ORACLE
Cloud Infrastructure

# Oracle Cloud Infrastructureフェデレーションの Okta構成およびプロビジョニング

ORACLE WHITEPAPER | 2019年2月

ORACLE

# 免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

# 目次

## 概要

このドキュメントは、Oktaによるフェデレーションおよびプロビジョニングのために Oracle Cloud Infrastructureを構成するステップを説明しています。プロビジョニングにより、APIキーおよびOracle Cloud Infrastructure資格証明をフェデレーテッド・ユーザーに追加できます。Oktaは、SAML 2.0をサポートしているため、Oracle Cloud Infrastructureの完全にサポートされたアイデンティティ・プロバイダ(IDP)です。

## 対象読者

このドキュメントの対象読者は次のとおりです。

- Oracle Cloud Infrastructureを評価し、Oktaをアイデンティティ・プロバイダとして使用してOracle Cloud Infrastructureコンソールで認証したいお客様
- Oracle Cloud Infrastructureの機能を顧客環境で実際に紹介したいコンサルタントおよびソリューション・アーキテクト

## サポートされている機能

Oracle Cloud Infrastructure (OCI)は、次のプロビジョニング機能をサポートしています。

- ユーザーの作成: Okta内の新規または既存ユーザーは、OCIにプッシュされ、フェデレーテッド・ユーザーとしてOCIコンソールに表示されます。
- ユーザーの非アクティブ化: Oktaで非アクティブ化されたユーザーは、OCIで自動的に非アクティブ化されます。
- グループのプッシュ: OktaグループをOCI内のグループにマップできます。

次の機能は、OCIではサポートされていません。

- ユーザーのインポート
- グループのインポート
- パスワードの同期
- ユーザー属性の更新

## 必要条件

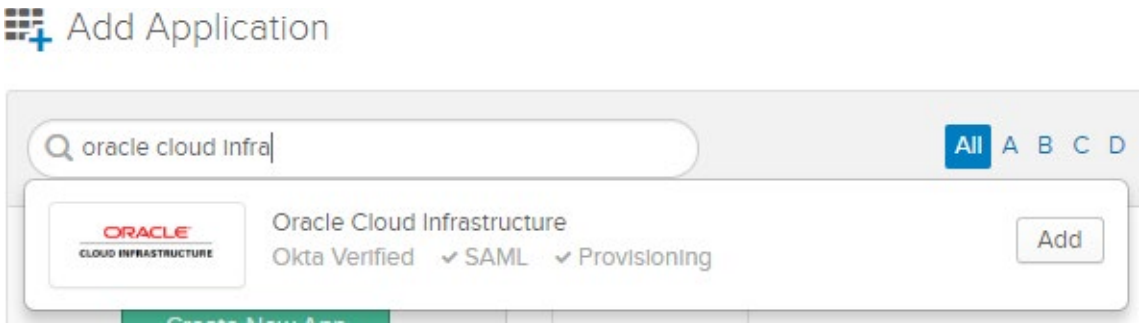
プロセスを開始する前に、次の前提条件を満たしていることを確認してください。

- Oktaアプリケーションを作成できるOktaアカウントを持っていること。Enterpriseアカウントと Developerアカウントのいずれでも構いません。
- 1人以上の管理ユーザーおよび1つ以上のグループが設定されているOracle Cloud Infrastructureテナンシを保有していること。
- Oktaでは、OCIAdminsまたはOCIUsersなどの簡単に認識できる接頭辞を使用してOracle Cloud Infrastructureにアクセスするためのグループを設定することをお薦めします。また、作成した各グループには、ユーザーも必要です。
- アイデンティティ・フェデレーションの一般的な概念に精通していること。

