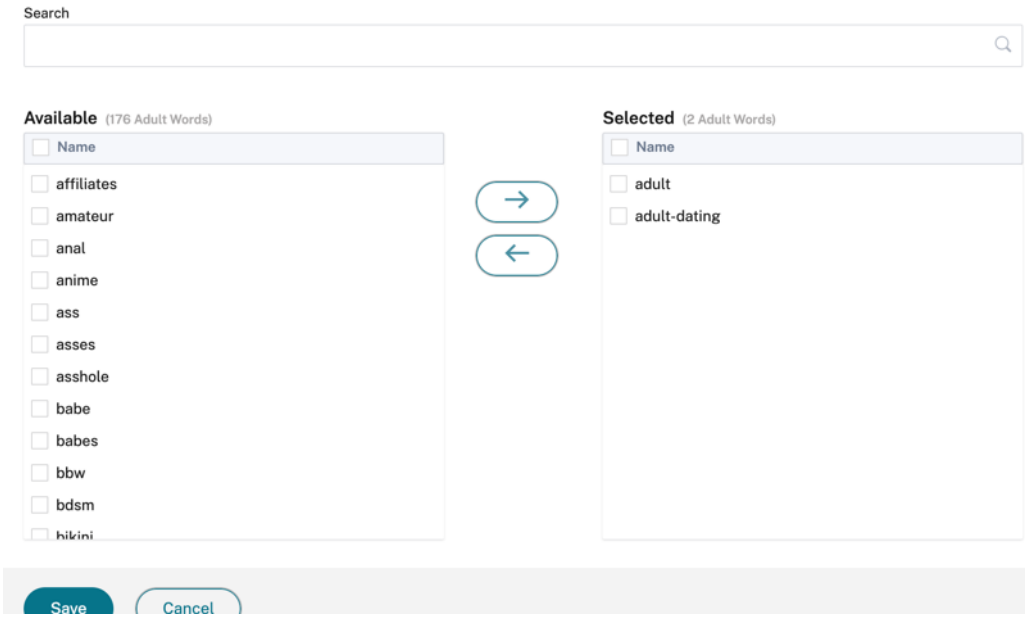
これら 20 個のグループはすべてデフォルトでオンになっています。必要に応じて、グループのオン/オフを切り替えることができます。セキュリティ設定に加えた変更は、選択したグループに適用されます。

- 既定のキーワードをブロックする: 定義したキーワードをブロックするには、[成人] と [高リスク] チェックボックスをオンにします。[**Edit]** オプションを使用すると、ブロックするキーワードのセットを設定できます。

  [編集] **[** 成人用語の選択]/[危険度の高い単語の選択] の順にクリックし、使用可能なキーワードを選択して選択したセクションに移動し、[保存] をクリックします。

  検索バーを使用すると、探しているキーワードをすばやく見つけることができます。

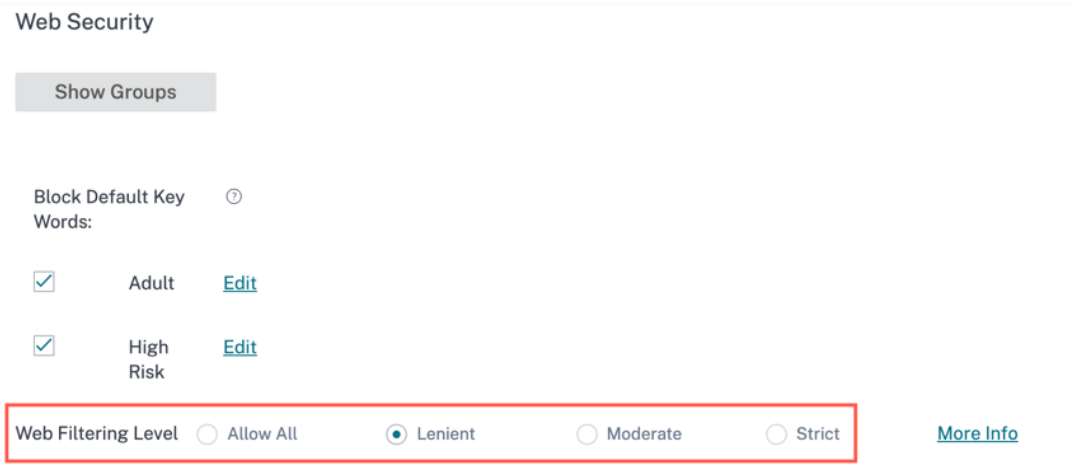
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Web** フィルタリングレベル:[**Web** フィルタリングレベル] で、[すべて許可]、**[**寛大**]**、**[**中**]**、または [厳格] プロファイルを選択しますこれらのフィルタリングレベルは、以下の表に示すように事前設定されたカテゴリに基づいて定義されます。

カテゴリ	寛大な	中	厳格
アダルト	禁止	禁止	禁止
コンピューターおよびインターネット	一部ブロックされた	一部ブロックされた	禁止
ギャンブル	禁止	禁止	禁止
違法で有害なコンテンツ	禁止	禁止	禁止
マルウェアとスパム	禁止	禁止	禁止
ビジネスと産業、金融	許可	禁止	禁止
メール、メッセージング、チャット、テレフォニー	許可	禁止	禁止
ニュース、エンターテインメント、社会	許可	一部ブロックされた	禁止
ソーシャルネットワーク	許可	禁止	禁止

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

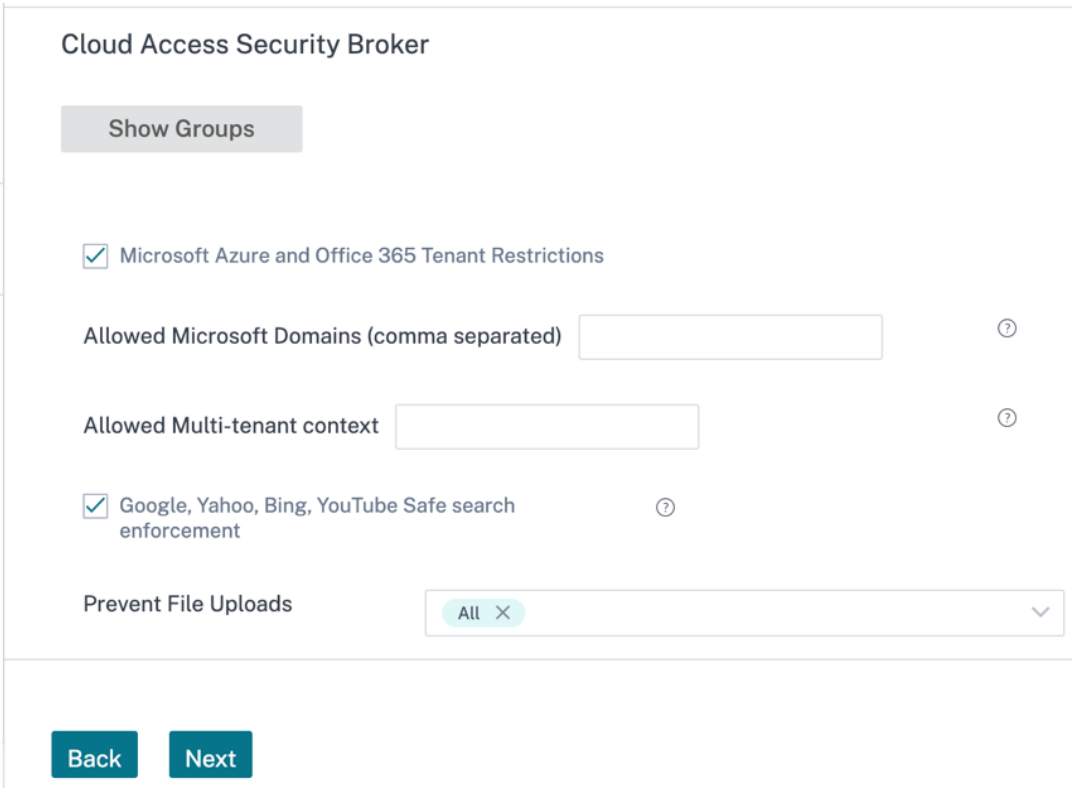


[**More Info**] リンクをクリックして、Web フィルタリングレベルの情報を表示します。

- クラウドアクセスセキュリティブローカー：さまざまなサービスへのファイルアップロードをブロックしたり、Google/Yahoo/Bing などのさまざまな検索エンジンで安全な検索を強制したりする機能を提供します。

  Microsoft Azure および **Office 365** テナント制限] チェックボックスがオンになっている場合は、セキュリティ設定を適用する許可されたドメイン名とマルチテナントコンテキストを指定します。

  ファイルのアップロードを禁止するドロップダウンリストから場所(すべて**/Dropbox/box/OneDrive/Google** ドライブ**/**汎用ファイルアップロード**/**なし）を選択し、ファイルのアップロードを禁止します。既定では、[すべて] が選択されています。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Internet Access では、スタンダード、アドバンスト、プレミアムの 3 種類の SKU を利用できます。

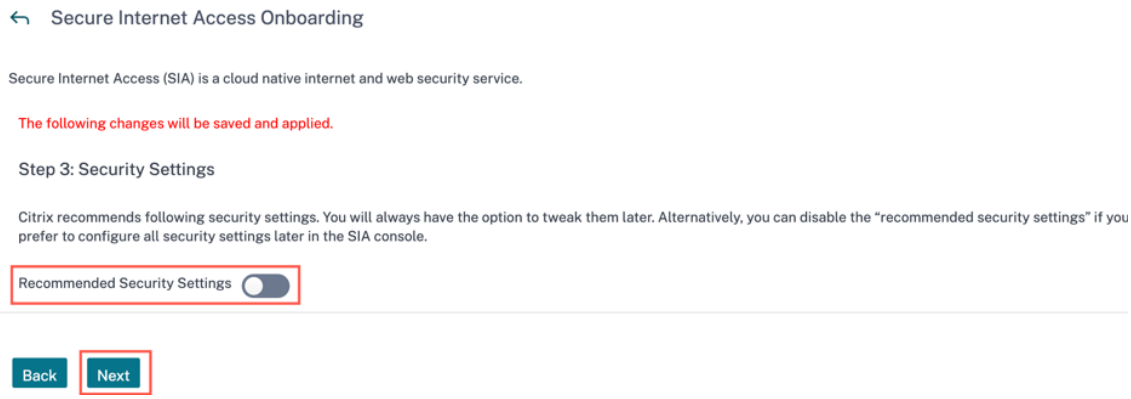
Citrix Secure Internet Access GUI で以下を実行します。

- マルウェア防御と侵入防御の設定オプションは、Advanced SKU と Premium SKU をお持ちのお客様のみが使用できます。
- 情報漏えい対策 **(DLP)** オプションは、Premium SKU をお持ちのお客様のみご利用いただけます。

標準プランでは、Citrix Secure Internet Access UI で［マルウェア防御と侵入防止］設定と［データ損失防止（**DLP**）］オプションを使用できません。

デフォルトでは、[マルウェア防御] と **[**侵入防御**]** の設定と **[**情報漏えい対策**] (DLP)** の両方について、すべてのオプションが事前にチェックされています。必要に応じて、設定をリセットしたり、オプションを選択したりできます。［次へ］をクリックします。

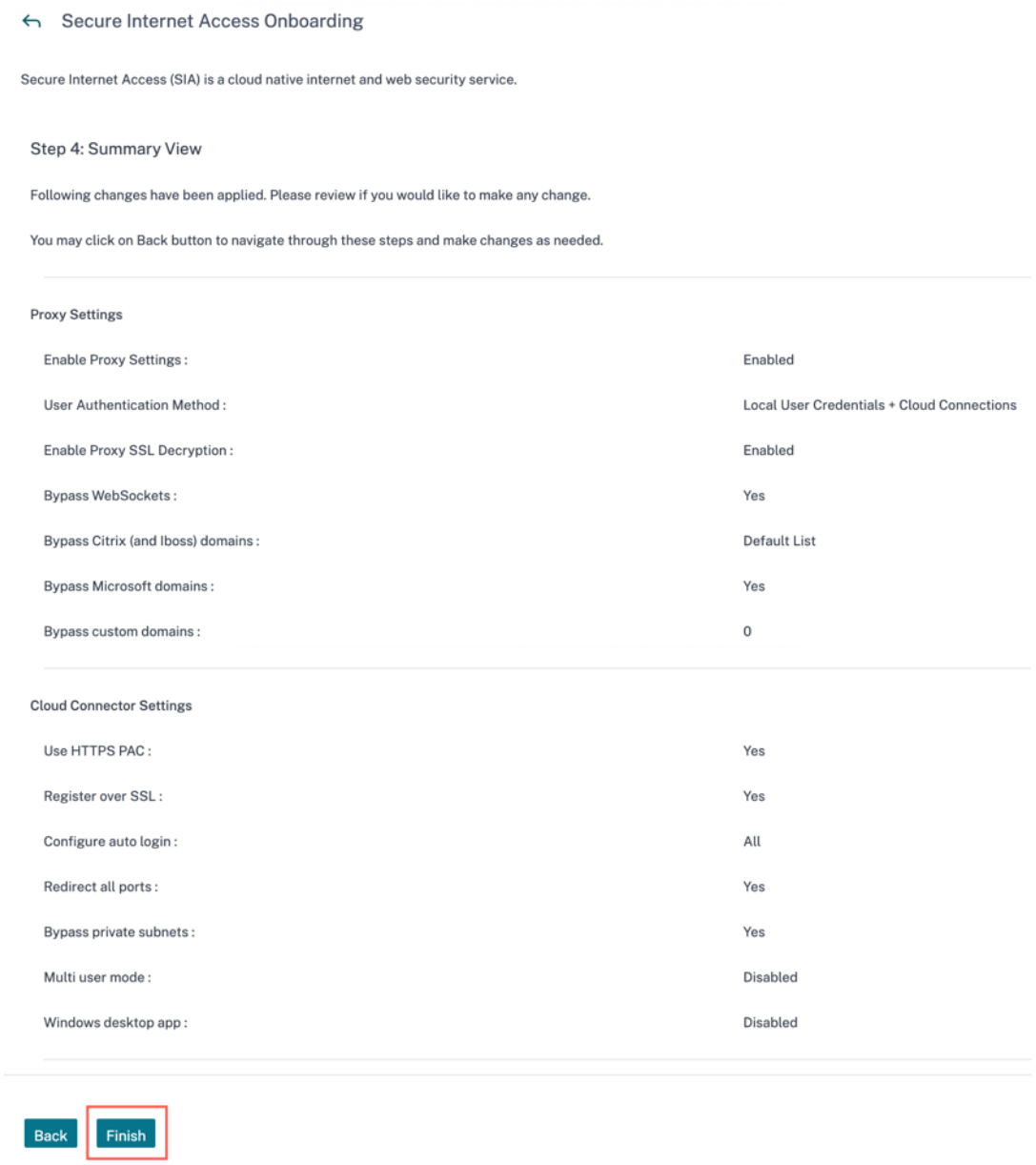
または、**[**セキュリティ設定**]** の設定をスキップする場合は、[推奨されるセキュリティ設定**]** ボタンを無効にできます。設定は後で CSIA コンソールで設定できます。



