Parallels Remote Application Server

SAML SSO 認証の例

19.2

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

目次

はじめに 4

前提条件 5

SAML 2.0 による Azure との統合 6

汎用 SAML アプリケーションの作成 6

Parallels RAS 用の Azure アプリケーションの構成 8

接続のテスト 14

SAML 2.0 による Okta Identity Cloud との統合 17

要件 17

Parallels RAS のサービス プロバイダー構成 17

Okta ID の IdP 構成 20

アプリケーションの作成 21

SAML 設定の構成 23

Parallels RAS 構成の完了 28

接続のテスト 30

SAML 2.0 による Ping ID との統合 32

汎用 SAML アプリケーションの作成 32

Parallels RAS のサービス プロバイダー構成 35

SAML アプリケーション構成の完了 39

接続のテスト 42

SAML 2.0 による Thales SafeNet Trusted Access との統合 44

汎用 SAML アプリケーションの作成 44

Parallels RAS のサービス プロバイダー構成 51

接続のテスト 54

第 1 章

はじめに

本書では、Parallels ® RAS で SAML 2.0 シングル サインオン (SSO) 認証を構成する方法と、SAML サービス プロバイダー (SP) として、SAML ID プロバイダー (IdP) として構成されたサードパーティの ID 管理ソリューションと Parallels RAS を統合する方法について順を追って説明します。本書で扱う IdP には、Microsoft Azure、Okta Identity、Ping Identity、Thales の Safenet が含まれます。SAML 2.0 SSO をサポートするその他の ID 管理ソリューションも、Parallels RAS で IdP として使用できます。

SAML は、ローカルの ID データベースを共有せずにユーザー認証を可能にすることで、異なる組織間でシングル サインオン (SSO) 機能を提供する XML ベースの認証メカニズムです。SAML SSO 認証プロセスの一環として、新しい Parallels RAS Enrollment Server は Microsoft 認証局 (CA) と通信し、ユーザーに代わってデジタル証明書の要求、登録、および管理を行い、ユーザーが Active Directory 認証情報を入力することなく認証を完了します。

複数の子会社を抱えるサービス プロバイダーや企業は、独自の内部 ID 管理ソリューションの維持やドメイン/フォレストの複雑な信頼関係を構築する必要はありません。サードパーティの SAML ID プロバイダーとの統合により、顧客およびパートナーは、エンドユーザーに真の SSO エクスペリエンスを提供できます。

第 2 章

前提条件

Parallels RAS で SAML SSO 認証を使用するための前提条件は、本書で説明するすべての SAML ID プロバイダーで共通です。システム要件および必要な RAS コンポーネントのインストールおよび構成方法の詳細は、「**Parallels RAS 管理者ガイド**」の「**SAML SSO 認証**」の章を参照してください。このガイドは、Parallels の Web サイトから入手できます (https://www.parallels.com/jp/products/ras/resources/) 。

第 3 章

SAML 2.0 による Azure との統合

この章の内容

汎用 SAML アプリケーションの作成.....6
Parallels RAS 用の Azure アプリケーションの構成.....8
接続のテスト.....14

汎用 SAML アプリケーションの作成

まず、以下のように Microsoft Azure で汎用 SAML アプリケーションを作成する必要があります。

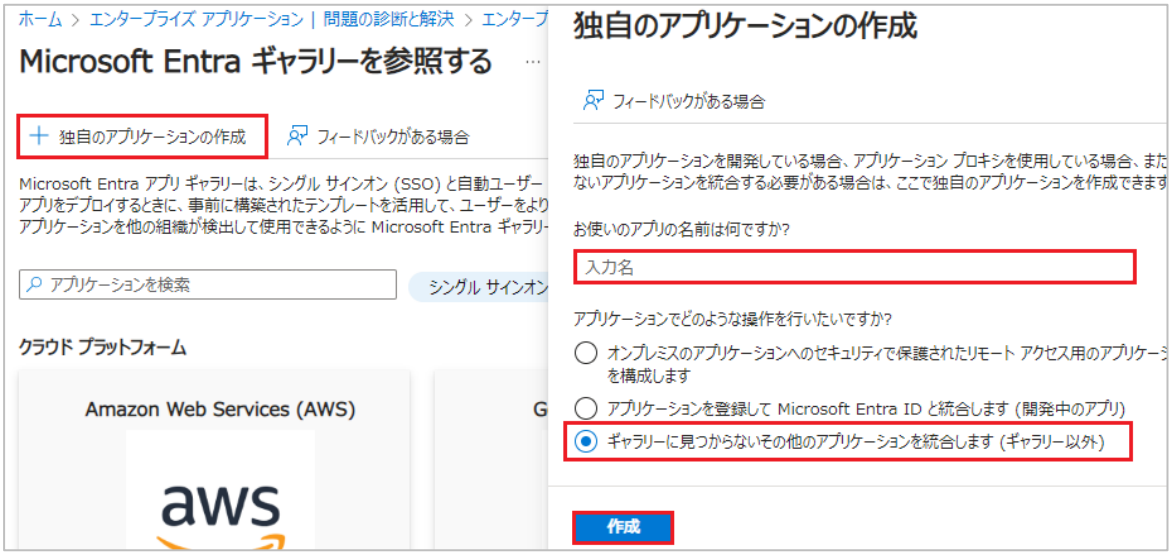
1 Azure Portal にサインインします。

2 ポータルメニューを開き、[**すべてのサービス**] > [**Microsoft Entra ID**] の順にクリックします。

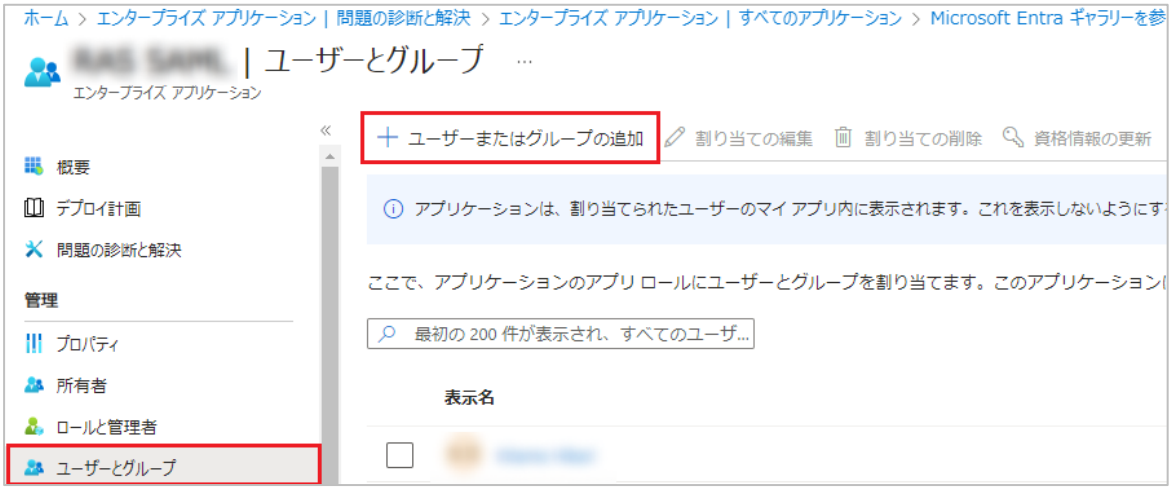
3 [**エンタープライズ アプリケーション**] をクリックします。

4 [**新しいアプリケーション**] をクリックします。

5 [**独自のアプリケーションの作成**] をクリックします。「独自のアプリケーションの作成」ページにて、[アプリの名前] を入力し、[**ギャラリー以外**] オプションを選択後に、[**作成**] をクリックしてアプリケーションを作成します。



6 作成したアプリケーションに対して、SAML SSO を使用するために必要なユーザーを追加します。左ペインで [**ユーザーとグループ**] を選択します。[**ユーザーまたはグループの追加**] をクリックし、ユーザーを選択します。



Parallels RAS 用の Azure アプリケーションの構成

Parallels RAS と連携するように Azure アプリケーションを構成する手順は以下の通りです。

1 先の節で作成したアプリケーションの左ペインで [**シングル サインオン**] を選択します。[**SAML**] をクリックし、「SAML ベースのサインオン」ページに遷移します。

2 「**(3) SAML 証明書**」セクションで、[**アプリのフェデレーション メタデータ URL**] の値をコピーします。

注 : 手動で設定する場合は、対応する [**ダウンロード**] リンクをクリックして、「**証明書 (Base 64)** 」と「**フェデレーション メタデータ XML**」をダウンロードできます。

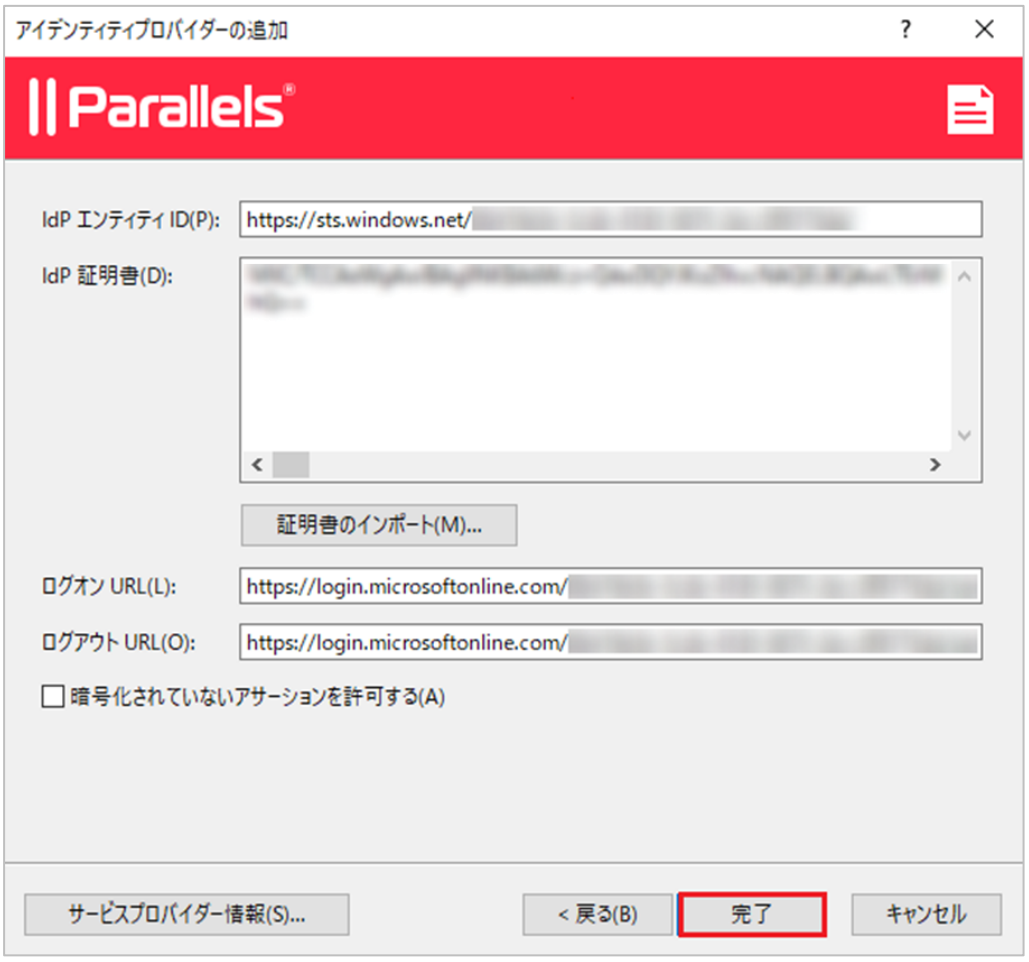
3 RAS Console を開き、[**接続**] > [**SAML**] タブに遷移し、[+] ボタン (または [**タスク**] > [**追加**]) をクリックします。

4 「**アイデンティティ プロバイダーの追加**」ウィザードで、ファイルから IdP メタデータをインポートするか、URL を指定して、IdP を関連付けるユーザー ポータル テーマを選択します。

5 [**次へ**] をクリックします。

6 ウィザードの次のページで、[**IdP 証明書**] と [**ログオン/ログアウト URL**] フィールドが自動的に入力されます。すべてが正しいことを確認し、[**完了**] をクリックします。

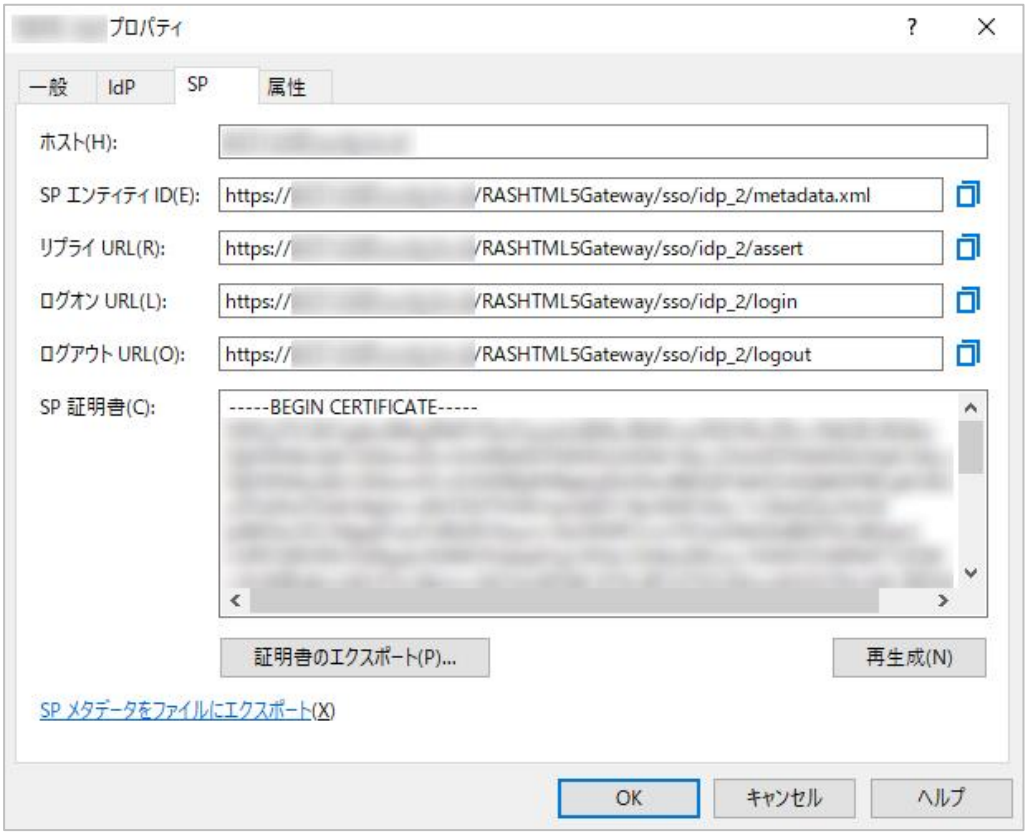
重要：Azure で暗号化アサーションを構成していない場合は、[**暗号化されていないアサーションを許可する**] オプションをオフにする必要があります。



7 RAS Console に戻り、先ほど作成した IdP プロバイダーを右クリックし、[**プロパティ**] を選択します。

8 開いたダイアログで、[**SP**] タブを選択します。

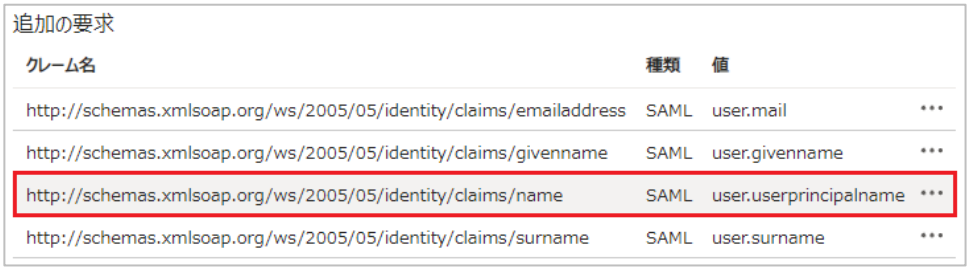
9 ホスト アドレスを入力します。IdP は、エンドユーザーのブラウザからアクセス可能な、このアドレスにリダイレクトします。このタブに表示されるその他の情報に注意してください。



