Informatica®

Informatica® Intelligent Cloud Services
October 2022

ユーザー管理

Informatica Intelligent Cloud Services ユーザー管理
October 2022

発行日: 2022-12-01

目次

序文

「*ユーザー管理*」を使用して、Informatica Intelligent Cloud Services℠のユーザーアカウントを手動で設定する方法、または SAML シングルサインオンを使用して設定する方法を確認します。ユーザーグループを作成する方法、ユーザーにロールを割り当てる方法、およびユーザープロファイルを編集する方法を確認します。

Informatica のリソース

Informatica は、Informatica Network やその他のオンラインポータルを通じてさまざまな製品リソースを提供しています。リソースを使用して Informatica 製品とソリューションを最大限に活用し、その他の Informatica ユーザーや各分野の専門家から知見を得ることができます。

Informatica マニュアル

Informatica マニュアルポータルでは、最新および最近の製品リリースに関するドキュメントの膨大なライブラリを参照できます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

製品マニュアルに関する質問、コメント、ご意見については、Informatica マニュアルチーム（infa_documentation@informatica.com）までご連絡ください。

Informatica Intelligent Cloud Services Web サイト

Informatica Intelligent Cloud Services Web サイト（http://www.informatica.com/cloud）にアクセスできます。このサイトには、Informatica Cloud 統合サービスに関する情報が含まれます。

Informatica Intelligent Cloud Services コミュニティ

Informatica Intelligent Cloud Services コミュニティを使用して、技術的な問題について議論し、解決します。また、技術的なヒント、マニュアルの更新情報、FAQ（よくある質問）への答えを得ることもできます。

次の Informatica Intelligent Cloud Services コミュニティにアクセスします。

https://network.informatica.com/community/informatica-network/products/cloud-integration

開発者は、次の Cloud 開発者コミュニティで詳細情報を確認したり、ヒントを共有したりできます。

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services マーケットプレース

Informatica マーケットプレイスにアクセスすると、データ統合コネクタ、テンプレート、およびマップレットを試用したり購入したりできます。

https://marketplace.informatica.com/

データ統合コネクタのドキュメント

データ統合コネクタのドキュメントには、マニュアルポータルからアクセスできます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

Informatica ナレッジベース

Informatica ナレッジベースを使用して、ハウツー記事、ベストプラクティス、よくある質問に対する回答など、製品リソースを見つけることができます。

ナレッジベースを検索するには、https://search.informatica.com にアクセスしてください。ナレッジベースに関する質問、コメント、ご意見の連絡先は、Informatica ナレッジベースチーム（KB_Feedback@informatica.com）です。

Informatica Intelligent Cloud Services Trust Center

Informatica Intelligent Cloud Services Trust Center は、Informatica のセキュリティポリシーおよびリアルタイムでのシステムの可用性について情報を提供します。

Trust Center（https://www.informatica.com/trust-center.html）にアクセスします。

Informatica Intelligent Cloud Services Trust Center にサブスクライブして、アップグレード、メンテナンス、およびインシデントの通知を受信します。Informatica Intelligent Cloud Services Status ページには、すべての Informatica Cloud 製品の実稼働ステータスが表示されます。メンテナンスの更新はすべてこのページに送信され、停止中は最新の情報が表示されます。更新と停止の通知がされるようにするには、Informatica Intelligent Cloud Services の 1 つのコンポーネントまたはすべてのコンポーネントについて更新の受信をサブスクライブします。すべてのコンポーネントにサブスクライブするのが、更新を逃さないようにするための最良の方法です。

登録するには、https://status.informatica.com/に移動し、**[更新を購読登録]** をクリックします。その後、電子メール、SMS テキストメッセージ、Webhook、RSS フィードとして、またはこの 4 つを任意に組み合わせて送信された通知を受信することを選択ができます。

Informatica グローバルカスタマサポート

電話またはオンラインでカスタマサポートセンターに連絡できます。

オンラインサポートについては、Informatica Intelligent Cloud Services の **[サポート要求の送信]** をクリックしてください。またオンラインサポートを使用して問題を記録することもできます。オンラインサポートを利用するには、ログインが必要です。https://network.informatica.com/welcome でログイン要求できます。

Informatica グローバルカスタマサポートの電話番号は、Informatica の Web サイト https://www.informatica.com/services-and-training/support-services/contact-us.html に掲載されています。

第 1 章

ユーザー管理

組織とアセットへのアクセスを許可するようにユーザーとユーザーグループを設定します。ユーザーは、組織への安全なアクセスを可能にする Informatica Intelligent Cloud Services の個別アカウントです。

ユーザーを設定するには、Microsoft Azure または SAML サードパーティ ID プロバイダを介してシングルサインオンを設定します。管理者で直接ユーザーを作成することもできます。Microsoft Azure を使用した SAML 構成の詳細については、第 2 章,「エコシステムのシングルサインオン」 (ページ 8)を参照してください。サードパーティの ID プロバイダを使用した SAML 構成の詳細については、第 3 章,「SAML のシングルサインオン」 (ページ 10)を参照してください。ユーザーアカウントを直接設定する方法に関する詳細については、第 4 章,「ユーザー」 (ページ 23)を参照してください。

ユーザーグループは、グループのすべてのメンバが同じタスクを実行し、さまざまなタイプのアセットに対して同じアクセス権を持つことができるユーザーアカウントのグループです。ユーザーグループの詳細については、第 5 章,「ユーザグループ」 (ページ 34)を参照してください。

ユーザーとグループは、割り当てられたロールに基づいてタスクを実行し、アセットにアクセスすることができます。ユーザーロールの詳細については、第 6 章,「ユーザーロール」 (ページ 37)を参照してください。

第 2 章

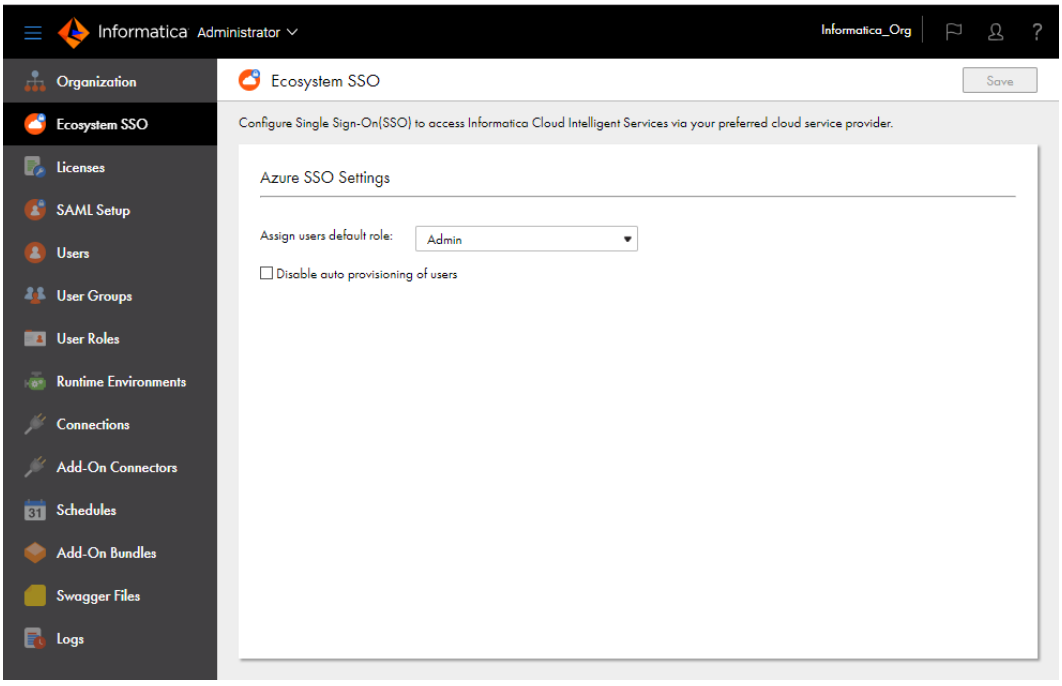
エコシステムのシングルサインオン

Informatica Intelligent Cloud Services で、Microsoft Azure ユーザーのシングルサインオン機能を有効にします。これにより、Microsoft Azure ユーザーはログイン情報を入力し直すことなく Informatica Intelligent Cloud Services にサインインできます。

Microsoft Azure で組織を作成する場合、Microsoft Azure ユーザー向けの一部のシングルサインオンプロパティを［**Ecosystem SSO（エコシステムの SSO）**］ページで設定できます。

注: Microsoft Azure 用に設定するエコシステムのシングルサインオンプロパティは、サードパーティの ID プロバイダからシングルサインオンを有効にするために設定する SAML のシングルサインオンプロパティとは異なります。組織の SAML シングルサインオンを設定するには、第 3 章, 「SAML のシングルサインオン」 (ページ 10)を参照してください。

次の図は、［**Ecosystem SSO（エコシステムの SSO）**］ページを示しています。



Microsoft Azure ユーザーに対して次のプロパティを設定できます。

Assign users default role（**ユーザーにデフォルトロールを割り当て**）

Microsoft Azure ユーザーが組織に初めてサインインしたときに、Informatica Intelligent Cloud Services によってユーザーが組織に追加され、ユーザーにデフォルトロールが割り当てられます。デフォルトでは、Informatica Intelligent Cloud Services によってユーザーに管理者ロールが割り当てられます。

デフォルトロールは、デザイナロールなどの別のロールに変更できます。デフォルトのユーザーロールを変更するには、**[Assign users default role（ユーザーにデフォルトロールを割り当て）]** リストで別のロールを選択します。

注: Microsoft Azure ユーザーが Secure Agent のダウンロード、インストール、登録を行えるようにする場合は、管理者ロールまたはデザイナロールを割り当てます。Secure Agent の作成、読み取り、および更新を行える特権を持つカスタムロールをユーザーに割り当てることもできます。

ユーザーの自動プロビジョニングの無効化

デフォルトでは、Microsoft Azure ユーザーが Azure のデータアクセラレータに初めてサインインしたときに、Informatica Intelligent Cloud Services によってユーザーが組織に追加されます。このプロセスを自動プロビジョニングと呼びます。

Microsoft Azure ユーザーの自動プロビジョニングは有効化または無効化できます。これを行うには、**[ユーザーの自動プロビジョニングの無効化]** オプションを有効または無効にします。

注: 自動プロビジョニングを無効にした場合、**[ユーザー]** ページで各ユーザーを作成する必要があります。ユーザーが Microsoft Azure からシングルサインオンを使用できるようにする場合は、[ユーザーの詳細] ページの **[認証]** フィールドを **[Azure SSO]** に設定する必要があります。

第 3 章

SAML のシングルサインオン

シングルサインオン（SSO）機能を有効にして、ユーザーがログイン情報を入力せずに組織にアクセスできるようにすることができます。SSO は、ユーザー認証、または組織内の認証と承認に使用できます。組織の SSO 機能は、**[SAML セットアップ]** ページで設定します。

Informatica Intelligent Cloud Services へのシングルサインオンは、Security Assertion Markup Language（SAML）2.0 Web ブラウザシングルサインオンプロファイルに基づいています。SAML Web ブラウザシングルサインオンプロファイルは、次のエンティティで構成されています。

ID **プロバイダ**

認証情報を管理し、セキュリティトークンを使用して認証サービスを提供するエンティティ。

サービスプロバイダ

Web サービスをプリンシパルに提供するエンティティ（Web アプリケーションをホストするエンティティなど）。Informatica Intelligent Cloud Services はサービスプロバイダです。

プリンシパル

HTTP ユーザーエージェントを介して対話するエンドユーザー。

SAML 2.0 は、セキュリティトークンを使用する XML ベースのプロトコルです。セキュリティトークンには、ID プロバイダとサービスプロバイダ間でプリンシパルに関する情報を渡すアサーションが含まれます。アサーションは、SAML オーソリティによって作成されるステートメントを提供する情報のパッケージです。SAML の詳細については、Oasis Web サイト（https://www.oasis-open.org）を参照してください。

ユーザーがブラウザに Informatica Intelligent Cloud Services URL を入力した際、またはチックレット経由で Informatica Intelligent Cloud Services を起動した際に発生するプロセスは、組織が認証のみに SAML SSO を使用しているか、または認証と承認に使用しているかによって異なります。

認証のみの SAML シングルサインオン

ユーザーが Informatica Intelligent Cloud Services にサインオンし、組織がユーザー認証にのみ SAML SSO を使用している場合、次のプロセスが発生します。

1. Informatica Intelligent Cloud Services は、SAML 認証要求を組織の ID プロバイダに送信します。
2. ID プロバイダはユーザーの ID を確認し、SAML 認証応答を Informatica Intelligent Cloud Services に送信します。認証応答には SAML トークンが含まれます。
3. Informatica Intelligent Cloud Services は、ID プロバイダから SAML 認証応答を受信すると、次のタスクを実行します。
   - ユーザーが存在する場合、Informatica Intelligent Cloud Services はユーザーセッションを確立し、ユーザーにログインします。
   - ユーザーが存在せず、ユーザーの自動プロビジョニングが有効になっている場合、Informatica Intelligent Cloud Services は SAML トークンからユーザー属性を取得してユーザーを作成し、設定さ

れている場合はユーザーにデフォルトのロールとデフォルトのグループを割り当てます。Informatica Intelligent Cloud Services はユーザーセッションを確立し、ユーザーにログインします。

- ユーザーが存在せず、ユーザーの自動プロビジョニングが無効になっている場合、Informatica Intelligent Cloud Services はログインに失敗します。

4. ユーザーが Informatica Intelligent Cloud Services からログアウトするか、セッションがタイムアウトすると、Informatica Intelligent Cloud Services は SAML ログアウト要求を ID プロバイダに送信します。
5. ID プロバイダは、ID プロバイダ側でユーザーセッションを終了します。

認証および承認用の SAML シングルサインオン

ユーザーが Informatica Intelligent Cloud Services にサインオンし、組織が認証と承認に SAML SSO を使用している場合、次のプロセスが発生します。

1. Informatica Intelligent Cloud Services は、SAML 認証要求を組織の ID プロバイダに送信します。
2. ID プロバイダはユーザーの ID を確認し、SAML 認証応答を Informatica Intelligent Cloud Services に送信します。認証応答には SAML トークンが含まれます。
3. Informatica Intelligent Cloud Services は、ID プロバイダから SAML 認証応答を受信すると、次のタスクを実行します。
   - ユーザーが存在する場合、Informatica Intelligent Cloud Services は、SAML トークンからユーザーのロール、グループ、および属性を取得します。対応する Informatica Intelligent Cloud Services のユーザーロールとグループを検索し、必要に応じてユーザーロールを更新します。Informatica Intelligent Cloud Services はユーザーセッションを確立し、ユーザーにログインします。
   - ユーザーが存在せず、ユーザーの自動プロビジョニングが有効になっている場合、Informatica Intelligent Cloud Services は SAML トークンからユーザーのロール、グループ、および属性を取得し、ユーザーを作成します。Informatica Intelligent Cloud Services はユーザーセッションを確立し、ユーザーにログインします。トークンに SAML ロールまたはグループ情報が含まれていない場合、Informatica Intelligent Cloud Services はログインに失敗します。
   - ユーザーが存在せず、ユーザーの自動プロビジョニングが無効になっている場合、Informatica Intelligent Cloud Services はログインに失敗します。
4. ユーザーが Informatica Intelligent Cloud Services からログアウトするか、セッションがタイムアウトすると、Informatica Intelligent Cloud Services は SAML ログアウト要求を ID プロバイダに送信します。
5. ID プロバイダは、ID プロバイダ側でユーザーセッションを終了します。

SAML のシングルサインオンの要件

Informatica Intelligent Cloud Services 組織の SAML シングルサインオンをセットアップするには、システムに適した ID プロバイダを使用する必要があります。また、適切なライセンスを使用する必要があります。

組織の SAML シングルサインオンをセットアップするには、次の要件が満たされていることを確認します。

- システムでは SAML 2.0 ベースの ID プロバイダを使用する必要があります。

  共通の ID プロバイダには、Microsoft Active Directory フェデレーションサービス（AD FS）、Okta、SSOCircle、OpenLDAP および Shibboleth が含まれています。DSA-SHA256 または RSA-SHA256 のいずれかのアルゴリズムを使用して署名を生成するように ID プロバイダを設定する必要があります。
- Informatica Intelligent Cloud Services の組織は SAML ベースのシングルサインオンライセンスを使用する必要があります。
- シングルサインオンを設定するために組織の管理者として組織にアクセスできる。