このシナリオでは、[次へ] をクリックして行った設定を確認し、[完了] をクリックして変更を保存します。

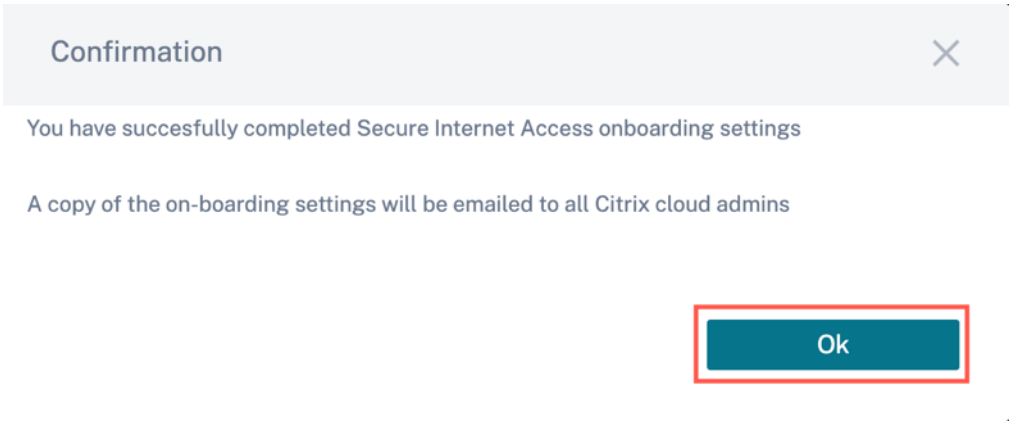
4. オンボーディングプロセスを完了するために設定したすべての設定を含むサマリページを表示できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



[**Finish**] をクリックすると、オンボーディング設定が正常に完了したことを確認するポップアップが表示されます。[**OK**] をクリックします。

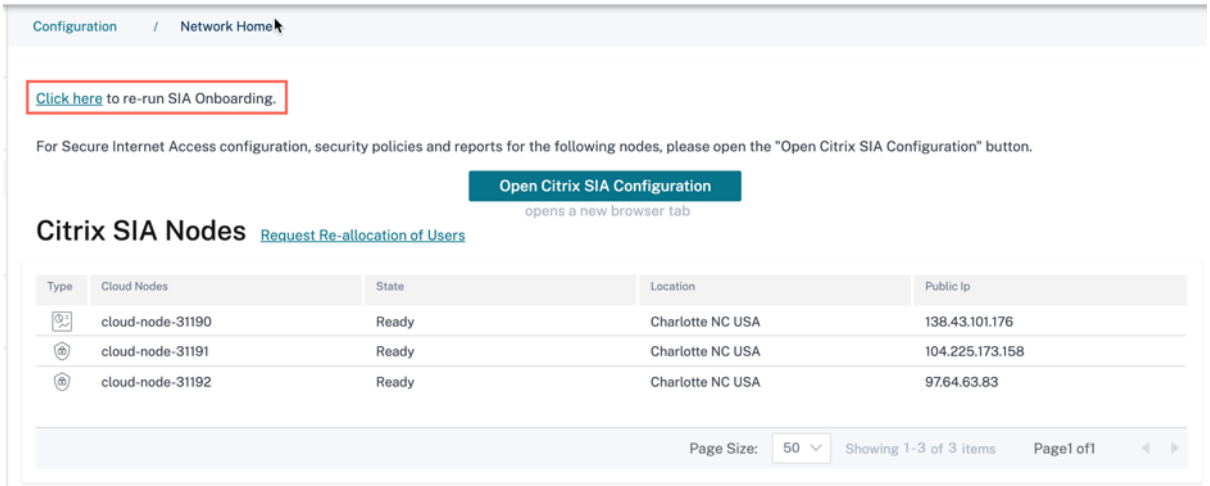
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



また、Citrix Internet Secure Access サービスのこの顧客アカウントで追加されたすべての Citrix Cloud 管理者に電子メールが送信されます。

オンボーディングが完了したら、［構成］>［ネットワーク構成ホーム］**>**［**Citrix SIA** 構成を開く］に移動し、［デバイスをクラウドに接続］を選択します。このページでは、指示に従って、エンドデバイス OS に適合する Cloud Connector をダウンロード/インストールできます。

オンボーディングプロセスは、[構成] **>** [ネットワーク構成のホーム] ページから再実行できます。設定を見逃した場合は、いつでもオンボーディングプロセスを再実行して、デフォルト設定または推奨設定に戻すことができます。



次は何だ

- ネットワーク内のノードのステータスを表示します。「ダッシュボード」を参照してください。
- サブスクライブしたライセンスエンタイトルメントに関する詳細を表示します。「ライセンスの詳細を表示する」を参照してください。
- 仮想配信エージェント（VDA）およびローカルホストシステムで CSIA Cloud Connector エージェントを設定します。Citrix Secure Internet Access Cloud Connector エージェントの構成を参照してください。
- Citrix SD-WAN 展開もある場合は、ブランチオフィスのトンネルを構成します。ブランチオフィス用のトンネルの設定を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Secure Internet Access 構成ポリシーポータルを使用して、クラウドコネクタとセキュリティ機能を構成し、レポートとログを監視します。「構成」を参照してください。

ライセンス

February 1, 2022

Citrix Secure Internet Access（CSIA）には 3 つのエディションがあります。

- **Standard**: クラウドベースのセキュリティソリューションで、クラウド内で一元化された管理と管理を提供します。Web およびインターネットコンテンツフィルタリング、SSL トラフィック管理、CASB などのコアセキュリティ機能が含まれています。
- **Advanced**: マルウェアの防止と侵害の検出、コマンドアンドコントロールのコールバック検出、インシデント対応などのセキュリティ機能が追加された完全なセキュリティソリューションです。
- プレミアム: 高度な機密コンテンツ検出と高度なコンテンツ分析エンジンを含む包括的なセキュリティソリューションです。

各エディションで利用できる機能の完全なリストについては、https://www.citrix.com/にある機能マトリックスを参照してください。

各エディションには次のものが含まれます。

- 500 GB のストレージ容量
- アカウントの 10 人のユーザごとに 1 つの IPSEC または GRE トンネル

保管スペースやトンネルを追加購入できます。

オンボーディングプロセスが完了すると 、サブスクライブしたライセンスと使用状況の詳細を把握できます。

ライセンス詳細の表示

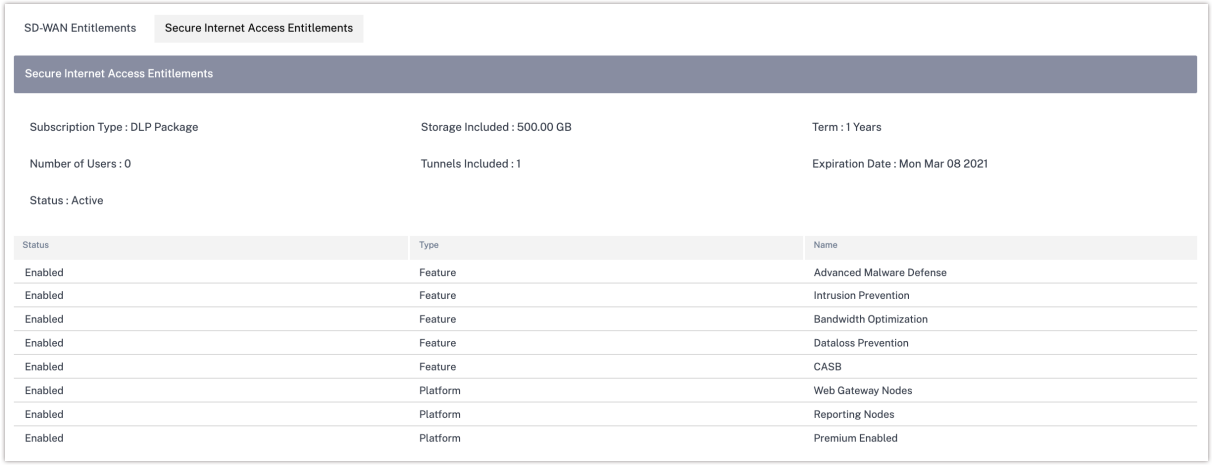
[管理] > [ライセンス] の順に移動して、サブスクライブしたライセンスエンタイトルメントの詳細を表示します。

[セキュリティで保護されたインターネットアクセス資格] タブでは、次の情報を表示できます。

- サブスクリプションの種類と、サブスクリプションで有効になっている機能のリスト。
- サブスクリプションパッケージに含まれるストレージ容量。デフォルトでは、各サブスクリプションには 500 GB のストレージ容量が含まれています。
- サブスクリプションパッケージに含まれるトンネルの数。デフォルトでは、各サブスクリプションには、アカウントの 10 人のユーザごとに 1 つのトンネルが含まれます。
- ライセンス期間と有効期限

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- このサブスクリプションに追加されたユーザー数
- エンタイトルメントのステータス



また、購入した追加のストレージスペースやトンネルに関する詳細も表示できます。

> 注
>
> Citrix SD-WAN 資格もある場合は、[SD-WAN] タブで SD-WAN ライセンスの詳細を表示できます。SD-WAN ライセンスの詳細については、「SD-WAN Orchestrator ライセンス」を参照してください。

ライセンス使用状況のインサイト

[管理] > [ライセンス使用状況インサイト] に移動すると、ライセンス使用状況に関するインサイトを取得できます。

所有しているユーザーライセンスの総数と、アクティブなユーザーライセンスの数を表示します。また、データストレージとトンネルの合計ライセンス数とアクティブなライセンス数も表示できます。

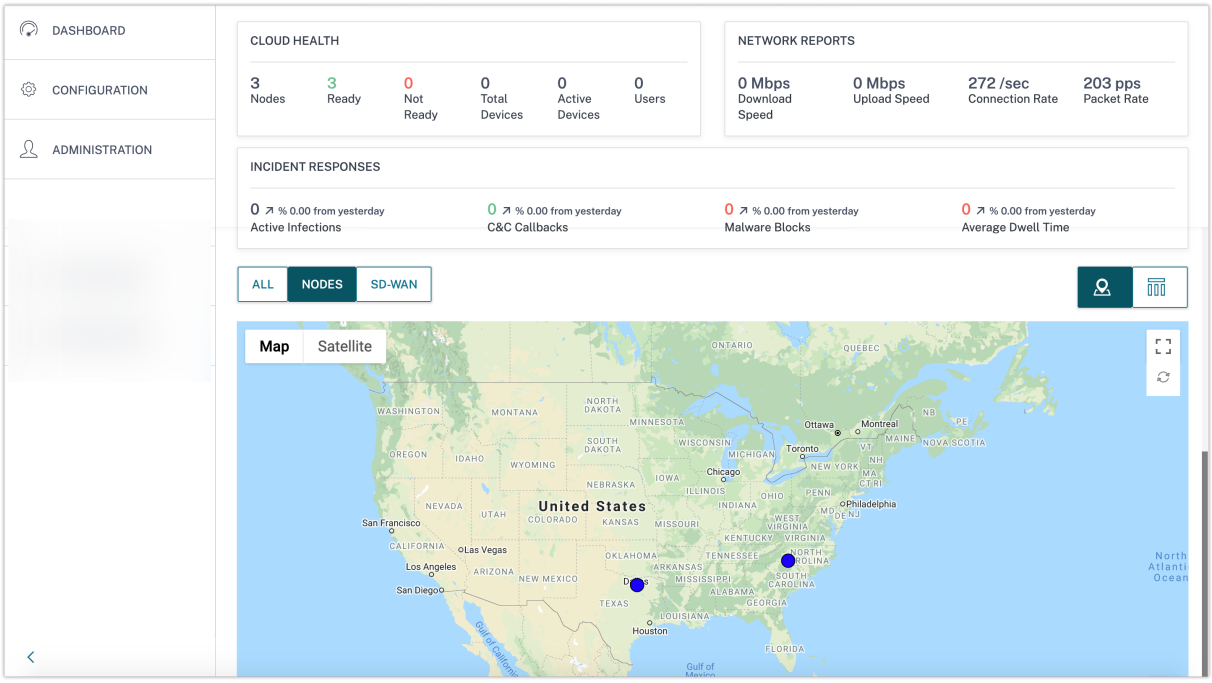
これらのインサイトは、ユーザーライセンス、ストレージ容量、またはトンネルを増やす必要があるかどうかを判断するのに役立ちます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ダッシュボード