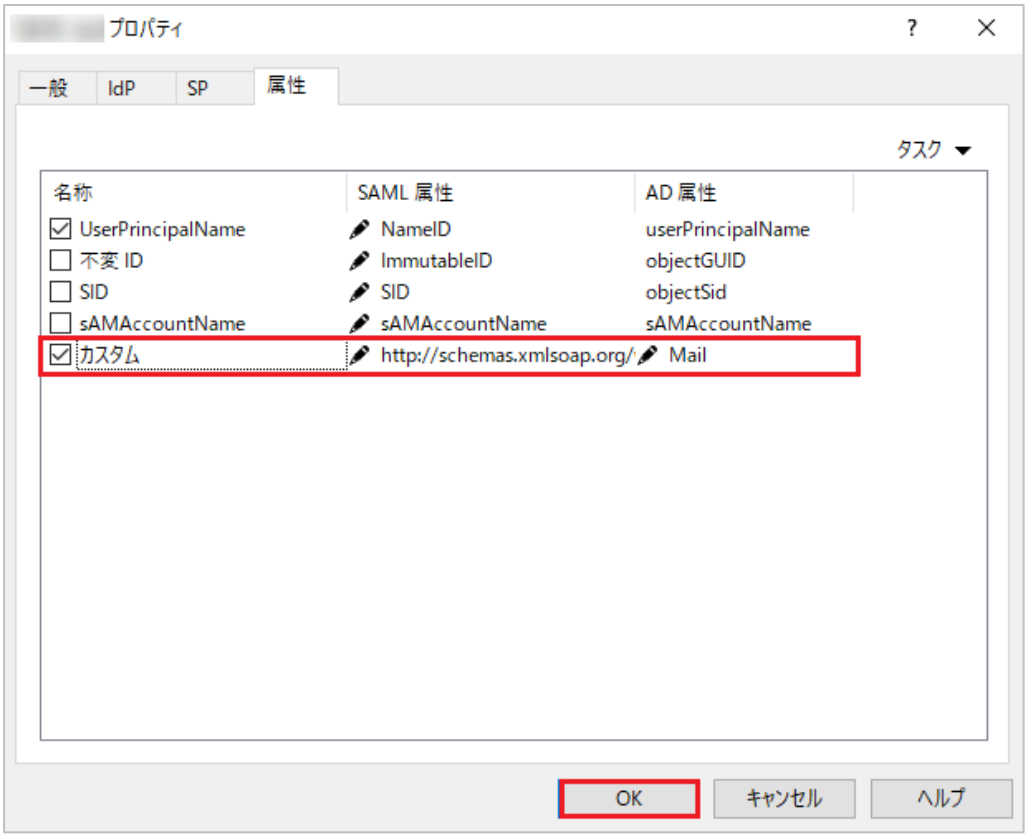
10 Azure Portal で SAML アプリケーションに切り替えます。RAS Console (上記参照) の [**SP**] タブの値に従って、「**(1) 基本的な SAML 構成**」セクションの値を設定します。

11 次に、IdP ユーザーと AD ユーザーを照合するように属性を設定します。この例では、以下の設定でカスタム属性を使用します。

- Azure Portal > [**SAML**] アプリ > [**シングル サインオン**] で、「**(2) 属性とクレーム**」セクションを開きます。
- [**クレーム名**] の一覧から、[**user.userprincipalname**] 値のクレーム名をコピーします。必要に応じて、他のカスタム要求を追加できます。



12 RAS Console に戻り、「**IdP プロバイダーのプロパティ**」ダイアログで、[**属性**] タブを選択し、[**カスタム**] 属性を有効にして、前の手順でコピーしたクレーム名に入力します。任意の属性を使用できるため、これは単なる例であることに注意してください。この特定のケースでは、(Azure へのログインに使用される) Azure ログイン ユーザー名/メールアドレスが、Active Directory で構成されているユーザーのメールアドレスと照合されます。



Microsoft Entra Connect を使用して、「Immutable ID」を介してユーザーを照合することもできます。そのためには、Active Directory で以下の値を使用して属性を作成します。

- **名前**: ImmutableID
- **ソース**: 属性
- **ソース属性**: user.onpremisesecurityidentifier

詳細については、docs.microsoft.com を参照してください。

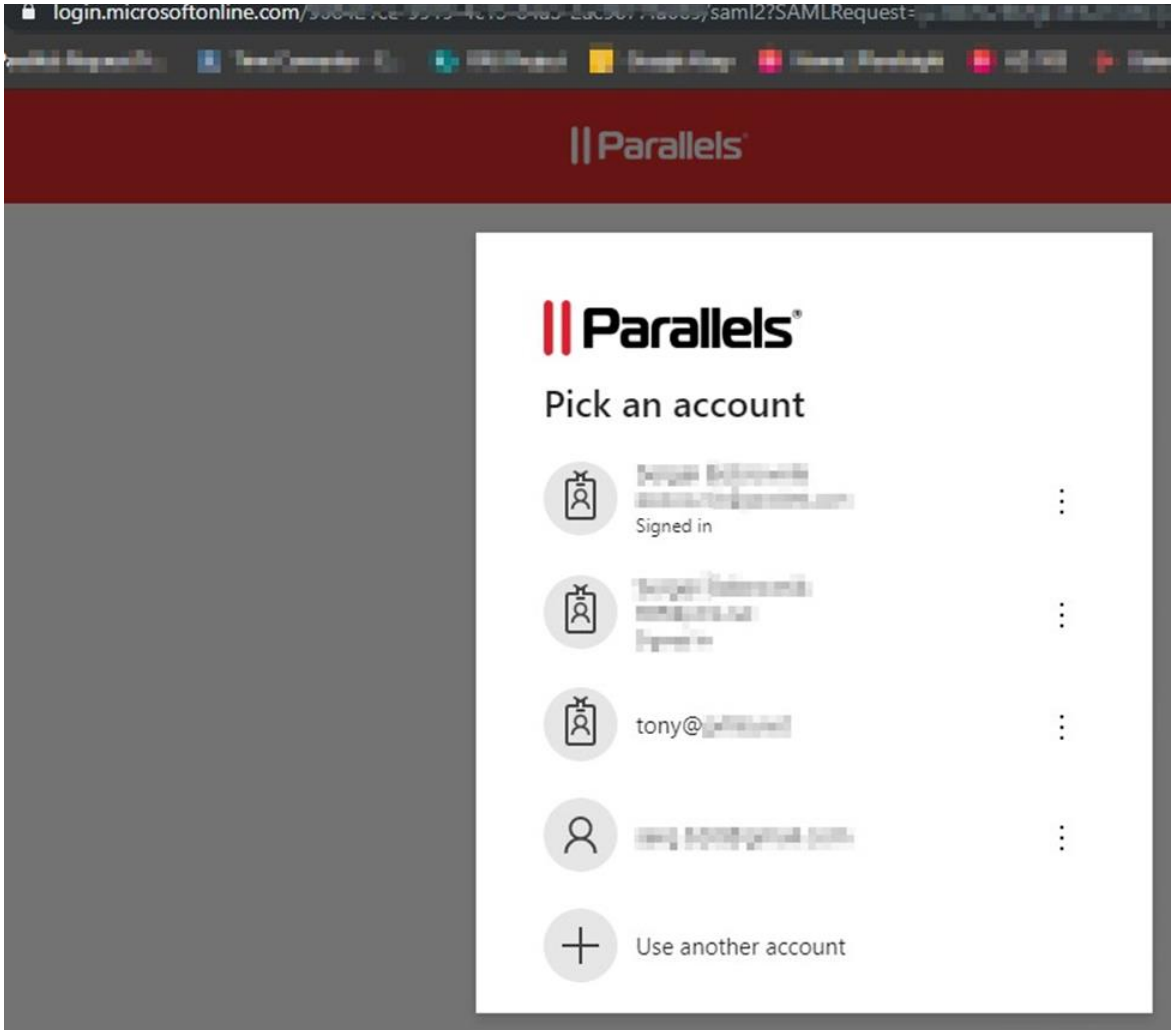
接続のテスト

SP 開始

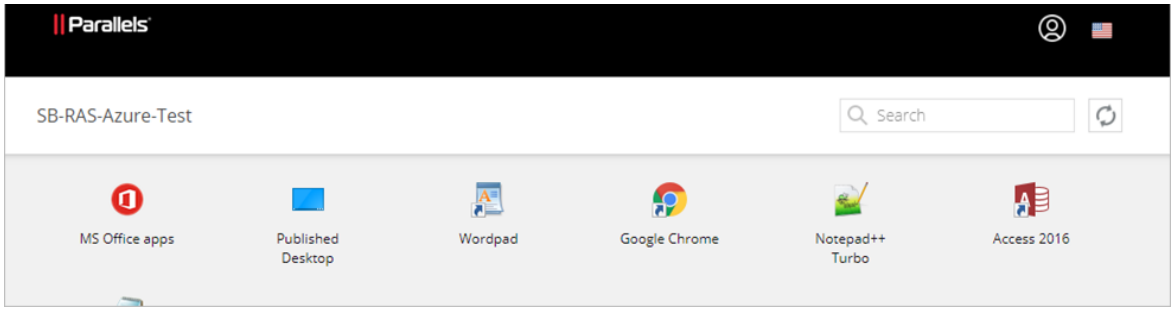
Parallels RAS と Microsoft Azure 間の接続をテストする手順は以下の通りです。

1 ウェブ ブラウザで [ユーザー ポータル] を開きます。SAML アプリに関連付けたテーマを使用します。

2 問題がなければ、login.microsoft.online にリダイレクトされ、サインインを続行できます。



3 認証が成功すると、ユーザーにアプリケーション リストが表示されます。



IdP 開始

1 Microsoft Azure portal にログインし、割り当てられたアプリケーションを起動します。

2 ユーザーは、割り当てられたテーマを使用してユーザー ポータルにリダイレクトされ、アプリケーション リストが表示されます。

第 4 章

SAML 2.0 による Okta Identity Cloud との統合

この章の内容

要件 17
Parallels RAS のサービス プロバイダー構成 17
Okta ID の IdP 構成 20
Parallels RAS 構成の完了 28
接続のテスト 30

要件

Okta Identity でアプリケーションを構成するには、SP アプリケーションから以下の設定が必要です。

- アサーション コンシューマ サービス (ACS) URL
- 対象ユーザーURI
- 必要な SAML 属性

したがって、RAS の設定から始める必要があります。

Parallels RAS のサービス プロバイダー構成

ID プロバイダー (IdP) を追加して、Parallels RAS をサービス プロバイダー (SP) として構成する必要があります。この手順は、後で Okta を IdP として設定することで完了します。

まず、RAS Console で ID プロバイダー (IdP) を以下のように追加します。

1 [**接続**] > [**SAML**] タブに遷移し、[+] ボタン (または [**タスク**] > [**追加**]) をクリックします。

2 プロバイダー名 (例 : Okta) を指定します。

3 [**テーマと一緒に使用する**] フィールドで、デフォルトの「<使用せず>」オプションをそのまま使用します。

4 [**IdP 情報を手動で入力します**] オプションを選択し、[**次へ**] をクリックします。

5 次のページで、フィールドを空白にしないように要件を満たす情報を入力し (後でメタデータファイルを使用して Okta 設定をインポートします)、[**完了**] をクリックします。

6 RAS Console の下部にある [**適用**] をクリックして、設定を適用します。

SP 設定 (メタデータ) のエクスポート

サービス プロバイダー設定をエクスポートするには、以下の操作を行います。

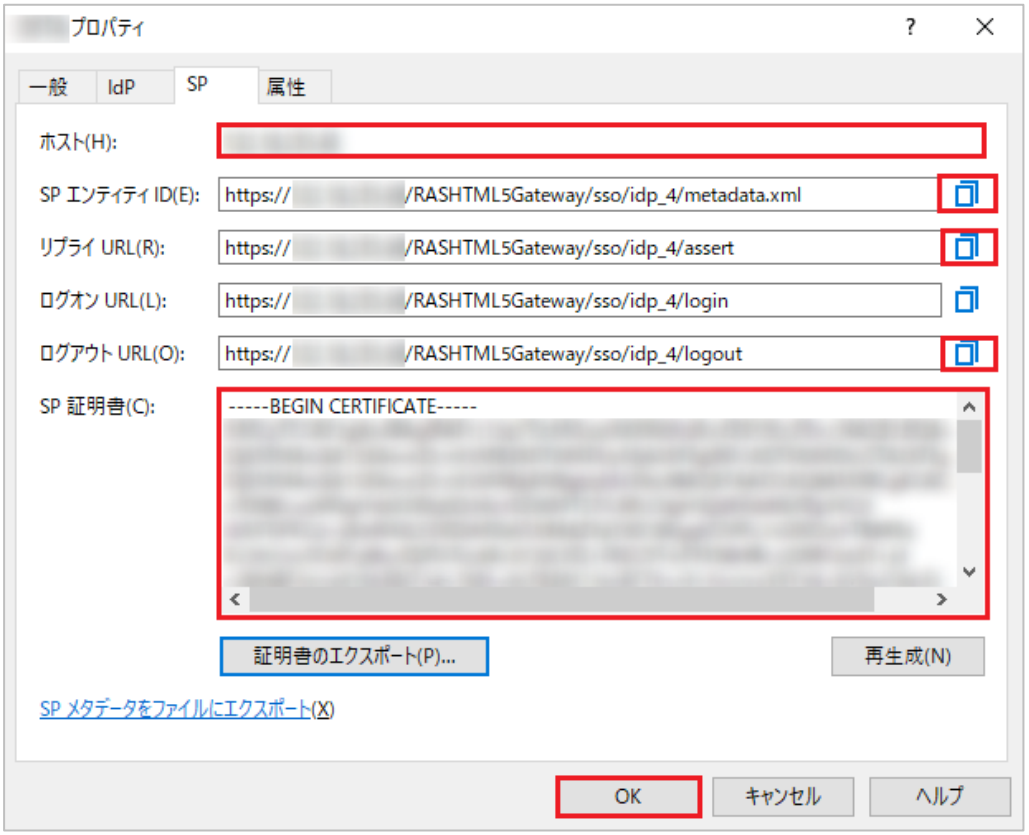
1 RAS Console で、前の手順で作成した「Okta」IdP プロバイダーを右クリックし、[**プロパティ**] をクリックします。

2 開いたダイアログで、[**SP**] タブを選択します。

3 [**ホスト**] フィールドに外部 FQDN または IP アドレスを指定します。

4 [**SP エンティティ ID**] フィールドと [**リプライ URL**] フィールドの値をコピーして保存します。

5 シングル ログアウト オプションを使用する場合は、[**ログアウト URL**] フィールドの値をコピーして保存します。また、[**SP 証明書**] フィールドの値をコピーし、拡張子が「.cer」のテキスト ファイルとして保存します。



以上で、Okta の構成に進む準備が完了しました。

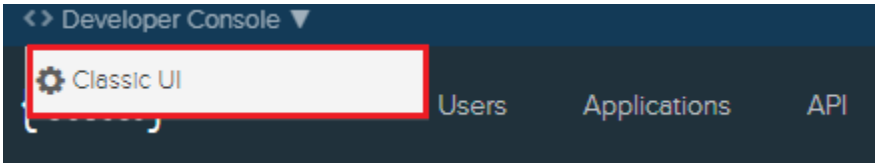
Okta ID の IdP 構成

EPC サーバーの DNS エイリアス (以下の例で使用する epc.company.com など) が定義されていることから、Okta でアプリケーションを作成する必要があります。

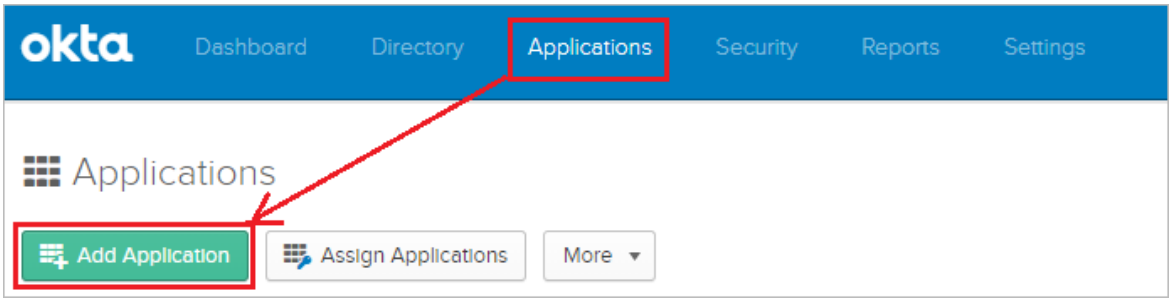
アプリケーションの作成

以下のように Okta でアプリケーションを作成します。

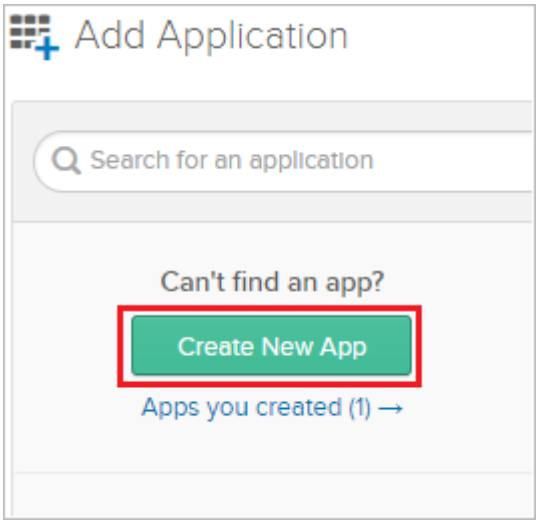
1 Okta Admin Console を開き、クラシック UI に切り替えます。



