



Informatica® Intelligent Cloud Services  
October 2025

# ユーザー管理

© 著作権 Informatica LLC 2021, 2025

本ソフトウェアおよびマニュアルは、使用および開示の制限を定めた個別の使用許諾契約のもとでのみ提供されています。本マニュアルのいかなる部分も、いかなる手段（電子的複製、写真複製、録音など）によっても、Informatica LLC の事前の承諾なしに複製または転載することは禁じられています。

米政府の権利プログラム、ソフトウェア、データベース、および関連文書や技術データは、米国政府の顧客に配信され、「商用コンピュータソフトウェア」または「商業技術データ」は、該当する連邦政府の取得規制と代理店固有の補足規定に基づきます。このように、使用、複製、開示、変更、および適応は、適用される政府の契約に規定されている制限およびライセンス条項に従うものとし、政府契約の条項によって適当な範囲において、FAR 52.227-19、商用コンピュータソフトウェアライセンスの追加権利を規定します。

Informatica、Informatica Cloud、Informatica Intelligent Cloud Services、PowerCenter、PowerExchange、および Informatica ロゴは、米国およびその他の国における Informatica LLC の商標または登録商標です。Informatica の商標の最新リストは、Web (<https://www.informatica.com/trademarks.html>) にあります。その他の企業名および製品名は、それぞれの企業の商標または登録商標です。

本ソフトウェアまたはドキュメンテーション（あるいはその両方）の一部は、第三者が保有する著作権の対象となります。必要な第三者の通知は、製品に含まれています。

本マニュアルの情報は、予告なしに変更されることがあります。このドキュメントで問題が見つかった場合は、[infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com) までご報告ください。

Informatica 製品は、それらが提供される契約の条件に従って保証されます。Informatica は、商品性、特定目的への適合性、非侵害性の保証等を含めて、明示的または黙示的ないかなる種類の保証をせず、本マニュアルの情報を「現状のまま」提供するものとします。

発行日: 2025-12-01

# 目次

<b>序文</b>	<b>6</b>
Informatica のリソース	6
Informatica マニュアル	6
Informatica Intelligent Cloud Services Web サイト	6
Informatica Intelligent Cloud Services コミュニティ	6
Informatica Intelligent Cloud Services マーケットプレイス	7
データ統合のコネクタのドキュメント	7
Informatica ナレッジベース	7
Informatica Intelligent Cloud Services Trust Center	7
Informatica グローバルカスタマサポート	7
<b>第 1 章 : ユーザー管理</b>	<b>8</b>
<b>第 2 章 : ユーザー認証</b>	<b>9</b>
多要素認証	9
多要素認証の設定	10
エコシステムのシングルサインオン	10
<b>第 3 章 : SAML のシングルサインオン</b>	<b>12</b>
SAML のシングルサインオンの要件	13
シングルサインオンの制限	14
SAML 認証によるユーザー管理	14
SAML 認証と承認からの切り替え	15
SAML 認証と承認によるユーザー管理	15
SAML 認証のみからの切り替え	16
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	16
Informatica Intelligent Cloud Services の SAML シングルサインオン設定	18
プロバイダ設定とマッピング属性の設定	18
SSO 設定のプロパティ	19
ID プロバイダ設定のプロパティ	20
サービスプロバイダ設定	21
SAML 属性マッピングのプロパティ	21
SAML ロールとグループマッピングのプロパティ	23
サービスプロバイダメタデータのダウンロード	24
JSON Web トークンを使用した OAuth	24
<b>第 4 章 : ユーザー</b>	<b>26</b>
アプリケーションの統合の匿名ユーザー	27
ユーザー統計	27
ユーザーの詳細	28

ユーザーの作成.....	32
サービスの割り当ておよび割り当て解除.....	33
ユーザーの無効化.....	34
ユーザーのリセット.....	34
ユーザーのスケジュール済みジョブの再割り当て.....	35
ユーザーの削除.....	35
<b>第 5 章 : ユーザグループ.....</b>	<b>36</b>
ユーザーグループの詳細.....	37
ユーザーグループの作成.....	38
ユーザーグループの名前変更.....	39
ユーザーグループの削除.....	39
<b>第 6 章 : ユーザーロール.....</b>	<b>40</b>
ロールの詳細.....	41
システム定義のロール.....	42
クロスサービスロール.....	43
管理者ロール.....	46
API センターのロール.....	47
API マネージャのロール.....	48
API Portal のロール.....	48
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ロール.....	49
B2B Gateway のロール.....	50
B2B パートナーポータルロール.....	50
Business 360 コンソールのロール.....	51
CLAIRE GPT ロール.....	52
PowerCenter 用クラウドデータ統合 (CDI-PC) のロール.....	52
Customer 360 SaaS のロール.....	52
データガバナンス&カタログのロール.....	53
データ取り込みおよびレプリケーションロール.....	54
データ統合ロール.....	54
データマーケットプレイスのロール.....	55
データプロファイリングロール.....	58
データ品質のロール.....	58
統合ハブのロール.....	59
メタデータコマンドセンターのロール.....	60
モニタロール.....	60
オペレーションインサイトロール.....	61
Product 360 SaaS のロール.....	61
Reference 360 のロール.....	62
Supplier 360 SaaS のロール.....	63
カスタムロール.....	64
カスタムロールの作成.....	64