シングルサインオンの制限

Informatica Intelligent Cloud Services への SAML シングルサインオンアクセスにはいくつかの制限があります。

SAML シングルサインオンアクセスには、次の制限が適用されます。

- ID プロバイダのライセンスの有効期限が切れると、シングルサインオンを使用して Informatica Intelligent Cloud Services にアクセスできなくなります。
- ID プロバイダがダウンしている場合、または Informatica Intelligent Cloud Services のサーバーが ID プロバイダにアクセスできない場合、ユーザーはシングルサインオンを使用して Informatica Intelligent Cloud Services にログインすることができません。
- Informatica Intelligent Cloud Services への SAML シングルサインオンで使用される ID プロバイダ証明書の有効期限が切れると、ユーザーはシングルサインオンを使用して Informatica Intelligent Cloud Services にアクセスできなくなります。
- 組織で信頼済み IP アドレス範囲を使用する場合、ユーザーは信頼済み IP アドレス範囲外の IP アドレスで Informatica Intelligent Cloud Services にログインすることができません。

SAML 認証によるユーザー管理

ユーザー認証のみに SAML SSO を使用している場合、Informatica Intelligent Cloud Services は、ユーザーが Informatica Intelligent Cloud Services へのサインオンを試みるたびユーザー資格情報を検証します。ユーザー認証は、ユーザーのグループとロールの割り当てを通じて Informatica Intelligent Cloud Services 内で管理されます。

認証のみに SAML SSO を使用するには、**［SAML セットアップ］**ページの**［SAML グループとロールのマッピング］**オプションを無効にします。このオプションはデフォルトで無効になっています。このオプションを無効にした場合、このページで新規ユーザーのデフォルトのユーザーロールを設定する必要があります。また、デフォルトのユーザーグループを設定することもできます。

認証のみに SAML を使用する場合、ユーザーは次の方法で管理されます。

自動プロビジョニングが有効な新規ユーザー

新規ユーザーが Informatica Intelligent Cloud Services に初めてサインオンし、自動プロビジョニングが有効である場合、Informatica Intelligent Cloud Services は、SAML トークンから名、姓、電子メールアドレスなどのユーザー属性を取得し、それらをリポジトリに格納します。また、ユーザーを作成し、ユーザーにデフォルトのロールと、設定されている場合はデフォルトのグループを割り当てます。

アセットへのユーザーのアクセスレベルを調整する場合は、ユーザーの詳細ページでユーザーのグループとロールの割り当てを更新します。

自動プロビジョニングが無効な新規ユーザー

自動プロビジョニングが無効である場合、ユーザーが Informatica Intelligent Cloud Services に初めてサインオンしようとしたときでも、組織に自動で追加されません。管理者でユーザーを作成する必要があります。

既存のユーザー

既存のユーザーがサインオンすると、Informatica Intelligent Cloud Services はユーザーを認証しますが、SAML トークンから SAML ロール、グループ、またはユーザー属性を取得しません。この情報が変更された場合は、ユーザーの詳細ページでユーザーのグループとロールを更新できます。

また、Administrator で資格情報を使用してネイティブユーザーアカウントを作成することもできます。この場合、ユーザー資格情報は Informatica Intelligent Cloud Services リポジトリに保存されます。これを行う場合、ユーザーはシングルサインオンを使用するのではなく、Informatica Intelligent Cloud Services に直接ログインする必要があります。

Informatica Intelligent Cloud Services からユーザーを削除すると、そのユーザーは Informatica Intelligent Cloud Services リポジトリから削除されますが、ID プロバイダからは削除されません。

すべての SAML ユーザーについて、ユーザープロファイルの情報は、タイムゾーン以外は読み取り専用です。パスワードとセキュリティの質問は、ユーザープロファイルに表示されません。

SAML 認証と承認からの切り替え

組織で認証と承認に SAML を使用しており、認証のみに SAML を使用するように変更する場合は、**[SAML グループとロールのマッピング]** オプションを無効にできます。

このオプションが有効であった場合、このオプションを無効にすると、**[SAML セットアップ]** ページのグループとロールのマッピング情報は読み取り専用となりますが、削除はされません。すべての SAML グループは、通常の Informatica Intelligent Cloud Services グループになります。グループの編集、削除、およびグループメンバーの追加と削除を行うことができます。

このオプションを無効にしてもユーザーの Informatica Intelligent Cloud Services ロールは変更されないため、スケジュールされたジョブに影響が及ぶことはありません。

SAML 認証と承認によるユーザー管理

ユーザーの認証と承認に SAML SSO を使用している場合、Informatica Intelligent Cloud Services はユーザーがサインオンを試みるたびにユーザーの資格情報を検証します。また、ユーザーの SAML グループとロールを取得し、対応する Informatica Intelligent Cloud Services ロールをユーザーに割り当てます。

認証と承認に SAML SSO を使用するには、**[SAML セットアップ]** ページで **[SAML グループとロールのマッピング]** オプションを有効にします。一部の ID プロバイダでは、SCIM 2.0 を使用してユーザーおよびグループ情報を Informatica Intelligent Cloud Services にプッシュすることもできます。

[SAML グループとロールのマッピング] オプションを有効にした場合は、**[SAML セットアップ]** ページで SAML グループとロールに Informatica Intelligent Cloud Services ロールをマッピングする必要があります。ロールとグループをマッピングすることで、ユーザーは Informatica Intelligent Cloud Services アセットに適切なレベルでアクセスできるようになります。管理者で、これらのユーザーのユーザーロールまたはグループを個別に設定することはできません。

[SAML セットアップ] ページでマッピングした SAML グループが Informatica Intelligent Cloud Services に存在しない場合、Informatica Intelligent Cloud Services はそれらのユーザーグループを作成します。これらのグループは **[ユーザーグループ]** ページで表示できますが、グループ情報を編集したり、グループメンバーを変更したりすることはできません。

Informatica Intelligent Cloud Services は、SAML グループおよびロールが **[SAML セットアップ]** ページにマッピングされていない場合、SAML トークンで返されたこれらのグループおよびロールを無視します。

認証と承認に SAML を使用している場合、ユーザーは次の方法で管理されます。

自動プロビジョニングが有効な新規ユーザー

新規ユーザーが Informatica Intelligent Cloud Services に初めてサインオンし、自動プロビジョニングが有効である場合、Informatica Intelligent Cloud Services は、SAML トークンから SAML ロール、グループ、およびユーザー属性を取得し、それらをリポジトリに格納します。また、ユーザーを作成して認証し、

［**SAML セットアップ**］ページにマッピングされている Informatica Intelligent Cloud Services ロールをユーザーに割り当てます。

SAML トークンにロールまたはグループがない場合、Informatica Intelligent Cloud Services はログインに失敗します。

自動プロビジョニングが無効な新規ユーザー

自動プロビジョニングが無効である場合、ユーザーが Informatica Intelligent Cloud Services に初めてサインオンしようとしたときでも、組織に自動で追加されません。管理者でユーザーを作成する必要があります。

既存のユーザー

既存のユーザーがサインオンすると、Informatica Intelligent Cloud Services はユーザーを認証し、SAML トークンから SAML ロール、グループ、およびユーザー属性を取得します。前回のログイン以降にこの情報が変更されている場合、Informatica Intelligent Cloud Services はユーザー属性とロールを更新します。

また、Administrator で資格情報を使用してネイティブユーザーアカウントを作成することもできます。この場合、ユーザー資格情報は Informatica Intelligent Cloud Services リポジトリに保存されます。これを行う場合、ユーザーはシングルサインオンを使用するのではなく、Informatica Intelligent Cloud Services に直接ログインする必要があります。これらのユーザーアカウントは、Administrator で削除できます。

すべての SAML ユーザーについて、ユーザープロファイルの情報は、タイムゾーン以外は読み取り専用です。パスワードとセキュリティの質問は、ユーザープロファイルに表示されません。

SAML 認証のみからの切り替え

組織で SAML 認証のみを使用しており、認証と承認に SAML を使用するように変更する場合は、［**SAML グループとロールのマッピング**］オプションを有効にできます。

このオプションが無効であった場合、このオプションを有効にすると、［**SAML セットアップ**］ページのグループとロールのマッピング情報が編集可能になります。グループまたはロールのマッピングが設定されていた場合、それらの設定は保持されます。

このオプションを有効にすると、Informatica Intelligent Cloud Services で新しい SAML トークンを使用して認証されたときに、ユーザーの認証情報が更新されます。ユーザーの特権が変更された場合、これはユーザーのスケジュールされたジョブに影響を及ぼす可能性があります。

SCIM 2.0 を使用したユーザーおよびグループ情報のプッシュ

認証と承認に SAML SSO を使用し、ID プロバイダが Okta または Azure Active Directory である場合、SCIM 2.0 を使用してユーザーとグループの情報を Informatica Intelligent Cloud Services にプッシュするという選択ができます。この選択を行うためには、［**SAML セットアップ**］ページで［**IdP を有効にし、SCIM 2.0 を使用してユーザー/グループをプッシュ**］オプションを有効にします。

このオプションを有効にすると、ID プロバイダはユーザーとグループの情報を定期的にプッシュして、新しいユーザーのプロビジョニング、ユーザーの削除、および Informatica Intelligent Cloud Services のユーザーロールに対する各ユーザーの SAML グループとロールの同期ができるようになります。この場合、ユーザーは SCIM 経由でプロビジョニングされるため、ユーザーの自動プロビジョニングは無効になります。管理者でユーザーを手動で作成することもできます。

Informatica Intelligent Cloud Services は、ID プロバイダが Informatica Intelligent Cloud Services で特定の操作を実行するために使用する SCIM エンドポイントをホストします。これらの操作には、ユーザーの作成と非アクティブ化、ユーザーグループの作成と削除、グループに対するユーザーの追加と削除、およびユーザー属性の更新が含まれます。

SCIM エンドポイントにアクセスするには、Azure Active Directory または Okta でプロビジョニングアプリを SCIM クライアントとして作成する必要があります。SCIM エンドポイントにアクセスするために特別な特権は必要ありません。アプリを作成する場合は、**[SAML セットアップ]** ページで生成したトークンを指定する必要があります。SCIM 2.0 のセットアップとプロビジョニングアプリの作成については、Informatica Network に関する次の H2L の記事を参照してください。

- Setting up SCIM with Azure Active Directory
- Setting up SCIM with Okta

SCIM プロビジョニングを有効にすると、表示名、従業員番号、組織、部署、部門などの追加のユーザー属性も Informatica Intelligent Cloud Services にプッシュされます。これらの属性を **[SAML セットアップ]** ページにマッピングする必要があります。ユーザーの詳細ページで、それぞれのユーザーに対するこれらの属性を表示できます。

また、個々のユーザーのユーザーおよびグループ情報が、シングルサインオン中に SAML トークンで渡されます。これにより、ユーザーの SAML ロール、グループ、または属性が変更された場合、Informatica Intelligent Cloud Services では、ユーザーがサインオンしたときにユーザー情報が更新されます。

Informatica Intelligent Cloud Services の SAML シングルサインオン設定

Informatica Intelligent Cloud Services と ID プロバイダは、シングルサインオンの設定時に設定情報を交換します。

認証要求と承認要求を ID プロバイダに送信するには、Informatica Intelligent Cloud Services に ID プロバイダメタデータが必要です。応答を Informatica Intelligent Cloud Services に送信するには、ID プロバイダに Informatica Intelligent Cloud Services のサービスプロバイダメタデータが必要です。

認証応答で渡されるデータを Informatica Intelligent Cloud Services でコンシュームできるように、SAML と Informatica Intelligent Cloud Services の属性をマッピングする必要があります。Informatica Intelligent Cloud Services でシングルサインオンを設定したら、Informatica Intelligent Cloud Services サービスプロバイダメタデータを ID プロバイダに渡します。

Informatica Intelligent Cloud Services のシングルサインオンを設定するには、次のタスクを実行します。

1. SAML ID プロバイダとサービスプロバイダを設定し、Informatica Intelligent Cloud Services で SAML の属性を Informatica Intelligent Cloud Services の属性にマッピングします。
2. Informatica Intelligent Cloud Services から Informatica Intelligent Cloud Services サービスプロバイダメタデータをダウンロードし、組織のメタデータおよび Informatica Intelligent Cloud Services シングルサインオン URL を SAML の ID プロバイダ管理者に配信します。

プロバイダ設定とマッピング属性の設定

[SAML セットアップ] ページで、SAML のシングルサインオンを設定して SAML の属性をマップします。

1. 組織の管理者として Informatica Intelligent Cloud Services にログインします。
2. 管理者で、**[SAML セットアップ]** を選択します。

3. **［SAML セットアップ］**ページで、次のプロパティを設定します。
   - SSO 設定のプロパティ
   - ID プロバイダ設定のプロパティ
   - サービスプロバイダ設定
   - SAML 属性マッピングのプロパティ
   - SAML ロールとグループマッピングのプロパティ（認証と承認に SAML SSO を使用する場合）
4. **［保存］**をクリックします。

   Informatica Intelligent Cloud Services はサービスプロバイダメタデータファイルを生成します。また、Informatica Intelligent Cloud Services は組織固有のトークンを生成し、このトークンを Informatica Intelligent Cloud Services リポジトリに保存します。組織のシングルサインオン URL にトークンが含まれます。例:

   `https://dm-us.informaticacloud.com/ma/sso/<組織のトークン>`

［SAML セットアップ］ページに変更を保存した後、サービスプロバイダメタデータをダウンロードし、Informatica Intelligent Cloud Services シングルサインオン URL と共にこのデータを ID プロバイダに送信します。

SSO 設定のプロパティ

［SAML セットアップ］ページでシングルサインオン設定のプロパティを定義します。

ID プロバイダ XML ファイルがある場合、そのファイルをアップロードして、一部のプロパティを取り込むことができます。Informatica Intelligent Cloud Services は、XML ファイルから大部分のデータを解析して抽出できます。ただし、名前識別子の形式などの特定のフィールドを手動で入力することが必要になる場合もあります。

以下の表に、SSO 設定のプロパティを示します。

プロパティ	説明
ID プロバイダファイルを使用	**［**SAML **セットアップ］**ページの多くのプロパティにデータを入力する ID プロバイダの XML ファイル。 ID プロバイダ XML ファイルを使用して ID プロバイダのプロパティを定義するには、**［参照］**をクリックし、ID プロバイダ XML ファイルに移動します。
ユーザーの自動プロビジョニングの無効化	SAML ユーザーの自動プロビジョニングを無効にします。 このオプションを有効にすると、ユーザーが Informatica Intelligent Cloud Services に初めてサインオンしようとしたときでも、組織に自動で追加されません。 自動プロビジョニングが無効な状態で ID プロバイダからユーザーおよびグループ情報をプッシュする際に SCIM 2.0 を使用しない場合は、管理者でユーザーを手動で作成する必要があります。 SCIM 2.0 を使用する場合、SCIM クライアントによってユーザーがプロビジョニングされるため、このオプションは無効になります。 デフォルトでは無効になっています。

プロパティ	説明
SAML グループとロールのマッピング	ユーザーが Informatica Intelligent Cloud Services にサインオンするたびに、SAML トークンからグループとロールをマッピングします。 認証と承認に SAML SSO を使用するには、このオプションを有効にします。認証のみに SAML SSO を使用するには、このオプションを無効にします。 デフォルトでは無効になっています。
IdP を有効にし、SCIM 2.0 を使用してユーザー/グループをプッシュ	ID プロバイダが SAML トークンでこれらの属性を渡すとともに、SCIM 2.0 を使用してユーザーおよびグループ情報を Informatica Intelligent Cloud Services にプッシュできるようにします。 このオプションを有効にする場合は、ID プロバイダ（SCIM クライアント）のベアラトークンを生成する必要があります。トークンを生成するには、**[トークンの生成]** をクリックします。 **警告:** ID プロバイダにトークンを提供した後に新しいトークンを生成した場合は、前のトークンが上書きされるため、ID プロバイダに新しいトークンを提供する必要があります。 このオプションを有効にすると、SCIM クライアント経由でユーザーがプロビジョニングされるため、ユーザーの自動プロビジョニングは無効になります。 デフォルトでは無効になっています。