February 1, 2022

次の図に示すように、ダッシュボードには、Citrix Secure Internet Access（CSIA）ネットワークのパフォーマンスの概要が表示されます。



ダッシュボードには、クラウドヘルス、ネットワークレポート、インシデント対応、ネットワークのマップビューという 4 つの主要セクションがあります。

[レポートと分析] ページで、より詳細なレポートにアクセスできます。そのためには、［構成］>［**Citrix SIA** 構成を開く］に移動します。

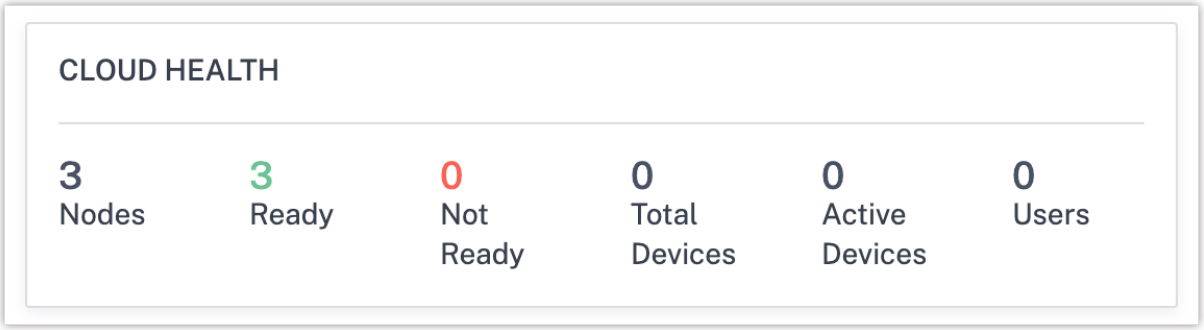
クラウドヘルス

このセクションには、ネットワーク内のノードのステータスが表示されます。自分用に構成されたノードの総数を表示します。また、準備が整っているノードの数と準備ができていないノードの数も表示します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Not **Ready** のノードが動作していないか、プロビジョニングされていません。この問題は、修正できるように調査または報告する必要があることを示しています。

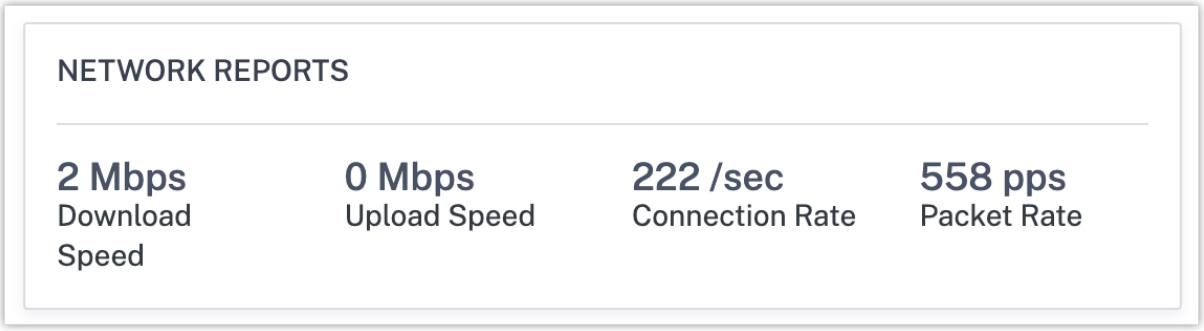
クラウドヘルスセクションには、ノードに接続されているデバイスの総数およびアクティブなデバイスの数に関するインサイトも表示されます。また、ネットワークに接続しているユーザーの数を追跡することもできます。



ネットワークレポート

このセクションでは、ネットワーク上のリアルタイムアクティビティの概要を説明します。接続されているすべてのデバイスのダウンロード速度やアップロード速度などの帯域幅使用量が一覧表示されます。このセクションでは、ネットワーク全体で使用される接続とパケットのレートについても説明します。

この情報により、対処する必要のあるネットワークの問題があるかどうかがわかります。



インシデント対応

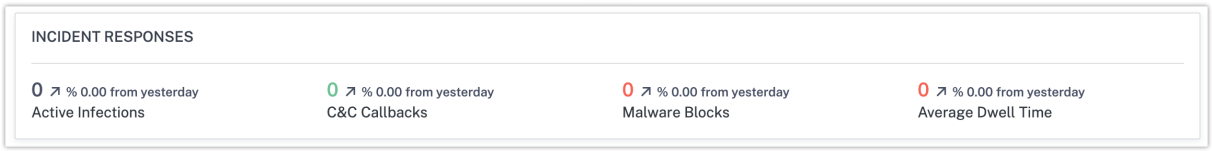
このセクションには、ネットワーク内の感染したデバイスと、調査または報告が必要なデバイスの概要が表示されます。

このセクションには、次のセキュリティデータが表示されます。

- ネットワーク内で現在活動している感染の数
- コマンドアンドコントロール (C&C) コールバックの数
- ネットワークへの侵入がブロックされたマルウェアの総数
- ネットワーク全体の感染の平均滞留時間。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

このセクションには、これらのインシデントが前日以降に増加した割合も表示されます。



通知

Citrix Secure Internet Access サービスのサブスクリプションに関連する重要な更新は、ダッシュボードに通知として送信されます。通知には次のものが含まれますが、これらに限定されません。

- ライセンスの有効期限に関する情報
- 新ビルドのリリースノート
- URL レビューリクエスト
- アラートとアドバイザリ

Citrix は、ベルのアイコンに数字が付いた通知があることを通知します。ダッシュボードの右上にベルのアイコンがあります。ベルアイコンを選択すると、通知ビューを展開できます。これらの通知はベルのアイコンにのみ表示され、電子メールでは送信されません。

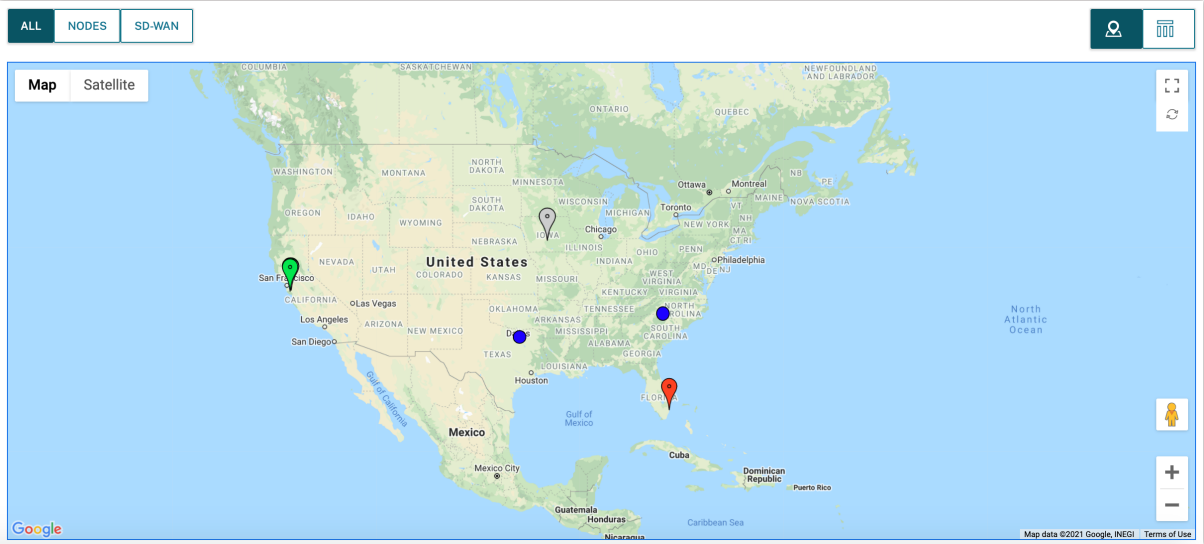
マップビュー

マップビューには、Citrix Secure Internet Access 展開環境のクラウドノードとゲートウェイノードの地理的な場所が表示されます。青い点はマップ上のノードを表します。

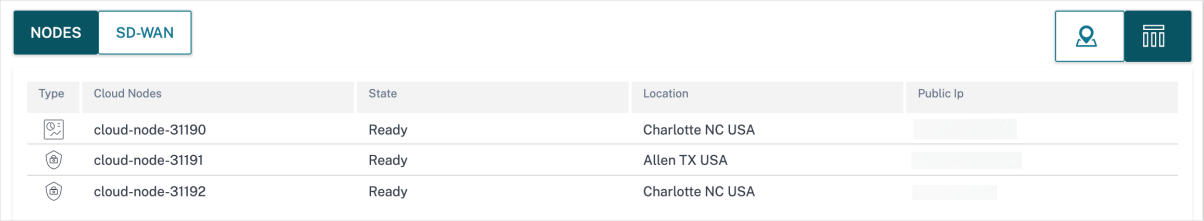
SD-WAN 資格がある場合は、SD-WAN サイトの地理的位置を確認できます。サイトはマップ上に緑、赤、または灰色で表示されます。

［ノード］タブを選択して Citrix Secure Internet **Access** ノードのみを表示するか、［SD-WAN］タブを選択して **SD-WAN** サイトに制限できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



この情報を表形式で表示するには、マップのすぐ右上にあるテーブルビューアイコンを選択します。マップビューに戻すには、テーブルビューアイコンの左にあるマップビューアイコンを選択します。



構成

February 1, 2022

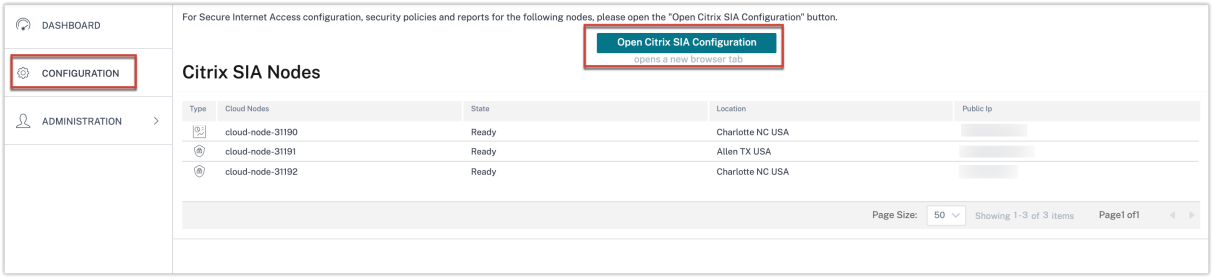
Citrix Secure Internet Access（CSIA）構成ポリシーポータルを使用して、クラウドコネクタとセキュリティポリシーを構成し、レポートとログを監視します。

設定ポリシーポータルにアクセスするには、次の手順を実行します。

1. Citrix Cloud にサインインします。
2. [セキュリティで保護されたインターネットアクセス] タイルで [管理] を選択します。
3. ナビゲーションペインで、［構成］を選択します。

   [Configuration] ページには、設定済みのクラウドノードに関する詳細も一覧表示されます。実行した設定はすべて、これらのノードに接続されます。
4. ［**Citrix SIA** 構成を開く］を選択して構成ポリシーポータルを表示し、機能とセキュリティポリシーの構成を開始します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



設定に関するヘルプの入手方法

設定の手順や設定ページのヘルプを表示するには、次のいずれかを実行できます。

- ヘルプドキュメントにアクセスします。設定ポリシーポータルの右上隅にあるメニュー (自分の名前が表示されている場所) をクリックし、[**HelpDocs**] を選択します。完全なヘルプドキュメントを参照できます。

  > 注
  >
  > このヘルプドキュメントには、iboss 用語、iboss ユーザーインターフェイス要素、Citrix でサポートされていない iboss 機能、iboss サポート情報に関する参照情報が含まれています。
  >
  > ヘルプドキュメントを使用する前に、Citrix Secure Internet Access と iboss の統合に関する記事を参照してください。この記事は、Citrix Secure Internet Access にサインインした後にのみアクセスできます。

- コンテキストヘルプにアクセスします。各設定ページの右上隅にあるヘルプアイコン **(?)** をクリックすると、そのページに関するヘルプドキュメントが表示されます。
- **Citrix** サポートに問い合わせてください。Citrix アカウントでサインインし、サポートケースを開いたり、ライブチャットを開始したり、サポートを受けるための他のオプションを調べたりできます。

Citrix Secure Internet Access Cloud Connector エージェントを構成する

CSIA Cloud Connector エージェントは、Citrix セキュアインターネットアクセスを介してインターネットトラフィックをリダイレクトするソフトウェアエージェントです。