ロールの名前変更. . . . .	65
ロールの削除. . . . .	65
ロールアセットと機能特権. . . . .	65
管理者のアセット特権と機能特権. . . . .	66
アプリケーションの統合機能特権. . . . .	69
データガバナンス&カタログの機能特権. . . . .	71
データ取り込みおよびレプリケーションの最小アセットと機能特権. . . . .	72
データ統合のアセット特権と機能特権. . . . .	73
データマーケットプレイスの機能特権. . . . .	75
データプロファイリングの機能特権. . . . .	75
データ品質の機能特権. . . . .	77
ドメイン管理サービスのアセット特権と機能特権. . . . .	77
ヒューマンタスクのアセットと機能特権. . . . .	79
メタデータコマンドセンターの機能特権. . . . .	79
モニタの機能特権. . . . .	81
オペレーションインサイトの機能特権. . . . .	81
ワークベンチサービスのアセット特権と機能特権. . . . .	82
<b>第 7 章 : ユーザー設定. . . . .</b>	<b>84</b>
通知カテゴリおよびサブカテゴリ. . . . .	84
<b>第 8 章 : ユーザー設定の例. . . . .</b>	<b>87</b>
<b>第 9 章 : ユーザープロファイルの編集. . . . .</b>	<b>89</b>
<b>第 10 章 : 組織へのユーザーの招待. . . . .</b>	<b>90</b>
<b>第 11 章 : 通知. . . . .</b>	<b>91</b>
<b>索引. . . . .</b>	<b>92</b>

# 序文

「ユーザー管理」を使用して、Informatica Intelligent Cloud Services<sup>SM</sup>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ィー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](mailto: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 マーケットプレイス

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/>

## データ統合のコネクタのドキュメント

データ統合の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](mailto: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。

サブスクライブするには、[Informatica Intelligent Cloud Services Status](#) ページで **【サブスクライブして更新】** をクリックします。電子メール、SMS テキストメッセージ、Webhook、RSS フィード、またはこの 4 つの任意に組み合わせとして送信される通知を受信するという選択ができます。

## Informatica グローバルカスタマサポート

グローバルサポートセンターには、Informatica Network または電話でお問い合わせください。

Informatica Network でオンラインサポートリソースを検索するには、Informatica Intelligent Cloud Services のヘルプメニューで **【サポートにお問い合わせください】** をクリックして、**Cloud Support** ページに移動します。**Cloud Support** ページには、システムステータス情報とコミュニティディスカッションが記載されています。追加のリソースを検索する場合や電子メールで Informatica グローバルカスタマサポートに問い合わせる場合は、Informatica Network にログインし、**【サポートが必要な場合】** をクリックしてください。

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、[「エコシステムのシングルサインオン」 \(ページ 10\)](#)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」 \(ページ 12\)](#)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」 \(ページ 26\)](#)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, 「ユーザーグループ」 \(ページ 36\)](#)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」 \(ページ 40\)](#)を参照してください。

各ユーザーは、ユーザープロフィールで、電子メール、パスワード、タイムゾーンなどの個人情報を設定することができます。ユーザーは、ユーザー設定で通知設定とソース管理の資格情報を設定することができます。詳細については、[第 9 章, 「ユーザープロフィールの編集」 \(ページ 89\)](#)と [第 7 章, 「ユーザー設定」 \(ページ 84\)](#)を参照してください。



## 第 2 章

# 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 Informatica Intelligent Cloud Services を通じて認証され、組織固有のユーザー名とパスワードを使用してログインします。ネイティブの人間のユーザーはユーザーインターフェースにログインすることができますが、人間以外のユーザーは API の使用に制限されます。

多要素認証を有効にして、人間のユーザーに対してセキュリティ層を追加することができます。

### 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、[「エコシステムのシングルサインオン」 \(ページ 10\)](#)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」 \(ページ 12\)](#)を参照してください。

## 多要素認証

ネイティブの人間のユーザーは、多要素認証を使用して、ユーザーインターフェースにログインするたびに電子メールで確認コードを受信できます。

組織の多要素認証を有効にしてから、ユーザーを次の ID タイプに分類することができます。

## 人間のユーザー

ユーザーインターフェースにログインして、サービスとデータのやり取りを行う実際の人物。多要素認証を有効にすると、人間のユーザーは電子メールで確認コードを受信します。それぞれの人間のユーザーの電子メールアドレスが有効であることを確認する必要があります。