ID プロバイダ設定のプロパティ

[SAML セットアップ] ページで ID プロバイダ設定のプロパティを定義します。

次表に、ID プロバイダ設定のプロパティを示します。

プロパティ	説明
発行者	ID プロバイダのエンティティ ID。これは、一意の識別子です。 ID プロバイダから Informatica Intelligent Cloud Services へのすべてのメッセージの発行者の値は、この値と一致する必要があります。例: `<saml:Issuer>http://idp.example.com</saml:Issuer>`
シングルサインオンサービス URL	SingleSignOnService に対する ID プロバイダの HTTP-POST SAML バインディング URL。これは、SingleSignOnService 要素の場所属性です。Informatica Intelligent Cloud Services はこの URL にログイン要求を送信します。
シングルログアウトサービス URL	SingleLogoutService に対する ID プロバイダの HTTP-POST SAML バインディング URL。これは、SingleLogoutService 要素の場所属性です。Informatica Intelligent Cloud Services はこの URL にログアウト要求を送信します。
署名証明書	Informatica Intelligent Cloud Services が ID プロバイダからの署名済み SAML メッセージの検証に使用する、Base64 でエンコードされた PEM 形式の ID プロバイダ証明書です。 **注:** ID プロバイダ署名アルゴリズムが DSA-SHA1 または RSA-SHA1 のいずれかである必要があります。
暗号化に署名証明書を使用します	署名証明書のパブリックキーを使用して、ユーザーが Informatica Intelligent Cloud Services からログアウトするときに ID プロバイダに送信されるログアウト要求を暗号化できます。
暗号化証明書	Informatica Intelligent Cloud Services が ID プロバイダに送信された SAML メッセージの暗号化に使用する、Base64 でエンコードされた PEM 形式の ID プロバイダ証明書です。 署名証明書を使用して暗号化しない場合に適用できます。

プロパティ	説明
名前識別子の形式	ID プロバイダが Informatica Intelligent Cloud Services に返す認証要求の名前識別子の形式。Informatica Intelligent Cloud Services は、名前識別子の値を Informatica Intelligent Cloud Services のユーザー名として使用します。 名前識別子は、ログインごとに変更される可能性のある一時的な値にすることはできません。特定のユーザーの Informatica Intelligent Cloud Services への各シングルサインオンログインには、同じ名前識別子の値が含まれている必要があります。 名前識別子が電子メールアドレスになるように指定する場合、名前識別子の形式は次のようになります。 `urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress`
ログアウトサービス URL (SOAP バインディング)	シングルログアウトサービスの ID プロバイダの SAML SOAP バインディング URL。Informatica Intelligent Cloud Services はこの URL にログアウト要求を送信します。
ログアウトページ URL	ユーザーが Informatica Intelligent Cloud Services からログアウトした後にリダイレクトされるランディングページです。 Informatica Intelligent Cloud Services では、次の方法でログアウトしたユーザーをランディングページにリダイレクトします。 - ログアウトページ URL を指定した場合、ログアウト後に Informatica Intelligent Cloud Services はユーザーをこの URL にリダイレクトします。 - ログアウトページ URL を指定していない場合、Informatica Intelligent Cloud Services はユーザーをデフォルトログアウトページにリダイレクトします。

サービスプロバイダ設定

[SAML セットアップ] ページで Informatica Intelligent Cloud Services のサービスプロバイダの設定を定義します。

次の表に、サービスプロバイダの設定を示します。

プロパティ	説明
Informatica Cloud プラットフォーム SSO	組織のシングルサインオン URL を表示します。この URL は Informatica Intelligent Cloud Services によって自動的に生成されます。
クロックスキュー	ID プロバイダからの SAML 応答のタイムスタンプと Informatica Intelligent Cloud Services のクロック間の最大許容時間を秒単位で指定します。 デフォルトは 180 秒（3 分）です。
名前識別子の値は、ユーザーの電子メールアドレスを表します	有効にした場合、Informatica Intelligent Cloud Services は、電子メールアドレスを名前識別子として使用します。 デフォルトでは有効になっています。
認証要求への署名	有効にした場合、Informatica Intelligent Cloud Services は、ID プロバイダへの認証要求に署名します。 デフォルトでは有効になっています。

プロパティ	説明
SOAP バインディングを使用して送信したログアウト要求に署名	有効にした場合、Informatica Intelligent Cloud Services は、ID プロバイダに送信されるログアウト要求に署名します。 デフォルトでは有効になっています。
ログアウト要求の名前 ID を暗号化	有効にした場合、Informatica Intelligent Cloud Services は、ログアウト要求の名前識別子を暗号化します。 **注**: このオプションを有効にする前に、ID プロバイダが名前識別子の復号化をサポートしていることを確認してください。 デフォルトでは無効になっています。

SAML 属性マッピングのプロパティ

名前、電子メールアドレス、ユーザーロールなどのユーザーログイン属性は、ID プロバイダから Informatica Intelligent Cloud Services への認証応答に含まれます。ID プロバイダが SCIM 2.0 を使用してユーザーおよびグループ情報を渡す場合、認証応答には、表示名、従業員番号、組織などの追加の SCIM 属性が含まれます。

Informatica Intelligent Cloud Services のユーザーフィールドを、**[SAML セットアップ]** ページの対応する SAML 属性にマッピングします。

注: 属性の形式は ID プロバイダによって異なります。詳細については、プロバイダのマニュアルを参照してください。

次の表に、SAML 属性マッピングのプロパティを示します。

プロパティ	説明
わかりやすい SAML 属性名を使用します	選択されている場合は、SAML 属性名のわかりやすい形式が使用されます。これは、OID や UUID など、属性名が複雑な場合やわかりにくい場合に役立つことがあります。
名	ユーザーの名を渡すために使用される SAML 属性。
姓	ユーザーの姓を渡すために使用される SAML 属性。
役職	ユーザーの役職を渡すために使用される SAML 属性。
電子メールアドレス	ユーザーの電子メールアドレスを渡すために使用される SAML 属性。このプロパティはマッピングする必要があります。
電子メール区切り文字	複数の電子メールアドレスが渡される場合に電子メールアドレスを区切る区切り文字。
電話番号	ユーザーの電話番号を渡すために使用される SAML 属性。
タイムゾーン	ユーザーの時間帯を渡すために使用される SAML 属性。
ユーザーロール	割り当てられているユーザーロールを渡すために使用される SAML 属性。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが有効になっている場合に使用できます。

プロパティ	説明
ロール区切り文字	複数のロールが渡される場合にロールを区切る区切り文字。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが有効になっている場合に使用できます。
ユーザーグループ	割り当てられているユーザーグループを渡すために使用される SAML 属性。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが有効になっている場合に使用できます。
グループ区切り文字	複数のグループが渡された場合にグループを区切るための区切り文字。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが有効になっている場合に使用できます。

以下の表に、追加の属性を示します。これらの属性は、**[IdP を有効にし、SCIM 2.0 を使用してユーザー/グループをプッシュ]** オプションが有効になっている場合に表示されます。

プロパティ	説明
表示名	ユーザーの displayName を渡すために使用される SCIM 属性。
Employee Number	エンタープライズユーザーの employeeNumber を渡すために使用される SCIM 属性。
Organization	エンタープライズユーザーの organization を渡すために使用される SCIM 属性。
Department	エンタープライズユーザーの department を渡すために使用される SCIM 属性。
Street Address	ユーザーの streetAddress を渡すために使用される SCIM 属性。
Locality	ユーザーの locality を渡すために使用される SCIM 属性。
Region	ユーザーの region を渡すために使用される SCIM 属性。
Post Code	ユーザーの postalCode を渡すために使用される SCIM 属性。
Country	ユーザーの country を渡すために使用される SCIM 属性。
Locale	ユーザーの locale を渡すために使用される SCIM 属性。
Preferred Language	ユーザーの preferredLanguage を渡すために使用される SCIM 属性。
ID	ユーザーの ID を渡すために使用される SCIM 属性。
External ID	ユーザーの externalId を渡すために使用される SCIM 属性。 Azure Active Directory の場合、これは objectID です。Okta の場合、これは ID です。

SAML ロールとグループマッピングのプロパティ

認証のみに SAML を使用する場合は、新規ユーザーに対するデフォルトのロールと、オプションとしてのデフォルトのユーザーグループを定義します。認証と承認に SAML を使用する場合は、SAML ロール名とグループ名を Informatica Intelligent Cloud Services ロール名にマッピングします。複数の SAML ロールおよびグループを単一の Informatica Intelligent Cloud Services ロールにマッピングできます。

[SAML セットアップ] ページで、SAML ロールとグループマッピングのプロパティを定義します。

次の表に、SAML ロールマッピングのプロパティを示します。

プロパティ	説明
Informatica Intelligent Cloud Services のロール	Informatica Intelligent Cloud Services のロールに相当する SAML ロール。複数のロールを入力する必要がある場合は、カンマを使用してロールを区切ります。 ロールマッピングフィールドは、[SAML **グループとロールのマッピング**] オプションが有効になっている場合に使用できます。
デフォルトロール	シングルサインオンユーザーのデフォルトユーザーロール。自動プロビジョニングが有効になっている場合、新しいユーザーが Informatica Intelligent Cloud Services に初めてサインオンしたときに、このロールが割り当てられます。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが無効になっている場合に表示されます。
デフォルトユーザーグループ	(オプション) シングルサインオンユーザーのデフォルトのユーザーグループ。自動プロビジョニングが有効になっている場合、新しいユーザーが Informatica Intelligent Cloud Services に初めてサインオンしたときに、このユーザーグループに割り当てられます。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが無効になっている場合に表示されます。

次の表に、SAML グループマッピングのプロパティを示します。

プロパティ	説明
Informatica Intelligent Cloud Services のロール	Informatica Intelligent Cloud Services のロールに相当する SAML グループ。複数のグループを入力する必要がある場合は、カンマを使用してグループを区切ります。最大で 4000 文字まで入力できます。 ロールマッピングフィールドは、[SAML **グループとロールのマッピング**] オプションが有効になっている場合に使用できます。
デフォルトロール	シングルサインオンユーザーのデフォルトユーザーロール。自動プロビジョニングが有効になっている場合、新しいユーザーが Informatica Intelligent Cloud Services に初めてサインオンしたときに、このロールが割り当てられます。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが無効になっている場合に表示されます。
デフォルトユーザーグループ	(オプション) シングルサインオンユーザーのデフォルトのユーザーグループ。自動プロビジョニングが有効になっている場合、新しいユーザーが Informatica Intelligent Cloud Services に初めてサインオンしたときに、このユーザーグループに割り当てられます。 このフィールドは、[SAML **グループとロールのマッピング**] オプションが無効になっている場合に表示されます。

サービスプロバイダメタデータのダウンロード

SAML シングルサインオンの設定プロセスを完了するには、ID プロバイダに SAML SAML サービスプロバイダメタデータおよび Informatica Intelligent Cloud Services URL が必要です。Informatica Intelligent Cloud

Services がサービスプロバイダメタデータファイルを生成したら、ファイルおよび Informatica Intelligent Cloud Services URL を ID プロバイダに配信します。

1. **［SAML セットアップ］**ページで、**［サービスプロバイダメタデータのダウンロード］**をクリックします。
   サービスプロバイダのメタデータファイルがマシンにダウンロードされます。
2. **［情報］**ダイアログボックスで、シングルサインオンアクセスの URL を Informatica Intelligent Cloud Services 組織に記録します。
3. **［OK］**をクリックして、**［情報］**ダイアログボックスを閉じます。
4. メタデータファイルおよび Informatica Intelligent Cloud Services シングルサインオン URL を ID プロバイダ管理者に送信します。

第 4 章

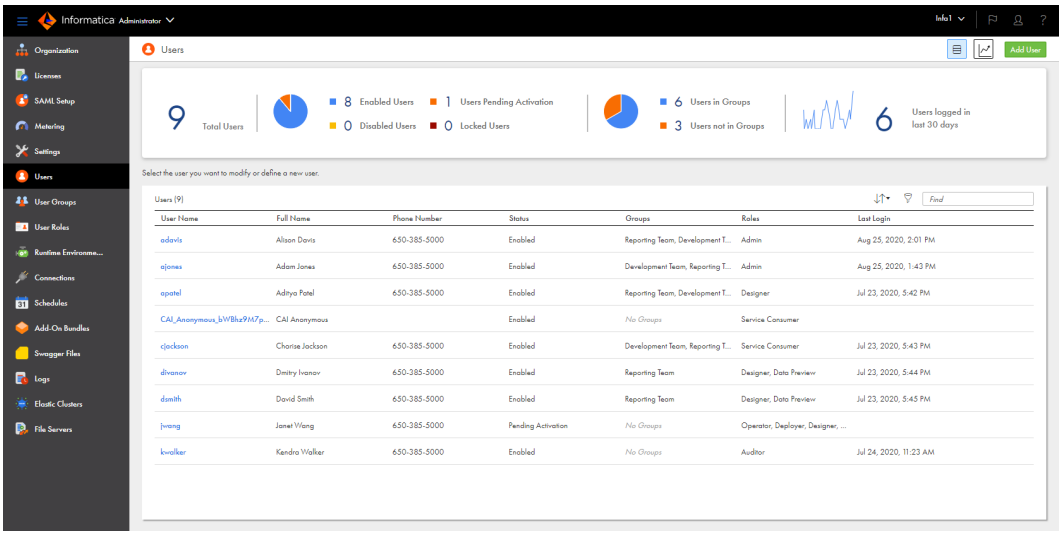
ユーザー

ユーザーは、組織への安全なアクセスを可能にする個別の Informatica Intelligent Cloud Services アカウントです。ユーザーは、そのユーザーに割り当てられたロールに基づいてタスクを実行し、アセットにアクセスできます。ロールは、ユーザーまたはユーザーが所属するグループに直接割り当てることができます。

管理者は、組織のユーザーアカウントを作成して設定できます。

[ユーザー] ページには組織のすべてのユーザーが一覧表示されます。[ユーザー] ページにアクセスするには、管理者で **[ユーザー]** を選択します。

次の図は、**[ユーザー]** ページを示しています。



[ユーザー] ページには、組織のユーザー統計が表示され、各ユーザーがリストされます。

統計領域には、ユーザーの総数、各ステータスのユーザー数、グループ内のユーザー数、および過去 30 日間にログインしたユーザー数が表示されます。過去 30 日間にログインしたユーザーの数は、組織のタイムゾーンを使用して計算され、現在の日付は除外されます。

[ユーザー] 領域には、各ユーザーが一覧表示されます。アプリケーションの統合を使用している場合、このリストにはアプリケーションの統合の匿名ユーザーとそのステータスも一覧表示されます。ユーザーの詳細情報を表示するには、ユーザー名をクリックします。

ユーザーに対して次のタスクを実行できます。

- ユーザーの詳細を表示および編集します。
- ユーザーを作成する。
- サービスを割り当ておよび割り当て解除する。

- ユーザーを無効にする。
- ユーザーをリセットする。
- ユーザーのスケジュール済みジョブを別のユーザーに再割り当てする。
- ユーザーを削除する。

ユーザー認証

Informatica Intelligent Cloud Services はさまざまなタイプのユーザー認証を使用します。ネイティブユーザーは Informatica Intelligent Cloud Services によって認証されます。Salesforce、Microsoft Azure、および SAML ユーザーは、それぞれの ID プロバイダによって認証されます。

Informatica Intelligent Cloud Services では、以下のタイプのユーザー認証を使用できます。

Native

ネイティブユーザーは、ユーザー名およびパスワードを使用して Informatica Intelligent Cloud Services のログインページから Informatica Intelligent Cloud Services にログインします。ユーザーは Informatica Intelligent Cloud Services によって認証されます。

Salesforce

Salesforce ユーザーは、Salesforce または Salesforce アプリケーションから Informatica Intelligent Cloud Services にサインインします。ユーザーは Salesforce によって認証されます。

Salesforce 認証の詳細については、データ統合のヘルプの Salesforce コネクタのヘルプを参照してください。

Microsoft Azure

Microsoft Azure ユーザーは Microsoft Azure から Informatica Intelligent Cloud Services にサインインします。ユーザーは Microsoft Azure によって認証されます。

Microsoft Azure 認証の詳細については、第 2 章, 「エコシステムのシングルサインオン」 (ページ 8)を参照してください。

SAML

SAML ユーザーは ID プロバイダから Informatica Intelligent Cloud Services にサインインします。ユーザーは ID プロバイダによって認証されます。