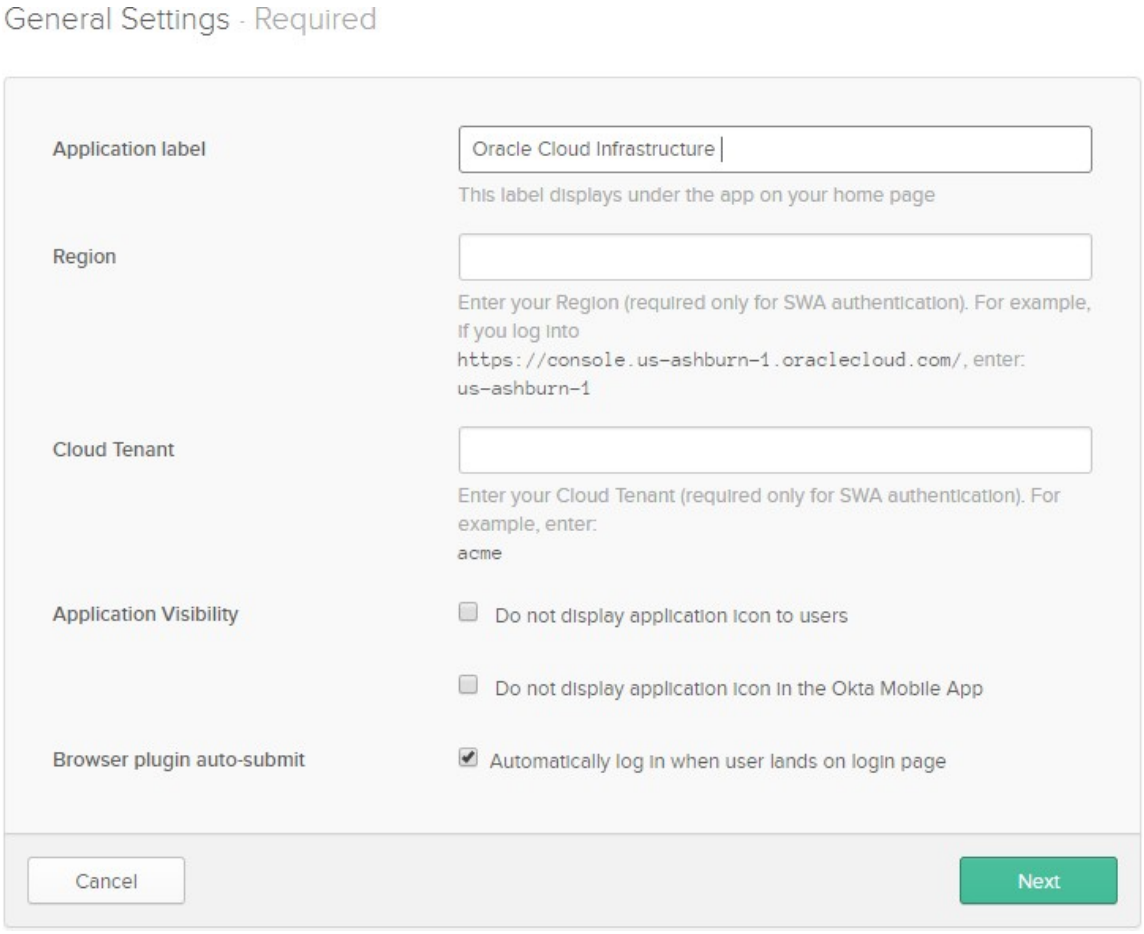
## 構成手順(段階的な説明)

1. Oktaアカウントにログインします。

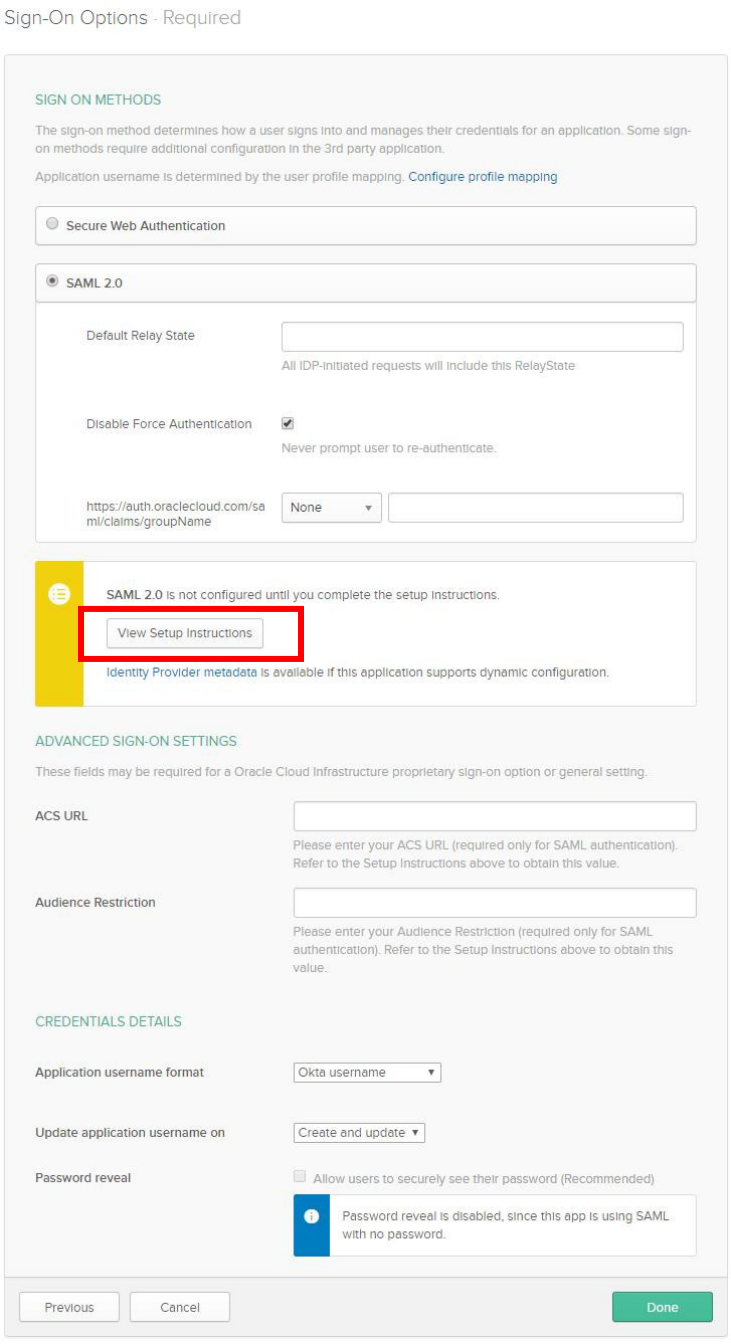
2. 「**Add Application**」をクリックします。"Oracle Cloud Infrastructure"を探し、「**Add**」をクリックします。