## 人間以外のユーザー

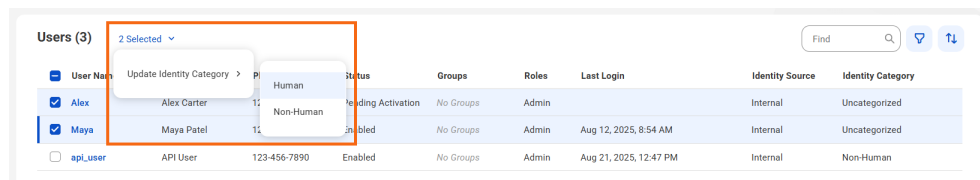
ソフトウェア、統合、自動化されたプロセス、および人間の操作なしでサービスにアクセスする API のユーザーアカウント。

ユーザーインターフェースを使用しないユーザーを人間以外のユーザーとして分類することができます。人間以外のユーザーはユーザーインターフェースにログインできないため、API を実行するために確認コードを入力する必要はありません。

# 多要素認証の設定

多要素認証を設定すると、ネイティブの人間のユーザーが Informatica Intelligent Cloud Services にログインするたびに確認コードを受け取ることができます。

1. **【組織】** ページで、多要素認証を有効にします。
2. **【ユーザー】** ページで、ユーザーを人間または人間以外のユーザーに分類します。
  - 個々のユーザーを分類するには、ユーザーをドリルダウンし、**【ID カテゴリ】** を人間または人間以外に設定します。
  - 複数のユーザーを同時に分類するには、それぞれのユーザーを選択します。次に、**【<数>個を選択】** > **【ID カテゴリの更新】** > **【人間】** または **【人間以外】** の順に選択します。次の画像に、複数のユーザーを分類するためのメニューオプションを示します。



**【ログ】** ページで、セキュリティログを確認して、ユーザーが多要素認証を使用してアカウントにログインしていることを確認します。

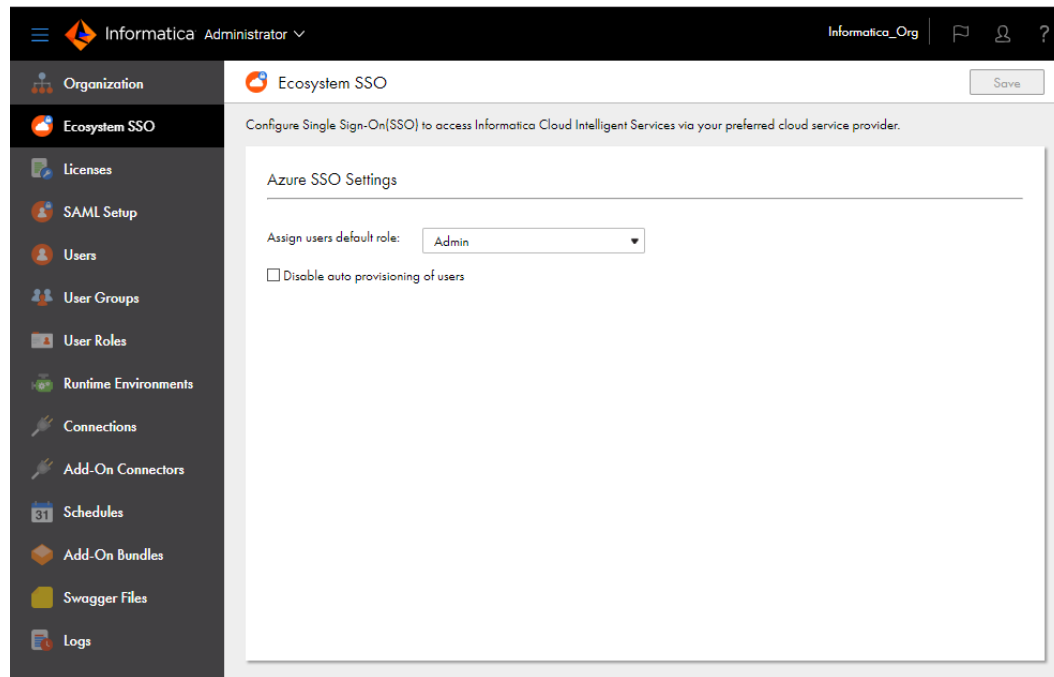
# エコシステムのシングルサインオン

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」 \(ページ 12\)](#) 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することもできます。

#### 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 オースト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、またはチケット経由で 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。

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する 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 SCIM 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。

## SCIM トークンの管理

それぞれのユーザーは、最大 2 つの SCIM トークンを作成して同時に使用することができます。各トークンは、生成してから 180 日間有効です。トークンの有効期限が切れると、既存の接続であっても、新しいトークンを生成する必要があります。

ベストプラクティスとしては、トークンを別の日に作成して、有効期限日と同じ日にならないようにします。例えば、ある日にトークンを生成したら、2 番目のトークンは 90 日後に生成することをお勧めします。Informatica Intelligent Cloud Services は、トークンの有効期限が近づいたときに通知します。