SAML シングルサインオンの設定の詳細については、第 3 章, 「SAML のシングルサインオン」 (ページ 10)を参照してください。

アプリケーションの統合の匿名ユーザー

Informatica Intelligent Cloud Services は、CAI_Anonymous_<Organization_ID>というシステムユーザーを作成します。アプリケーションの統合では、データ統合タスクを呼び出す匿名プロセスを開始する場合にこのユーザーを必要とします。

重要: データ統合タスクを呼び出す匿名プロセスを開始する必要がある場合は、アプリケーションの統合の匿名ユーザーを編集または削除しないでください。

データ統合タスクにカスタム権限を割り当てて、アプリケーション統合プロセスまたはガイドを介してデータ統合タスクを呼び出す場合は、次のいずれかのタスクを実行する必要があります。

- アプリケーション統合の匿名ユーザーに、関連するデータ統合アセットの実行権限を付与します。
- アプリケーション統合の匿名ユーザーを、関連するデータ統合アセットの実行権限を持つユーザーグループに追加します。

Model Serve システムユーザー

Informatica Intelligent Cloud Services は、ModelServe_System_<Organization_ID>というシステムユーザーを作成します。

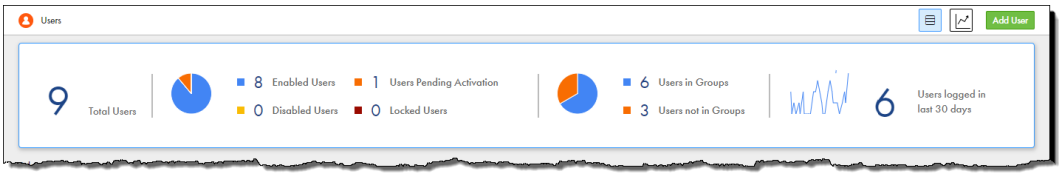
Model Serve では、機械学習モデルをデプロイするためのリソースのプロビジョニングなどのタスクを実行する場合にこのユーザーが必要になります。Model Serve システムユーザーを編集または削除することはできません。

ユーザー統計

管理者ロールを持つ場合、または「読み取りユーザー」および「監査ログ - 表示」特権を持つ場合は、組織のユーザー統計を表示できます。

[ユーザー] ページの統計領域には、組織内のユーザー数、ステータスごとのユーザー数、特定の期間にログインしたユーザー数などの統計が表示されます。

次の図は、統計領域を示しています。



統計領域を使用して、**[ユーザー]** ページ上のユーザーをフィルタできます。例えば、ステータスが「アクティベーション保留」であるユーザーのみを表示するには、**[アクティベーション保留ユーザー]** をクリックします。すべてのユーザーをリストするには、**[合計ユーザー]** をクリックします。

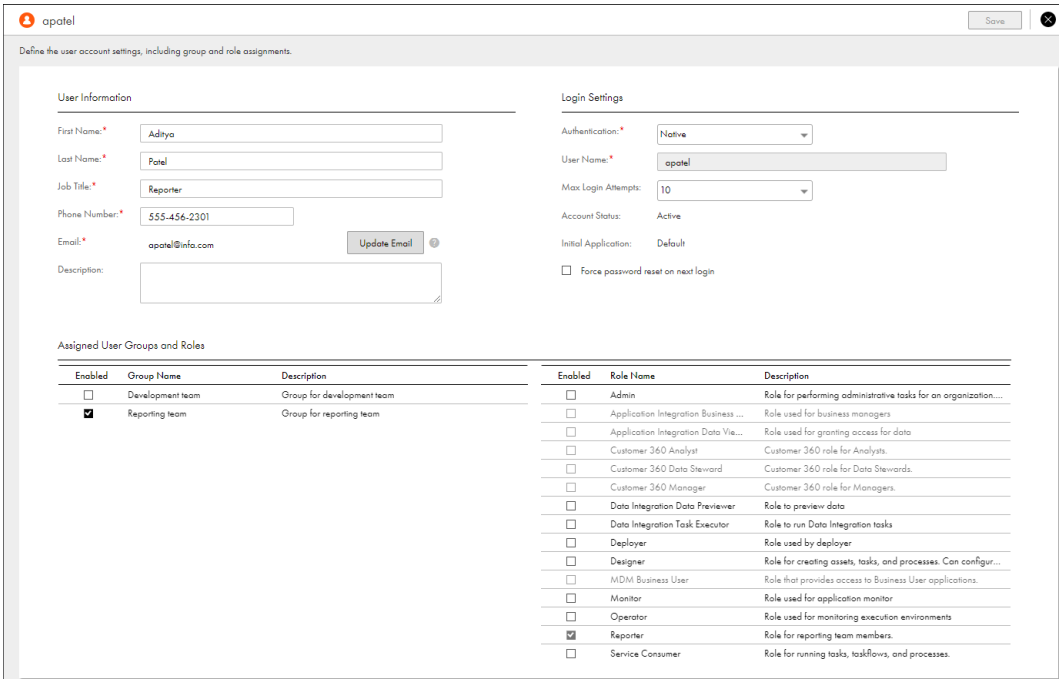
管理者ロールを持つ場合、または「ユーザーの作成」および「監査ログ - 表示」特権を持つ場合は、過去 7 日間、30 日間、または 90 日間の 1 日あたりのログインしたユーザー数のグラフを表示できます。グラフを表示するには、**[チャートビュー]** をクリックし、適切な期間を選択します。その期間における各ユーザーのログイン日時がリストされたレポートをダウンロードすることもできます。

[ユーザー] ページのリストビューに戻るには、**[リストビュー]** をクリックします。

ユーザーの詳細

ユーザー名、電子メール、ログイン設定、割り当てられたユーザーグループとロールなどのユーザーの詳細を［ユーザーの詳細］ページで設定できます。［ユーザーの詳細］ページを表示するには、管理者で **［ユーザー］** を選択し、ユーザー名をクリックします。

次の図は、［ユーザーの詳細］ページを示しています。



ユーザーに対して次の詳細を構成できます。

ユーザー情報

以下の表に、ユーザー情報を示します。

プロパティ	説明
名	ユーザーの下の名前。
姓	ユーザーの姓。
役職	ユーザーの役職。
電話番号	ユーザーの電話番号。

プロパティ	説明
電子メール	ユーザーの電子メールアドレス。 次の形式で有効な電子メールアドレスを指定する必要があります: <local_part>@<domain>例: jsmith@mycompany.com 電子メールアドレスを更新するには、**[電子メールを更新]** をクリックします。Informatica Intelligent Cloud Services から新しい電子メールアドレス宛てに確認メールが送信されます。電子メールには、24 時間有効なリンクが含まれています。ユーザーが確認メール内のリンクをクリックすると、新しい電子メールアドレスが確認され、ユーザーの詳細ページとユーザーのプロファイルに表示されます。リンクの有効期限が切れた場合は、確認メールを再送信できます。 管理者で SAML ユーザーの電子メールアドレスを更新することはできません。SAML ユーザーの電子メールアドレスを更新するには、ID プロバイダで電子メールアドレスを更新します。
説明	ユーザーの説明（省略可能）。

拡張ユーザー属性

組織で認証と承認に SAML シングルサインオンを使用しており、ID プロバイダが SCIM 2.0 を使用してユーザーとグループの情報を IICS にプッシュした場合、このタブには、表示名、従業員番号、組織、部門などの SCIM 属性が表示されます。

このタブは、SAML 以外のユーザーには表示されません。

ログイン設定

以下の表に、ログイン設定を示します。

プロパティ	説明
認証	認証方法。次のいずれかの値を指定できます。 - ネイティブ。ユーザーは Informatica Intelligent Cloud Services によって認証されます。ユーザーは Informatica Intelligent Cloud Services の URL からログインします。 - Salesforce。ユーザーは Salesforce または Salesforce アプリケーションからサインインし、Salesforce によって認証されます。 - Azure SSO。ユーザーは Microsoft Azure からサインインし、Microsoft Azure によって認証されます。 - IDP と SAML。ユーザーは SAML ID プロバイダからサインインし、SAML ID プロバイダによって認証されます。
検証コード使用のアクティブ化/ Salesforce OAuth 使用のアクティブ化	Salesforce ユーザーのアカウントのアクティブ化方法。次のいずれかのオプションを選択します。 - 検証コード使用のアクティブ化。ユーザーが Salesforce アプリケーションから Informatica Intelligent Cloud Services にサインインする場合は、このオプションを選択します。 このオプションを選択すると、ユーザーは検証コードが含まれる電子メールを受信します。このユーザーが Salesforce にログインするとユーザーアカウントがアクティブ化され、Salesforce アプリが開くので、検証コードを入力します。 - Salesforce OAuth 使用のアクティブ化。Salesforce OAuth を使用してユーザーアカウントをアクティブ化するには、このオプションを選択します。 このオプションを選択すると、ユーザーは**［アカウントの確認］**リンクが含まれる電子メールを受信します。このユーザーが**［アカウントの確認］**リンクをクリックして Salesforce のユーザー名およびパスワードを入力すると、ユーザーアカウントがアクティブ化されます。 これらのオプションは認証方法が Salesforce の場合に表示されます。
環境	Salesforce 組織環境。プロダクションまたはサンドボックスです。 このオプションは、ユーザーのアクティブ化方法が Salesforce OAuth の場合に表示されます。
ユーザー名	Informatica Intelligent Cloud Services のユーザー名。Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。 このプロパティは、認証方法がネイティブである場合に表示されます。
Salesforce のユーザー名	Salesforce のユーザー名。Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。 Salesforce ユーザーの場合、Informatica Intelligent Cloud Services ユーザー名は、Informatica Intelligent Cloud Services の組織内でこの名前がすでに使用されていない限り、Salesforce ユーザー名と同じです。名前がすでに使用されている場合、Informatica Intelligent Cloud Services は、「.Salesforce」、「.Salesforce1」、「.Salesforce2」などの文字列を Salesforce ユーザー名の最後に追加し、Informatica Intelligent Cloud Services の一意のユーザー名を形成します。 このプロパティは、認証方法が Salesforce である場合に表示されます。

プロパティ	説明
Azure ユーザー名	Microsoft Azure ユーザー名 Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。 Microsoft Azure ユーザーの場合、Informatica Intelligent Cloud Services ユーザー名は、Informatica Intelligent Cloud Services の組織内でこの名前がすでに使用されていない限り、Azure ユーザー名と同じです。名前がすでに使用されている場合、Informatica Intelligent Cloud Services は、「.Azure」、「.Azure1」、「.Azure2」などの文字列を Azure ユーザー名の最後に追加し、Informatica Intelligent Cloud Services の一意のユーザー名を形成します。 このプロパティは、認証方法が Azure SSO である場合に表示されます。
SAML ユーザー名	SAML ユーザー名。Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。 SAML ユーザーの場合、Informatica Intelligent Cloud Services ユーザー名は、Informatica Intelligent Cloud Services の組織内でこの名前がすでに使用されていない限り、SAML 名前識別子と同じです。名前がすでに使用されている場合、Informatica Intelligent Cloud Services は、「.SAML」、「.SAML1」、「.SAML2」などの文字列を SAML 名前識別子の最後に追加し、Informatica Intelligent Cloud Services の一意のユーザー名を形成します。 このプロパティは、認証方法が SAML の IDP である場合に表示されます。
最大ログイン試行回数	ロックアウトされるまでにユーザーが試行できるログインの最大試行回数。数値または「制限なし」を選択します。 ロックアウトされている場合、ユーザーが［ログイン］ページの**［パスワードを忘れた場合］**リンクをクリックするか、組織管理者が**［ユーザー］**ページでユーザーをリセットすることができます。 このプロパティは、認証方法がネイティブである場合に表示されます。
アカウントステータス	アカウントのステータス。次のいずれかを指定します。 - アクティベーション保留。ユーザーアカウントは作成またはリセットされていますが、ユーザーがまだアカウントをアクティブ化していません。 - 有効: ユーザーアカウントが作成および検証されており、ユーザーは Informatica Intelligent Cloud Services にログインできます。 - ロック状態。ネイティブユーザーアカウントに適用されます。ログイン試行の最大数を超えたため、アカウントがロックされています。ユーザーのロックを解除するには、ユーザーが［ログイン］ページの**［パスワードを忘れた場合］**リンクをクリックするか、管理者が**［ユーザー］**ページでユーザーをリセットすることができます。 - 利用不可状態。ユーザーアカウントは管理者によって無効にされています。ユーザーは Informatica Intelligent Cloud Services にログインする事が出来ません。
初期アプリケーション	このフィールドは、将来使用するために予約されています。
次回のログイン時にパスワードのリセットを強制	ユーザーが次回ログインしようとしたときに、ユーザーにパスワードのリセットを強制します。 このプロパティは、認証方法がネイティブである場合に表示されます。

割り当て済みのユーザーグループおよびロール

各ユーザーには、少なくとも 1 つのユーザーグループまたはロールを割り当てる必要があります。ユーザーグループまたはロールを割り当てるか、または削除するには、グループまたはロールを有効または無効にしてから、**［保存］**をクリックします。

グループをユーザーに割り当てると、そのグループに関連付けられているすべてのロールが有効になります。これらのロールを個別に削除することはできません。ロールを削除するには、グループを削除する必要があります。

注: 組織で認証と承認に SAML を使用している場合、SAML ユーザーのユーザー詳細を編集することはできません。ユーザーの詳細は、**［SAML セットアップ］**ページのマッピング済みの属性、ロール、およびグループに従って自動的にマッピングされます。

ユーザーの作成

［ユーザー］ページでユーザーを作成します。ユーザーを作成すると、認証方法に基づいてユーザーステータスが［アクティベーション保留］または［有効］に設定されます。

1. 管理者で **［ユーザー］**を選択します。
2. **［ユーザーの追加］**をクリックします。
3. ユーザー情報を入力します。
4. 以下の手順でログイン設定を入力します。
   a. 認証方法を選択します。
   b. Salesforce ユーザーの場合は、検証コードまたは Salesforce OAuth を使用してユーザーアカウントをアクティブにするかどうかを指定します。
   c. Informatica Intelligent Cloud Services のユーザー名、またはサードパーティの ID プロバイダシステムのユーザー名を入力します。

      ネイティブユーザーの場合は、Informatica Intelligent Cloud Services のユーザー名を入力してください。Salesforce、Microsoft Azure、SAML のユーザーの場合は、サードパーティの ID プロバイダシステムのユーザー名を入力してください。

      ユーザー名は、Informatica Intelligent Cloud Services 組織内で一意にする必要があります。ユーザーの作成後にユーザー名を変更する事は出来ません。
   d. ネイティブユーザーの場合は、最大ログイン試行回数を選択します。
5. ［割り当て済みのユーザーグループおよびロール］セクションで、ユーザーに割り当てるユーザーグループとロールを選択します。

   ユーザーにシステム定義およびカスタムロールを割り当てることができます。グループを割り当てると、そのグループに関連付けられているすべてのロールがユーザーに継承されます。
6. **［保存］**をクリックします。

ユーザーを作成すると、ユーザーステータスが認証方法に基づいて次のように設定されます。

- ネイティブユーザーは［アクティベーション保留］に設定されます。ユーザーは、アカウントを確認するための電子メールを受信します。ユーザーが電子メール内の **［アカウントの確認］**リンクをクリックすると、パスワードとセキュリティの質問を設定するように求められます。設定が完了するとステータスが［有効］に変わり、ユーザーは Informatica Intelligent Cloud Services にログインできるようになります。
- Salesforce ユーザーは［アクティベーション保留］に設定されます。

  検証コードを使用してユーザーをアクティブ化すると、ユーザーは検証コードを使用して電子メールを受信します。このユーザーが Salesforce にログインするとユーザーアカウントがアクティブ化され、Salesforce アプリが開くので、検証コードを入力します。

Salesforce OAuth を使用してユーザーをアクティブ化すると、ユーザーは**［アカウントの確認］**リンクを使用して電子メールを受信します。このユーザーが**［アカウントの確認］**リンクをクリックして Salesforce のユーザー名およびパスワードを入力すると、ユーザーアカウントがアクティブ化されます。