2 [**Applications** (アプリケーション)] リンクをクリックし、[**Add Application** (アプリケーションの追加)] をクリックします。

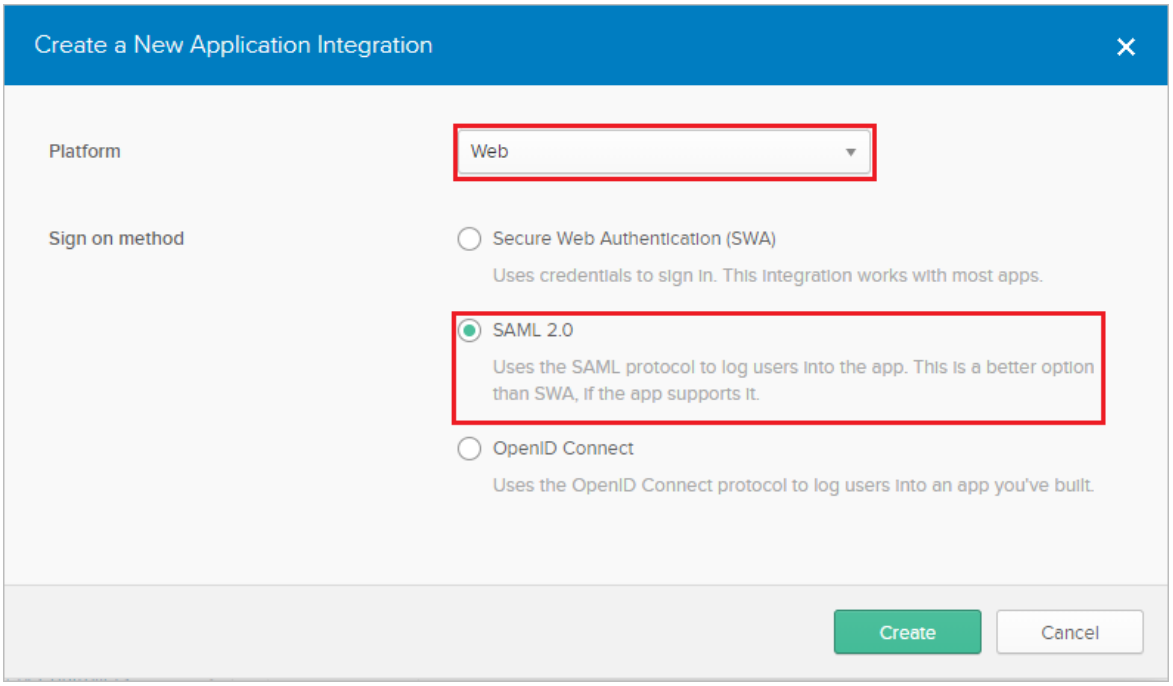


3 [**Create New App** (新規アプリの作成)] をクリックします。

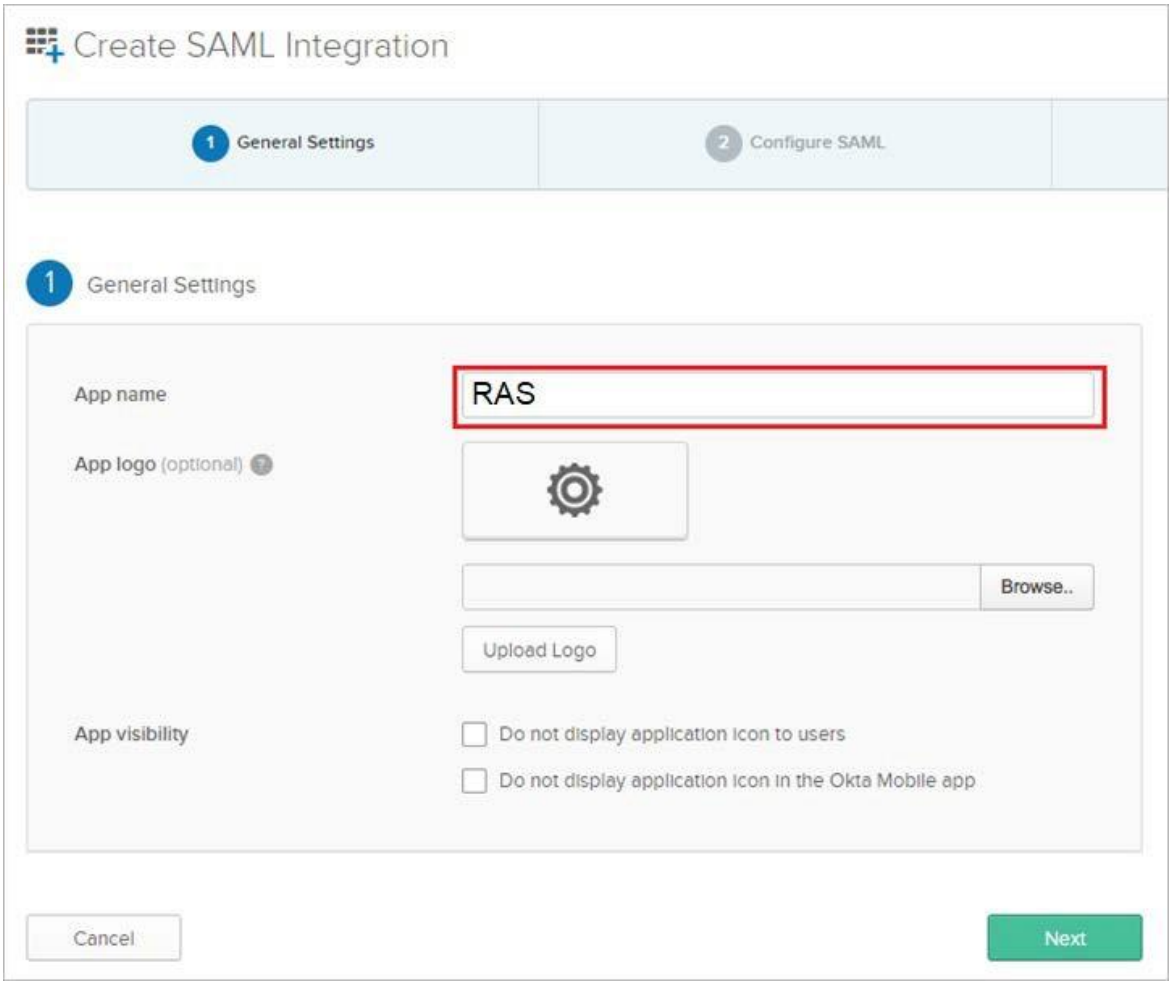


4 [**Platform** (プラットフォーム)] フィールドで「Web」を選択し、[**Sign on method** (サインオン方式)] セクションで「SAML 2.0」プロトコルを選択します。

5 [**Create** (作成)] をクリックします。



6 [**App name** (アプリ名)] フィールドに、構成の名前 (例 : RAS) を入力し、[**Next** (次へ)] をクリックします。



SAML 設定の構成

一般設定

[**Configure SAML** (SAML の設定)] ビューで、以下を指定します。

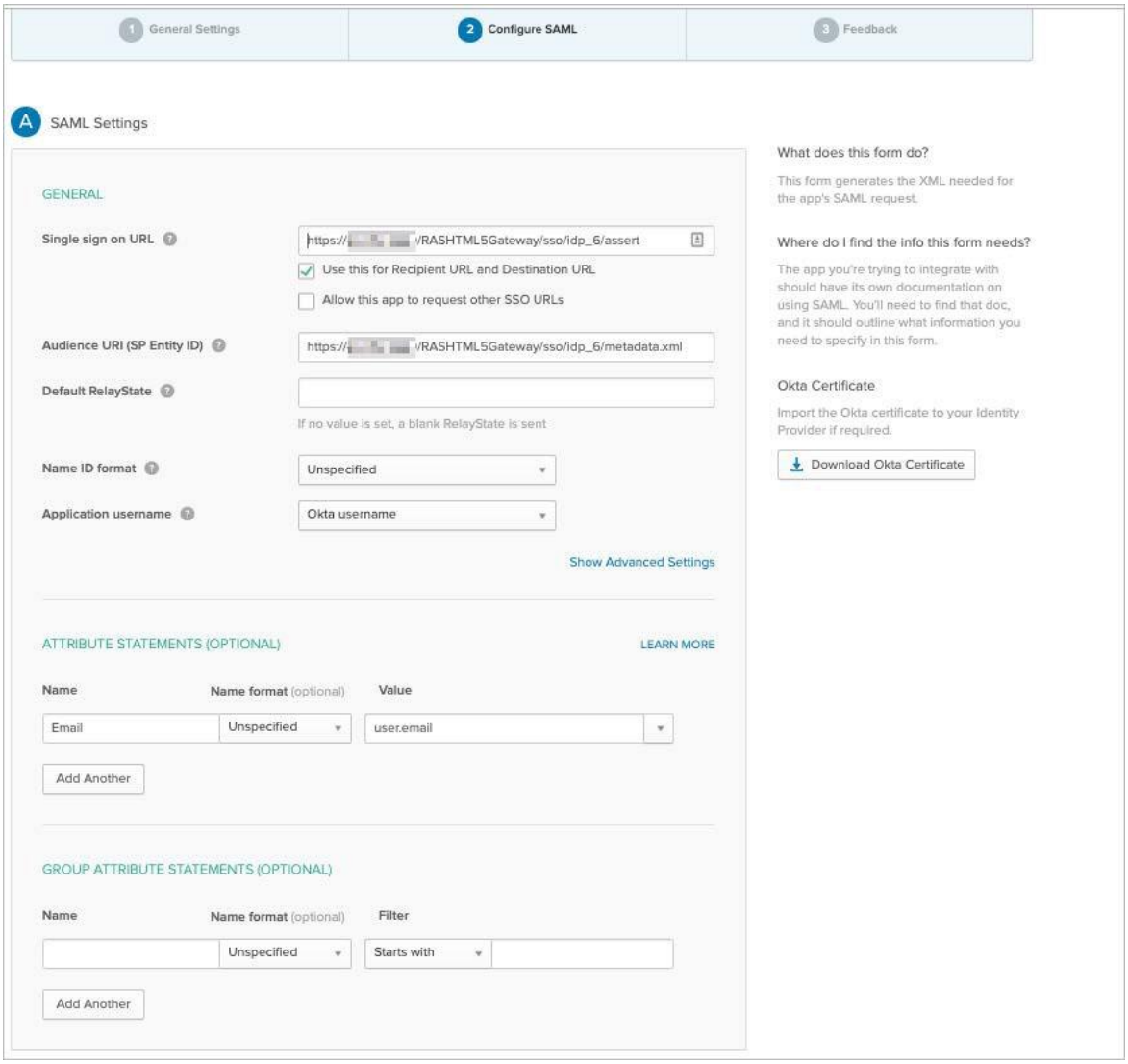
- **Single sign on URL** (シングル サインオン URL) : RAS サーバーから取得した [**リプライ URL**] の値を貼り付けます。
  例 : https://40.85.122.19/userportal/sso/idp_6/assert

  [**Use this for Recipient URL and Destination URL** (受信者 URL と宛先 URL に使用します)] オプションを選択したままにします。

- **Audience URI (SP Entity ID)** (オーディエンス URI (SP エンティティ ID)) : RAS サーバーから取得した [**SP エンティティ ID**] の値を貼り付けます。
  例 : https://40.85.122.19/userportal/sso/idp_6/metadata.xml

- **Default RelayState** (デフォルト RelayState) : 空白のままにします。

- **Name ID format** (名前 ID の形式) : 「Unspecified」の値のままにします。
- **Application username** (アプリケーション ユーザー名) : 「Okta username」値のままにします。



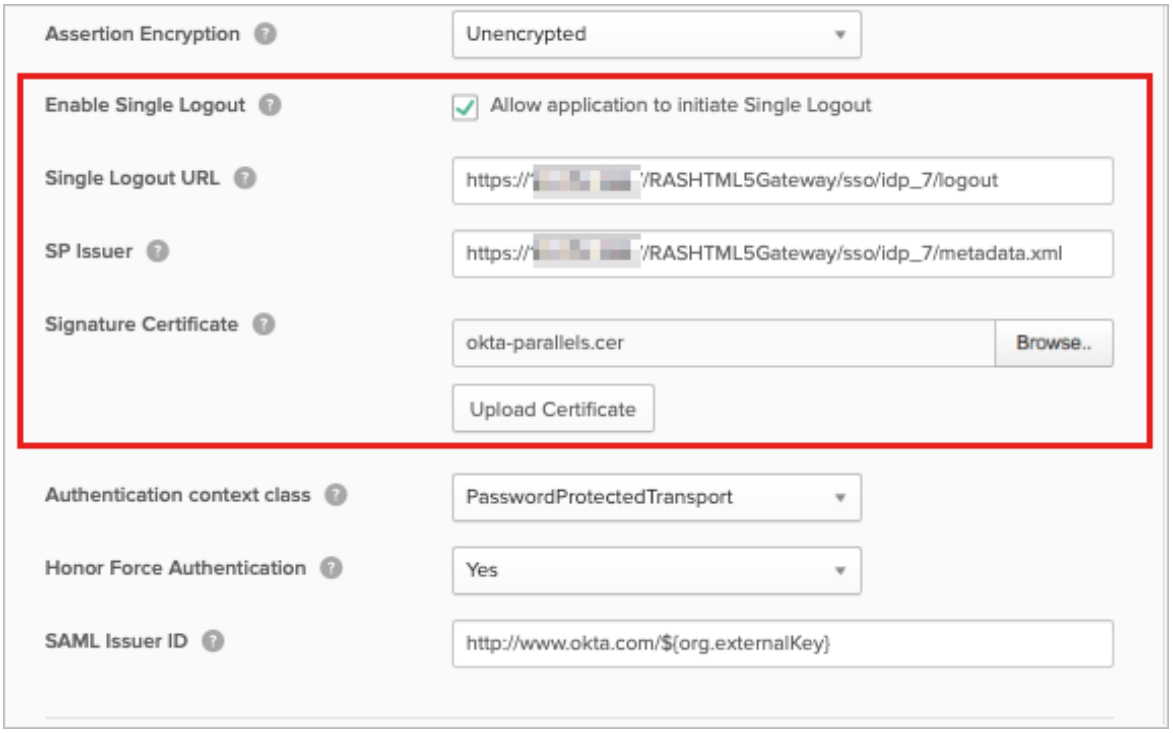
詳細設定 - シングル ログアウトの有効化

[**Show Advanced Settings** (詳細設定の表示)] リンクをクリックすると、追加のオプションが表示されます。このダイアログでシングル ログアウトを有効にします。

1 [**Allow application to initiate Single Logout** (アプリケーションによるシングル ログアウトの開始を許可する)] オプションを選択します。

2 保存した [**Logout URL** (ログアウト URL)] の値をコピーして貼り付けます。

3 前の手順で「.cer」ファイルに保存した SP 証明書を選択してアップロードします。



4 完了したら、ダイアログを閉じます。

属性ステートメント

[**Configure SAML** (SAML の設定)] ビューに戻り、[**Attribute Statements (Optional)** (属性ステートメント (オプション))] セクションで、以下の属性マッピングを追加します。

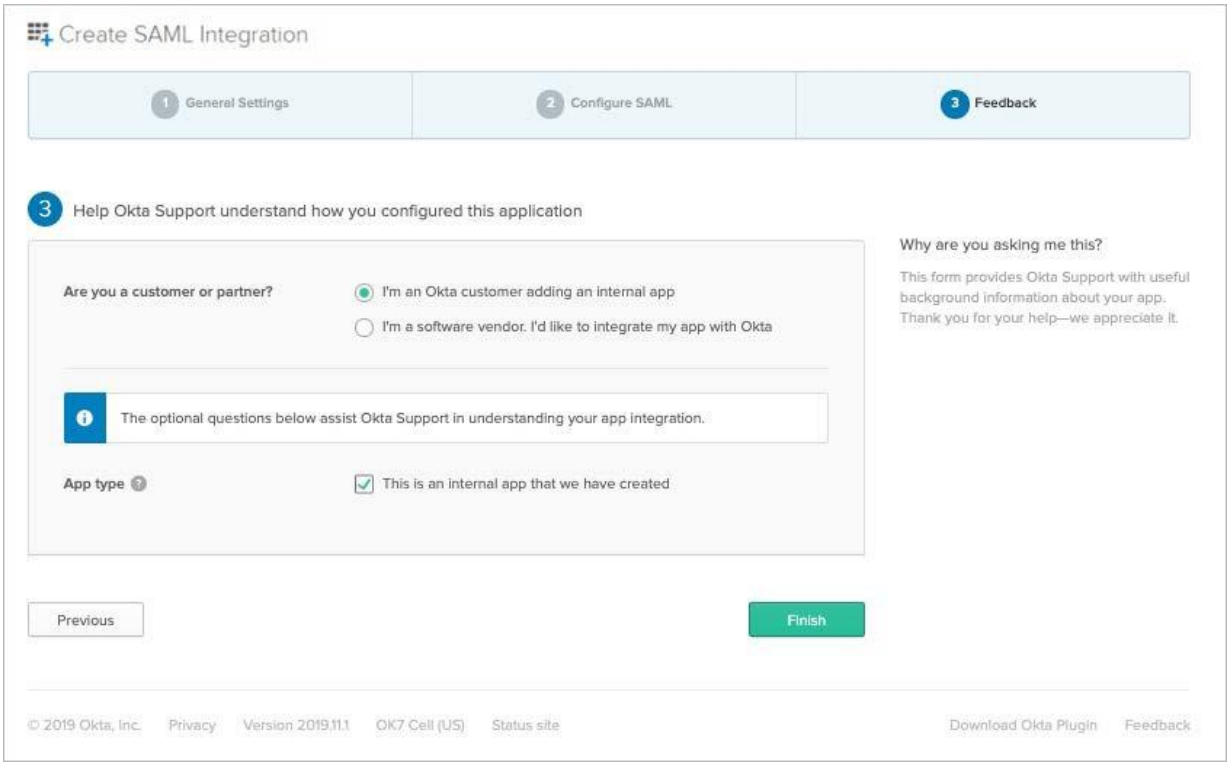
- **Name** (名称) : E メール
- **Name format** (名前の形式) : 指定なし
- **Value** (値) : user.email