オンボーディングプロセスが完了したら、次の操作を行います。

- **Virtual Delivery Agent**（**VDA**）に **CSIA Cloud Connector** エージェントをインストールする：Citrix Workspace 上の仮想デスクトップから認可されていない Web および SaaS アプリケーションに安全にアクセスするには、Citrix Secure Internet Access 経由でトラフィックをリダイレクトするように CSIA Cloud Connector エージェントを構成します。

  構成手順の詳細については、「Citrix Virtual Apps and Desktops を使用した Citrix Secure Internet Access」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

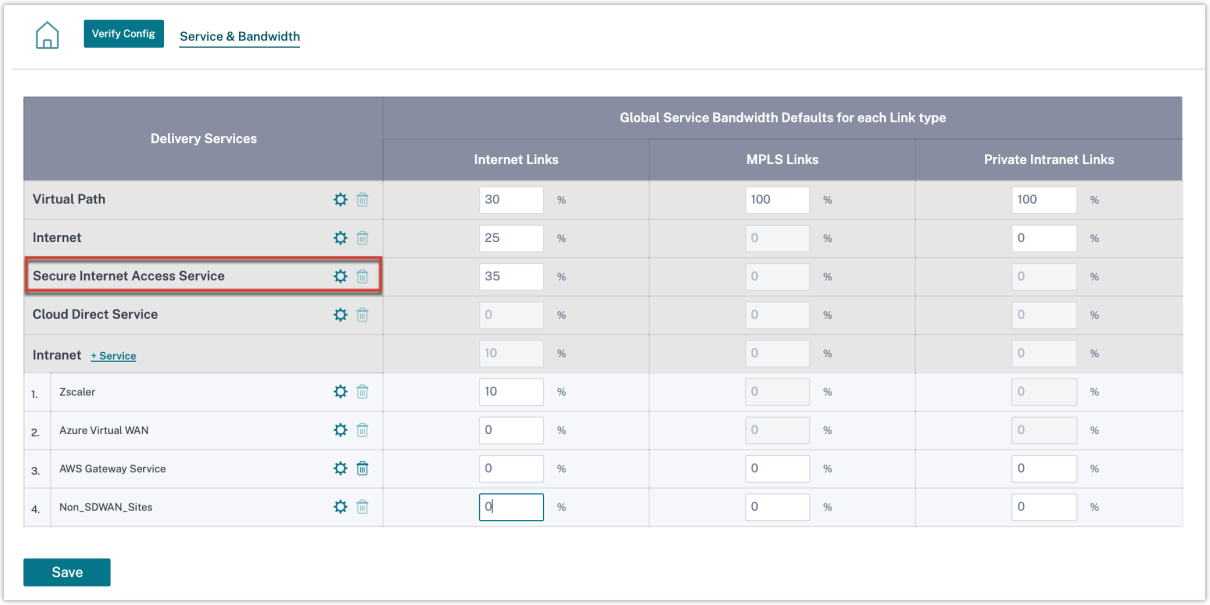
- **CSIA Cloud Connector** エージェントをホストデバイスにインストールする：ラップトップやモバイルデバイスなどのホストシステムからの直接インターネットトラフィックに安全にアクセスするには、各デバイスに Cloud Connector エージェントをインストールします。

ブランチオフィスにトンネルを設定する

ブランチオフィスに Citrix SD-WAN 展開がある場合は、IPSEC トンネルまたは GRE トンネルを構成する必要があります。これにより、Citrix Secure Internet Access を介して、認可されていない Web および SaaS アプリケーションにブランチトラフィックがリダイレクトされます。Citrix SD-WAN Orchestrator を使用してトンネルを構成します。

Citrix SD-WAN Orchestrator では、［構成］>［デリバリーサービス］>［サービスと帯域幅］で、**Citrix Secure Internet Access** サービスを利用できます。

> 注
>
> サービスリンクは、SD-WAN Orchestrator のお客様で、Citrix Secure Internet Access 資格を持っている場合にのみ表示されます。



この構成には、次の大まかな手順が含まれます。

1. インターネットリンクの帯域幅の割合とプロビジョニングの割合を指定して、Citrix Secure Internet Access サービスを作成します。
2. SD-WAN サイトを Citrix Secure Internet Access サービスに追加してマッピングし、適切なトンネル（IPSEC または GRE）を選択します。次に、構成をアクティブにして、Citrix SD-WAN と Citrix Secure Internet Access PoP 間のトンネル確立を有効にします。
3. アプリケーションルートを作成して、トンネルを通過するトラフィックを誘導します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

詳細な手順については、「デリバリーサービス-Citrix Secure Internet Access サービス」を参照してください。

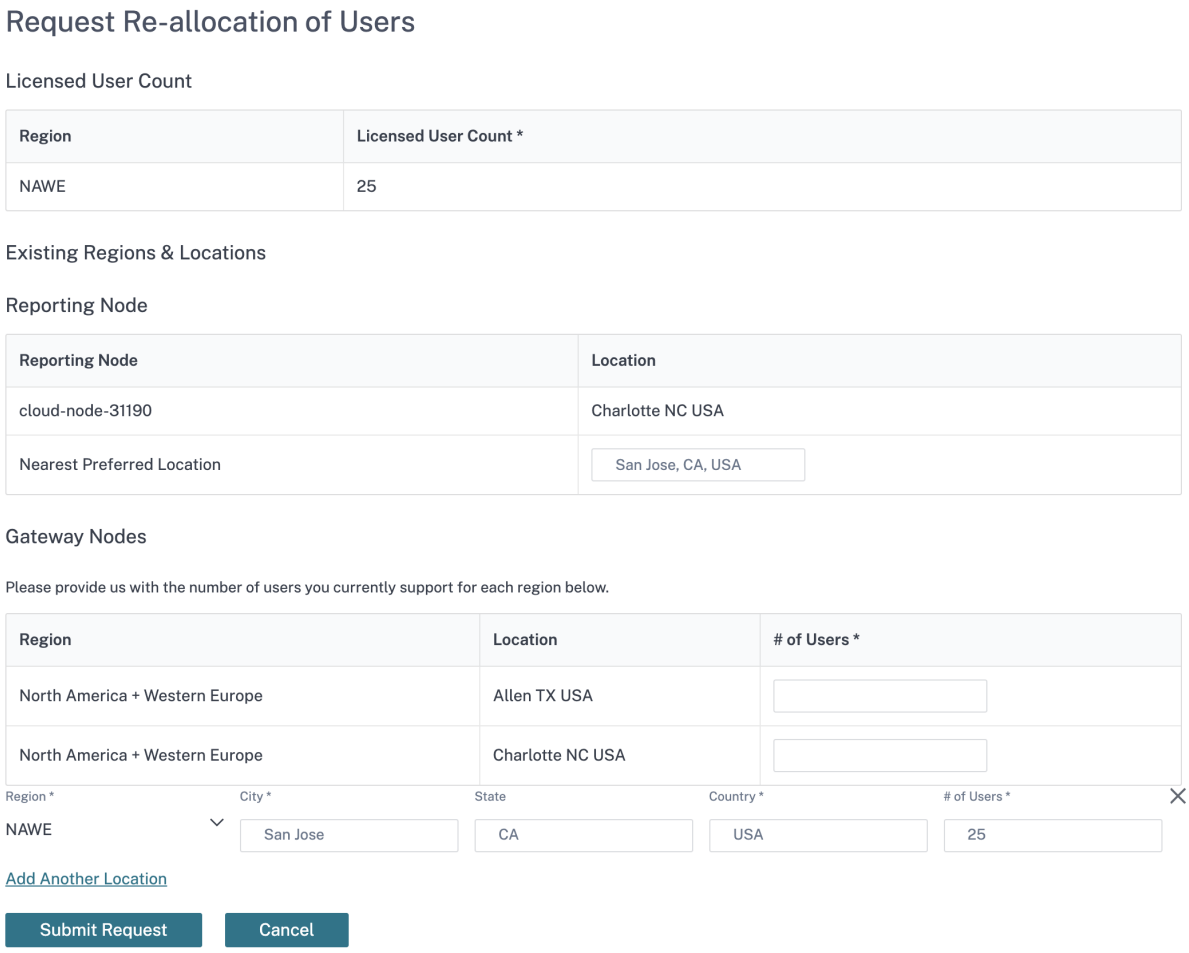
ユーザー再割り当て

地理的リージョン内でクラウドノードを再分散することで、特定のロケーションにいるユーザーのレイテンシーを最小限に抑えることができます。

使用状況データを収集するレポートノードと、セキュリティ機能を実行するゲートウェイノードの両方を再配布するよう要求できます。Citrix は、ノードの可用性に基づいて、ユーザーに最も近いノードを提供することを目的としています。

> 重要
>
> ノードを再割り当てすると、サービスが短時間中断します。通常、この操作はアカウントのアクティブ化の直後、クライアントコネクタが構成および配布される前に実行されます。ユーザーに最も近いノードを再配置し、頻繁に再割り当てしないように、展開の開始時にノードの再割り当てをリクエストすることをお勧めします。

ノードにまだ割り当てられていない場合は、ノード間でユーザーを移動したり、ノードに追加したりすることもできます。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ノードを表示、再配布、および保守するには、左側のメニューの [**Configuration**] タブに移動し、表の上にある [ユーザーの再割り当てを要求] を選択します。

> 注
>
> ノードは、同じ地理的リージョン内でのみ再配布できます。

クラウド設定

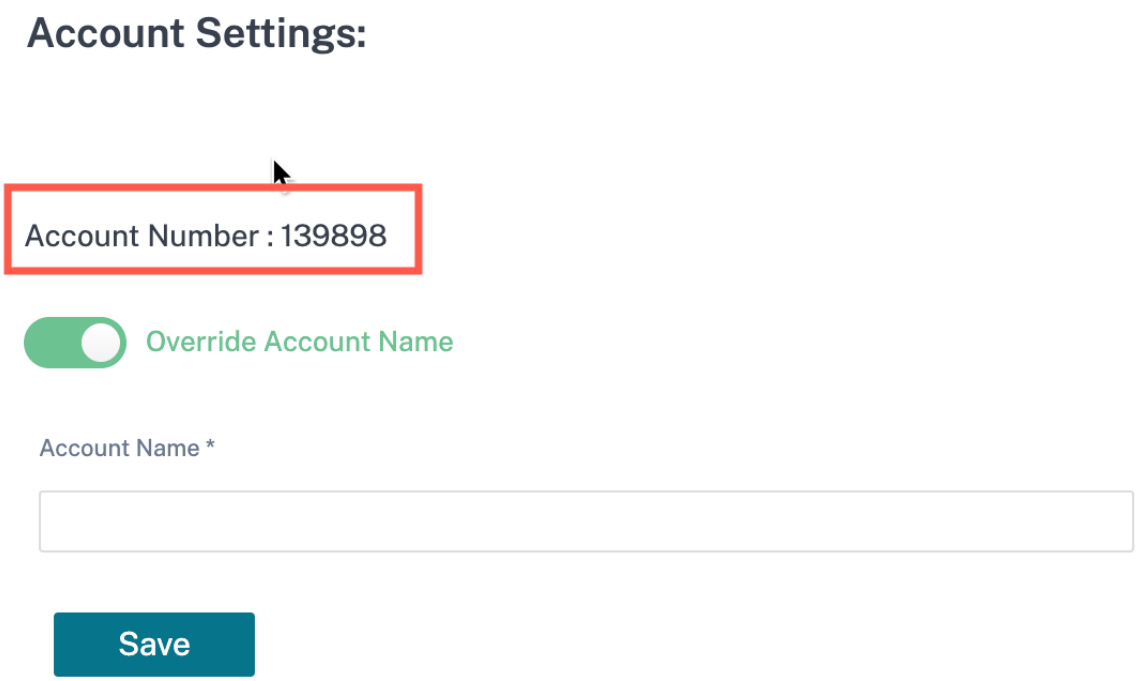
ネットワークタイムプロトコル (NTP) サーバー、プラットフォームメンテナンス、およびアップデートリリースの設定を構成するには、[構成] タブに移動し、[クラウド設定] を選択します。

アカウント設定

アカウント設定機能は、Citrix Secure Internet Access サービスポータルに表示されるアカウント名を変更または上書きするのに役立ちます。

アカウント名を上書きするには、[構成] **> [**クラウド設定**] > [**アカウント設定**]** に移動します。

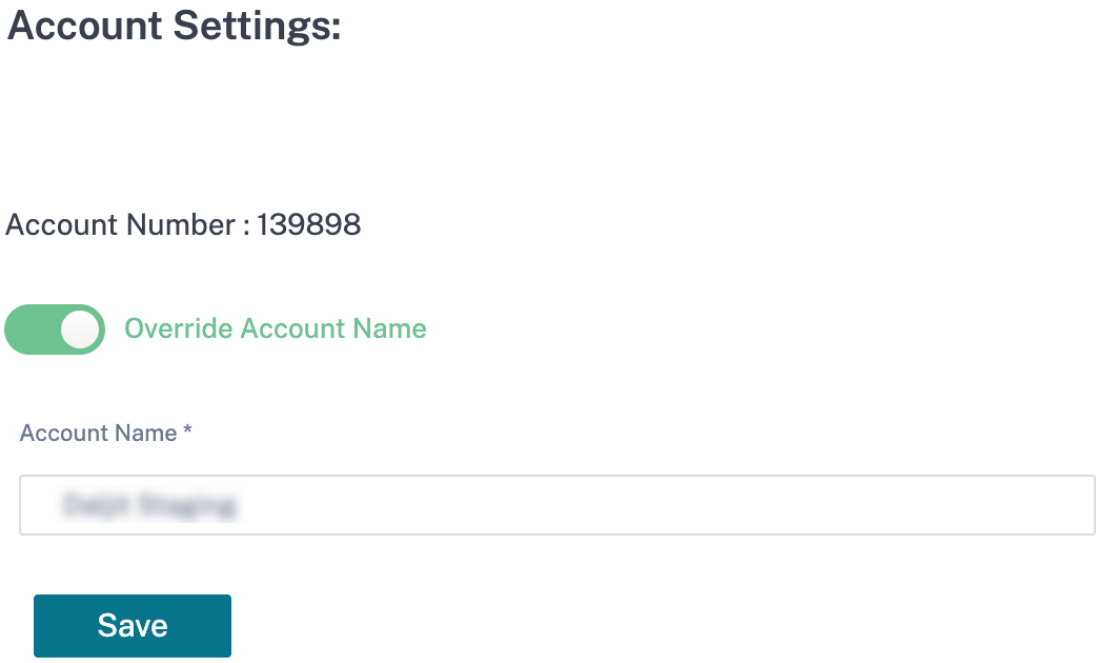
Citrix Secure Internet Access アカウント番号を表示できます。