**注:** 1 つまたは両方のトークンの有効期限が切れた場合でも、2 つ以上のトークンを生成することはできません。2 つのトークンを使用しており、新しいトークンを生成する必要がある場合は、最初に既存のトークンの 1 つを削除する必要があります。

scimTokens REST API リソースを使用して SCIM トークンを管理することもできます。詳細については、『*REST API リファレンス*』を参照してください。

1. 管理者の **[SAML セットアップ]** ページで、**[トークンの管理]** をクリックします。

このオプションは、**[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]** オプションを有効にしている場合に有効になります。

**[SCIM トークン]** ダイアログボックスには、作成した SCIM トークンと、それぞれのトークンの有効期限およびステータスが表示されます。2 つのトークンが表示されている場合は、新しいトークンを生成する前にどちらかのトークンを削除する必要があります。

2. トークンを生成するには、**[トークンの生成]** をクリックし、トークンをクリップボードにコピーします。  
このトークンは、プロビジョニングアプリで SCIM を有効にするときに必要になります。
3. トークンを削除するには、削除対象のトークンの **[削除]** アイコンをクリックします。

# 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 XML ファイルを使用	<p><b>[SAML セットアップ]</b> 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。</p> <p>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、<b>[参照]</b> をクリックし、ID プロバイダ XML ファイルに移動します。</p>
ユーザーの自動プロビジョニングの無効化	<p>SAML ユーザーの自動プロビジョニングを無効にします。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>デフォルトでは無効になっています。</p>
SAML グループとロールのマッピング	<p>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。</p> <p>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。</p> <p>デフォルトでは無効になっています。</p>
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	<p>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。</p> <p>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、<b>[トークンの管理]</b> をクリックします。ベアラトークンの生成と管理の詳細については、<a href="#">「SCIM トークンの管理」 (ページ 17)</a>を参照してください。</p> <p><b>警告:</b> 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。</p> <p>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。</p> <p>デフォルトでは無効になっています。</p>

## 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: <code>&lt;saml:Issuer&gt;http://idp.example.com&lt;/saml:Issuer&gt;</code>
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。 <b>注:</b> 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。
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。 <code>urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress</code>
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。 <ul style="list-style-type: none"><li>- 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。</li><li>- 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。</li></ul>

## 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。
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。 <b>注:</b> 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。

プロパティ	説明
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。
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。

プロパティ	説明
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。

**注:** グループを Azure Active Directory にマッピングする方法については、ナレッジベースの記事 [HOW TO: Create a SAML Group Mapping with Azure AD](#) を参照してください。

**[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。

### SAML ロールマッピング

**[SAML グループとロールのマッピング]** オプションを有効にすると、Informatica Intelligent Cloud Services の各ロールを同等の SAML ロールにマッピングできます。複数のロールを入力する場合は、カンマを使用してロールを区切ります。最大で 255 文字まで入力できます。

**[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は、次の SAML ロールマッピングプロパティを定義できます。

プロパティ	説明
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。
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。

### SAML グループマッピング

**[SAML グループとロールのマッピング]** オプションを有効にすると、Informatica Intelligent Cloud Services の各ロールを同等の SAML グループにマッピングできます。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。



**[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は、次の SAML グループマッピングプロパティを定義できます。

プロパティ	説明
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。
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。

## 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。

## JSON Web トークンを使用した OAuth

組織が SAML を使用するように設定されていて、組織が Informatica Intelligent Cloud Services REST API を使用している場合、ユーザーは JSON Web トークン（JWT）を使用してログインし、REST API セッションを開始できます。

JWT アクセストークンの使用は、SAML アサーションの使用と類似しています。ただし、SAML アサーションを使用する場合とは異なり、ユーザーは ID プロバイダから JWT アクセストークンを取得し、ログイン要求にそのトークンを含めます。

ユーザーが JWT アクセストークンを使用する前に、次のタスクを完了してください。

- SAML を使用するように組織を設定し、ユーザーを SAML ユーザーとして設定します。
- OAuth ID プロバイダを設定します。Azure Active Directory や Okta などの ID プロバイダを使用することができます。
- ID プロバイダから JWT アクセストークンを取得するメソッドを設定します。
- Informatica Intelligent Cloud Services REST API を使用して ID プロバイダを登録します。



ログインするには、ユーザーは ID プロバイダから JWT アクセストークンを取得し、loginOAuth POST 要求にそのトークンを含めます。トークンは、1 つの REST API セッションに使用することができます。ログイン要求が成功した場合、応答には、後続の API 呼び出しで使用するセッション ID が含まれます。

Azure Active Directory を使用した OAuth の設定については、次の記事を参照してください:

[Set up OAuth with Azure AD](#)