必要に応じて、他のカスタム ステートメントを追加できます。

Okta 証明書をダウンロードして続行

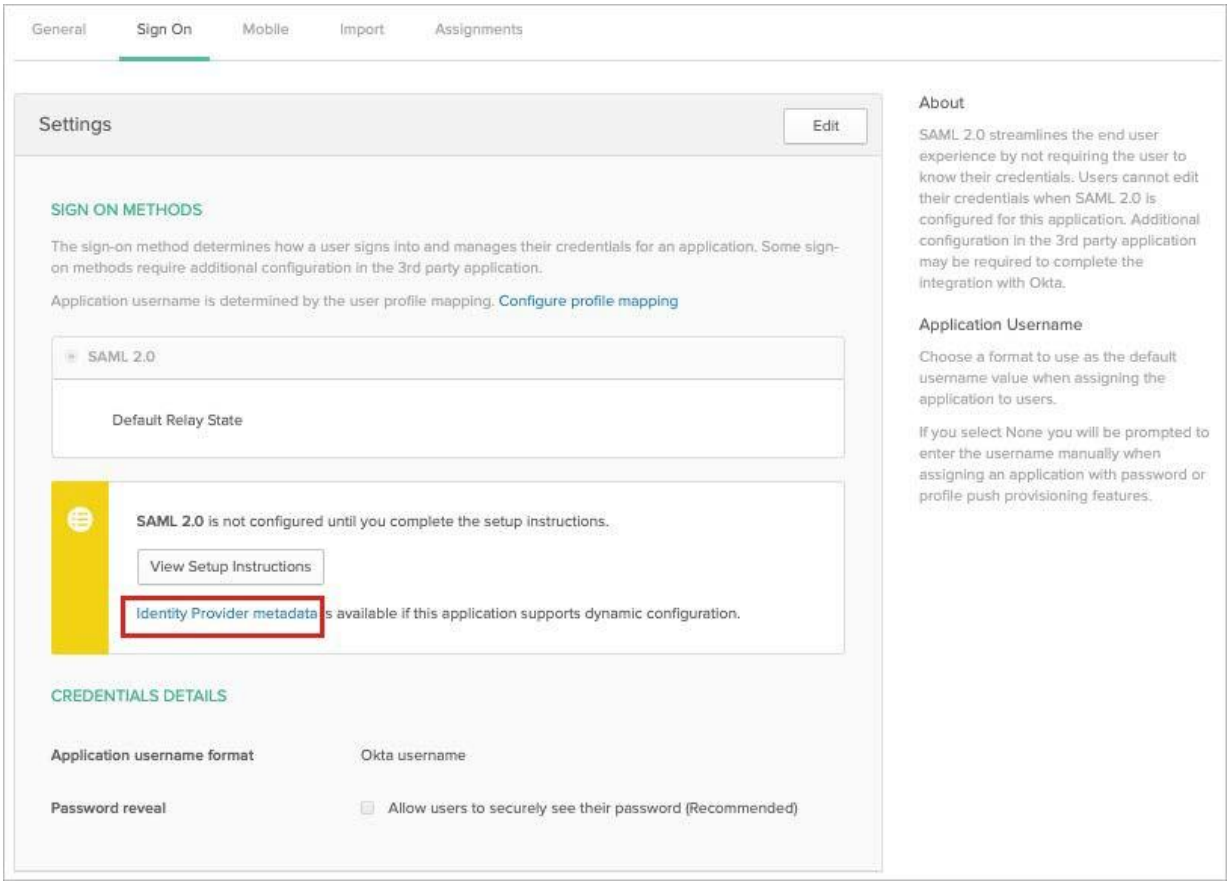
SAML 設定の右側にあるボタンをクリックして Okta 証明書をダウンロードし (これは、RAS Console の IdP 構成で必要になります)、下部にある [**Next** (次へ)] をクリックします。

Okta 関係の種類を選択し、[**Finish** (完了)] をクリックします。



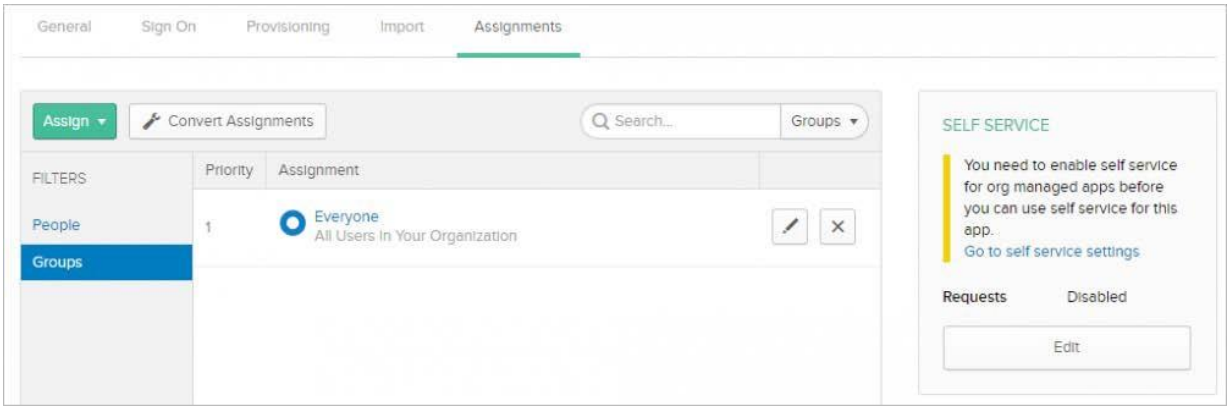
Okta IdP プロバイダー メタデータのダウンロード

[**Identity Provider metadata** (ID プロバイダーのメタデータ)] リンクをクリックして ID プロバイダーのメタデータをエクスポートし、XML ファイルを既知の場所 (「マイドキュメント」など) に保存します。



ユーザーまたはグループをアプリケーションに割り当てる

アプリケーションの [**Assignments** (割り当て)] タブに切り替え、RAS アプリケーションを使用する権限を持つ組織内のすべてのユーザーをアプリケーションに割り当てます。



Parallels RAS 構成の完了

IdP メタデータを取得したので、Parallels RAS をサービス プロバイダーとして設定します。

ID プロバイダーのメタデータをインポートします。

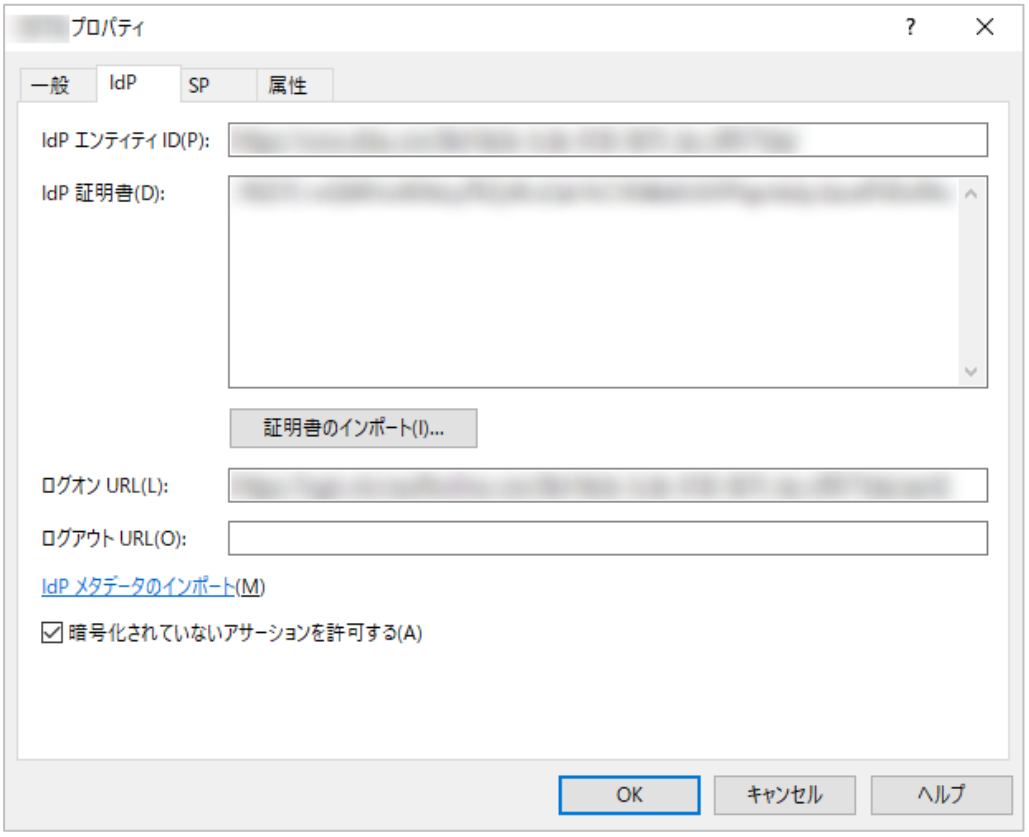
1 RAS Console を開き、[**接続**] カテゴリーを選択します。

2 [**SAML**] タブを選択します。

3 「Okta」の IdP プロバイダーを右クリックし、[**プロパティ**] を選択します。

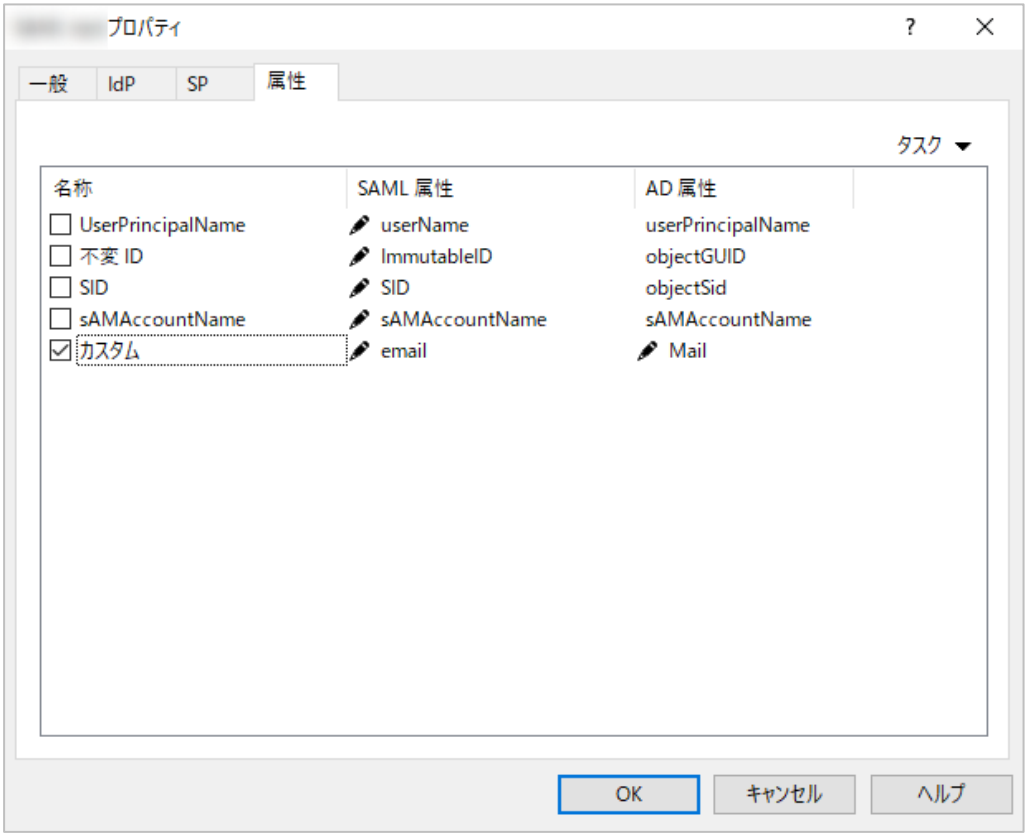
4 開いたダイアログで、[**IdP**] タブを選択します。

5 [**IdP メタデータのインポート**] リンクをクリックします。前の手順で Okta からダウンロードした ID プロバイダーのメタデータ ファイルを選択してインポートします。設定値が置き換えられたことを確認します。



6 [**属性**] タブに切り替えます。

7 [**カスタム**] 属性を選択し、[**SAML 属性**] 値を「Email」に、[**AD 属性**] 値を「Mail」に設定します。任意の属性を使用できるため、これは単なる例であることに注意してください。この特定のケースでは、Okta ログイン ユーザー名/メールアドレス (Okta へのログインに使用) を Active Directory で構成されたユーザーのメールアドレスと照合します。



8 [**一般**] タブに切り替え、IdP で使用するテーマを選択します。

9 [**OK**] と [**適用**] をクリックします。

接続のテスト

SP 開始

1 ウェブ ブラウザで [ユーザー ポータル] を開きます。SAML アプリケーションに関連付けたテーマを使用します。

2 ユーザーは認証のために Okta ポータルにリダイレクトされます。

3 認証が成功すると、アプリケーション リストがユーザーに表示されます。

IdP 開始

1 Okta ポータルにログインし、割り当てられたアプリケーションを起動します。

2 ユーザーは、割り当てられたテーマを使用してユーザー ポータルにリダイレクトされ、アプリケーション リストが表示されます。

第 5 章

SAML 2.0 による Ping ID との統合

この章の内容

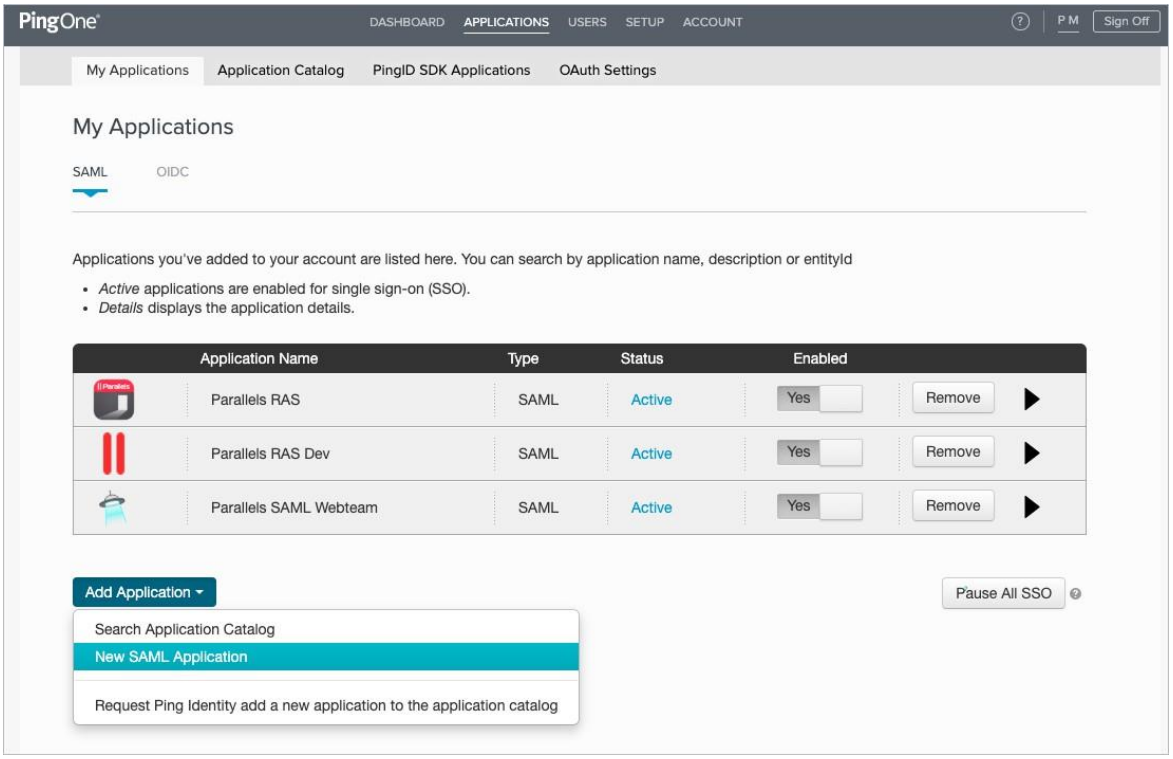
汎用 SAML アプリケーションの作成.....32
Parallels RAS のサービス プロバイダー構成.....35
SAML アプリケーション構成の完了 39
接続のテスト.....42