> (注)
>
> 名前を作成していない場合や、[アカウント名のオーバーライド（**Override Account Name**）] が無効になっている場合、初期設定されたアカウント名は CSIA ポータルに引き続き存在します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. [アカウント名の上書き] を有効にして、名前を入力します。既定では、[アカウント名の上書き] は無効になっています。



   ポータルで更新されたアカウント名が表示されるまでしばらくお待ちください。アカウント名を変更したら、再ログインが必要になる場合があります。

2. [保存] をクリックします。

NTP サーバ

日付と時刻を同期するには、[クラウド設定] の [**NTP Server**] に移動します。タイムゾーン、日付形式、NTP サーバのアドレス、およびサマータイム情報を入力します。

タイムゾーンは、タイムスタンプに使用される地域の標準時間を定義します。タイムゾーンを変更すると、レポート内のイベントのタイムスタンプが新しいタイムゾーンに合わせて変更され、継続性が維持されます。タイムスタンプは、新しいタイムゾーンに対する相対値です。

[日付形式] は、日付の構造を数値形式で定義します。このパラメータは、**mm/dd/yyyy** または **dd/mm/yyyy** のいずれかに設定できます。

NTP サーバは NTP サーバのアドレスを定義します。

サマータイムは、タイムゾーンがサマータイムに準拠しているかどうかを定義します。このパラメーターは、タイムゾーンの地域に応じて [米国] または [英国] のいずれかに設定できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

プラットフォームメンテナンス

この機能により、メンテナンスを行う日時をスケジュールして、ピーク時にネットワークを利用できるようにすることができます。

ユーザーに代わって実行される自動メンテナンスをスケジュールするには、[クラウド設定] の **[**** プラットフォームのメンテナンス] に移動し、[**** 優先メンテナンスウィンドウ] を有効にします。次に、自動メンテナンスの希望の日時を選択します。

リリース設定の更新

ユーザーに代わってインストールされるアップデートの種類を選択するには、[クラウド設定] の **[**** リリース設定の更新 ****] に移動し、次のリリースレベルのいずれかを選択します。

- 必須です。新機能、機能の更新、バグ修正、パフォーマンスの強化など、重要なプラットフォームの更新とセキュリティ修正に使用されます。
- 推奨されるが、重要な修正が含まれていないリリースの場合は省略可能です。
- アーリーアクセス：新機能、アップデート、バグ修正、パフォーマンス強化に早期アクセスできます。

メール設定

アラート、定期レポート、その他の通知を含むメールを中継するように、メールサーバーの設定を構成できます。Web ゲートウェイとレポートノードが電子メール通知を送信できるようにするには、[クラウド設定] の **[電子メール設定] のフォームに入力します ****。このプロセスでは、電子メール通知を受信できるように SMTP サーバアドレスを設定します。

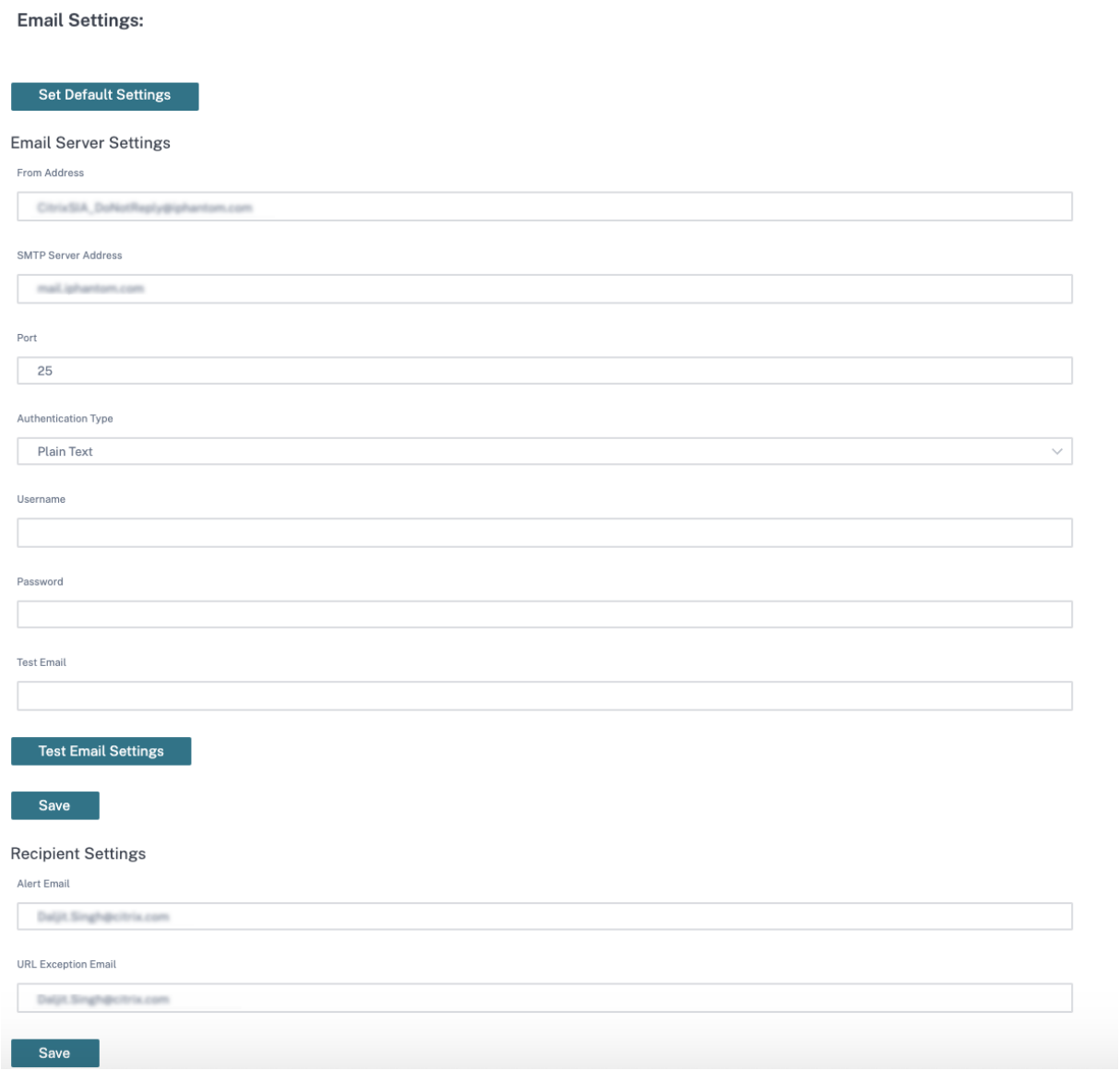
電子メール設定は、[電子メール設定のテスト] オプションを使用して検証できます。また、[既定の設定を設定] ボタンを使用して、既定の電子メール設定を設定することもできます。

ユーザーアラートと URL 例外リクエストを受信するメールアドレスを設定します。

- アラートメール: リスクの高いキーワードによってトリガーされるアラートの送信先アドレス。
- **URL** 例外電子メール: ブロックページから送信された URL 例外要求の宛先アドレス。

> 注:
>
> [リアルタイムアラート] ページでは、追加の電子メールアラートを使用できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 注:
>
> 通常、SMTP サーバーはスパムを防止するために IP ベースの許可一覧を使用して構成されます。そのため、すべてのノードの IP アドレスを SMTP サーバーの許可リストに追加する必要があります。
>
> また、スパムを減らすために、SMTP サーバーは DKIM などの他のメカニズムを使用する場合があります。SMTP サーバーでは、Web ゲートウェイとレポートノードをこれらの制限から除外する必要がある場合があります。

独自の内部 SMTP サーバーがない場合は、Google の SMTP サービスのいずれかを使用できます。このためには、有効な Gmail アカウントが必要です。

Google SMTP サーバーでは、ポート 25、465、587、またはこれらを組み合わせて使用します。最も人気があるのは **smtp.gmail.com** で、ポート 465 (SSL を使用) または 587 (TLS を使用) を使用します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> SMTP サーバーは通常、TCP ポート 25、465、または 587 でリッスンしますが、動作するように構成されている任意のポートをリッスンできます。SSL 経由の SMTP はポート 465 を使用し、TLS 経由の SMTP はポート 587 を使用します。ポート 465 と 587 はいずれも認証サービスが必要です。ポート 25 は暗号化されておらず、認証は不要です。
>
> ローカル Web ゲートウェイまたはレポートノードを操作する場合は、必要なポートが制限されていないことを確認してください。

3 つの Google SMTP サーバの設定は次のとおりです。

完全修飾ドメイン名	設定要件	認証の要件
smtp-relay.gmail.com	ポート 25、465、または 587。セキュア・ソケット・レイヤー (SSL) またはトランスポート・レイヤー・セキュリティ (TLS) プロトコル、および 1 つ以上の静的 IP アドレスを持つポート。	IP アドレス。
smtp.gmail.com	SSL を使用する場合はポート 465、または TLS を使用する場合はポート 587。動的 IP は許可されます。	Gmail または G Suite の完全なメールアドレス。
aspmx.l.google.com	メールは Gmail または G Suite ユーザーのみに送信できます。動的 IP は許可されます。	なし。

smtp-relay.gmail.com は、関連付けられた IP アドレスで認証することにより、組織からメールを送信するために使用されます。ポート 25、465、または 587 を使用して、ドメイン内外の誰にでもメッセージを送信できます。

smtp.gmail.com は、ドメイン内外の誰にでもメールを送信するために使用されます。Gmail または G Suite のアカウントとパスワードで認証する必要があります。SSL (ポート 465) または TLS (ポート 587) 経由の SMTP を使用できます。

aspmx.l.google.com は、Gmail または G Suite ユーザーにのみメッセージを送信するために使用されます。このオプションは認証を必要としません。この SMTP サーバーでは SSL または TLS を使用できないため、トラフィックはプレーンテキスト形式なので、お勧めしません。

匿名化されたロギング

法規制の遵守と機密保持のため、**Cloud Settings** の **Anonymized Logging** は、委任された管理者がネットワークの使用状況を監視するために使用する個人ユーザー情報を暗号化します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

匿名化ロギングを有効にする前に、**[**匿名化ログを有効にする**]** トグルの **[**** キーの追加] ボタンを選択して、暗号化キーを作成する必要があります。** 暗号化キーの 64 文字の値を [Encryption **Key**] フィールドに入力します。独自の暗号化キーを入力することも、[**Auto Generate Key**] オプションを使用することもできます。

> 重要**:**
>
> 続行する前に、暗号化キーを別の場所に記録することを強くお勧めします。暗号化キーは、プラットフォーム上でアクティブである限り、関連付けられているデータを復号化するために必要です。

[カテゴリの暗号化] で次のトグルを有効にすると、特定のカテゴリの識別可能なデータを暗号化するようにキーを設定できます。

- 個人情報。報告されたユーザーアクティビティのユーザー名、フルネーム、マシン名など、個人を特定できるすべての情報の暗号化を有効または無効にします。
- データソース。報告されたユーザーアクティビティのデータソースに関連するすべての情報の暗号化を有効または無効にします。
- **[**グループ名**]**。報告されたユーザアクティビティに関連付けられているグループ名の暗号化を有効または無効にします。

[**Group Association**] タブで、暗号化キーを特定のグループにのみ適用するように構成することもできます。**[Select All]** トグルが有効な場合、現在設定されている暗号化キーがすべてのセキュリティグループに適用されます。**[Select All]** トグルが無効になっている場合、暗号化キーで暗号化するセキュリティグループを選択できます。