3. 次のスクリーンショットに示すように、"Oracle Cloud Infrastructure"などの理解しやすいアプリケーション・ラベルを入力します。「**Region**」および「**Cloud Tenant**」フィールドは無視してください。「**Next**」をクリックします。



4. 「**Sign On**」タブをクリックし、「**Edit**」ボタンをクリックします。「**View Setup Instructions**」をクリックし、詳細説明を表示して、SAML設定を完了します。設定の説明に従います。(この説明は、ここでも参照できます。)




5. 「**General**」タブ、「**Sign On**」タブおよび「**Import**」タブのデフォルト設定はそのままにします。

6. 「**Provisioning**」をクリックし、次に「**Configure API Integration**」をクリックします。「**Enable API Integration**」を選択します。

   「**API Integration**」設定を完了するには、SCIMベースURLおよび資格証明(ユーザー名およびパスワード)を入力する必要があります。これらの入手方法を次に示します。

   SCIMベースURLは次の規則に従います:

   https://<OCI-region-name>.scim.oci.oraclecloud.com/v2

   <OCI-region-name>は、ステップ4で取得したACSの場所URLのリージョン名と同じです。たとえば、ACSの場所URLは次のようになります。

   https://auth.**us-ashburn-1**.oraclecloud.com/v1/saml/ocid1.tenancy.oc1..aaaaaakdjsk...

   リージョン名は次のとおりです: us-ashburn-1

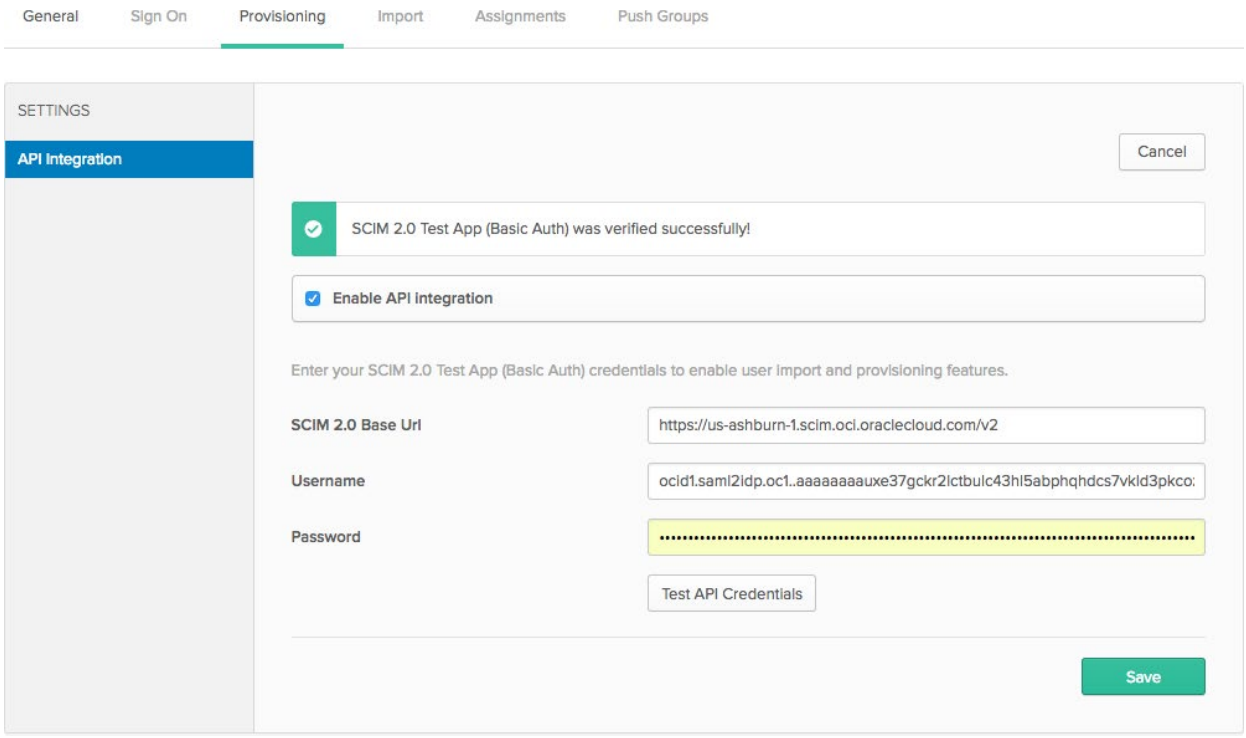
   ユーザー名およびパスワードは、Oracle Cloud Infrastructure設定のクライアントIDおよびシークレットです。