ID プロバイダの設定の詳細については、ID プロバイダのマニュアルを参照してください。

ID プロバイダの登録と JWT アクセストークンを使用したログインの詳細については、『REST API リファレンス』を参照してください。

## 第 4 章

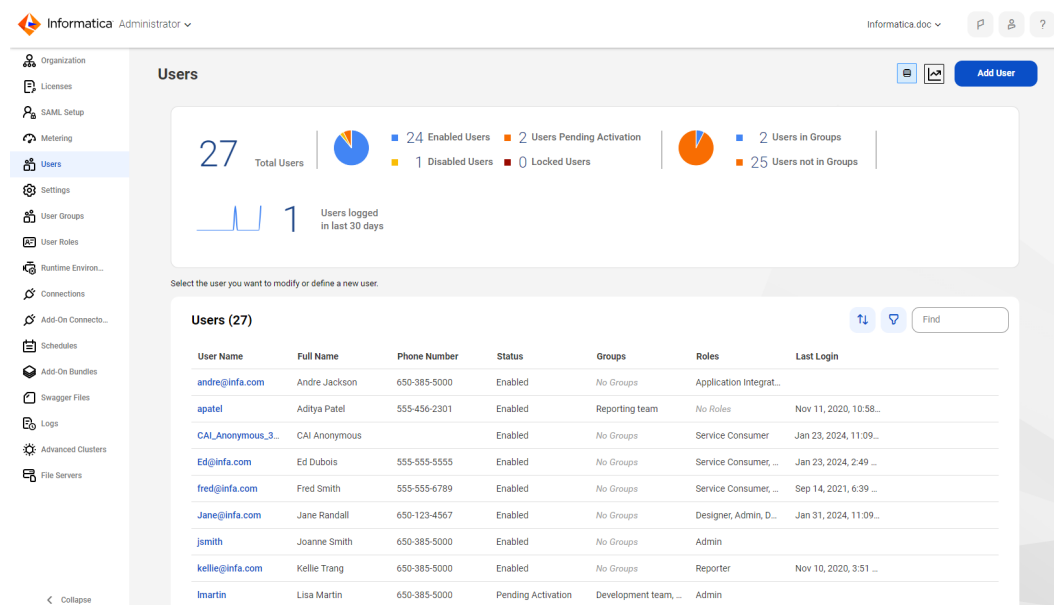
# ユーザー

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。

**注:** ユーザーを検索する場合は、ユーザー名、またはユーザーの姓または名で検索します。ユーザーのフルネームで検索することはできません。

## 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。

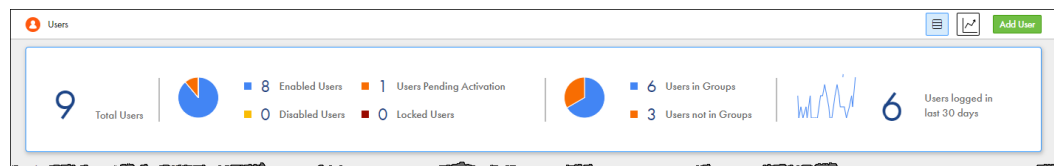
- アプリケーション統合の匿名ユーザーに、関連するデータ統合アセットの実行権限を付与します。
- アプリケーション統合の匿名ユーザーを、関連するデータ統合アセットの実行権限を持つユーザーグループに追加します。

## 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。

jsmith.ma

Save

Define the user account settings, including group and role assignments.

User Information

First Name: \*

John

Last Name: \*

Smith

Job Title: \*

Designer

Phone Number: \*

650-385-5000

Email: \*

jsmith.ma@informatica.com

Update Email

Description:

Admin, Designer

Login Settings

Authentication: \*

Native

Identity Category: \* ⓘ

Uncategorized

User Name: \*

jsmith.ma

Max Login Attempts:

10

Account Status:

Enabled

Initial Application:

Default

Effective Default Service: ⓘ

None

☐ Force password reset on next login.

Group, Role, and Service Assignment

Find

Groups

Roles

Services

☒ Group Name

Description

☒ Development team

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。 電話番号は 10 文字から 25 文字で、数字、スペース、括弧、ピリオド、および最初の文字としてのプラス記号のみを使用できます。

プロパティ	説明
電子メール	<p>ユーザーの電子メールアドレス。</p> <p>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: &lt;local_part&gt;@&lt;domain&gt;例: jsmith@mycompany.com</p> <p>電子メールアドレスを更新するには、<b>[電子メールを更新]</b> 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。</p> <p>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。</p>
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	<p>認証方法。次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>- <b>ネイティブ</b>。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。</li> <li>- <b>Salesforce</b>。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。</li> <li>- <b>Azure SSO</b>。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。</li> <li>- <b>IDP と SAML</b>。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。</li> </ul>
ID カテゴリ	<p>ID タイプ。次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>- <b>人間</b>。ユーザーインターフェースにログインして、サービスとデータのやり取りを行う実際の人物。</li> <li>- <b>人間以外</b>。ソフトウェア、統合、自動化されたプロセス、および人間の操作なしでサービスにアクセスする API のユーザーアカウント。</li> </ul> <p>多要素認証が有効になっている場合、ログイン時に確認コードを受け取るためにユーザーを人間として分類する必要があります。</p>