汎用 SAML アプリケーションの作成

まず、以下のように PingOne で汎用 SAML アプリケーションを作成する必要があります。

1 PingOne (https://admin.pingone.com/web-portal/login) にログインします。

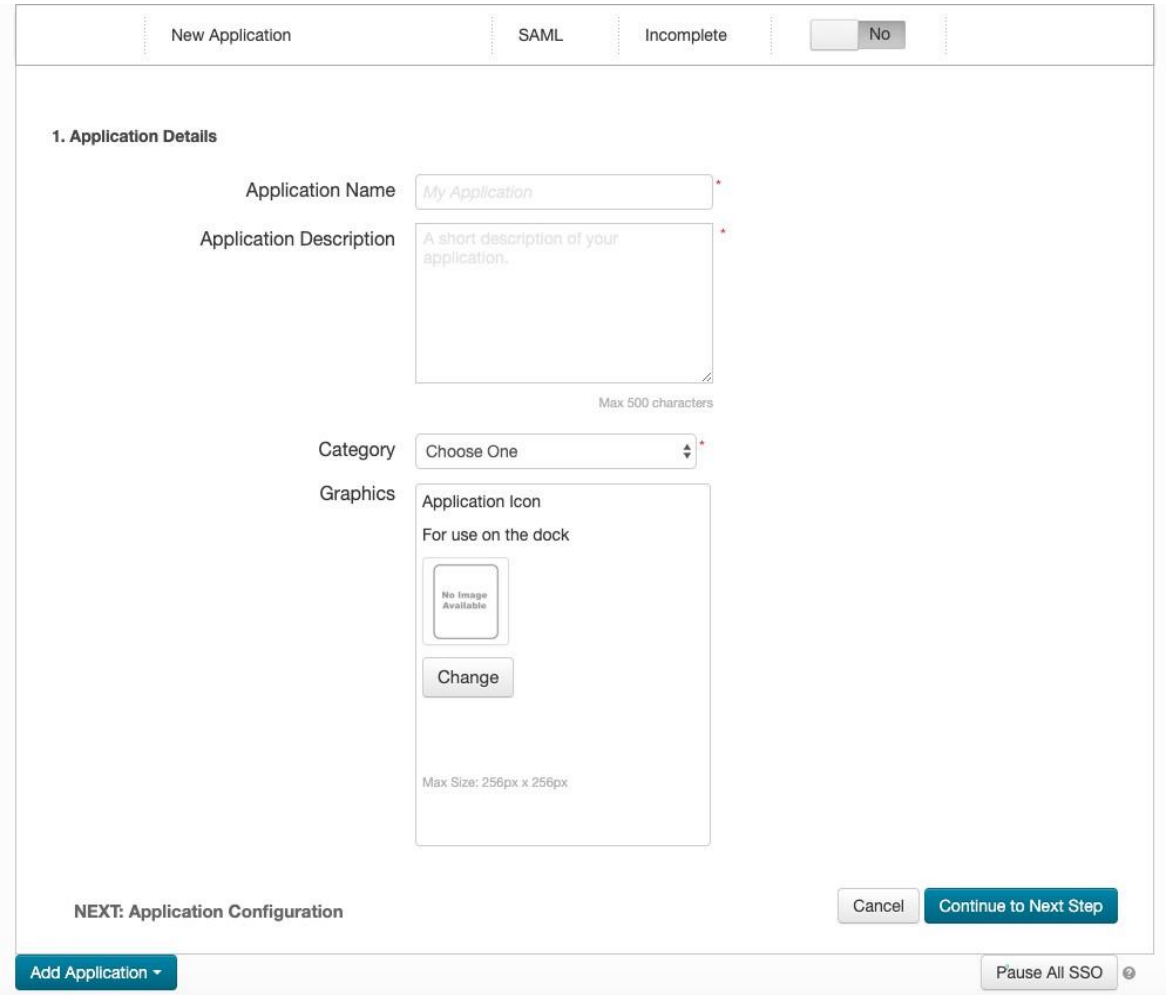
2 以下のスクリーンショットに示すように、[**My Applications** (マイ アプリケーション)] タブを選択します。



3 [**Add Application** (アプリケーションの追加)] をクリックし、[**New SAML Application** (新しい SAML アプリケーション)] を選択します。新規アプリケーション ウィザードが開きます。

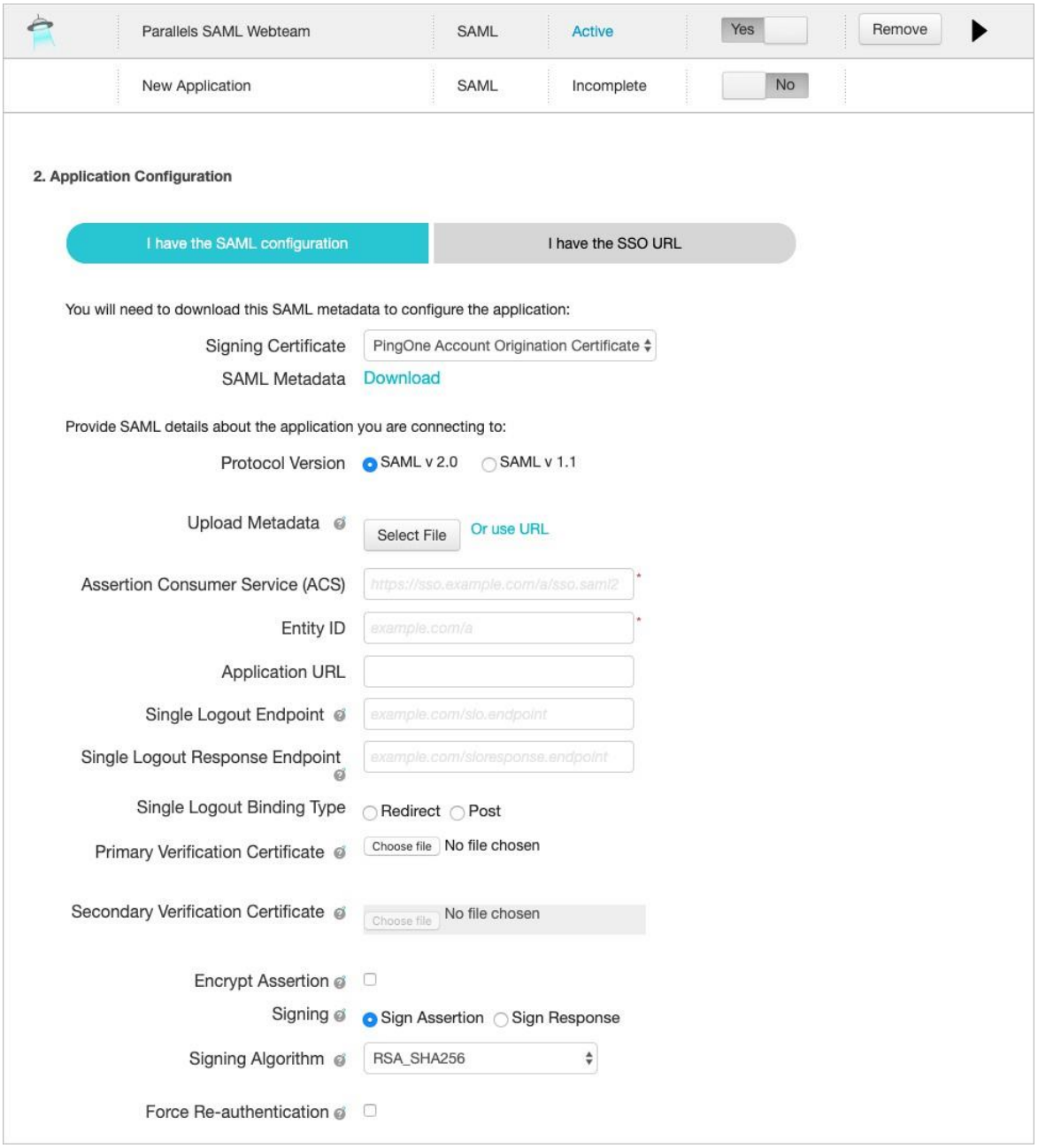
4 「**1 . Application Details** (アプリケーション詳細) 」ページで、以下のデータを追加します。

- **Application Name** (アプリケーション名) : Parallels RAS (または任意の名前) 。
- **Application Detail** (アプリケーションの詳細) : Remote Application Server (または任意の名前) 。
- **Categor** (カテゴリー) : その他
- **Graphics** (グラフィックス) : 必要に応じて、256 x 256 ピクセルのアイコンを png 形式でアップロードします。



5 [**Continue to Next Step** (次のステップへ進む)] をクリックします。

6 「**2 . Application configuration** (アプリケーション設定) 」ページが開きます



7 このページで、Ping Identity から SAML メタデータをダウンロードする必要があります。[**SAML Metadata** (SAML メタデータ)] ラベルの横の [**Download** (ダウンロード)] リンクをクリックします。

8 メタデータファイル (.xml) をローカル ドライブに保存します。

9 Parallels RAS Console に切り替えます。

Parallels RAS のサービス プロバイダー構成

ID プロバイダーとして PingOne を追加し、Parallels RAS をサービス プロバイダー (SP) として構成する必要があります。

RAS Console で、以下のように ID プロバイダーを追加します。

1 [**接続**] カテゴリーを選択します。

2 [**SAML**] タブを選択します。

3 [**タスク**] > [**追加**] をクリックします。

4 [**アイデンティティ プロバイダーを追加**] ウィザードで、プロバイダー名を入力し、プロバイダーに関連付けるテーマを選択します。

5 [**ファイルから IdP メタデータをインポートする**] オプションを選択し、前の手順で PingOne からダウンロードした SAML メタデータ ファイルを指定します。

6 [**次へ**] をクリックします。

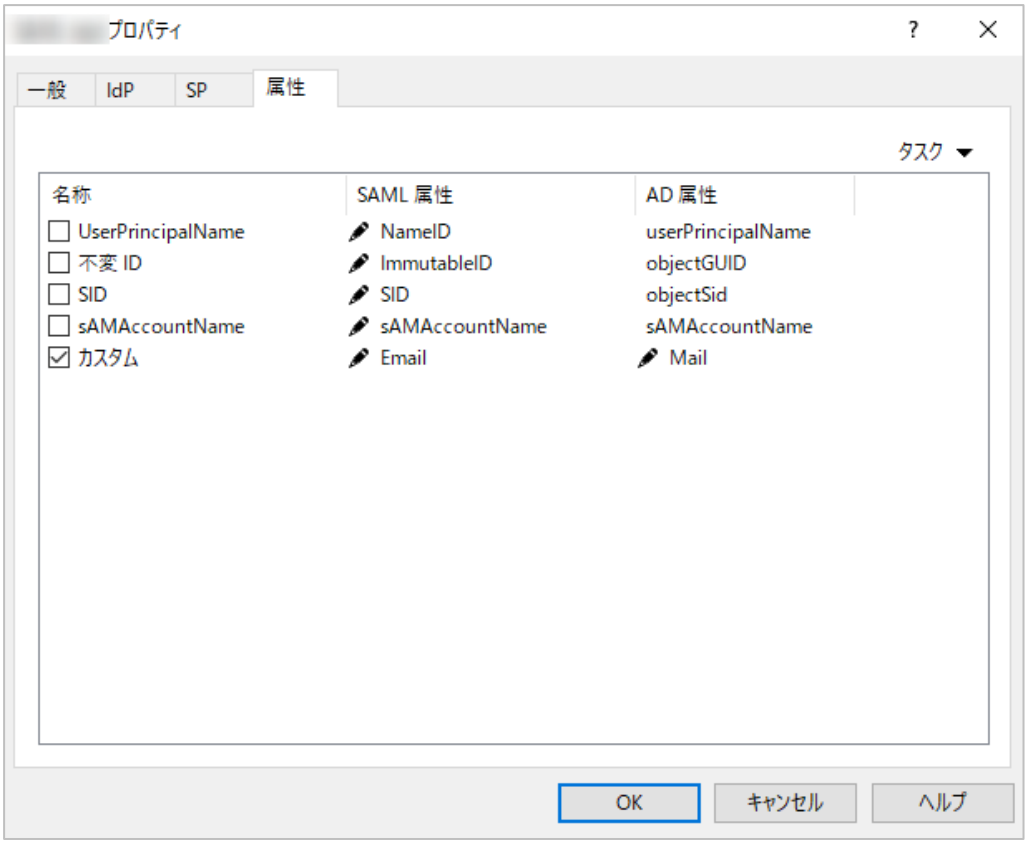
7 次のページでは、[**IdP エンティティ ID**]、[**IdP 証明書**]、[**ログオン URL**]、および [**ログアウト URL**] フィールドが、インポートされたメタデータを利用して自動的に設定されます。

8 RAS Console で [**完了**] をクリックし、[**適用**] をクリックします。

9 作成した IdP プロバイダーを右クリックし、[**プロパティ**] をクリックします。

10 [**属性**] タブを選択します。

11 [**カスタム**] 属性名を選択し、[**SAML 属性**] を [**Email**] に変更します。[**userPrincipalName**] 属性をクリアします。

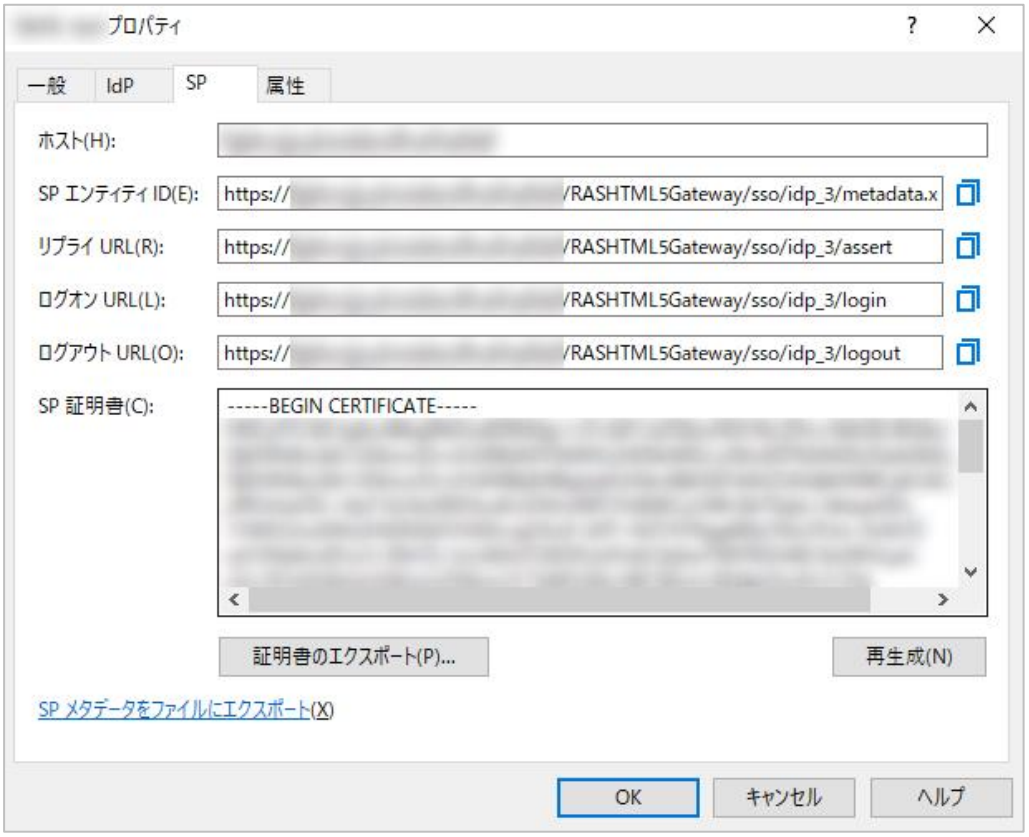


12 RAS Console で [**OK**] をクリックし、[**適用**] をクリックします。

13 IdP プロバイダーの [**プロパティ**] のダイアログを再度開き、[**SP**] タブに切り替えます。

14 SP 構成を XML ファイルにエクスポートし、ローカル ドライブに保存します。

15 [**ログオン URL**] をクリップ ボードにコピーするか、ファイルに保存します。次のセクションで説明するように、PingOne 管理者コンソールで指定する必要があります。