   - OCIコンソールで、「フェデレーション」詳細ページに移動し、ここで、Oktaフェデレーションを設定します。ナビゲーション・メニューを開き、「**ガバナンスと管理**」で「**アイデンティティ**」に移動し、「**フェデレーション**」をクリックします。Oktaフェデレーションに割り当てた名前をクリックし、詳細ページを表示します。

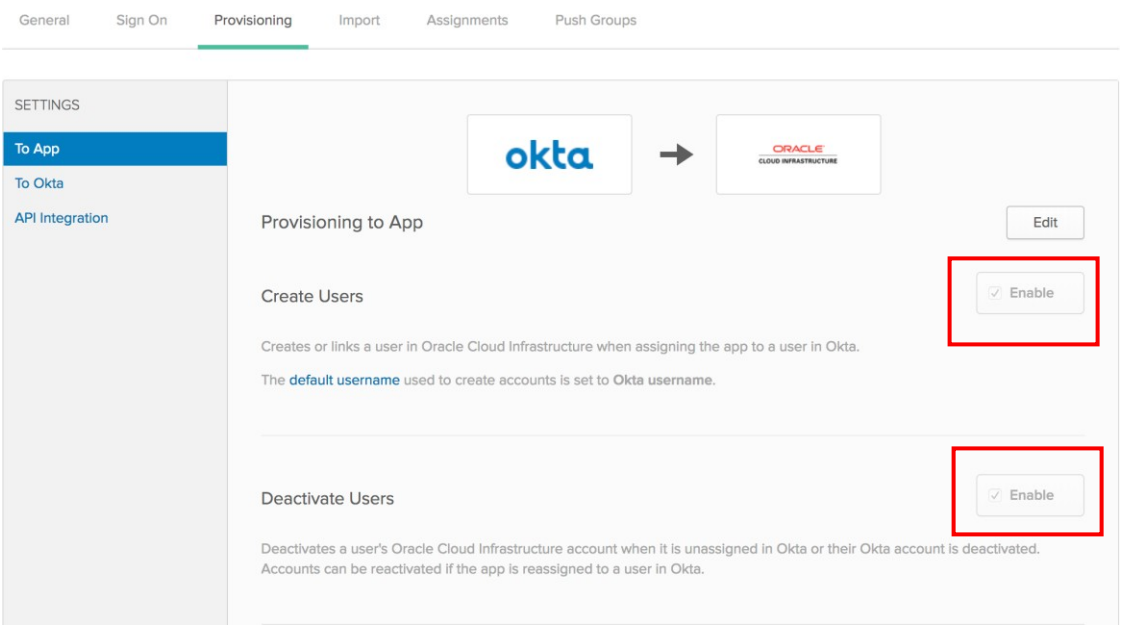
   - 次のスクリーンショットに示された「**資格証明のリセット**」をクリックし、資格証明を表示します。クライアントIDおよびシークレットをコピーします。