- Microsoft Azure および SAML ユーザーは［有効］に設定されます。ユーザーは、ユーザーの ID プロバイダを介してサインインできます。

サービスの割り当ておよび割り当て解除

ユーザーを作成すると、そのユーザーは組織のライセンスおよびユーザーのロールに基づいてサービスにアクセス出来るようになります。これらのサービスに対するユーザーのアクセスを制限出来ます。

ユーザーによる特定のサービスへのアクセスを許可または拒否するには、ユーザーに対してサービスを割り当てまたは割り当て解除します。**［ユーザー］**ページで、ユーザーに対してサービスを割り当ておよび割り当て解除します。

サービスをユーザーに割り当てると、割り当てられたサービスが**［マイサービス］**ページに表示されます。ユーザーのロールでこのサービスが許可されていれば、このサービスにアクセスして使用出来ます。

サービスを割り当て解除すると、ユーザーの**［マイサービス］**ページにはサービスが表示されなくなります。ユーザーのロールに関係なく、ユーザーはサービスにアクセス出来ず使用する事も出来ません。

例えば、サービスコンシューマロールを持つアプリケーション開発者に対し、API ポータルは使用出来るがデータ統合やアプリケーションの統合は使用出来ないようにします。API ポータルサービスをユーザーに割り当て、データ統合サービスおよびアプリケーションの統合サービスを割り当て解除します。これにより、アプリケーション開発者の**［マイサービス］**ページには、データ統合サービスおよびアプリケーションの統合サービスが表示されなくなります。サービスコンシューマロールには上記サービスに関連する特権がありますが、アプリケーション開発者はこれらのサービスを使用出来ません。

1. 管理者で**［ユーザー］**を選択します。
2. ユーザーを含む行で**［アクション］**をクリックし、**［サービスの割り当て］**を選択します。
3. **［サービスの割り当て］**ダイアログボックスでユーザーに割り当てるサービスを選択し、割り当て解除するサービスの選択を解除します。
4. **［保存］**をクリックします。

ユーザーの無効化

［ユーザー］ページでユーザーを無効にします。ユーザーを無効にすると、そのユーザーは Informatica Intelligent Cloud Services にログイン出来なくなります。

ユーザーを無効にする前に、そのユーザーがタスクまたはタスクフローをスケジュールしていない事を確認してください。タスクまたはタスクフローをスケジュールしているユーザーを無効にすると、スケジュール済みのジョブが失敗します。

ユーザーを無効にしても、そのユーザーは組織および Informatica Intelligent Cloud Services リポジトリに残ります。ユーザーの詳細を表示できますが、編集する事は出来ません。ユーザーが作成または更新したアセットも、組織に残ります。［参照］ページの［作成者］および［更新者］列にユーザーが無効化されている事が表示されます。

1. 管理者で**［ユーザー］**を選択します。

2. 無効にするユーザーを含む行で**［アクション］**をクリックし、**［無効化］**を選択します。

   注: ファイルリスナを一括取り込みファイルで（トリガまたはソースとして）使用する場合、またはタスクフローで（トリガまたは File Watch として）使用する場合は、REST API を使用して、ユーザーを削除する前に、あるユーザーから別のユーザーにファイルリスナの関連付けの所有権を再割り当てする必要があります。詳細については、『*REST API リファレンス*』ガイドを参照してください。

ユーザーのリセット

［ユーザー］ページでユーザーをリセットします。アカウントが無効になっているユーザーやアカウントがロックされているユーザーをリセットできます。ユーザーをリセットすると、ユーザーステータスが認証方法に基づいて［アクティベーション保留］または［有効］に設定されます。

1. 管理者で**［ユーザー］**を選択します。
2. ユーザーを含む行で**［アクション］**をクリックし、**［リセット］**を選択します。

ユーザーをリセットすると、ユーザーステータスが認証方法に基づいて次のようにリセットされます。

- ネイティブユーザーは［アクティベーション保留］に設定されます。ユーザーは、アカウントを確認するための電子メールを受信します。ユーザーが電子メール内の**［アカウントの確認］**リンクをクリックすると、パスワードとセキュリティの質問をリセットするように求められます。これで、ユーザーが Informatica Intelligent Cloud Services にログインできるようになります。
- Salesforce ユーザーは［アクティベーション保留］に設定されます。

  検証コードを使用してユーザーをアクティブ化すると、ユーザーは検証コードを使用して電子メールを受信します。このユーザーが Salesforce にログインするとユーザーアカウントがアクティブ化され、Salesforce アプリが開くので、検証コードを入力します。

  Salesforce OAuth を使用してユーザーをアクティブ化すると、ユーザーは**［アカウントの確認］**リンクを使用して電子メールを受信します。このユーザーが**［アカウントの確認］**リンクをクリックして Salesforce のユーザー名およびパスワードを入力すると、ユーザーアカウントがアクティブ化されます。
- Microsoft Azure および SAML ユーザーは［有効］に設定されます。ユーザーは、ユーザーの ID プロバイダを介してサインインできます。

ユーザーのスケジュール済みジョブの再割り当て

［ユーザー］ページでユーザーのスケジュール済みジョブを再割り当てします。スケジュール済みタスクまたはタスクフローのあるユーザーが組織を離れるときに、スケジュール済みジョブを再割り当てする必要がある場合があります。ユーザーを削除する前に、ユーザーのスケジュール済みジョブを再割り当てする必要があります。

スケジュール済みジョブの所有者は、スケジュール済みタスクまたはタスクフローを最後に保存した人です。例えば、組織でユーザー Arun がスケジュールを作成し、ユーザー Beth がマッピングタスクを作成し、スケジュールをタスクに割り当ててから、Chandra がタスクを更新して保存したとします。Chandra がこのスケジュール済みジョブの所有者になります。Chandra が組織を離れる場合、彼女のユーザーアカウントを削除する前に、彼女のスケジュール済みジョブを他のユーザーに再割り当てする必要があります。

1. 管理者で**［ユーザー］**を選択します。

2. ユーザーを含む行で［**アクション**］をクリックし、［**スケジュール済みジョブの再割り当て**］を選択します。
3. スケジュール済みジョブを再割り当てするユーザーを選択します。

   選択するユーザーは有効なユーザーである必要があります。
4. ［**再割り当て**］をクリックします。

REST API を使用して、ユーザーが持つファイルリスナの関連付けの所有権を別のユーザーに再割り当てすることができます。詳細については、『*REST API リファレンス*』を参照してください。

ユーザーの削除

［**ユーザー**］ページでユーザーを削除します。ユーザーを削除すると、そのユーザーは組織および Informatica Intelligent Cloud Services リポジトリから削除されます。組織で認証と承認に SAML を使用している場合、管理者で作成したものではない SAML ユーザーを削除することはできません。

ユーザーを削除する前に、ユーザーのスケジュール済みジョブを別のユーザーに再割り当てする必要があります。

注: 削除したユーザーをリセットする事は出来ません。ユーザーアカウントを再びアクティブにする可能性がある場合は、ユーザーを削除するのではなく無効にしてください。

1. 管理者で［**ユーザー**］を選択します。
2. 削除するユーザーを含む行で［**アクション**］をクリックし、［**削除**］を選択します。
3. ユーザーがスケジュール済みタスクまたはタスクフローの所有者である場合、管理者によって、ジョブを別のユーザーに再割り当てするよう求めるプロンプトが表示されます。ジョブを再割り当てするユーザーを選択し、［**再割り当てして削除**］をクリックします。

   注: ファイルリスナを一括取り込みファイルで（トリガまたはソースとして）使用する場合、またはタスクフローで（トリガまたは File Watch として）使用する場合は、REST API を使用して、ユーザーを削除する前に、あるユーザーから別のユーザーにファイルリスナの関連付けの所有権を再割り当てする必要があります。詳細については、『*REST API リファレンス*』ガイドを参照してください。

ユーザーがスケジュール済みタスクまたはタスクフローを所有していない場合、管理者によってそのユーザーが削除されます。ユーザーがスケジュール済みタスクまたはタスクフローの所有者である場合、管理者によってジョブが再割り当てされ、そのユーザーが削除されます。

第 5 章

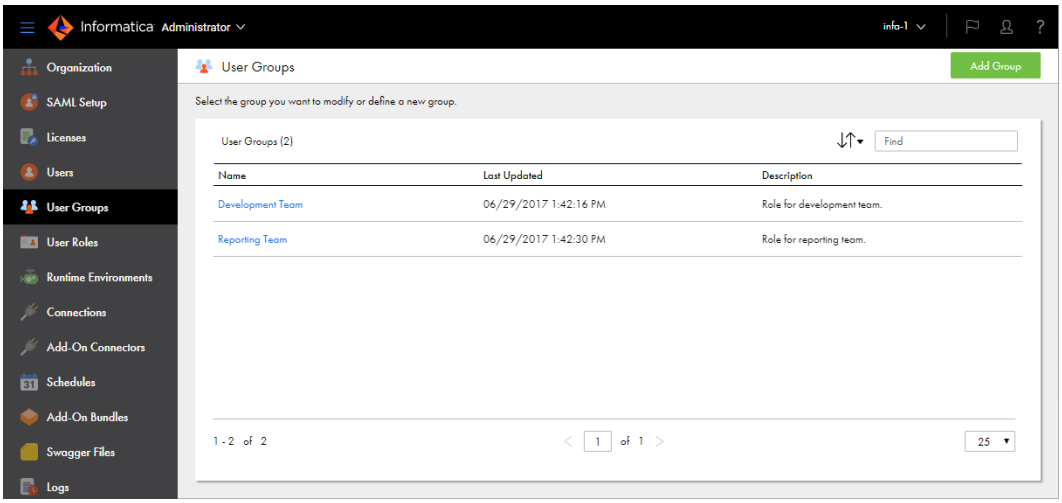
ユーザグループ

ユーザーグループは、すべてのメンバが同じタスクを実行し、さまざまなタイプのアセットに対して同じアクセス権を持つことができるユーザーのグループです。グループのメンバは、そのグループに割り当てたロールに基づいてタスクを実行し、アセットにアクセスできます。

管理者は、組織のユーザーグループを構成できます。

[ユーザーグループ] ページには、組織のすべてのユーザーグループが一覧表示されます。**[ユーザーグループ]** ページにアクセスするには、管理者で **[ユーザーグループ]** を選択します。

次の図は、**[ユーザーグループ]** ページを示しています。



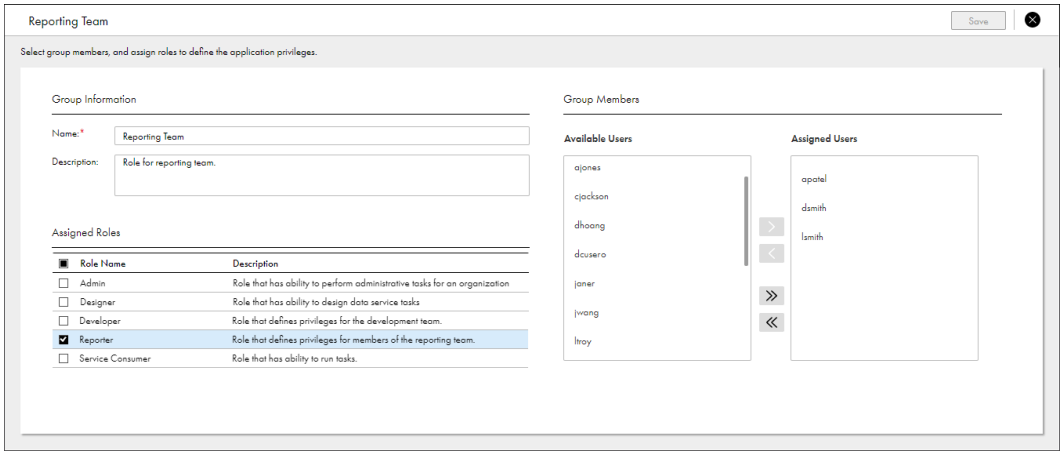
ユーザーグループに対して次のタスクを実行できます。

- グループの詳細を表示および編集する。
- グループを作成する。
- グループの名前を変更する。
- グループを削除する。

ユーザーグループの詳細

グループ情報、割り当てられたロール、グループメンバなどユーザーグループに関する詳細を［グループの詳細］ページで設定できます。［グループの詳細］ページを表示するには、管理者で**［ユーザーグループ］**をクリックし、グループ名をクリックします。

次の図は、［グループの詳細］ページを示しています。



ユーザーグループに対して次の詳細を構成できます。

プロパティ	**説明**
名前	必須。ユーザーグループの名前。組織内で一意である必要があります。 グループ名は、作成後に変更できます。
説明	ユーザーグループの説明（省略可能）。
割り当てロール	グループのすべてのメンバに割り当てられているロール。各グループには、少なくとも 1 つのロールを割り当てる必要があります。 ロールを割り当てるか、または削除するには、グループまたはロールを有効または無効にしてから、**［保存］**をクリックします。
グループメンバ	グループに割り当てられているユーザー。 ユーザーをグループに割り当てるには、**［利用可能なユーザー］**の一覧から**［割り当てユーザー］**の一覧にユーザーを移動し、**［保存］**をクリックします。ユーザーをグループから削除するには、**［割り当てユーザー］**の一覧から**［利用可能なユーザー］**の一覧にユーザーを移動し、**［保存］**をクリックします。 ユーザーをグループに割り当てると、そのグループに割り当てられているすべてのロールが自動的に割り当てられます。

注: SAML グループのグループの詳細を編集することはできません。SAML グループは、［グループ情報］領域の**［SAML グループのミラーリング: <グループ名>］**というラベルで識別されます。

ユーザーグループの作成

組織内の複数のユーザーが同じタスクを実行し、さまざまな種類のアセットに対して同じアクセス権を必要とする場合は、ユーザーグループを作成します。グループメンバは、そのグループに割り当てたロールに基づいてタスクを実行し、アセットにアクセスできます。**[ユーザーグループ]** ページでユーザーグループを作成します。

1. 管理者で、**[ユーザーグループ]** を選択します。
2. **[グループの追加]** をクリックします。
3. グループの名前を入力し、必要に応じて説明を入力します。

   グループ名は、組織内で一意である必要があります。
4. ［割り当てロール］セクションで、グループに割り当てるロールを選択します。

   グループにシステム定義およびカスタムロールを割り当てることができます。ロールは、グループのすべてのメンバに適用されます。
5. 必要に応じて、ユーザーをグループに割り当てます。

   ユーザーをグループに割り当てるには、**[利用可能なユーザー]** の一覧から **[割り当てユーザー]** の一覧にユーザーを移動します。SAML ユーザーはグループに割り当てることができないため、利用可能なユーザーのリストには SAML ユーザーは表示されません。

   ユーザーを作成または編集するときに、ユーザーをグループに割り当てることもできます。
6. **[保存]** をクリックします。

ユーザーグループの名前変更

[ユーザーグループ] ページでユーザーグループの名前を変更します。また、［グループの詳細］ページでは、ユーザーグループの編集やグループ名の変更ができます。SAML グループの名前を変更することはできません。

1. 管理者で、**[ユーザーグループ]** を選択します。
2. ユーザーグループを含む行で **[アクション]** をクリックし、**[名前の変更]** を選択します。
3. 新しい名前を入力し、**[保存]** をクリックします。

ユーザーグループの削除

[ユーザーグループ] ページでユーザーグループを削除します。組織が認証と承認に SAML SSO を使用している場合、SAML グループを削除することはできません。

ヒント: Informatica Intelligent Cloud Services を中断なく継続して使用できるように、ユーザーグループを削除する前に、すべてのグループメンバが適切なロールを持っているか、または他のグループに割り当てられていることを確認します。

1. 管理者で、**[ユーザーグループ]** を選択します。
2. ユーザーグループを含む行で **[アクション]** をクリックし、**[削除]** を選択します。

第 6 章

ユーザーロール

ロールとは、ユーザーおよびグループへの割り当ての可能な特権の集まりです。すべてのユーザーがアセットにアクセスして組織内のタスクを実行できるようにするには、各ユーザーまたはユーザーグループに 1 つ以上のロールを割り当てます。

ロールは、さまざまなタイプのアセットとサービス特権に対する特権を定義します。例えば、デザイナロールを持つユーザーは、ほとんどのタイプのデータ統合アセットに対する権限を作成、読み取り、更新、削除、および設定できます。ただし、サブ組織や監査ログなど、特定の管理者サービス機能にはアクセスできません。