16 PingOne 管理コンソールに戻り、新しい SAML アプリケーションの構成を完了します。続きを読む。

SAML アプリケーション構成の完了

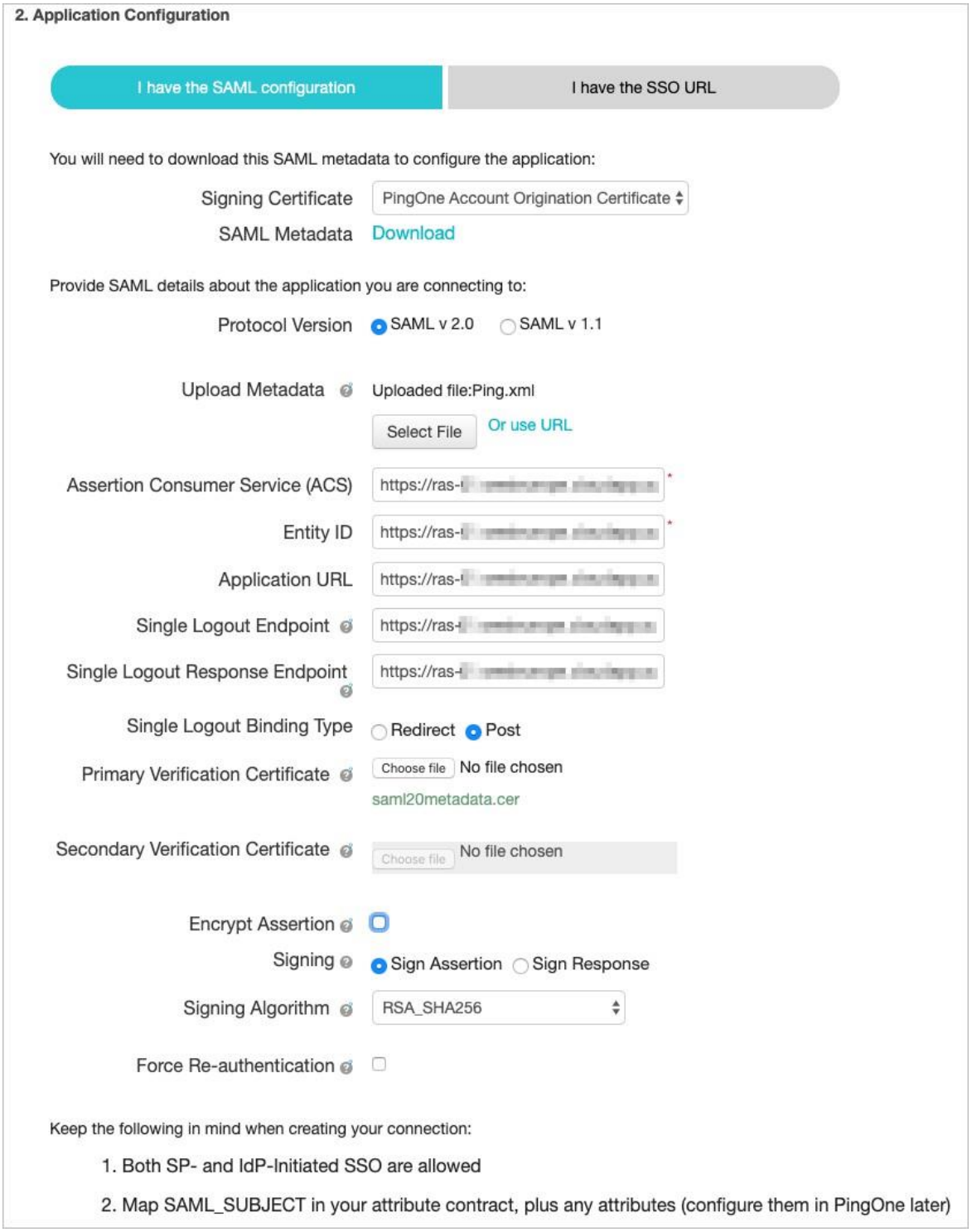
SP メタデータをファイルにエクスポートしたら、PingOne をアップロードして SAML アプリケーションの構成を完了する必要があります。

PingOne 管理コンソールで、以下の手順を実行します。

1 「**2. Application Configuration** (アプリケーション構成) 」ページに戻ります。

2 [**Protocol Version** (プロトコル バージョン)] プロパティを [**SAML v 2.0**] に設定します (以下のスクリーン ショットを参照) 。

3 RAS Console に保存した SP メタデータをアップロードするには、[**Select File** (ファイルの選択)] ボタンをクリックして XML ファイルを選択します。

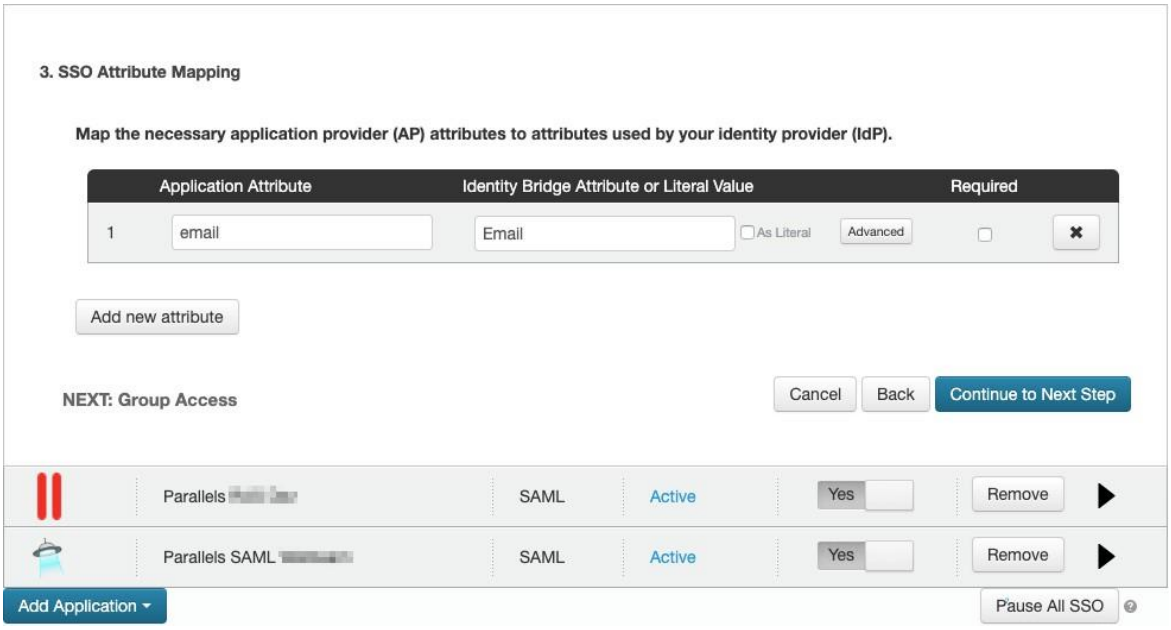


4 残りのアプリケーション プロパティを以下のように設定します。

- **Application URL** (アプリケーション URL) : RAS Console の「IdP プロバイダー プロパティ」ダイアログの [**SP**] タブにある [**ログオン URL**] リンク (前のセクションでコピーまたは保存するように指示したリンク) を貼り付けます。
- **Single Logout Response Endpoint** (シングル ログアウト レスポンス エンドポイント) : [**Single Logout Endpoint**] フィールドからリンクをコピーし、ここに貼り付けます。
- **Single Logout Binding Type** (シングル ログアウト バインディング タイプ) : [**Post**] オプションを選択します。
- **Encrypt Assertion** (アサーションの暗号化) : チェックボックスをオフにします。
- **Signing** (署名) : [**Sign Assertion** (署名アサーション)] オプションを選択します。
- **Signing Algorithm** (署名アルゴリズム) : [**RSA_SHA 256**] に設定します。
- **Force Re-authentication** (強制再認証) :チェック ボックスをオフにします。

5 [**Continue to Next Step** (次のステップへ進む)] をクリックします。

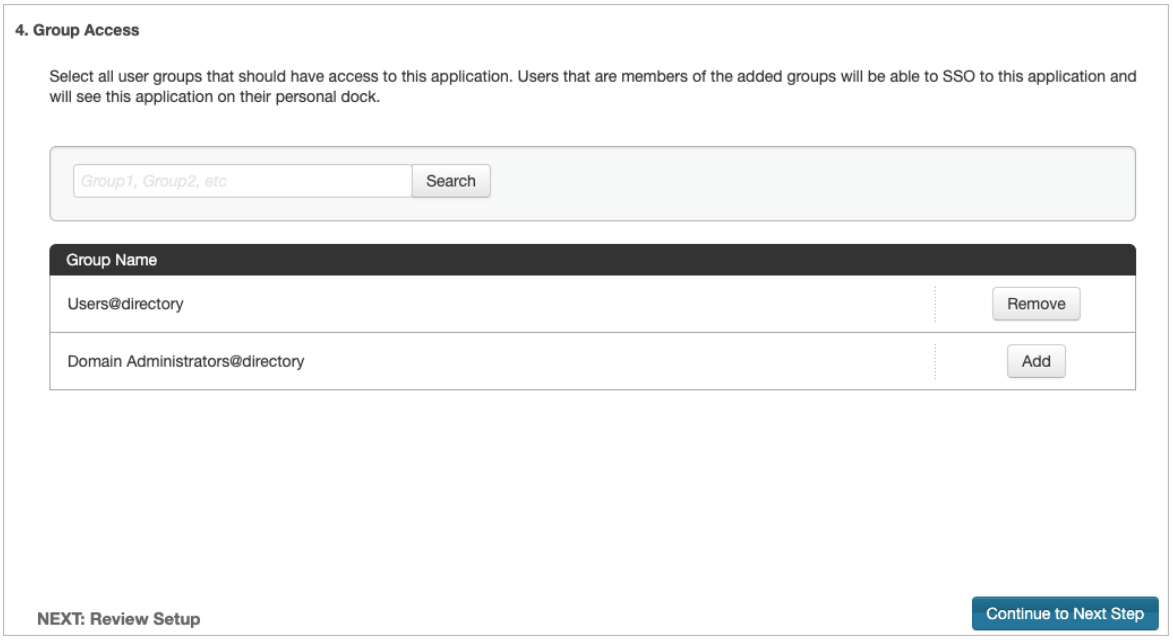
6 「**3. SSO Attributes Mapping** (SSO 属性マッピング) 」ページで、[**Add new attribute** (新規属性の追加)] をクリックします。



7 [**Application Attribute** (アプリケーション属性)] フィールドに「email」と入力し、[**Identity Bridge Attribute** (ID ブリッジ属性)] フィールドで [**Email**] を選択します。

8 [**Continue to Next Step** (次のステップへ進む)] をクリックします。

9 「**4. Group Access** (グループ アクセス) 」ページで、必要に応じて新規アプリケーションのユーザーまたはグループを割り当てます。



10 [**Continue to Next Step** (次のステップへ進む)] をクリックします。

11 ウィザードの最後のページで設定を確認し、[**Finish** (完了)] をクリックします。

接続のテスト

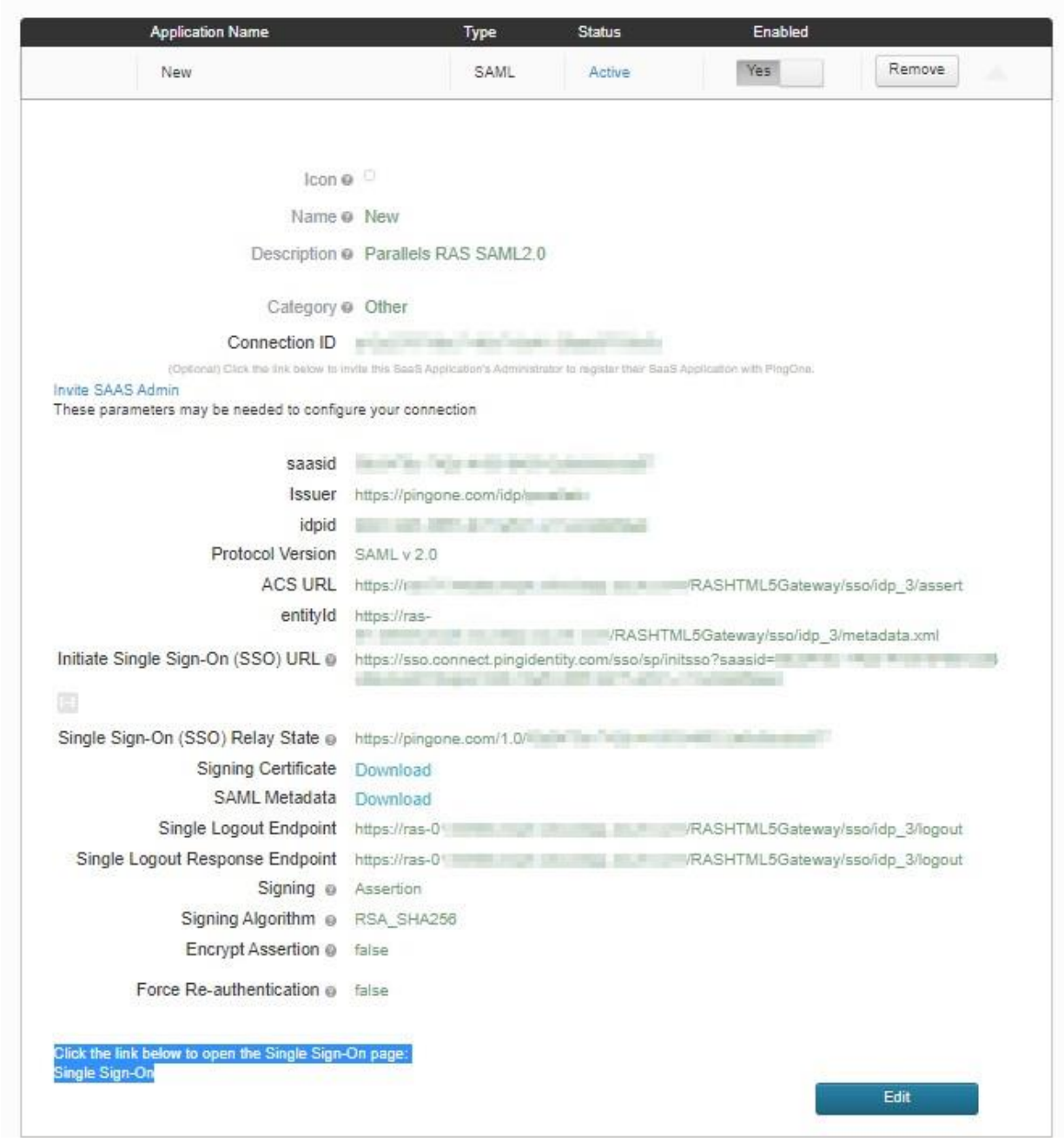
SP 開始

1 ウェブ ブラウザでユーザー ポータル ページ (例 : https://ras01.westeurope.cloudapp.azure.com/userportal) を開きます。SAML アプリケーションに関連付けたテーマを使用します。

2 すべてが正しい場合は、PingOne ID ポータルにリダイレクトされ、サインインを続行できます。

IdP 開始

IdP によって開始された SAML 認証を PingOne から直接確認するには、[**Applications** (アプリケーション)] メニューでアプリケーションをクリックします。



リンクをクリックして「**Single Sign-On** (シングル サインオン)」ページを開くと、RAS ユーザー ポータルの認証ページにリダイレクトされます。