7. (Oktaの)「**API Integration**」設定で、「**Username**」テキスト・ボックスにクライアントIDを入力します。「**Password**」テキスト・ボックスにシークレットを入力します。

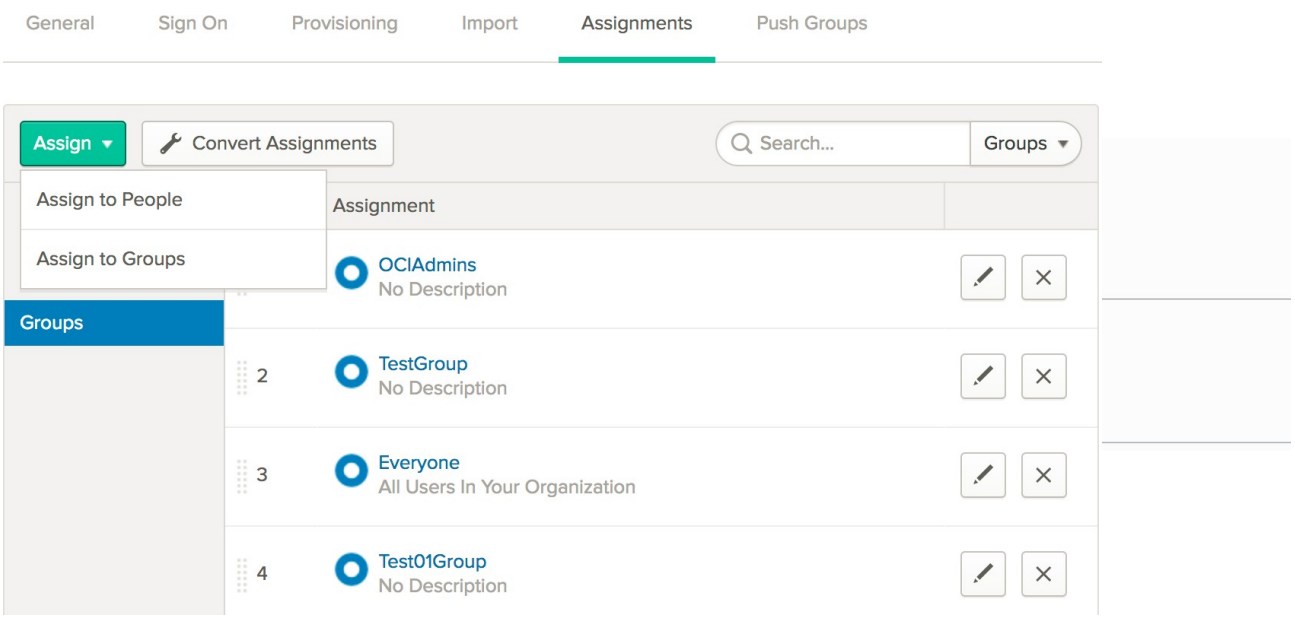
8. 「**Test API Credentials**」をクリックし、資格証明が正しいことを確認します。成功の確認メッセージが表示されれば、正しく機能していたことになります。「**Save**」をクリックします。



9. 前のステップを完了すると、「**To App**」および「**To Okta**」構成が「**Settings**」の下に作成されます。「**Provisioning to App**」設定で、「**Create Users**」および「**Deactivate Users**」を有効化します。




10. 「**Assignments**」タブをクリックします。次のスクリーンショットに示すように、Oracle Cloud Infrastructureへのログインを可能にするグループまたは個人に、このアプリケーションを割り当てる必要があります。



# 既知の問題/トラブルシューティング

- OktaグループをOCIに手動でプッシュしない限り、Oktaグループのリストが OCIグループ・マッピング・ダイアログ・ボックスに表示されません。詳細は、Oktaヘルプ・トピックのグループ・プッシュの使用を参照してください。
- グループのプッシュの完了後、グループがOracle Cloud Infrastructureコンソールにただちに表示されません。「**Edit Mappings**」をクリックして、グループをOCIグループに手動でマップする必要があります。
- ユーザーがOktaで非アクティブ化された場合、ユーザーはOCIに引き続き存在しますが、Okta資格証明を使用できません。
- グループをプッシュする際、Oracle Cloud Infrastructureは、Oracle Cloud Infrastructureで作成された既存のグループとOktaで作成されたグループの関連付けをサポートしません。

**Oracle Corporation, World Headquarters**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates.All rights reserved.本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否定し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。*0219*

Oracle Cloud Infrastructureフェデレーションの Okta構成およびプロビジョニング
2019年2月
著者: オラクル社

Oracle is committed to developing practices and products that help protect the environment