管理者は、組織のロールを構成および割り当てることができます。

ユーザーによる割り当ての可能なロールには、次の種類があります。

システム定義

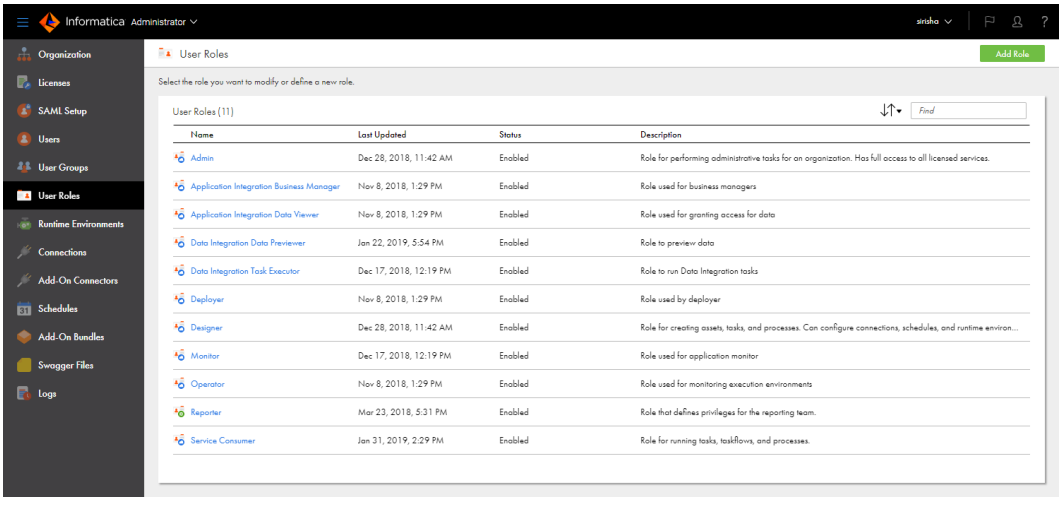
システム定義ロールは、組織で使用されるサービスのアクセス特権を定義した定義済みのロールです。ユーザーおよびグループに割り当てることのできるシステム定義ロールは、組織のライセンスによって異なります。これらのシステム定義ロールを編集、名前変更、または削除することはできません。管理者ロール以外のシステム定義ロールのクローンを作成できます。

カスタムロール

カスタムロールは特権を個別に設定するために作成するロールです。カスタムロールを作成するには、適切なライセンスが必要です。カスタムロールは、ユーザーによる編集、クローン作成、名前変更、および削除が可能です。

[ユーザーロール] ページでは、システム定義のロールおよびカスタムロールの両方を表示できます。**[ユーザーロール]** ページには、組織内のすべてのロールの一覧が表示されます。**[ユーザーロール]** ページにアクセスするには、管理者で **[ユーザーロール]** を選択します。

次の図は、**[ユーザーロール]** ページを示しています。



［ステータス］列は、組織に対してロールが有効か無効かを示します。ライセンスの有効期限が切れると、ロールは無効になります。

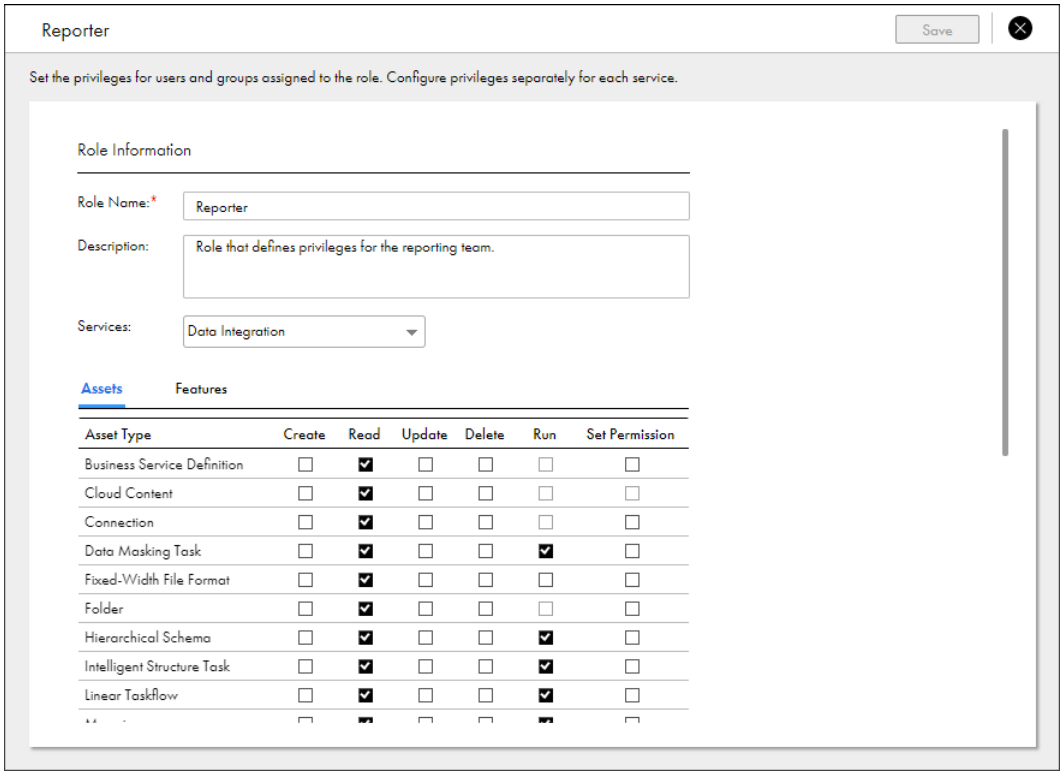
複数のロールをユーザーまたはユーザーグループに割り当てることができます。複数のロールを割り当てる場合、そのユーザーまたはグループはそれらのロールすべてに関連付けられたアクセス特権を継承します。

ロールの詳細

［ロールの詳細］ページには、ロールに関連付けられているアセットや機能特権など、ロールに関する情報が表示されます。システム定義ロールの場合、ロール情報や特権を表示出来ます。カスタムロールの場合、ロール情報および割り当てられているアセットや機能特権を表示および変更出来ます。

［ロールの詳細］ページを表示するには、管理者で**［ユーザーロール］**を選択し、ロール名をクリックします。

次の図に、［ロールの詳細］ページを示します。



各ロールには、次のプロパティがあります。

役割名

ロールの名前。カスタムロールの場合、ロール名を変更出来ます。

説明

ロールの説明。カスタムロールの場合、ロールの説明を変更出来ます。

サービス

特権が有効または無効になっているサービスの名前。サービスを選択して、そのサービスに関連付けられているアセットや機能特権を表示します。

サービスのライセンスが期限切れの場合、そのサービスは無効とマークされます。無効なサービスに関連付けられているアセットや機能特権は表示出来ます。

アセット

選択したサービスのアセット特権。アセット特権は、さまざまなタイプのアセットへのアクセスを制御します。例えば、サービスコンシューマロールを持つユーザーは、データ統合のマッピングを表示および実行することは出来ますが、マッピングに対する権限を作成、更新、削除、または設定することはできません。

以下の表に、アセット特権を示します。

特権	説明
作成	選択したタイプのアセットを作成します。Secure Agent の場合、この特権により、ユーザーは Secure Agent をダウンロードしてインストールできます。 自動的に付与される読み取りおよび更新の特権が必要です。
読み取り	選択したタイプのアセットを開きます。タスクの場合、この特権によって、ユーザーはタスク内の接続またはスケジュールを使用することもできます。
更新	選択したタイプのアセットを編集します。 自動的に付与される読み取り特権が必要です。
削除	選択したタイプのアセットを削除します。
実行	選択したタイプのアセットを実行します。 データ統合サービスでは、ユーザーはマッピング、タスク、またはタスクフローを実行出来ます。また、ユーザーはマッピング、タスク、またはタスクフローのインスタンスを監視、停止、および再起動出来ます。 Hub の統合サービスでは、ユーザーはパブリケーションまたはサブスクリプションを実行出来ます。
権限の設定	選択したタイプのアセットの権限を構成します。例えば、この特権をプロジェクトに付与すると、そのロールを持つユーザーはプロジェクトを選択し、選択したプロジェクトの権限を他のユーザーとグループが読み取り、更新、削除、または変更できるようにすることができます。 この特権を設定するには、組織に適したライセンスが必要です。

特権がアセットタイプに適用されない場合、その特権は無効になります。例えば、フォルダに対する実行特権は無効になっています。

カスタムロールの場合、サービスが無効になっていない限り、そのサービスのアセット特権を有効または無効にすることが出来ます。

機能

選択したサービスの機能特権。機能特権は、サービスの機能を使用する権限を制御する一般的な特権です。例えば、デザイナロールを持つユーザーは、データ統合でデータカタログ検出を実行することは出来ますが、データをプレビューすることはできません。

カスタムロールの場合、サービスが無効になっていない限り、そのサービスの機能特権を有効または無効にすることが出来ます。

アプリケーションの統合機能特権

カスタムロールを作成するにはアプリケーションの統合機能特権を使用します。

重要: ユーザーのロールにフォルダとプロジェクトのアセット特権を割り当てる必要があります。これを行うには、データ統合サービスを選択し、フォルダアセットとプロジェクトアセットの CRUD オプションを選択します。

カスタムロールを作成する場合は、次のアプリケーションの統合機能特権を有効化できます。

管理

ユーザーにアプリケーションの統合とアプリケーション統合コンソールへの完全な設計時およびランタイム管理者アクセスを提供したい場合は、ロールに管理特権を割り当てます。

管理特権を持つユーザーは次のタスクを実行できます。

- すべてのアプリケーションの統合アセットの表示、作成、更新、削除。
- サービスの管理と開始。
- 実行中のサービスの停止。
- デプロイされたプロセスのインスタンスとログの表示。
- アプリケーション統合コンソールへのプロセス開発者 BPR ファイルのデプロイ。
- デプロイされたカタログの管理。
- 複数のシステム全体のデプロイされた WSDL ファイルの表示。
- プロセスサーバーのメトリックの表示。

注: アプリケーションの統合管理特権は、ユーザーに Informatica Intelligent Cloud Services 全体の管理特権を付与するものではありません。例えば、アプリケーションの統合管理特権のみを持つユーザーは、サブ組織を作成することはできません。

コンソール管理

ユーザーにアプリケーション統合コンソールへのほぼ完全なアクセスを提供したい場合は、ロールにコンソール管理特権を割り当てます。

コンソール管理特権を持つユーザーは次のタスクを実行できます。

- デプロイされたプロセスのインスタンスの表示。
- 実行中のサービスの停止。
- デプロイされたプロセス開発者 BPR とカタログの表示。
- 複数のシステム全体のデプロイされた WSDL ファイルの表示。
- プロセスサーバーのメトリックの表示。

コンソール管理特権を持つユーザーは BPR ファイルをデプロイできません。

データビューア

アプリケーション統合コンソールで詳細なログにアクセスする必要があるユーザーにはデータビューア特権を割り当てます。

例えば、組織全体のログを参照する必要があるユーザーにこの特権を割り当てることができます。開発者にこのロールを普段から割り当てないほうがよいでしょう。

注: 詳細なログを取得するには、プロセスログレベルを［詳細］に設定する必要があります。

開発

場合によってプロセスをデバッグする必要がある開発者には開発特権を割り当てます。

開発特権を持つユーザーは次のタスクを実行できます。

- すべてのアプリケーションの統合アセットの表示、作成、更新、削除。
- サービスの開始。
- アプリケーション統合コンソールの［Detailed Process Instance（プロセスインスタンス詳細）］ページの表示。
- プロセスインスタンスの管理。

監視

アプリケーション統合コンソールの詳細なログ以外のすべての部分を表示する必要があるユーザーには、監視特権を割り当てます。

アプリケーション統合アセットのパブリッシュ

アプリケーションの統合プロセス、ガイド、接続、サービスコネクタをパブリッシュする必要があるユーザーには、アプリケーション統合アセットのパブリッシュ特権を割り当てます。

アプリケーション統合コンソールの表示

アプリケーション統合コンソールサービスにアクセスする必要があるユーザーには、アプリケーション統合コンソールの表示特権を割り当てます。アプリケーション統合コンソールの操作を含む特権を持つロールには、この特権を割り当てる必要があります。

例えば、開発特権と共にこの特権を割り当てる必要があります。

アプリケーション統合デザイナの表示

アプリケーションの統合サービスにアクセスする必要があるユーザーには、アプリケーション統合デザイナの表示特権を割り当てます。アプリケーション統合コンソールの操作を含む特権を持つロールには、この特権を割り当てる必要があります。

例えば、アプリケーション統合アセットのパブリッシュ特権と共にこの特権を割り当てる必要があります。

Data Quality の機能特権

ユーザーにデータ品質アセットでのプレビュー機能へのアクセス権を付与するには、Data Quality の機能特権を使用します。カスタムロールを作成するときに、この機能特権を有効化できます。

Data Quality の次の機能特権を有効にできます。

データプレビュー - ディクショナリ

次の場合にユーザーがディクショナリのコンテンツを表示できるようにするには、ロールのデータプレビュー - ディクショナリ特権を有効にします。

- ユーザーが［エクスプローラ］ページからディクショナリを開いたとき。
- ユーザーが Data Quality アセットでディクショナリを選択したとき。

データプレビュー - テストパネル

ユーザーが Data Quality アセットのテストパネルでデータを表示できるようにするには、ロールのデータプレビュー - テストパネル特権を有効にします。

管理者ロールとデザイナロールでは、Data Quality の機能特権がデフォルトで有効になっています。

注: ディクショナリアセットのデータプレビュー - ディクショナリ機能特権と読み取り特権は、互いに独立して機能します。読み取り特権があると、［エクスプローラ］ページからディクショナリを開くことができます。データプレビュー - ディクショナリ特権があると、ディクショナリデータを表示できます。

データプレビュー - ディクショナリ特権なしでディクショナリを開くと、Data Quality によりデータを表示するための十分な権限がないことを通知するメッセージが表示されます。

一括取り込みデータベースのアセットと機能の特権

データベース取り込みタスクを作成、表示、または編集するには、次の最低限必要なアセット特権を含むユーザーロールを割り当てます。

- 一括取り込みサービスの場合、データベース取り込みタスクアセットの作成、読み取り、および更新の特権を選択します。
- Administrator サービスの場合、次のアセットタイプの読み取り特権を選択します。

  - 接続

  - Secure Agent

  - Secure Agent グループ

  また、コネクタ - 表示機能を有効にします。

これらの特権を含む管理者やデザイナなどのシステム定義のロールを使用することも、それらを含むカスタムロールを定義することもできます。

システム定義のロール

Informatica Intelligent Cloud Services には、ユーザーまたはユーザーグループに割り当てることができるシステム定義のロールが用意されています。システム定義のロールを変更または削除することはできません。

ユーザーおよびグループに割り当てることのできるシステム定義ロールは、組織のライセンスによって異なります。例えば、組織にアプリケーションの統合または API Manager へのアクセス権がない場合、デプロイヤ、アプリケーション統合ビジネスマネージャ、アプリケーション統合データビューア、またはオペレータロールを組織のユーザーまたはグループに割り当てることはできません。

実行する必要のあるタスクに基づいて、ユーザーおよびグループにシステム定義ロールを割り当てます。

システム定義のロールには、次の 2 つのタイプがあります。

- クロスサービスロールは複数のサービスにまたがるアクセス特権を定義します。
- サービス固有のロールは、1 つのサービス、または密接な関連のあるサービスのグループのアクセス特権を定義します。

クロスサービスロール

クロスサービスロールは、複数のサービスにまたがるアクセス権限を定義するシステム定義ロールです。

例えば、デザイナロールを持つユーザーはデータ統合でアセットとタスクを作成し、Cloud Integration Hub でアセットを作成し、アプリケーションの統合でプロセスを作成できます。また、アプリケーション統合コンソールにもアクセスできます。モニタロールを持つユーザーは、データ統合ジョブ、Cloud Integration Hub アセット、およびアプリケーションの統合プロセスインスタンスを監視できます。

次のロールがクロスサービスロールです。

- 管理
- データ統合プレビューア
- デプロイヤ
- デザイナ
- モニタ

- 演算子
- サービスコンシューマ

注: データ統合プレビューアロールは、データ統合およびデータプロファイリングのデータをユーザーがプレビューできるようにするための補足的なロールです。サービスに対するアクセスは提供しません。このロールを、データ統合またはデータプロファイリングにユーザーがアクセスできるようにするための別のロールとともに割り当てます。