第 6 話

SAML 2.0 による Thales SafeNet Trusted Access との統合

この章の内容

汎用 SAML アプリケーションの作成.....44
Parallels RAS のサービス プロバイダー構成.....51
接続のテスト.....54

汎用 SAML アプリケーションの作成

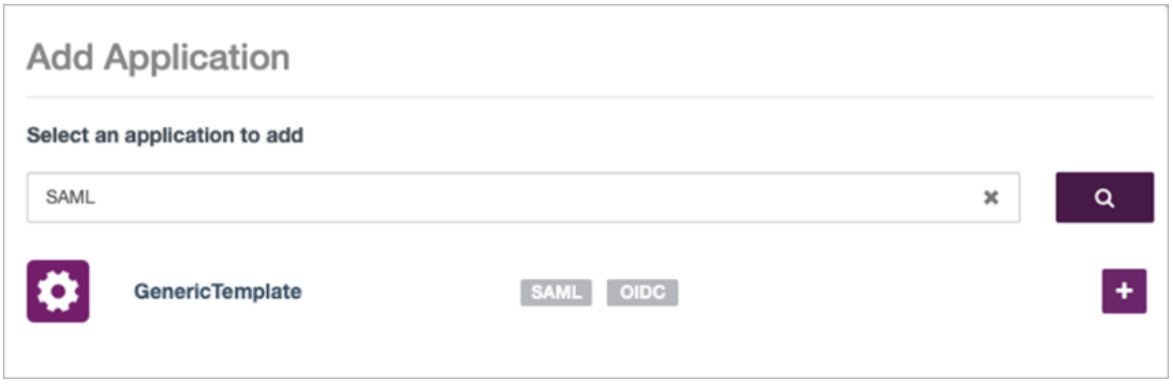
汎用 SAML アプリケーションを作成します。

1 管理者資格情報を使用して SafeNet Trusted Access ポータルにログインします。

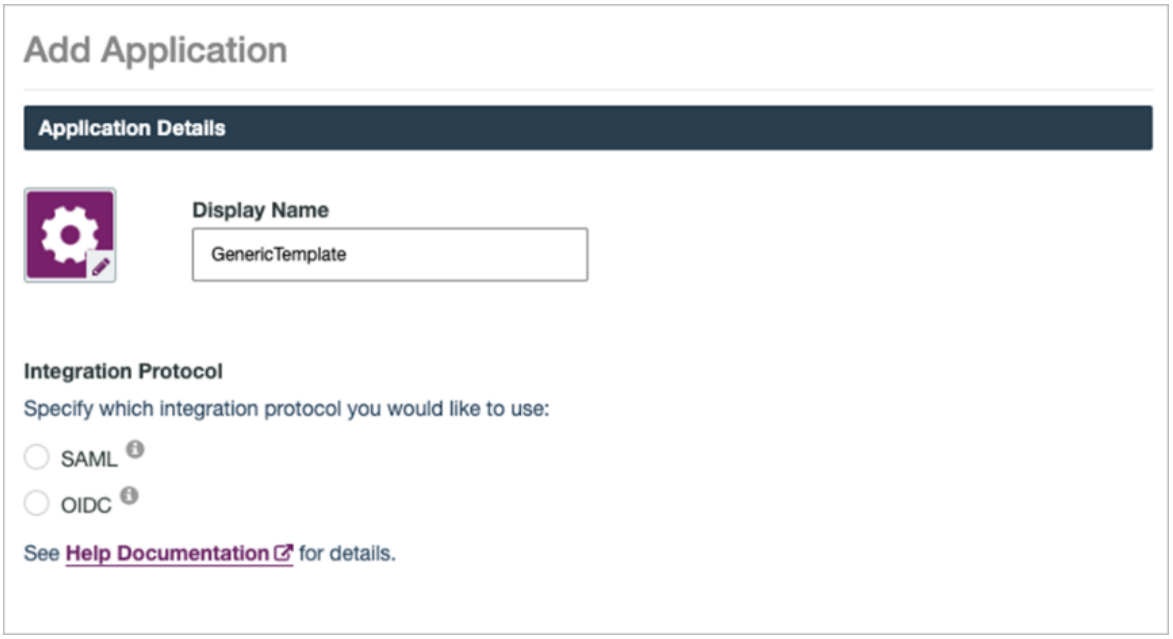
2 [**Applications** (アプリケーション)] に切り替え、[**+**] アイコンをクリックして新しいアプリケーションを追加します。

3 「**Add Application** (アプリケーションの追加) 」ページで、「SAML」と入力します。

4 虫眼鏡アイコンをクリックし、「GenericTemplate」を検索します。見つかったら、[+] アイコンをクリックします。

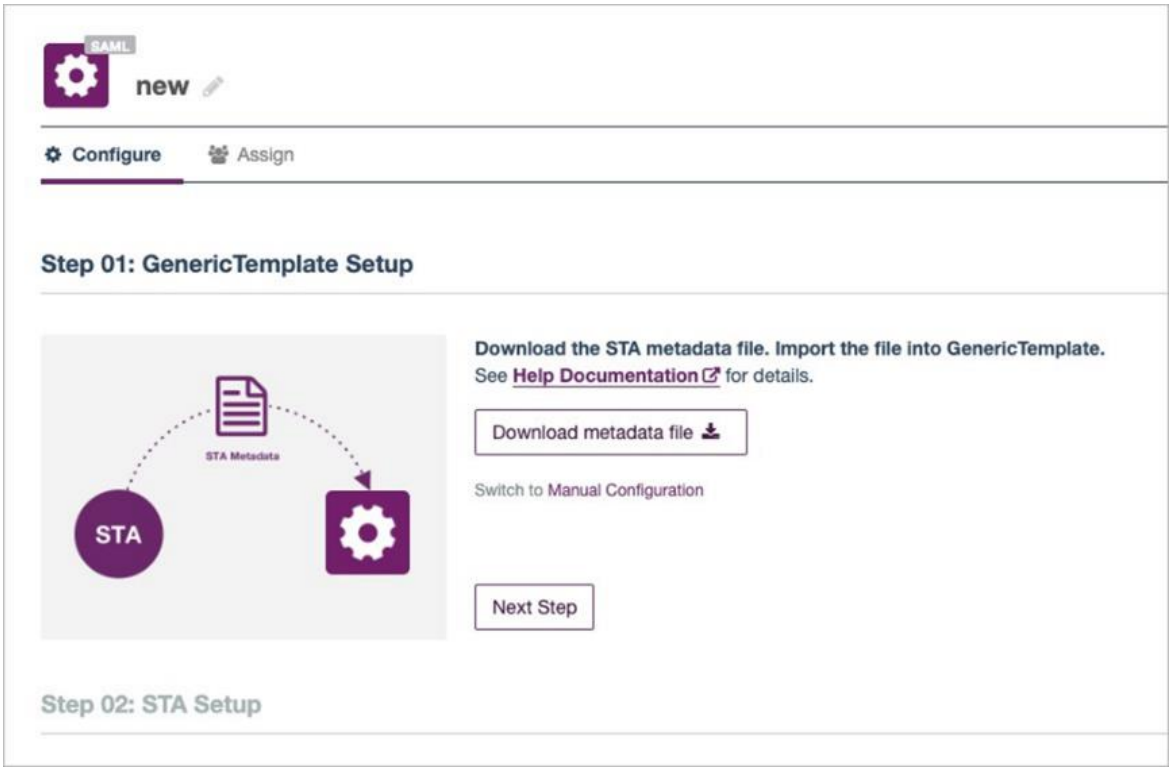


5 [**Display Name** (表示名)] フィールドにアプリケーションの名前を入力し、[**SAML**] を選択して [**Add** (追加)] をクリックします。



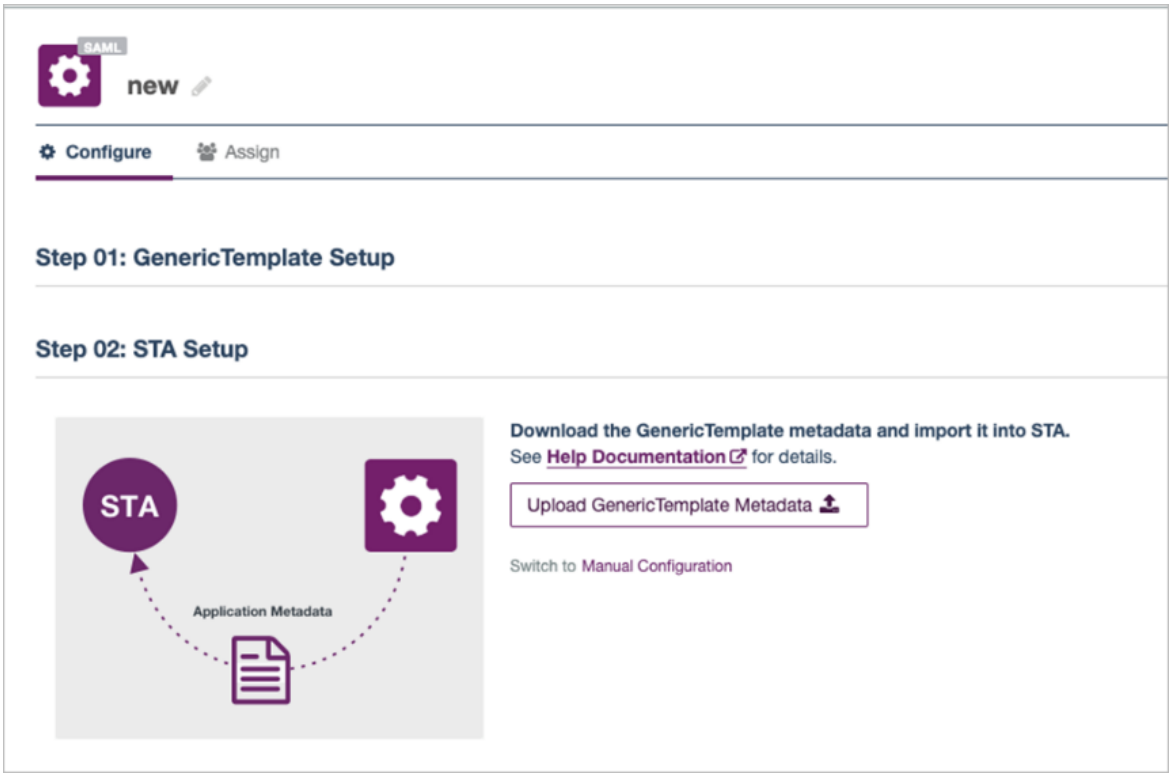
6 「**Step 01 : GenericTemplate Setup** (汎用テンプレートの設定) 」ページで、[**Download metadata file** (メタデータ ファイルのダウンロード)] ボタンをクリックし、ファイルをローカル ドライブ (例 : mydocs\Safanet.xml) に保存します。

7 [**Next** (次へ)] をクリックします。



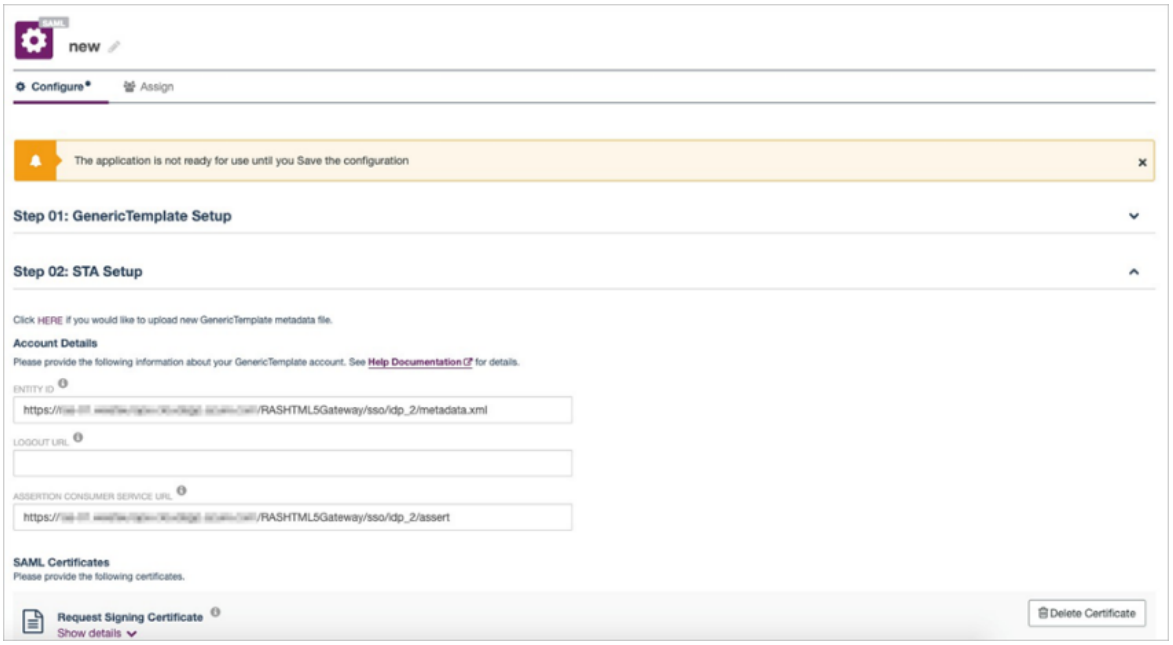
8 「**Step 02 : STA Setup** (STA 設定) 」ページが表示されましたら、RAS Console に移動して新しい IdP プロバイダーを作成する必要があります。この手順の詳細については、「Parallels RAS のサービス プロバイダー構成**エラー! 参照元が見つかりません。** (p. 51) 」節を参照してください。そのセクションで説明されている手順を実行してから、ここに戻ってください。

9 SafeNet ポータルに戻り、[**Upload GenericTemplate Metadata** (汎用テンプレートメタデータのアップロード)] をクリックして、前の手順で RAS Console にエクスポートした XML ファイルを選択します。



10 アップロード後、ページが更新され、STA 設定の構成を続行できます。

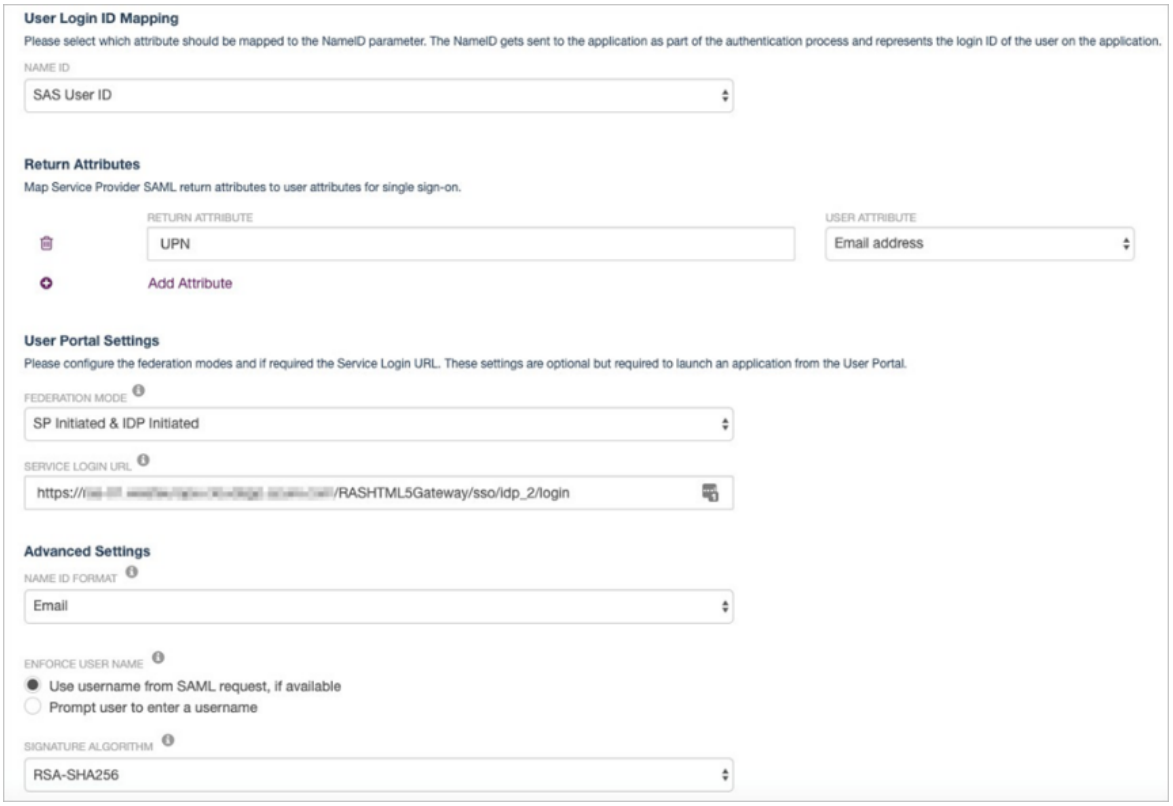
11 [**Account Details** (アカウント詳細)] セクションで、RAS Console の [**SP**] タブにある完全なログアウト URL をコピーして貼り付けます。