暗号化キーを設定したら、匿名化されたロギングを有効にして、ユーザーのオンラインアクティビティの匿名化されたログに基づいてネットワークの使用状況を監視します。

定義済みの暗号化キーを削除するには、テーブル内の対応する暗号化キーの横にある省略記号を選択し、[**Delete**] を選択します。

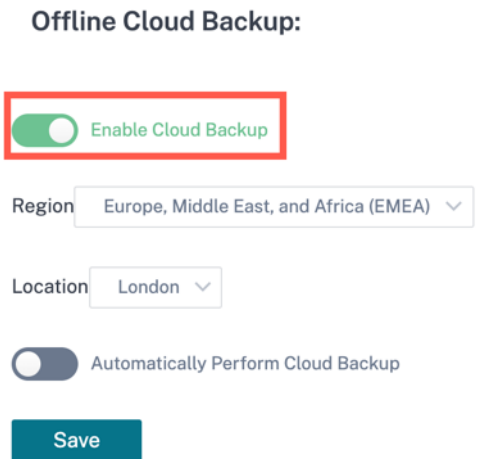
クラウド・バックアップ

Offline Cloud Backup 設定では、選択したリージョン、ロケーション、および時間に基づいて、レポートノードのバックアップ設定とログを保存/保存できます。オフラインクラウドバックアップオプションを使用すると、CSIA インターフェイスを介してクラウドバックアップを保存できます。

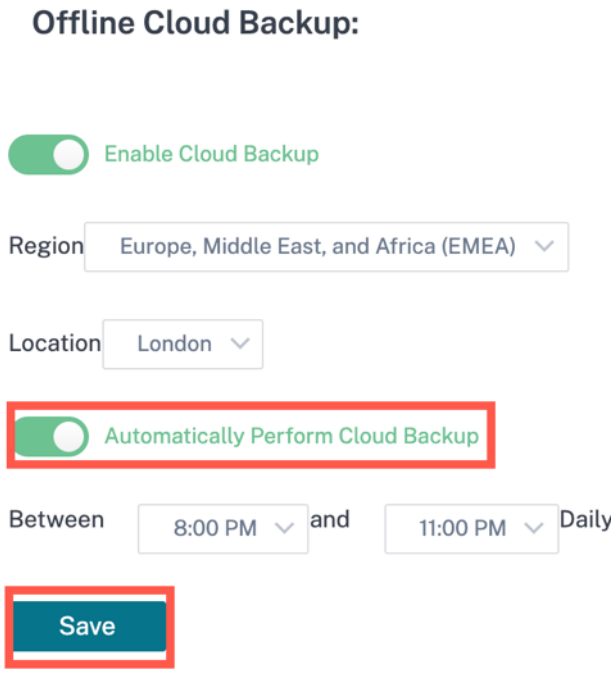
クラウドバックアップ設定を有効にするには、[構成**] ** [**** クラウド設定] の順に選択し、[クラウドバックアップ] を選択します。

1. [クラウドバックアップを有効にする] トグルボタンを有効にし、ドロップダウンリストから [リージョン] と [ロケーション] を選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. また、[クラウドバックアップを自動的に実行] トグルボタンを有効にして、実行する時間間隔を設定し、日次バックアップを作成することもできます。[保存] をクリックします。



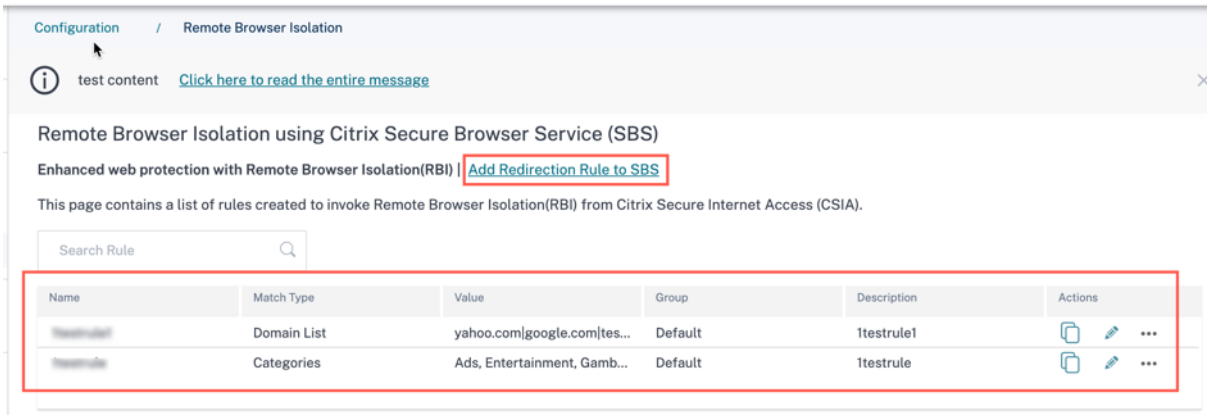
リモートブラウザ分離

リモートブラウザ隔離は、マルウェアや悪意のある脅威からセキュリティを確保する高度な Web 保護機能です。リモートブラウザ分離により、Citrix Secure Internet Access Web フィルタリング機能をセキュアブラウザサービス（SBS）とともに使用して、企業ネットワークをブラウザベースの攻撃から保護できます。詳しくは、「Secure Browser サービス」を参照してください。

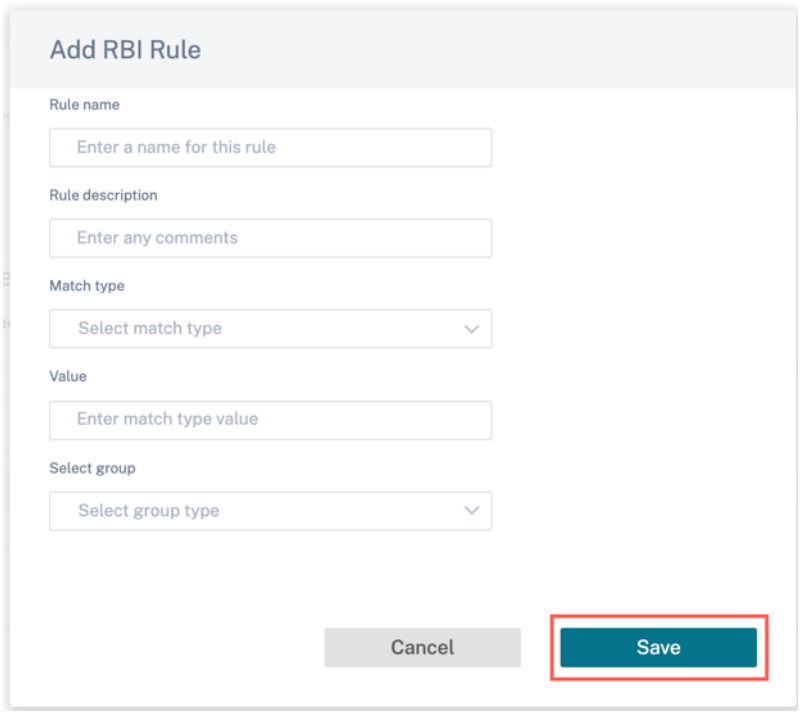
リモートブラウザ隔離機能を使用すると、信頼されていない一部のターゲット Web サイトに対して、リモートのクラウドベースのセキュアブラウザサービスを介してのみ隔離および起動するようにルールを設定できます。このルールを作成して、分離するユーザグループとトラフィックの種類の組み合わせに適用できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

リモートブラウザアイソレーションを呼び出すために作成されたルールの一覧を表示できます。



呼び出す必要があるトラフィックのリダイレクトルールを設定するには、[構成] **>** [リモートブラウザ隔離] に移動し、[リダイレクトルールを **SBS** に追加] をクリックします。



- ルール名: ルール名を指定します。
- ルールの説明: ルールの説明を入力します。
- [一致タイプ]: ドロップダウンリストから [ドメイン正規表現]、[ドメインリスト]、[IP アドレス]、[URL]、[カテゴリ] などの一致タイプを選択します。
- [値]: 照合値の種類を入力します。
- [グループを選択]: ドロップダウンリストからグループを選択します。

[**SBS** にリダイレクトルールを追加（**Add Redirect Rule to SBS** ）] オプションを使用すると、セキュアインターネットアクセスポータルに Web フィルタリングルールを作成して、トラフィックをブラウザサービスにリダイレクトできます。リモートブラウザ分離ルールごとに、セキュリティで保護されたブラウザ URL が関連付けられていま

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

す。つまり、セキュアなインターネットアクセスサービスを介して URL が起動されたときに、その URL が定義済みのリモートブラウザ分離一致ルールのいずれかに一致すると、要求は関連付けられたセキュアブラウザサービスにリダイレクトされます。

管理

February 1, 2022

管理者の役割は、Citrix Secure Internet Access（CSIA）サービスで機能を表示したり、さまざまなアクティビティを実行したりするための権限を定義します。

Citrix Secure Internet Access サービスの一部として、次の機能が含まれています。

- ダッシュボード。最上位のレポートへのアクセス
- ウェブゲートウェイ。Secure Web Gateway サービスへのアクセス。
- レポートと分析。より詳細なレポートにアクセスできます。
- 場所とジオマッピング。クラウドノードとゲートウェイノードの地理的な場所へのアクセス。
- ノードコレクション管理。ノードコレクション管理機能にアクセスします。
- ライセンス。サービスのライセンス詳細を取得する機能。
- ユーザー管理。カスタムロールを作成し、カスタムロールを他の管理者に割り当てることができます。

役割ベースのアクセス制御

Citrix SD-WAN Orchestrator と同様に、Citrix Secure Internet Access サービスリソースへのアクセスは、個々の管理者に割り当てられた役割に基づいて管理されます。Citrix Secure Internet Access サービスの管理者ユーザーに割り当てることができるアクセスレベルには、カスタマーマスター管理者、カスタマーマスター読み取り専用管理者、カスタマーアクセスなし、およびカスタマーマスター読み取り専用管理者プライバシーモードの 4 つのレベルがあります。

- **Customer-Master-Admin** レベルは、管理者が次の操作を行うことができるフルアクセスロールです。
  - Citrix Secure Internet Access サービスのすべての機能を管理します。
  - 管理者をサービスに追加します。
  - 管理者をサービスから削除します。
  - カスタマーネットワーク内でロールを割り当て、編集、削除します。
  - カスタムロールを作成する。
- **Customer-master-readonly-Admin** レベルは読み取り専用の役割で、管理者は Citrix Secure Internet Access サービスの機能のみを表示できます。
- **Citrix** Secure Internet Access サービスのすべての機能へのアクセスが拒否されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Customer-master-readonly-admin-Privacy Mode** レベルでは、** ライセンスとユーザー設定を除くすべての **Citrix****Secure Internet Access サービス機能への読み取り専用アクセス権が付与されます。このロールを持つユーザは、自分のアカウント内の他の管理者ユーザ、割り当てられたロール、またはライセンス関連情報の一覧を表示できません。

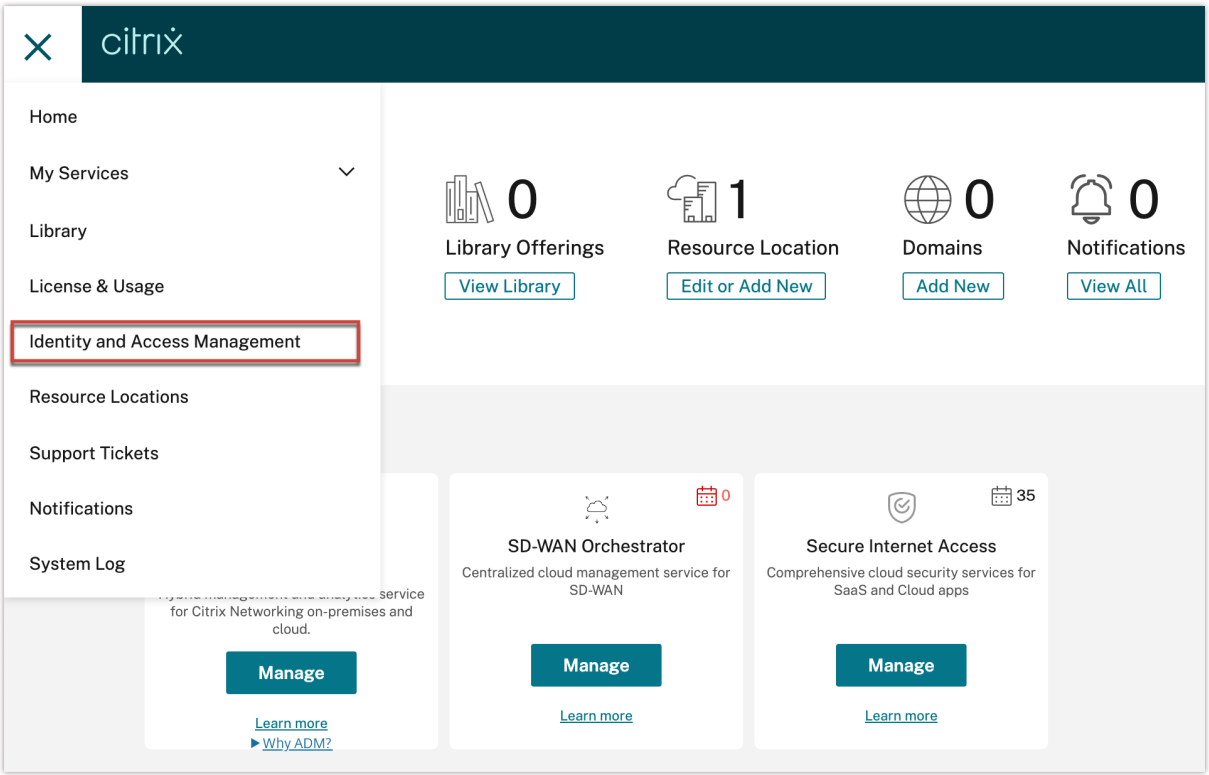
> 注:
>
> Citrix Secure Internet Access サービスの場合、役割は顧客レベルで割り当てられます。Citrix SD-WAN Orchestrator サービスの場合、** 役割は顧客レベルとプロバイダーレベルの両方で割り当てられます。その結果、**Citrix SD-WAN Orchestrator** サービスには、** カスタマーマスター管理者の役割とプロバイダー-マスター-管理者-すべての役割の両方を使用できます **。