プロパティ	説明
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	<p>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。</p> <ul style="list-style-type: none"> <li>- 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。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>- 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。</li> </ul> <p>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。</p> <p>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。</p>
環境	<p>Salesforce 組織環境。プロダクションまたはサンドボックスです。</p> <p>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。</p>
ユーザー名	<p>Informatica Intelligent Cloud Services のユーザー名。有効な電子メールアドレスか、または英数字、ハイフン、アンダースコア、ピリオド、アポストロフィーのみで構成された名前にすることができます。</p> <p>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。ユーザーの保存後に名前を変更することはできません。</p> <p>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。</p>
Salesforce ユーザー名	<p>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。</p> <p>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。</p> <p>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。</p>
Azure ユーザー名	<p>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。</p> <p>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。</p> <p>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。</p>

プロパティ	説明
SAML ユーザー名	<p>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。</p> <p>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。</p> <p>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。</p>
最大ログイン試行回数	<p>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失敗回数。数値を選択します。デフォルトは 3 です。</p> <p>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。</p> <p>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。</p>
アカウントステータス	<p>アカウントのステータス。次のいずれかを指定します。</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> <li>- 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越えたため、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。</li> <li>- 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。</li> </ul>
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。
有効なデフォルトサービス	管理者が設定した、ユーザーがログインしたときに開くデフォルトのサービス。ユーザーは、[マイサービス] ページでデフォルトのサービスを選択することで、この設定を上書きできます。
次のログイン時にパスワードのリセットを強制	<p>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。</p> <p>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。</p>

## グループ、ロール、およびサービス割り当て

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。

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。

ユーザーのグループメンバーシップによってユーザーのサービス割り当てを定義できるようにするか、ユーザーのグループメンバーシップでサービスへのアクセスが許可されているかどうかに関係なく、ユーザーにサービスを割り当てることができます。

**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】** ページを開きます。
2. **【ユーザーの追加】** を選択します。
3. ユーザー情報を入力します。
4. **【ログイン設定】** セクションで、認証方法を選択し、適切なログイン設定を入力します。
  - ネイティブユーザーの場合は、ID カテゴリを選択し、Informatica Intelligent Cloud Services ユーザー名を入力して、ログイン試行の最大回数を選択します。
  - 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。次に、サードパーティの ID プロバイダのシステムにユーザー名を入力します。
  - Microsoft Azure または SAML のユーザーの場合は、サードパーティの ID プロバイダのシステムにユーザー名を入力します。

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ことはできません。

5. **【グループ、ロール、およびサービス割り当て】** セクションで、ユーザーに割り当てるユーザーグループまたは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. 必要に応じて、ユーザーにサービスを割り当て、ユーザーがログインしたときに開くデフォルトのサービスを設定します。

デフォルトでは、ユーザーは組織のライセンスとユーザーが属するユーザーグループに基づいてサービスにアクセスできます。

ユーザーは、**【サービス】** ページでデフォルトのサービスを選択するときに、選択したデフォルトのサービスを上書きできます。

7. **【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、ユーザーは組織のライセンス、ユーザーのロール、およびユーザーが属するグループに基づいてサービスにアクセスできます。

ユーザーは通常、ユーザーグループに割り当てられたサービスを継承します。ただし、**【ユーザー】** ページでサービスへのアクセスを具体的に許可または拒否することができます。

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 ポータルは使用でき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。ユーザーに対して明示的に API ポータルサービスを許可し、データ統合サービスとアプリケーションの統合サービスを拒否します。この操作を行うと、サービスコンシューマロールに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に関連する特権が割り当てられている場合でも、アプリケーション開発者の **【サービス】** ページにはそれらのサービスが表示されなくなります。

ユーザーがサービスにアクセスできる場合、そのサービスは **【サービス】** ページに表示されます。ユーザーは、アクセスが許可されている限り、サービスにアクセスして使用できます。

ユーザーがサービスにアクセスできなくなると、そのユーザーの **【サービス】** ページにはサービスが表示されなくなります。

**重要:** サービスを許可または拒否しても、そのサービスがユーザーインターフェースに表示されるか非表示になるだけです。サービスを明示的に拒否した場合でも、ユーザーは、割り当てられたロールに関連付けられているすべての特権を保持します。つまり、アクセスが拒否された場合でも、ユーザーは API を介してアクションを実行できる可能性があります。ベストプラクティスとして、ユーザーに割り当てられたサービスと一致する特権のみを割り当てるようにしてください。

ユーザーに割り当てられたサービスから、ユーザーがログインしたときに開くデフォルトのサービスを選択できます。

デフォルトのサービスは、ユーザーレベルまたはユーザーグループレベルで設定できます。ユーザーは、**【サービス】** ページでデフォルトのサービスを選択することもできます。デフォルトのサービスが複数のレベルで設定されている場合は、ユーザーが **【サービス】** ページで行った設定が優先され、次にユーザーレベル、ユーザーグループレベルの順に設定が使用されます。