以下の表に、各クロスサービスロールでアクセスできるサービスを示します。

サービス	ロール
管理者	- 管理 - デザイナ - モニタ - サービスコンシューマ
API Manager	- 管理 - デザイナ - サービスコンシューマ
API Portal	- Admin - サービスコンシューマ
アプリケーションの統合	- Admin - デプロイヤ - デザイナ - モニタ - 演算子 - サービスコンシューマ
アプリケーション統合コンソール	- Admin - デプロイヤ - デザイナ - モニタ - 演算子 - サービスコンシューマ
B2B Gateway	- 管理 - デザイナ - モニタ
B2B パートナーポータル	- Admin
Business 360 コンソール	- 管理 - デザイナ
データ統合	- 管理 - デザイナ - モニタ - サービスコンシューマ
Data Quality	- Admin - デプロイヤ - デザイナ - モニタ - 演算子 - サービスコンシューマ

サービス	ロール
データプロファイリング	- 管理 - デザイナ - モニタ - 演算子
Integration Hub	- 管理 - デザイナ - モニタ
一括取り込み	- Admin - デプロイヤ - デザイナ - モニタ
Model Serve	- 管理 - デザイナ - モニタ - 演算子
モニタ	- 管理 - デザイナ - モニタ
オペレーションインサイト	- Admin - 演算子

クロスサービスロールのアクセス特権

Informatica Intelligent Cloud Services のさまざまなサービスへの特権アクセスが必要なユーザーにはクロスサービスロールを割り当てます。各クロスサービスロールは異なるアクセス特権を提供します。

クロスサービスロールには次のアクセス特権があります。

管理者

管理者ロールを持つユーザーは、ライセンス供与されたすべてのサービスにフルアクセスできます。管理者ロールとサービスコンシューマロールの両方が割り当てられている場合は、組織内のすべてのタスクを実行できます。

注: 一括取り込みサービスでは、サービスコンシューマロールは使用されません。

ベストプラクティスは、1 つまたは 2 つの信頼されたユーザーに管理者ロールを割り当て、すべてのアセットタイプに対する完全な権限を持つ管理ユーザーグループにそのユーザーを割り当てることです。これらのユーザーは代替の組織の管理者として活動し、アクセス制御や組織のセキュリティの問題のトラブルシューティングを支援することができます。

注: OAuth 2.0 クライアント管理のためのすべての特権を含めて、API Manager サービスへのフルアクセスを提供するには、ユーザーに管理者ロールとサービスコンシューマロールの両方を割り当てます。

データ統合プレビューア

データ統合プレビューアロールを持つユーザーは、マッピングまたはタスクで使用するソース、ターゲット、またはルックアップオブジェクトを選択したときに、データをプレビューできます。データ統合また、プロファイルを作成するとき、またはプロファイル結果をデータプロファイリングで表示するときに、ソースオブジェクトデータを表示することもできます。

データ統合プレビューアロールは補足的なロールです。ユーザーがデータ統合およびデータプロファイリングにアクセスできるようにするために、このロールは、デザイナロールなどの別のロールと一緒に割り当てます。

一括取り込みサービスでは、データ統合プレビューアロールは使用されません。

デプロイヤ

デプロイヤロールを持つユーザーはアプリケーションの統合アセットをデプロイでき、API Manager から API を管理できます。このロールはデプロイアクセスが一般的に禁止されているプロダクション環境で割り当ててください。

注: OAuth 2.0 クライアント管理のためのすべての特権を含めて、API Manager サービスへのフルアクセスを提供するには、ユーザーにデプロイヤロールとサービスコンシューマロールの両方を割り当てます。

Data Quality では、デプロイヤ特権を持つユーザーはアセットを表示できます。

一括取り込みサービスでは、デプロイヤ特権を持つユーザーは、アプリケーション取り込みタスク、データベース取り込みタスク、およびストリーミング取り込みタスクを表示できます。

以下の表に、デプロイヤロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
API Manager	サービスコンシューマロールも割り当てられている場合、このサービスにフルアクセスでき、OAuth 2.0 クライアント管理特権を持ちます。
アプリケーションの統合	アセットの詳細を表示できます。
アプリケーション統合コンソール	[プロセス]、[ログ]、[サーバー設定]、[デプロイ済みアセット]、[リソース] の各ページでアセットをデプロイし、設定を表示できます。プロセス開発者が生成したオーケストレーションアーティファクト（BPR）をアップロードおよびデプロイできます。
Data Quality	アセットの詳細を表示できます。
一括取り込み	アプリケーション取り込みタスク、データベース取り込みタスク、およびストリーミング取り込みタスクを表示できます。

デザイナ

デザイナロールを持つユーザーは、アセット、タスク、およびプロセスを作成できます。接続、スケジュール、およびランタイム環境を設定できます。また、組織のジョブおよび詳細クラスタを監視できます。

注: デザイナロールを持つ一括取り込みユーザーは、詳細クラスタを監視できません。

以下の表に、デザイナロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
管理者	接続、ランタイム環境、スケジュール、Swagger ファイル、および詳細設定を設定できます。アドオンコネクタをインストールすること、およびアドオンバンドルをアンインストールすることができます。Secure Agent サービスのアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。
アプリケーションの統合	このサービスにフルアクセスできます。
アプリケーション統合コンソール	サーバー設定プロパティを除くすべての設定を表示および編集できます。
B2B Gateway	このサービスにフルアクセスできます。
データ統合	このサービスにフルアクセスできます。
Data Quality	このサービスにフルアクセスできます。
Data Profiling	このサービスにフルアクセスできます。
Integration Hub	このサービスにフルアクセスできます。
一括取り込み	アプリケーション取り込みタスク、データベース取り込みタスク、およびストリーミング取り込みタスクに対して、権限を作成、表示、編集、削除、実行、および設定できます。
Model Serve	機械学習モデルを作成、表示、編集、および削除できます。モデルデプロイメントを作成、表示、編集、削除、および実行できます。
モニタ	このサービスにフルアクセスできます。

モニタ

モニタロールを持つユーザーは、組織のデータ統合ジョブ、一括取り込みジョブ、Cloud Integration Hub アセット、Data Quality アセット、Model Serve アセット、およびアプリケーションの統合プロセスインスタンスを監視できます。

以下の表に、モニタロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
管理者	Secure Agent サービスのスケジュールおよびアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。
アプリケーションの統合	アセットの詳細を表示できます。

サービス	アクセス特権
アプリケーション統合コンソール	設定を表示できます。
B2B Gateway	アセットの詳細を表示できます。
データ統合	アセットの詳細を表示できます。
Data Quality	アセットの詳細を表示できます。
Data Profiling	アセットの詳細を表示できます。
Integration Hub	アセットの詳細を表示できます。
一括取り込み	アプリケーション取り込みジョブ、データベース取り込みジョブ、およびストリーミング取り込みジョブとジョブの詳細を表示できます。
Model Serve	アセットの詳細を表示できます。
モニタ	データ統合ジョブとジョブの詳細を表示できます。エクスポートジョブとインポートジョブは表示できません。

オペレータ

オペレータはプロセスの実行管理とプロセスサーバーの設定更新を担当します。オペレータロールを持つユーザーはアセットの詳細を表示できますが、それらを変更することはできません。プロセスインスタンスの管理と一部の運用サーバーパラメータの変更を行うことができます。

以下の表に、オペレータロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
アプリケーションの統合	アセットの詳細を表示できます。
アプリケーション統合コンソール	プロセスサーバーの設定と一部のクラウドサーバーの設定を表示および編集できます。例えば、オペレータロールを持つユーザーは警告サービスを作成できますが、テナントの詳細は表示できません。
データプロファイリング	アセットの詳細を表示できます。
Data Quality	アセットの詳細を表示できます。
Model Serve	アセットの詳細を表示できます。
オペレーションインサイト	クラウドおよびドメインインフラストラクチャを表示できます。ドメインおよびインフラストラクチャである Secure Agent のアラート設定を編集できます。ドメインインフラストラクチャを編集できます（ドメインの登録など）。

一括取り込みサービスでは、オペレータロールは使用されません。

サービスコンシューマ

サービスコンシューマロールを持つユーザーはタスク、タスクフロー、プロセスを実行できますが、アセットの作成と編集はできません。API を通してデータ統合ジョブとアプリケーションの統合プロセスを実行する必要があるユーザーにこのロールを割り当てます。

注: API Manager サービスへのフルアクセスを提供するには、ユーザーにサービスコンシューマロールとデプロイヤロールの両方を割り当てるか、ユーザーにサービスコンシューマロールと管理者ロールの両方を割り当てます。

以下の表に、サービスコンシューマロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
管理者	Secure Agent サービスのスケジュール、Swagger ファイル、およびアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。
API Manager	デプロイヤロールまたは管理者ロールも割り当てられている場合は、このサービスにフルアクセスできます。
API Portal	このサービスにフルアクセスできます。
アプリケーションの統合	アプリケーションの統合プロセスを呼び出すことができます。
データ統合	タスクの表示、タスクの実行、マッピングのテスト実行、タスクフローの実行、およびワークフロー XML のダウンロードを行うことができます。
Data Quality	アセットの詳細を表示できます。

一括取り込みサービスでは、サービスコンシューマロールは使用されません。

サービス固有のロール

サービス固有のロールは、1 つのサービス、または密接な関連のあるサービスのグループのアクセス特権を定義するシステム定義ロールです。例えば、アプリケーションの統合のサービス固有のロールでは、アプリケーションの統合とアプリケーション統合コンソールの両方へのアクセスが提供されます。

複数のサービスにアクセスする必要がないユーザーにはサービス固有のロールを割り当てます。サービス固有のロールには、特権が適用されるサービスに基づいてさまざまなアクセス特権があります。

次の表に、ロールを使用するサービスごとのサービス固有のロールを示します。

サービス	サービス固有のロール
アプリケーションの統合	アプリケーション統合ビジネスマネージャ アプリケーション統合データビューア
Business 360 コンソール	MDM デザイナ

サービス	サービス固有のロール
Customer 360	Customer 360 アナリスト Customer 360 マネージャ Customer 360 データスチュワード MDM ビジネスユーザー
データ統合	データ統合タスク実行者
Model Serve	Model Serve 管理者 ModelServe 予測ユーザー ModelServe システムロール
Product 360	Product 360 読み取り専用 Product 360 マネージャ
Reference 360	Reference 360 管理者 Reference 360 ビジネスアナリスト Reference 360 ビジネススチュワード Reference 360 プランナ Reference 360 プライマリオーナー Reference 360 ステークホルダー
Supplier 360	Supplier 360 読み取り専用 Supplier 360 アナリスト Supplier 360 データスチュワード Supplier 360 タスク管理者 Supplier 360 リスクマネージャ Supplier 360 契約マネージャ Supplier 360 クレジットマネージャ Supplier 360 商品マネージャ

アプリケーション統合ロールのアクセス特権

アプリケーションの統合およびアプリケーション統合コンソールのアクセス特権が必要なユーザーには、アプリケーションの統合ロールを割り当てます。各ロールは異なるアクセス特権を提供します。

次のサービス固有のロールは、アプリケーションの統合およびアプリケーション統合コンソールのアクセス特権を定義します。

アプリケーション統合ビジネスマネージャ

アプリケーション統合ビジネスマネージャはビジネスアクティビティを監視します。アプリケーション統合ビジネスマネージャロールを持つユーザーは、アセットとプロセスインスタンスに関する情報を表示できますが、それらを変更することはできません。

以下の表に、アプリケーション統合ビジネスマネージャロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
アプリケーションの統合	フォルダとアセットのリスト、アセットの詳細を表示できます。
アプリケーション統合コンソール	［プロセス］ページにアクセスできます。

アプリケーション統合データビューア

アプリケーション統合データビューアロールを持つユーザーは、アプリケーション統合コンソールサービスで詳細なログを表示できます。

注: 詳細ログを表示するユーザーのアーティファクトのログレベルは、詳細に設定する必要があります。

アプリケーション統合データビューアロールは補足的なロールです。このロールは、他の 1 つ以上のロールと共に割り当てます。例えば、デザイナロールを持つユーザーが詳細なプロセスサーバーログを表示する場合は、このユーザーにアプリケーション統合データビューアとデザイナのロールを割り当て、プロセスサーバーのログレベルを詳細に設定します。

Business 360 コンソールロールのアクセス特権

Business 360 コンソールのアクセス特権が必要なユーザーに Business360 コンソールのロールを割り当てます。

次のサービス固有のロールで、Business 360 コンソールのアクセス特権を定義します。

MDM **デザイナ**

MDM デザイナのロールを持つユーザーは、Business 360 コンソールで参照データを定義できます。

Customer 360 ロールのアクセス特権

Customer 360 に対するアクセス特権が必要なユーザーに Customer 360 ロールを割り当てます。それぞれのロールは、異なるアクセス特権を提供します。

次のサービス固有のロールで Customer 360 のアクセス特権を定義します。

Customer 360 **アナリスト**

Customer 360 アナリストロールを持つユーザーは、Customer 360 でレコードを作成および編集できます。Customer 360 アナリストがレコードを作成または編集すると、変更によってレビュープロセスがトリガされ、Customer 360 マネージャによる承認が必要になります。

Customer 360 **マネージャ**

Customer 360 マネージャのロールを持つユーザーは、顧客レコードを確認および承認したり、顧客レコードを更新したりできます。また、承認なしにレコードを作成または編集することもできます。管理者は、階層を作成および更新することもできます。

Customer 360 **データスチュワード**

Customer 360 データスチュワードのロールを持つユーザーは、Customer 360 で任意のタスクを実行できます。承認なしでレコードを作成および編集し、ジョブを実行し、顧客レコードを確認および承認することができます。データスチュワードは階層を作成および更新することもできます。

MDM **ビジネスユーザー**

MDM ビジネスユーザーのロールを持つユーザーは、Customer 360 でレコードを表示できます。Customer 360 でレコードを作成または編集することはできません。

データ統合ロールのアクセス特権

データ統合タスク実行者ロールによって、データ統合のアクセス権限が決まります。データ統合タスク実行者ロールを持つユーザーは、データ統合のタスクおよびタスクフローの実行、マッピングのテスト実行を行うことができます。データ統合ジョブを監視することもできます。

以下の表に、データ統合タスク実行者ロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

サービス	アクセス特権
管理者	Secure Agent サービスのスケジュールおよびアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。
データ統合	アセットおよびアセット詳細の表示、タスクおよびタスクフローの実行、マッピングのテスト実行を行うことができます。ユーザー独自のデータ統合ジョブおよびジョブ詳細の表示、ユーザー独自のジョブの開始および停止、セッションログのダウンロードを行うことができます。エクスポートジョブとインポートジョブは表示できません。
モニタ	データ統合ジョブおよびジョブ詳細の表示、データ統合ジョブの開始および停止、セッションログのダウンロードを行うことができます。エクスポートジョブとインポートジョブは表示できません。

Model Serve ロールのアクセス特権

Model Serve に対するアクセス特権が必要なユーザーに Model Serve ロールを割り当てます。それぞれのロールは、異なるアクセス特権を提供します。

次のサービス固有のロールで Model Serve のアクセス特権を定義します。

Model Serve **管理者**

Model Serve 管理者ロールを持つユーザーは、他の Model Serve ユーザーに権限を割り当て、機械学習モデルを登録およびデプロイできます。

ModelServe **予測ユーザー**

Model Serve 予測ユーザーロールを持つユーザーは、デプロイされた機械学習モデルから予測を生成できます。モデルデプロイメントアセットを表示できますが、アセットを変更することはできません。

ModelServe **システムロール**

このロールによって、必要な権限を Model Serve システムユーザーに割り当てます。これにより、システムユーザーはモデルデプロイメント用リソースのプロビジョニングなどのタスクを実行できるようになります。Model Server システムユーザーの詳細については、第 4 章, 「ユーザー」 (ページ 23)を参照してください。

Product 360 ロールのアクセス特権

Product 360 SaaS に対するアクセス特権が必要なユーザーに Product 360 ロールを割り当てます。それぞれのロールは、異なるアクセス特権を提供します。

次のサービス固有のロールで Product 360 のアクセス特権を定義します。

Product 360 **読み取り専用**

Product 360 読み取り専用ロールを持つユーザーは、Product 360 のレコードを表示できます。Product 360 のレコードを作成または編集することはできません。