RBAC を適用するには、まず Citrix Cloud サービスに管理者としてユーザーを追加する必要があります。

Citrix Cloud サービスに新しいユーザーを追加する

Citrix Cloud の［**ID** およびアクセス管理］機能を使用して、**Citrix Secure Internet Access** サービスに管理者を追加できます。新しい管理者は、既存の Citrix アカウントの資格情報を使用したり、必要に応じて新しいアカウントを設定したりできます。

新しい管理者を追加するには、Citrix Cloud ホームページのメニューから［**ID** およびアクセス管理］を選択し、ユーザーインターフェイスの指示に従います。詳しくは、「Citrix Cloud 管理者の管理」を参照してください。



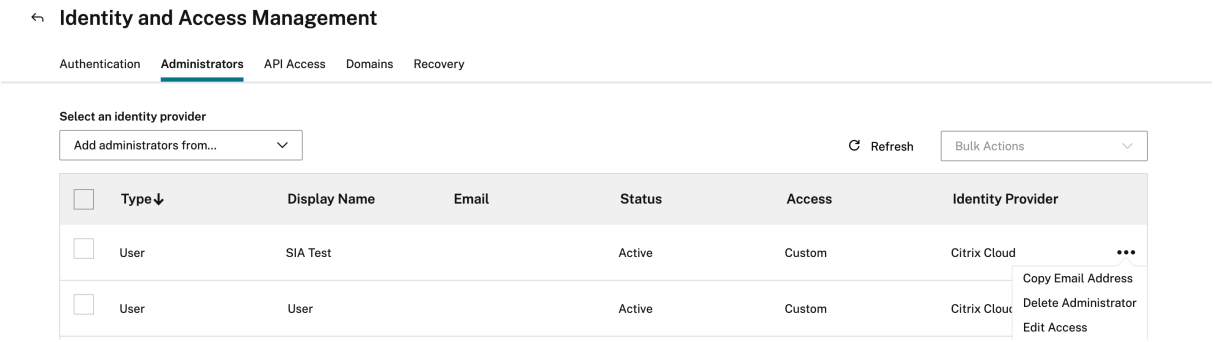
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

新しく追加した管理者には、Citrix Cloud サービスへのフルアクセスが自動的に割り当てられます。管理者が Citrix Cloud のどの部分を表示および管理できるかをより細かく編集できます。

新規ユーザーのアクセス権を編集

Citrix **ID** およびアクセス管理で新しい管理者を追加したら、その役割を設定できます。

作成したアカウントに対するアクションのリストから［アクセスの編集］を選択し、［フルアクセス］（Citrix Cloud サービスへの）または［カスタムアクセス］を選択します。



Citrix Secure Internet Access サービスへのフルアクセスを許可し、サブ機能をカスタマイズせずに許可するには（［カスタムアクセス］>［全般的な管理］）、高レベルの［フルアクセス］オプションを選択します。

次のいずれかまたは両方に該当する場合は、[カスタムアクセス] を選択します。

- [全般的な管理] にリストされているサブ機能へのアクセスを規制する場合。
- 特に、Citrix Secure Internet Access サービスへのアクセスレベルを規制したい。

[カスタムアクセス] を選択した場合は、セキュリティで保護されたインターネットアクセスのアクセスレベルを [一般的な管理] とは別に指定する必要があります。このアクセスには、フルアクセス、読み取り専用アクセス、読み取り専用アクセス (プライバシーモード)、またはアクセスなしがあります。

Customer Admin：フルアクセスが割り当てられているユーザーは、高レベルの［フルアクセス］オプション（［カスタムアクセス］の上にあります）で付与された Citrix Secure Internet Access サービスへのアクセス権と同じアクセス権を持ちます **。[** 顧客管理者：フルアクセス］を選択すると、Citrix Secure Internet Access サービス機能へのフルアクセスが許可され、［全般的な管理］でサブ機能へのさまざまなレベルのアクセス権も選択できます。

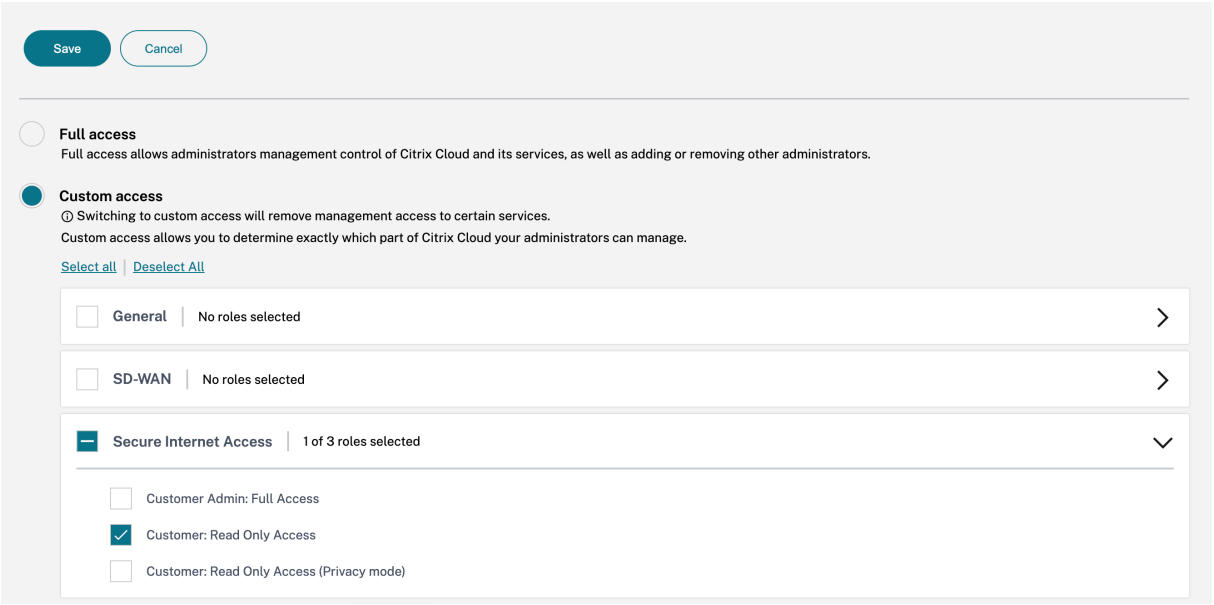
> 重要
>
> [セキュリティで保護されたインターネットアクセス] の下のボックスを **1** つ選択するか、選択しないか両方のチェックボックスをオンにすると、最高レベルの権限が管理者に付与され、セキュリティ上のリスクが生じます。

Customer: Read Only Access が割り当てられているユーザーは、サービスの機能を表示することしかできません。**Customer: Read Only Access (**プライバシーモード**)** が割り当てられているユーザーは、** ライセンスとユーザー設定を除くサービスのすべての機能を表示するための読み取り専用アクセス権を持ちます **。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

どちらのオプションも選択しない場合、ユーザーは Citrix Secure Internet Access 機能にアクセスできなくなります。

> 注
>
> Citrix Secure Internet Access Service（アイデンティティおよびアクセス管理）でアクセスが拒否された場合、その管理者のロールは編集できません。Citrix Secure Internet Access Service で管理者を表示および編集するには、管理者を追加したときにフルアクセスまたは読み取り専用アクセスを付与する必要があります。



> 重要
>
> それ以降にユーザーのアクセス権を変更する場合は、Citrix Secure Internet Access サービスのユーザー設定で行う必要があります。［**ID** およびアクセス管理］で編集された管理者の既存の権限は、Citrix Secure Internet Access Service には送信されません。場合によっては、管理者を削除して再度招待する必要が生じることがあります。

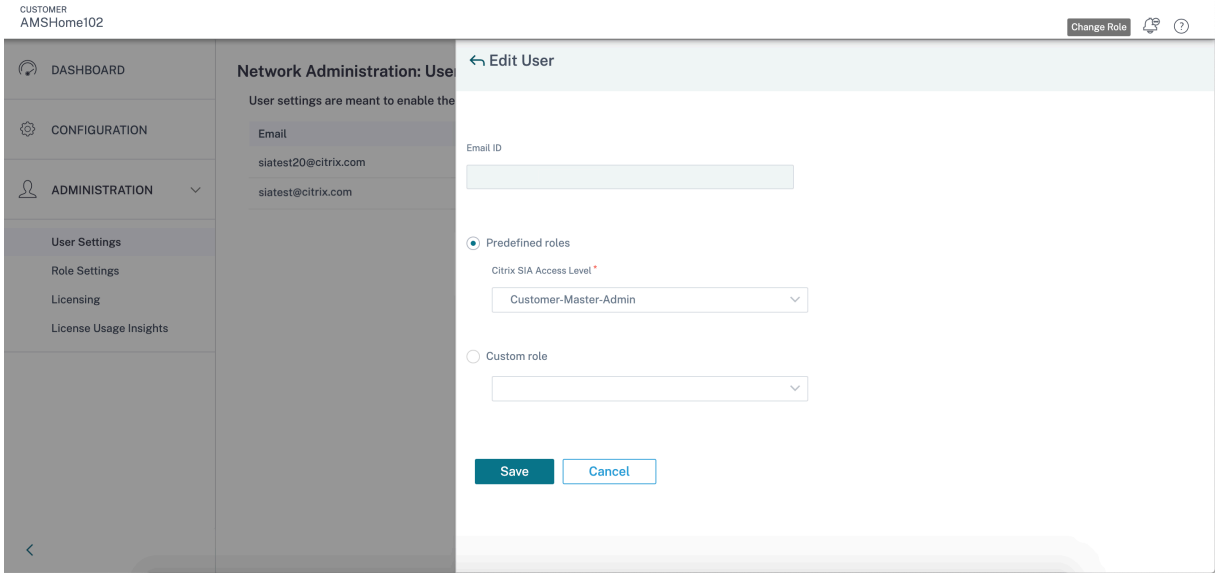
ユーザーロールの設定

このセクションでは、Citrix Secure Internet Access サービスの機能に対する管理者アクセスを詳細に定義および管理する方法について説明します。

> 注**:**
>
> Citrix Secure Internet Access サービスサブスクリプションと Citrix SD-WAN Orchestrator サービスサブスクリプションの両方を所有しているお客様は、[管理] **>** [ユーザー設定] を共有します。

Citrix Secure Internet Access サービスの管理者としての既存のユーザーの役割を編集するには、［管理］>［ユーザー設定］に移動します。定義済みの役割のリストとカスタム役割のリストから、役割を割り当てることができます。いずれかのメニューから適切なロールベースのアクセス権を選択し、選択内容を保存します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