12 その他のフィールドには以下のように入力します (以下のスクリーンショットを参照) 。

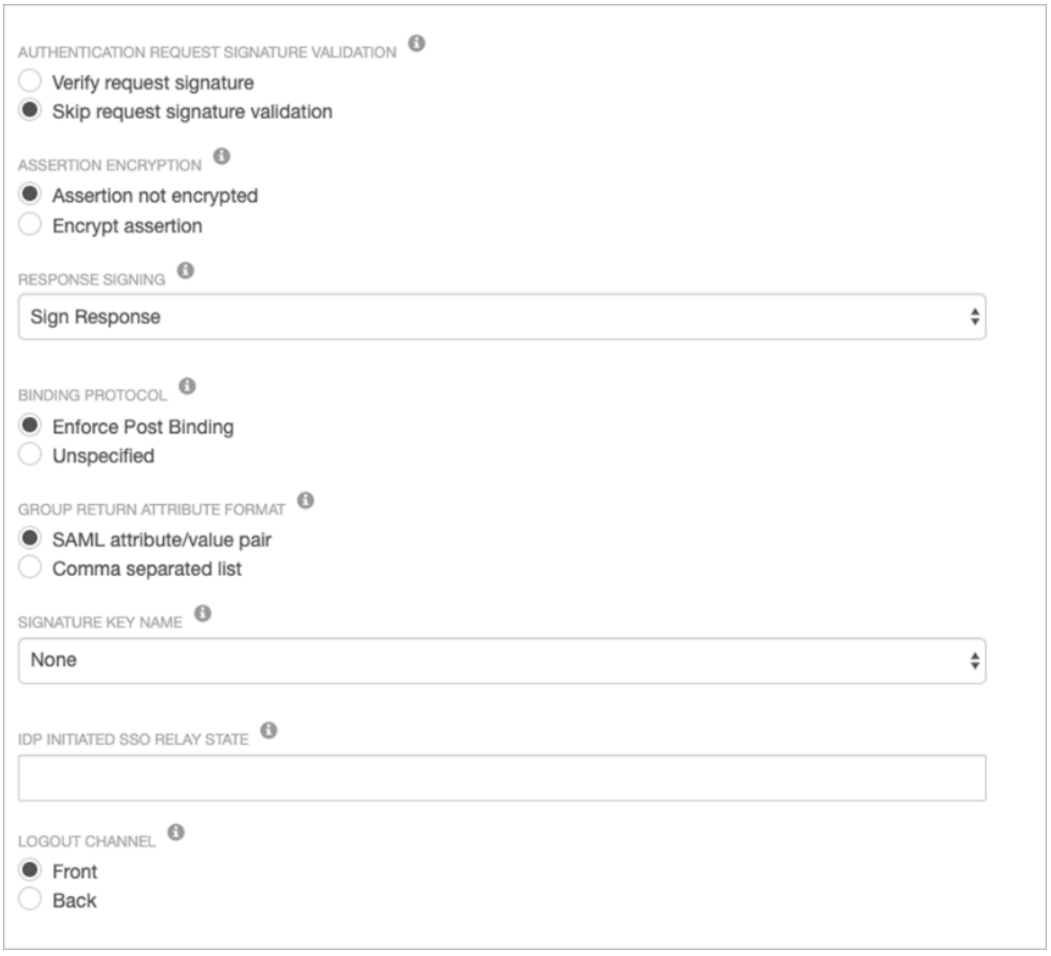
- [**User Login ID Mapping** (ユーザーログイン ID の割り当て)] > [**Name ID** (名前 ID)] : [**SAS user ID** (SAS ユーザーID)] を選択します。
- [**Return Attributes** (リターン属性)] > [**Return Attributes** (リターン属性)] :「UPN」と入力します。
- [**Return Attributes** (リターン属性)] > [**User Attribute** (ユーザー属性)] : [**Email address** (メールアドレス)] を選択します。
- [**User Portal Settings** (ユーザー ポータル設定)] > [**Service Login URL** (サービス ログイン URL)] : RAS Console の [**SP**] タブから URL をコピー＆ペーストします。
- [**Advanced Settings** (詳細設定)] > [**Name ID Format** (名前 ID 形式)] : [**Email**] を選択します。
- **Enforce User Name** (ユーザー名の強制) : 使用可能な場合は、[**Use username from SAML** (SAML リクエストのユーザー名を使用)] を選択します。

- **Signature Algorithm** (署名アルゴリズム) : [**RSA-SHA 256**] を選択します。

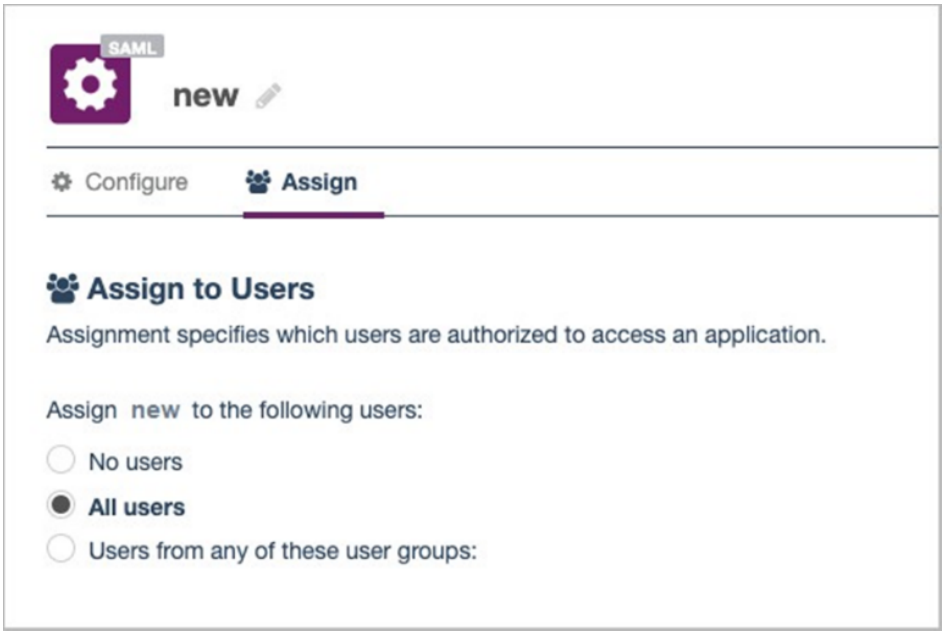


13 以下のようにオプションを設定します (以下のスクリーンショットを参照) 。

- **Authentication Request Signature Validation** (認証要求署名検証) : [**Skip request signature validation** (要求署名検証をスキップ)] を選択します。
- **Assertion Encryption** (アサーション暗号化) : [**Assertion not encrypted** (アサーションは暗号化されていません)] を選択します。
- **Response Signing** (応答の署名) : [**Sign Response** (レスポンスに署名する)] を選択します。
- **Binding Protocol** (バインディング プロトコル) : [**Enforce Post Binding** (ポストバインディングの実施)] を選択します。
- **Signature Key Name** (署名キー名) : [**None** (なし)] を選択します。
- **Idp Initiated Sso Relay State** : 空白のままにします。
- **Logout Channe** (ログアウト チャネル) : [**Front**] を選択します。


AUTHENTICATION REQUEST SIGNATURE VALIDATION
Verify request signature
Skip request signature validation
ASSERTION ENCRYPTION
Assertion not encrypted
Encrypt assertion
RESPONSE SIGNING
Sign Response
BINDING PROTOCOL
Enforce Post Binding
Unspecified
GROUP RETURN ATTRIBUTE FORMAT
SAML attribute/value pair
Comma separated list
SIGNATURE KEY NAME
None
IDP INITIATED SSO RELAY STATE
LOGOUT CHANNEL
Front
Back

14 [**Save configuration** (設定の保存)] をクリックし、[**Assign** (割り当て)] に切り替えます。



15 [**All users** (すべてのユーザー)] を選択するか、ユーザー/グループを選択して [**Save configuration** (構成の保存)] をクリックします。

16 アプリケーションが [**active** (アクティブ)] として表示されます。

Parallels RAS のサービス プロバイダー構成

この手順では、ID プロバイダーとして SafeNet Trusted Access を追加することにより、Parallels RAS をサービス プロバイダー (SP) として構成する必要があります。

ID プロバイダーを追加するには、以下の手順に従います。

1 RAS Console で、[**接続**] カテゴリーを選択します。

2 [**SAML**] タブを選択します。

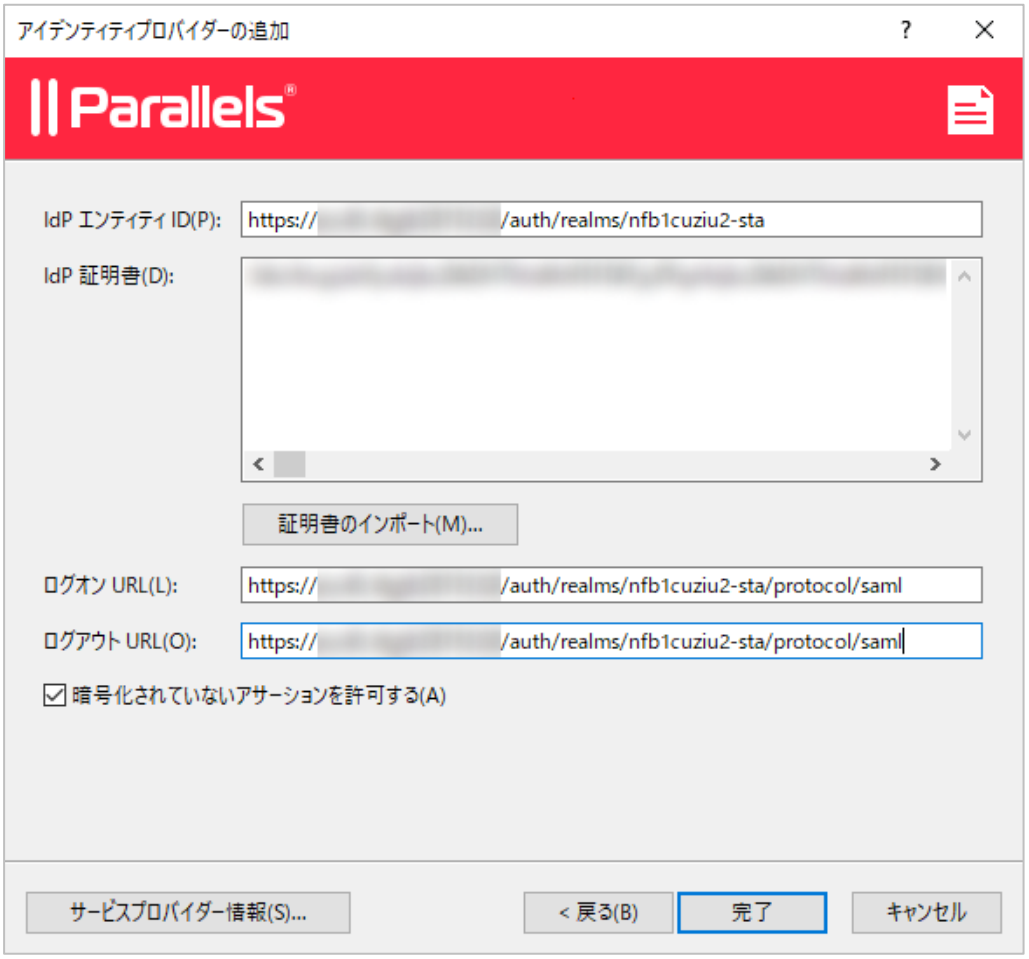
3 [**タスク**] > [**追加**] をクリックします。

4 [**ID プロバイダーを追加**] ウィザードで、プロバイダー名を入力し、ユーザー ポータル テーマを選択します。

5 [**ファイルから IdP メタデータをインポートする**] オプションを選択し、以前に SafeNet Trusted Access ポータルからダウンロードした SAML メタデータ ファイルを指定します。「汎用 SAML アプリケーションの作成 (p. 44) 」を参照してください。

6 [**次へ**] をクリックします。

7 次のページでは、[**IdP エンティティ ID**]、[**IdP 証明書**]、[**ログオン URL**]、および [**ログアウト URL**] フィールドが、インポートされたメタデータを使用して自動的に入力されます。

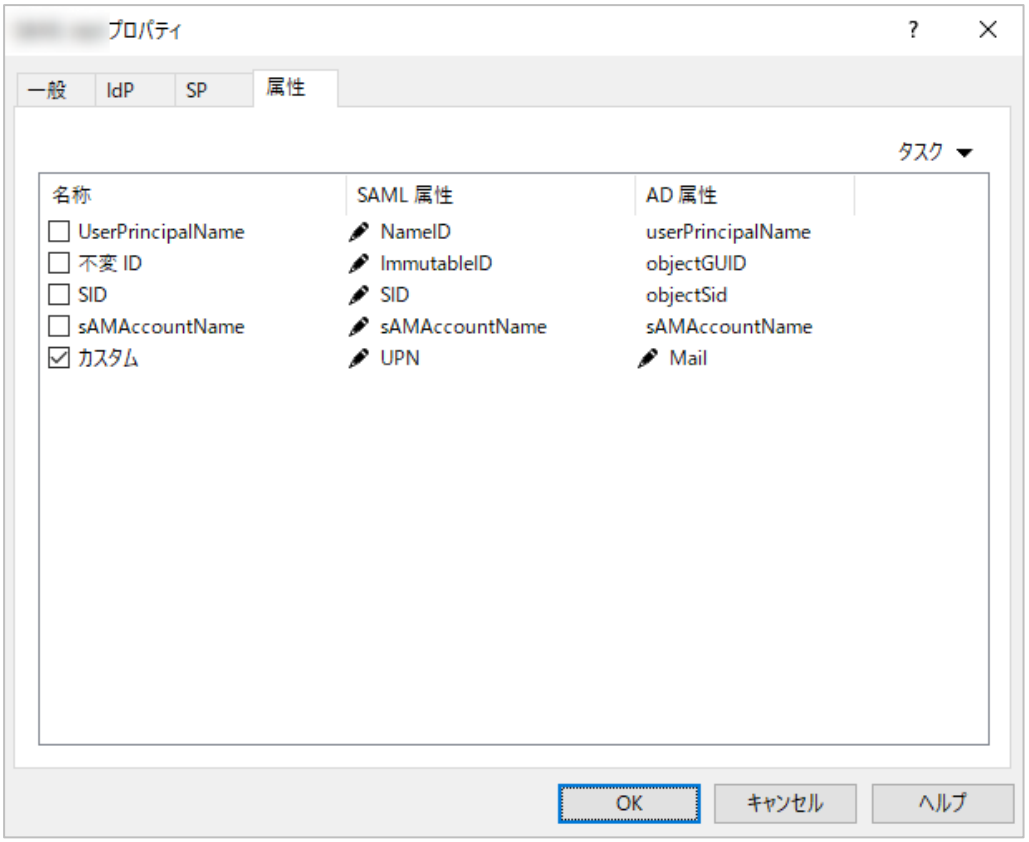


8 RAS Console で [**完了**] をクリックし、[**適用**] をクリックします。

9 [**SAML**] タブで、作成した IdP プロバイダーを右クリックし、[Properties] をクリックします。

10 [**属性**] タブに切り替え、[**カスタム**] 属性を選択します。[**SAML 属性**] 値を「UPN」に、AD 属性値を「Mail」に設定します。

11 [**UserPrincipalName**] 属性が選択されている場合はクリアします。



12 RAS Console で [**OK**] をクリックし、[**適用**] をクリックします。

13 IdP プロバイダーの [**プロパティ**] ダイアログを再度開き、[**SP**] タブに切り替えます。

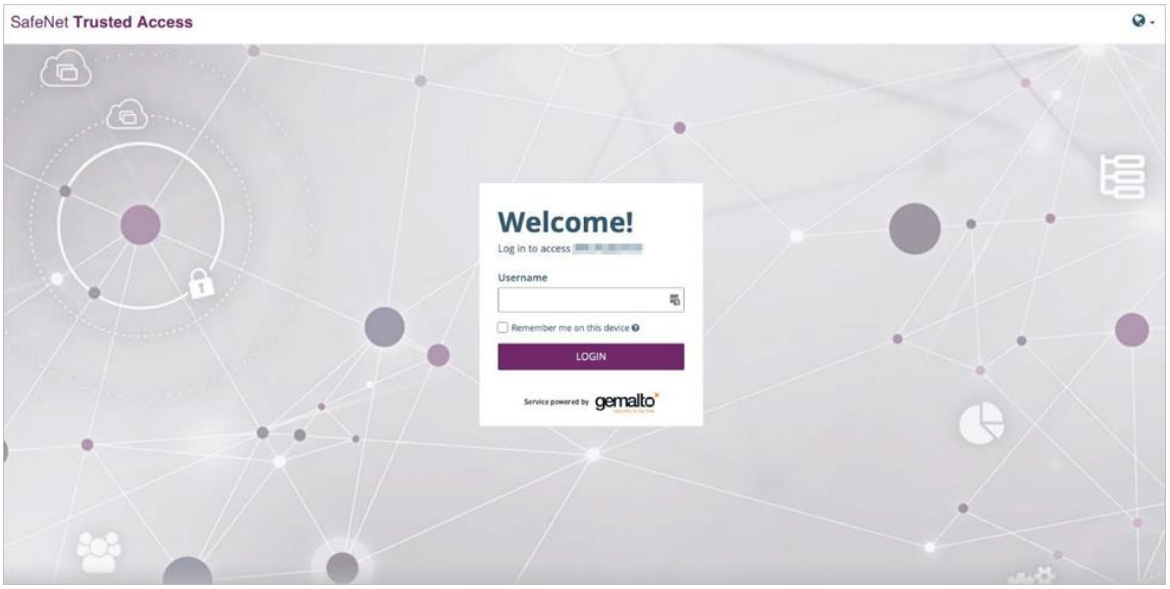
14 SP 構成を XML ファイルにエクスポートし、ローカル ドライブに保存します。これは、「汎用 SAML アプリケーションの作成 (p. 44) 」セクションの説明に従って、SafeNet Trusted Access ポータルにインポートする必要があるファイルです。

接続のテスト

SP 開始

1 ウェブ ブラウザで RAS ユーザー ポータルを開きます。SAML アプリケーションに関連付けたテーマを使用します。

2 ユーザーは、認証のために SafeNet Trusted Access ポータルにリダイレクトされます。



3 認証が成功すると、アプリケーション リストがユーザーに表示されます。

IdP 開始

1 SafeNet Trusted Access ポータルにログインし、割り当てられたアプリケーションを起動します。

2 ユーザーは、割り当てられたテーマを使用してユーザー ポータルにリダイレクトされ、アプリケーション リストが表示されます。