1. 管理者で **【ユーザー】** を選択します。
2. ユーザーのリストから、ユーザーの名前をクリックします。
3. **【グループ、ロール、およびサービス割り当て】** セクションの **【サービス】** タブで、それぞれのサービスに対して次のいずれかのタスクを実行します。
  - ユーザーがサービスにアクセスできるかどうかをユーザーのグループメンバーシップで定義できるようにするには、**【許可】** オプションおよび **【拒否】** オプションを選択解除したままにします。グループのサービスが変更されると、サービスへのユーザーのアクセスも自動的に変更されます。
  - ユーザーのグループで定義されている内容に関係なく、サービスへのアクセスを許可するには、**【許可】** オプションを選択します。

**ヒント:** 割り当てるサービスが表示されない場合は、組織のライセンスにそのサービスが存在しないことを意味します。
  - サービスへのアクセスを拒否するには、ユーザーのグループがそのサービスへのアクセスを許可しているかどうかに関係なく、**【拒否】** オプションを選択します。
4. 必要に応じて、ユーザーがログインしたときに開くデフォルトのサービスを選択します。
5. **【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（トリガまたはソースとして）一括取り込みファイルで使用する場合、または（トリガとして）タスクフローで使用する場合は、ユーザーを無効化する前に、REST API を使用してファイルリスナの関連付けの所有権をあるユーザーから別のユーザーに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*』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（トリガまたはソースとして）一括取り込みファイルで使用する場合、または（トリガとして）タスクフローで使用する場合は、ユーザーを削除する前に、REST API を使用してファイルリスナの関連付けの所有権のあるユーザーから別のユーザーに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*』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

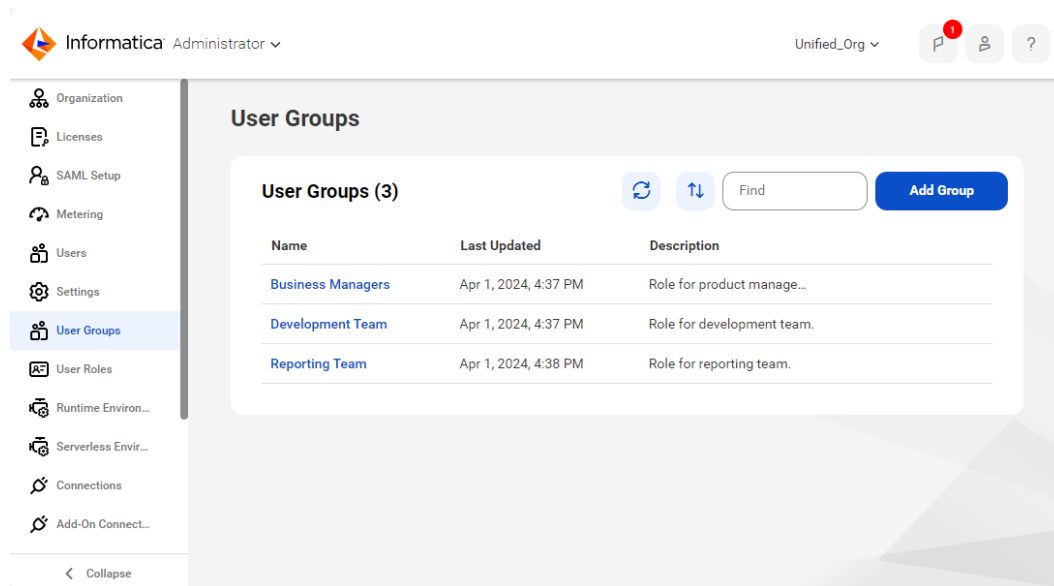
# ユーザグループ

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、組織のユーザグループを構成できます。

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

次の図は、[ユーザグループ] ページを示しています。



ユーザ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、グループメンバー、割り当てられたサービス、およびログイン時に開くデフォルトのサービスなど、ユーザーグループに関する詳細を設定できます。[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。

**Development team** Save X

Name: \* Development team

Description:

**Role, Membership, and Service Assignment**

Roles Members (0) Services

Enabled	Role Name	Description
<input type="checkbox"/>	Deployer	Role used by deployer
<input checked="" type="checkbox"/>	Designer	Role for creating assets, tasks, and processes. Can configure connections, schedules, and runtime environ...
<input type="checkbox"/>	Designer_CLONE	Role for creating assets, tasks, and processes. Can configure connections, schedules, and runtime environ...
<input type="checkbox"/>	Elastic RTE Dev Ops Engin...	Role for managing Elastic Runtime Environments

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）。
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。