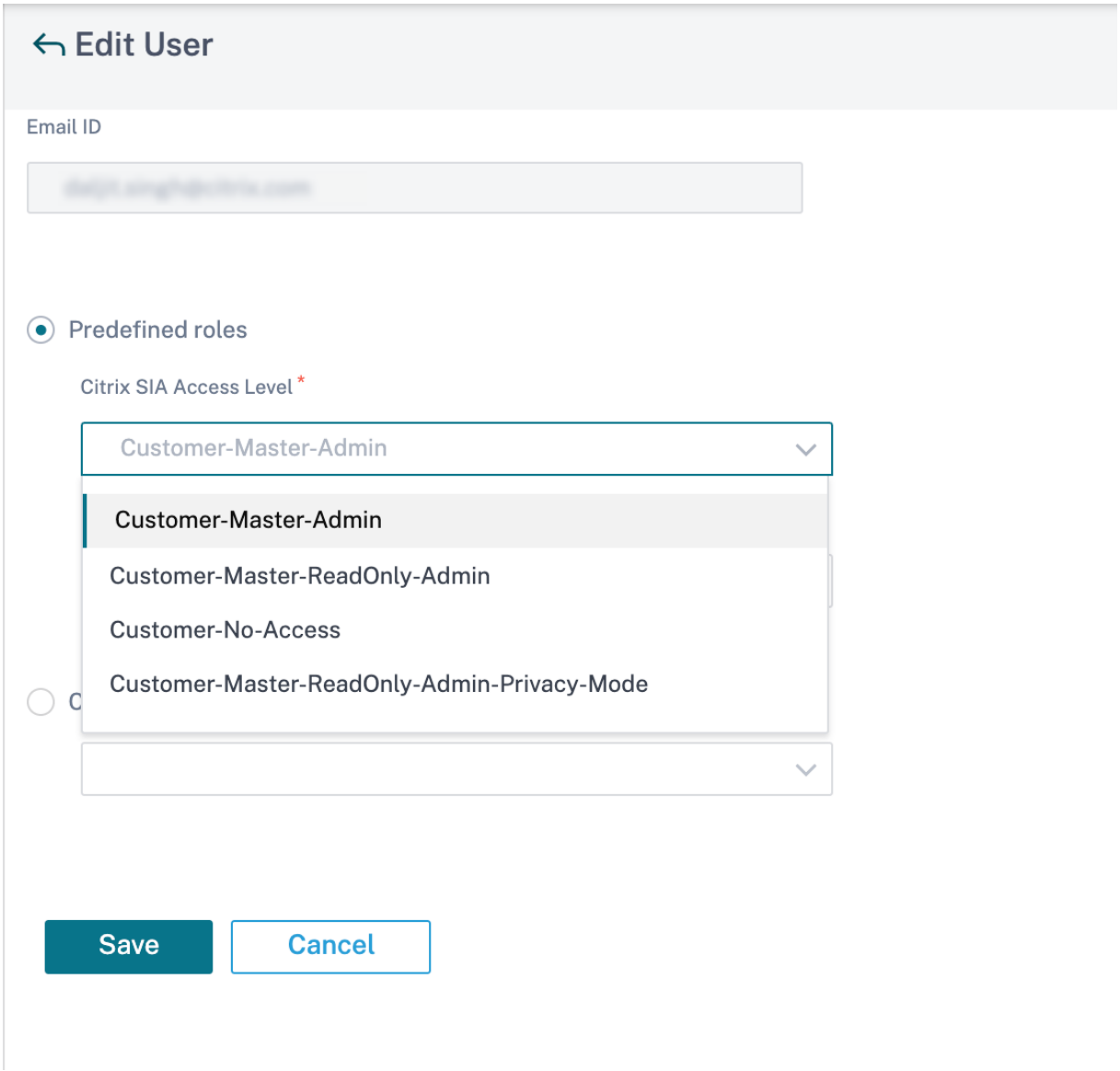


事前定義された役割

Citrix Secure Internet Access サービスでは、顧客レベルで事前定義された役割が **4** つあります。

- カスタマーマスター管理者の役割（デフォルト）により、管理者は **Citrix** Secure Internet Access の情報を表示および編集できます。
- **Customer-master-readonly-Admin** ロールを使用すると、管理者は編集権限なしで Citrix Secure Internet Access の情報を表示できます。
- **Customer-No-Access** ロールは、Citrix Secure Internet Access サービス機能への管理者アクセスを拒否
- **Customer-master-readonly-admin-Privacy Mode** レベルでは、**** ライセンスとユーザー設定を除くすべての **Citrix****Secure Internet Access サービス機能への読み取り専用アクセス権が付与されます。このロールを持つユーザは、自分のアカウント内の他の管理者ユーザ、割り当てられたロール、ライセンス関連情報の一覧を表示できません。

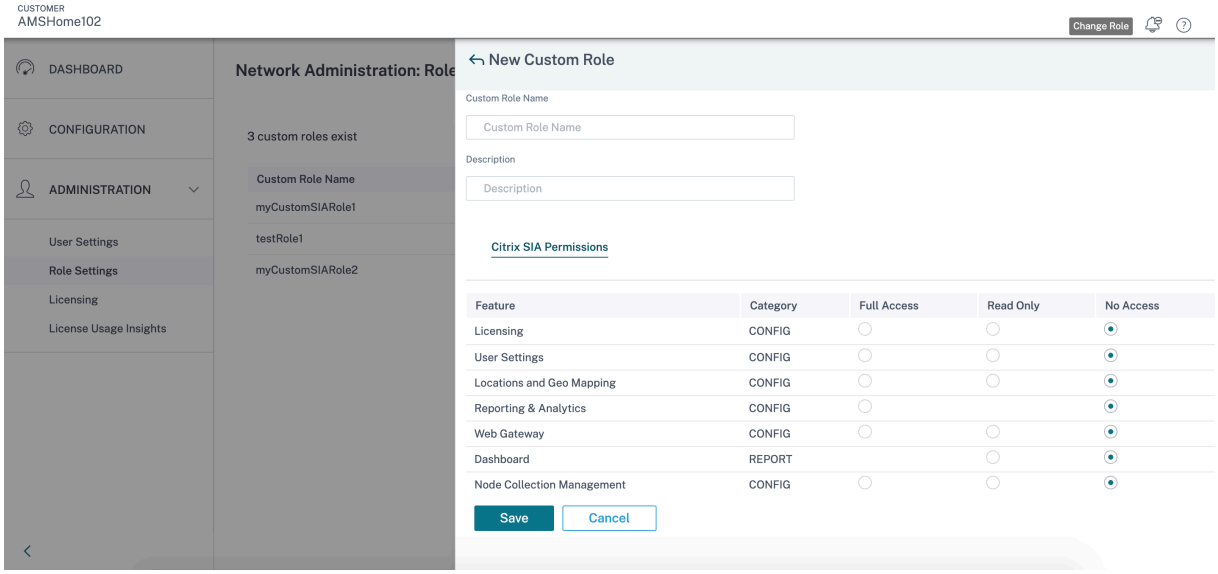
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



カスタムロール

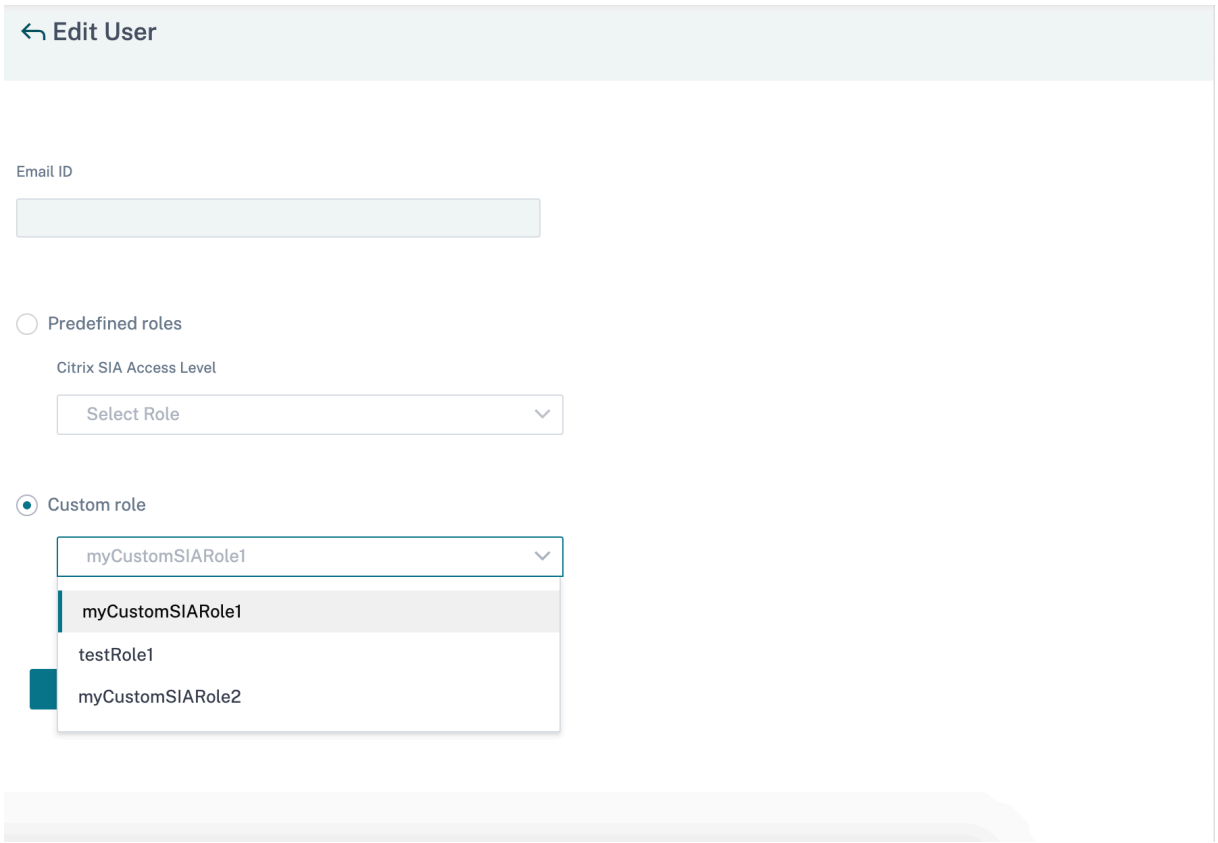
Citrix Secure Internet Access サービスの個々の機能に対するさまざまな権限に基づいて、カスタムの役割を作成できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



管理者に割り当てることができるカスタム管理者ロールを作成するには、[管理] > [ロール設定] に移動します。[新しいカスタムロール] フォームでは、Citrix Secure Internet Access サービスの個々の機能に対して異なるアクセスレベルを選択できます。

作成したカスタムロールは、[ユーザ設定] のカスタムロールの一覧に表示されます。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

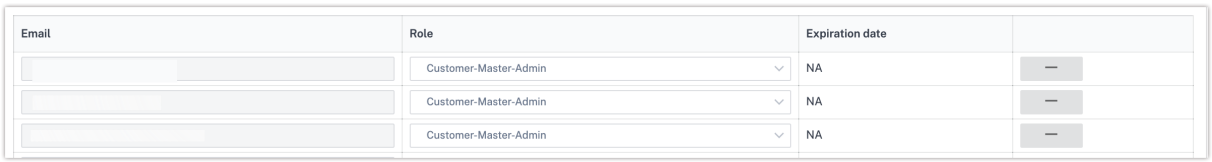
複数のロール

ユーザーが複数の顧客の管理者である場合、Citrix Secure Internet Access Service では複数の役割が割り当てられ、アカウントを切り替えることができます。このようなシナリオでは、ユーザーはアカウントごとに異なるロールを持つことができます。

ロールを切り替えるには、画面右上のベルアイコンの横にある [**Change Role**] を選択します。

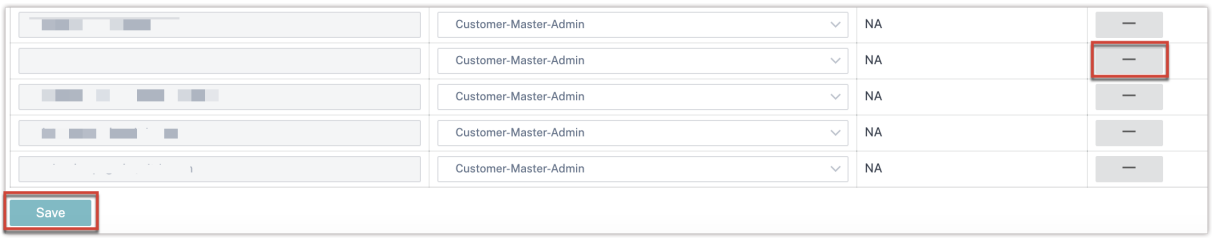
管理者の詳細を表示する

すべての管理者のロールと電子メールアドレスを表示できます。管理者の詳細を表示するには、[管理] > [管理者] に移動します。



管理者を削除する

Citrix Secure Internet Access サービスから管理者を削除するには、［管理］ > ［管理者］ に移動します。削除するアカウントの [削除] ボタンを選択し、[保存] を選択します。



用語集

February 1, 2022

Citrix Cloud: Citrix Cloud は、Citrix サービスをホストおよび管理するプラットフォームです。どのクラウドやインフラストラクチャ（オンプレミス、パブリッククラウド、プライベートクラウド、またはハイブリッドクラウド）を使用する場合でも、コネクタ経由でローカルのリソースに接続します。これにより、アプリとデータを含むワークスペースを 1 つのコンソールからエンドユーザーに作成、管理、デプロイできます。

Citrix SD-WAN: Citrix SD-WAN は、SaaS アプリケーション、仮想デスクトップ、または従来のデータセンターへのアクセスを支援する、信頼性が高く高性能なワークスペースエクスペリエンスにより、ブランチネットワークを簡素化します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Workspace Access：Citrix Secure Workspace Access サービスにより、管理者はシングルサインオン、リモートアクセス、コンテンツ検査を単一のソリューションに統合してエンドツーエンドのアクセス制御を実現する一貫したエクスペリエンスを提供できます。Citrix Secure Workspace Access Service を使用すると、管理者は特定の Web サイトや Web サイトカテゴリへのアクセスをフィルタリングして、組織のネットワークとエンドユーザーデバイスをマルウェアやデータ漏洩から保護することもできます。

Citrix Workspace：Citrix Workspace は、組織内での個人の役割に関連する情報、アプリ、その他のコンテンツへの安全なアクセスを提供できる、完全なデジタルワークスペースソリューションです。ユーザーは、利用可能なサービスをサブスクライブし、場所とデバイスを選ばずにアクセスできます。Citrix Workspace を使用して、ユーザーがコラボレーション、意思決定の改善、作業への完全な集中に必要とする最も重要な詳細を整理および自動化できます。

Citrix Workspace space アプリ：Citrix Workspace アプリを使用すると、ユーザーは使いやすいオールインワンインターフェイスから、すべての SaaS および Web アプリ、ファイルとモバイルアプリ、および仮想アプリとデスクトップに即座にアクセスできます。Citrix Workspace アプリを使用することで、ユーザー用のすべてのワークスペースサービスに 1 か所からアクセスできます。ユーザーは、埋め込み型のブラウザーやシングルサインオンなどの機能を含め、生産性を維持するために必要なすべてのアプリにシームレスかつセキュアにアクセスできます。

Virtual Delivery Agent（VDA）：VDA は Citrix Virtual Apps and Desktops の主要コンポーネントです。サイトでユーザーが利用可能な各物理マシンおよび仮想マシン上に VDA をインストールします。VDA により、これらのマシンが Controller に登録され、ユーザーがこれらのマシンおよびマシン上でホストされるリソースを使用できるようになります。VDA は、マシンとユーザーデバイスとの間の接続を確立して管理します。また、VDA は Citrix ライセンスがユーザーまたはセッションで使用可能であることを確認し、セッションに対して構成されているポリシーを適用します。

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).