Product 360 **マネージャ**

Product 360 マネージャロールを持つユーザーは、レコードを確認および承認できます。また、承認なしでレコードの作成、編集、削除を行うこともできます。

Reference 360 ロールのアクセス特権

Reference 360 のアクセス特権を必要とするユーザーに Reference 360 ロールを割り当てます。各ロールは異なるアクセス特権を提供します。

次のサービス固有のロールで Reference 360 のアクセス特権を定義します。

Reference 360 **管理者**

Reference 360 管理者のロールを持つユーザーは、Reference 360 環境を構成します。

Reference 360 **ビジネスアナリスト**

Reference 360 ビジネスアナリストのロールを持つユーザーは、Reference 360 アセットを表示および分析します。アセットの変更を提案することはできません。

Reference 360 **ビジネススチュワード**

Reference 360 ビジネススチュワードのロールを持つユーザーは、参照データの対象分野のエキスパートです。コードリストのコード値とクロスウォークの値マッピングを作成および管理します。ビジネススチュワードは、他のユーザーから提案された変更を承認する責任があります。承認のために独自の変更を送信することや、承認なしで変更を直接パブリッシュすることができます。ユーザーにクロスウォークへのアクセスを割り当てることができます。

Reference 360 **プランナ**

Reference 360 プランナのロールを持つユーザーは、階層を作成および管理します。ユーザーに階層へのアクセスを割り当てます。

Reference 360 **プライマリオーナー**

Reference 360 プライマリオーナーのロールを持つユーザーは、参照データセットやコードリストなどの参照データ構造を作成および定義します。プライマリオーナーはコードリストを削除し、コードリストのコード値の変更を提案できます。ビジネススチュワードのロールを持つユーザーは、提案された変更を承認する必要があります。また、プライマリオーナーは、ユーザーにコードリストと参照データセットへのアクセスを割り当てることができます。

Reference 360 **ステークホルダー**

Reference 360 のロールを持つユーザーは、コード値の変更を提案します。ビジネススチュワードのロールを持つユーザーは、提案された変更を承認する必要があります。

上記ロールの詳細については、Reference 360 のヘルプを参照してください。

Supplier 360 ロールのアクセス特権

Supplier 360 SaaS に対するアクセス特権が必要なユーザーに Supplier 360 ロールを割り当てます。それぞれのロールは、異なるアクセス特権を提供します。

次のサービス固有のロールで Supplier 360 のアクセス特権を定義します。
Supplier 360 **読み取り専用**

Supplier 360 読み取り専用ロールを持つユーザーは、Product 360 のレコードを表示できます。Supplier 360 のレコードを作成または編集することはできません。

Supplier 360 **アナリスト**

Supplier 360 アナリストロールを持つユーザーは、Supplier 360 のレコードを作成、読み取り、編集、および削除できます。Supplier 360 アナリストがレコードを作成または編集すると、変更によって確認プロセスがトリガされ、Supplier 360 マネージャによる承認が必要になります。

Supplier 360 **データスチュワード**

Supplier 360 データスチュワードロールを持つユーザーは、承認なしでのレコードの作成、編集、削除や、ジョブの実行、レコードの確認と承認、およびレコードの照合、マージ、マージ解除を実行できます。

Supplier 360 **タスク管理者**

Supplier 360 タスク管理者ロールを持つユーザーは、要求されていないすべての評価タスクを表示し、評価タスクを割り当てまたはリリースできます。また、設定に基づく作成者と承認者の特権を持ちます。

Supplier 360 **リスクマネージャ**

Supplier 360 リスクマネージャロールを持つユーザーは、リスク評価タスクの要求と拒否、およびリスク評価タスクへの対処ができます。また、レコードの作成、読み取り、編集、および削除ができます。また、設定に基づく作成者と承認者の特権を持ちます。

Supplier 360 **契約マネージャ**

Supplier 360 契約マネージャロールを持つユーザーは、契約評価タスクの要求と拒否、および承認ワークフローの契約評価タスクへの対処ができます。また、レコードの作成、読み取り、編集、および削除ができます。また、設定に基づく作成者と承認者の特権を持ちます。

Supplier 360 **クレジットマネージャ**

Supplier 360 クレジットマネージャロールを持つユーザーは、クレジット評価タスクの要求と拒否、および承認ワークフローのクレジット評価タスクへの対処ができます。また、レコードの作成、読み取り、編集、および削除ができます。また、設定に基づく作成者と承認者の特権を持ちます。

Supplier 360 **商品マネージャ**

Supplier 360 商品マネージャロールを持つユーザーは、商品評価タスクの要求と拒否、および承認ワークフローの商品評価タスクへの対処ができます。また、レコードの作成、読み取り、編集、および削除ができます。また、設定に基づく作成者と承認者の特権を持ちます。

カスタムロール

カスタムロールは、組織のニーズに基づいて作成するロールです。例えば、ロール、ユーザーグループ、およびアクセス制御を構成できるが、データ統合タスクを作成、編集、または実行できないカスタム管理ロールを作成する場合があります。

カスタムロールを作成するには、組織が適切なライセンスを持っている必要があります。カスタムロールは、作成後に編集、名前変更、および削除できます。

組織が新しいライセンスを取得した場合は、カスタムロールを編集できます。ロールを編集して、新しいアセットタイプと機能へのアクセス権限を付与します。組織が新しいライセンスを取得したときに、Informatica Intelligent Cloud Services はカスタムロールに追加の権限を付与しません。

注: カスタムロールに、ロールを作成、更新、または削除する特権を割り当てることはできません。ロールを変更する必要がある場合は、システム定義管理者ロールを持つユーザーとして Informatica Intelligent Cloud Services にログインします。

カスタムロールの作成

[ユーザーロール] ページでカスタムロールを作成します。ロールを作成する場合は、ロールに関連付けられている特権を構成する必要があります。特権は、サービスごとに別途構成します。

カスタムロールを作成するには、新しいロールを作成するか、既存のロールのクローンを作成します。新しいロールには、構成するまで特権がありません。クローンが作成されたロールには、クローン作成元のロールと同じ特権がありますが、特権は変更できます。

1. 管理者で、**[ユーザーロール]** を選択します。
2. 以下のいずれかのアクションを実行します。
   - 新規ロールを作成するには、**[ロールの追加]** をクリックします。
   - 既存のロールのクローンを作成するには、クローン作成するロールが含まれている行で **[アクション]** をクリックし、**[クローン]** を選択します。管理者ロール以外のロールのクローンを作成できます。
3. ロールの名前を入力し、必要に応じて説明を入力します。
4. **[サービス]** フィールドで、特権を構成するサービスを選択します。

   例えば、データ統合の特権を構成するには、**[データ統合]** を選択します。管理者特権を構成するには、**[管理者]** を選択します。
5. アセット特権を構成するには、**[アセット]** を選択し、各アセットタイプに対して適切な特権を有効または無効にします。

   例えば、ロールを持つユーザーがフォルダを作成できるようにするには、**[フォルダ]** の横にある **[作成]** を有効にします。
6. 機能特権を構成するには、**[機能]** を選択し、各アセットタイプに対して適切な特権を有効または無効にします。

   例えば、ロールを持つユーザーがアセットをインポートしないようにするには、**[アセット - インポート]** を無効にします。
7. 各サービスに対して、4 から 6 の手順を繰り返します。
8. **[保存]** をクリックします。

ロールを作成した後、ユーザーまたはユーザーグループに割り当てることができます。ユーザーまたはグループにロールを割り当てるには、ユーザーまたはグループを編集します。

ロールの名前変更

[ユーザーロール] ページでロールの名前を変更します。カスタムロールの名前を変更できます。システム定義のロールの名前を変更することはできません。

1. 管理者で、**[ユーザーロール]** を選択します。
2. 名前を変更するロールが含まれている行で **[アクション]** をクリックし、**[名前の変更]** を選択します。
3. ロールの新しい名前を入力します。
4. **[保存]** をクリックします。

ロールの削除

[ユーザーロール] ページでロールを削除します。ユーザーまたはユーザーグループに割り当てられているカスタムロールを削除することはできません。システム定義のロールを削除することはできません。

1. 管理者で、**[ユーザーロール]** を選択します。
2. 削除するロールが含まれている行で **[アクション]** をクリックし、**[削除]** を選択します。

B2B パートナーポータルのユーザーロール

組織で B2B Gateway を使用する場合、外部の取引パートナーのために B2B パートナーポータルへのアクセスを有効にする必要がある場合があります。B2B パートナーポータルへのアクセス権を取引パートナーに付与するには、カスタムロールを作成し、それをパートナーユーザーに割り当てます。

パートナーユーザーのカスタムロールを作成する場合、ロールには、B2B パートナーポータルのユーザー用のロールであるとわかるような名前を付けます。例えば、ロールには「B2B パートナーポータルのユーザー」などの名前を付けます。

オプションとして、ロールに説明を付与できます。パートナー会社のユーザー用のロールであるとわかるような明確な説明を付与します。例えば、ロールには「パートナー会社のユーザーが B2B パートナーポータルサービスにアクセスできるようにするためのロール」などの説明を付与します。

B2B パートナーポータルのユーザー用のカスタムロールを作成する場合、B2B パートナーポータルサービスのパートナーポータル機能特権を有効にします。カスタムロールの作成について詳しくは、「カスタムロールの作成」 (ページ 54)を参照してください。

パートナー会社のユーザーにカスタムロールを割り当てます。B2B パートナーポータルのユーザー用のロールは 1 つだけ作成すれば済みます。同じロールを B2B パートナーポータルのすべての外部ユーザーに割り当てます。

第 7 章

ユーザー設定の例

次の例は、ビジネスニーズに応じて Informatica Intelligent Cloud Services へのアクセスを制御するユーザー、ユーザーグループ、およびロールを構成する方法を示しています。

開発チームにデータ統合でタスクとタスクフローの作成を依頼するとします。開発チームは、開発環境のサンプルデータを表示できるようにする必要がありますが、プロダクションデータへのアクセスは制限したいと考えています。

1. 開発チームの開発者ロールを作成します。タスクおよび関連アセットのすべての権限を持つロールを構成しますが、接続に対しては読み取り特権のみを設定します。
2. 開発チームのユーザーグループを作成し、開発チームのすべてのメンバをそのグループに追加します。
3. 開発チームグループに開発者ロールを割り当てます。
4. 可能であれば、サンプルデータへの開発接続を作成します。開発とプロダクションの両方の接続がある場合は、開発チームグループがこれらの接続に対する読み取り権限を持たないように、プロダクション接続を構成します。これにより、開発チームグループのユーザーが、タスクのプロダクション接続を使用できないようにします。
5. テストが完了し、タスクをプロダクション環境に移行する準備ができたら、管理者または他の資格あるユーザーよって、プロダクション接続を使用するようにタスクが設定されるようにします。
6. 開発者ロールを編集し、タスクを実行する特権を削除します。タスクのタイプに対して開発が完了した場合は、タスクを読み取りおよび更新するための特権を削除することもできます。読み取り特権を削除すると、開発者ロールを持つユーザーが、プロダクションタスクに関する情報にアクセスできなくなります。

データ統合でタスクを実行する必要があっても、タスクを安全に設定する技術的な知識を持っていないレポートチームも存在します。

1. レポートチームのレポータロールを作成します。タスクおよびタスクフローの読み取りと実行、およびスケジュールの読み取り、作成、および更新を行う特権を持つロールを構成します。組織内のアセットに対する特権を作成、更新、削除、または設定する権限を有効にしないでください。
2. レポートチームのユーザーグループを作成し、レポートチームのすべてのメンバをそのグループに追加します。
3. レポートチームグループにレポータロールを割り当てます。

ロールとユーザーグループの割り当てやアクセス制御の設定を行うことができても、タスクを作成、編集、または実行できないセキュリティ管理者を指定するとします。

1. Security Administrator（セキュリティ管理者）という名前のカスタムロールを作成します。
2. Security Administrator（セキュリティ管理者）ロールを編集し、タスク、接続、およびスケジュールを作成、更新、削除、実行するための特権を除くすべての特権を付与します。
3. Security Administrator（セキュリティ管理者）ロールをセキュリティ管理者に割り当てます。

組織の管理者を簡単に追跡したいとします。

「組織の管理者」というユーザーグループを作成し、このグループに管理者ロールを割り当てます。組織のすべての管理者を、このグループに追加します。

組織では、OrderProcessing API を使用して大規模なサプライヤへの注文を管理します。この API は、CreateOrder、ApproveOrder、GetOrder を含むアプリケーションの統合のプロセスからなります。管理者は、ApproveOrder プロセスにアクセスできるユーザーを少数に制限する必要があります。

1. 承認者という名前のカスタムロールを作成します。承認者ロールのアプリケーション統合アセットに実行特権を設定します。
2. 注文承認者という名前のユーザーグループを作成します。
3. 承認者ロールを注文承認者グループに割り当てます。
4. サービスコンシューマロールを注文承認者グループに割り当てます。サービスコンシューマロールでプロセスにアクセスして呼び出すことができるように割り当てる必要があります。
5. ApproveOrder プロセスを呼び出すことができるユーザーを注文承認者グループに割り当てます。
6. ApproveOrder プロセスでは、次のフィールドのいずれかを構成する必要があります。
   - ユーザーのグループにアクセス権を割り当てるには、**[許可されたグループ]** フィールドに注文承認者グループを入力します。
   - 特定のユーザーにアクセス権を割り当てるには、**[許可されたユーザー]** フィールドにユーザーを入力します。フィールドには、複数のユーザーを入力できます。

[許可されたユーザー] フィールドで指定された注文承認者グループとユーザーのメンバーのみが ApproveOrder プロセスを呼び出すことができます。

アプリケーションの統合開発者がアプリケーション統合コンソールの詳細なプロセスログの表示以外のすべての機能を実行できるようにしたいとします。

1. Custom_Dev というロールを作成し、そのロールに次の特権を設定します。
   a. アプリケーションの統合サービスを選択し、**[アセット]** タブに移動して、**[アプリケーション統合アセット]** のすべての CRUD 特権を有効にします。
   b. **[機能]** タブに移動し、ロールに、開発、コンソール管理、アプリケーション統合アセットのパブリッシュ、アプリケーション統合コンソールの表示、アプリケーション統合デザイナの表示の各特権を追加します。
   c. データ統合サービスを選択し、**[アセット]** タブに移動して、**[プロジェクト]** と **[フォルダ]** アセットのすべての CRUD 特権を有効にします。
2. Custom_Dev ロールを開発者に割り当てます。

第 8 章

ユーザープロファイルの編集

ユーザープロファイルには Informatica Intelligent Cloud Services のユーザーアカウントの詳細が含まれます。

プロファイル内の次の情報を更新できます。

- 姓名
- 役職
- 電子メールアドレス
- 電話番号
- タイムゾーン（**[すべてのジョブ]**、**[実行中のジョブ]**、**[マイジョブ]**、**[インポート/エクスポートログ]**、**[マインインポート/エクスポートログ]** ページのジョブ実行のタイムスタンプで使用）
- パスワード
- セキュリティの質問および回答

注: SAML を使用して Informatica Intelligent Cloud Services にサインオンし、組織の管理者が管理者の **[SAML セットアップ]** ページで SAML グループとロールのマッピングを有効にしている場合、更新できるのはタイムゾーンのみです。その他の属性は、Informatica Intelligent Cloud Services にログインするたびにエンタープライズディレクトリから直接更新されます。

1. Informatica Intelligent Cloud Services ウィンドウ右上隅にある **[ユーザー]** アイコンをクリックして、**[プロファイル]** を選択します。
2. **[プロファイル]** ページで、氏名、役職、電話番号、タイムゾーンなどの個人情報を追加または編集します。
3. 電子メールアドレスを更新するには、**[電子メールを更新]** をクリックします。

   Informatica Intelligent Cloud Services から新しい電子メールアドレス宛てに確認メールが送信されます。電子メールには、24 時間有効なリンクが含まれています。電子メール内のリンクをクリックすると、新しいアドレスが確認され、プロファイルに表示されます。リンクの有効期限が切れた場合は、確認メールを再送信できます。
4. 必要に応じて、パスワードまたはセキュリティの質問を変更します。
5. **[保存]** をクリックします。

索引

ゆ

ろ