プロパティ	説明
メンバー	<p>グループに割り当てられているユーザー。</p> <p>リストにユーザーを追加するか、リストからユーザーを削除するには、<b>【ユーザーの管理】</b> ボタンを使用します。</p> <p>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とサービスが自動的に割り当てられます。</p>
サービス	<p>グループがアクセスできるサービスと、ユーザーグループのメンバーであるユーザーがログインしたときに開くデフォルトのサービス。</p> <p>このリストには、組織のライセンスに含まれるすべてのサービスが含まれています。</p> <p>デフォルトでは、ユーザーグループには、組織が使用ライセンスを取得しているすべてのサービスが割り当てられています。</p> <p>ユーザーをグループに追加すると、次の条件をすべて満たす場合、そのユーザーはグループのすべてのサービスにアクセスできるようになります。</p> <ul style="list-style-type: none"> <li>- ユーザーの1つ以上のロールにサービスへのアクセスが許可されている。</li> <li>- ユーザーによるサービスへのアクセスが明示的に「拒否」されていない。</li> </ul> <p>ユーザーのロールの詳細については、<b>「ユーザーの詳細」</b> (ページ 28) を参照してください。</p> <p>ユーザーによるサービスへのアクセスを明示的に許可または拒否する方法の詳細については、<b>「サービスの割り当ておよび割り当て解除」</b> (ページ 33) を参照してください。</p> <p><b>注:</b> アクセスを明示的に許可することで、ユーザーは、ユーザーのグループメンバーシップに含まれていないサービスにアクセスできるようになります。</p>

**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、異なるタイプのアセットに対して同じアクセス権を必要とする場合、または同じサービスにアクセスする必要がある場合は、ユーザーグループを作成します。グループメンバーは、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. **【ロール、メンバーシップ、およびサービス割り当て】** セクションの **【ロール】** タブで、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ーに適用されます。
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、**【メンバー】** タブで **【ユーザーの管理】** をクリックし、リストからユーザーを選択します。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. **【サービス】** タブで、グループに対して有効になっているサービスを選択します。  
ユーザーレベルでサービスアクセスをオーバーライドして、このユーザーグループのメンバーがユーザーグループとは異なるサービスにアクセスできるようにすることができます。
7. 必要に応じて、ユーザーグループのメンバーであるユーザーがログインしたときに開くデフォルトのサービスを選択します。  
ユーザーが複数のユーザーグループに属している場合は、指定されたデフォルトのサービスを持つ最後に変更されたユーザーグループを使用して、ユーザーがログインしたときに開くサービスが決定されます。
8. **【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、デザイナー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。

組織の管理者は、組織のロールの設定および割り当てを行うことができます。

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

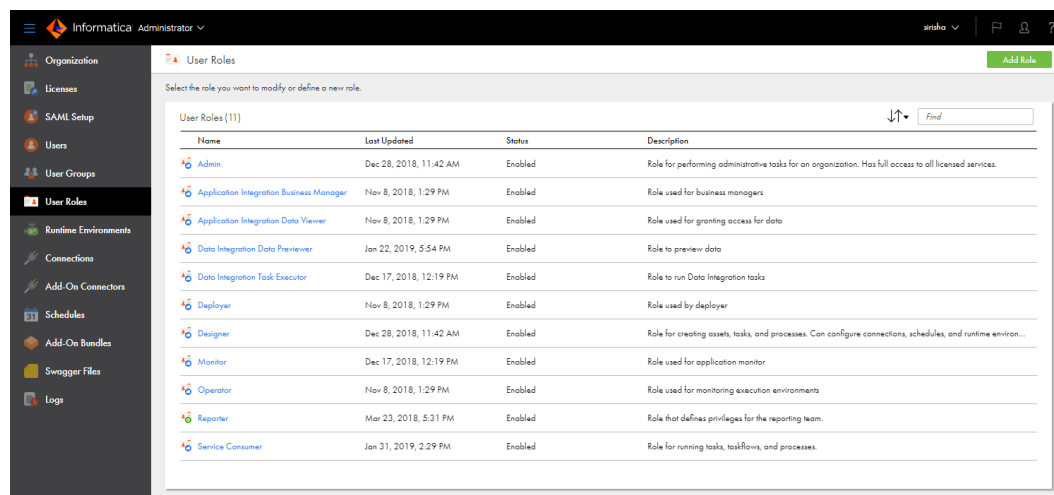
システム定義ロールは、組織で使用されるサービスのアクセス特権を定義した定義済みのロールです。ユーザーおよびユーザーグループに割り当てることのできるシステム定義ロールは、組織のライセンスによって異なります。システム定義のロールを編集、名前変更、または削除することはできません。管理者ロール以外のシステム定義ロールのクローンを作成できます。

### 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。



Name	Last Updated	Status	Description
Admin	Dec 28, 2018, 11:42 AM	Enabled	Role for performing administrative tasks for an organization. Has full access to all licensed services.
Application Integration Business Manager	Nov 8, 2018, 1:29 PM	Enabled	Role used for business managers
Application Integration Data Viewer	Nov 8, 2018, 1:29 PM	Enabled	Role used for granting access for data
Data Integration Data Previewer	Jan 22, 2019, 5:54 PM	Enabled	Role to preview data
Data Integration Task Executor	Dec 17, 2018, 12:19 PM	Enabled	Role to run Data Integration tasks
Deployer	Nov 8, 2018, 1:29 PM	Enabled	Role used by deployer
Designer	Dec 28, 2018, 11:42 AM	Enabled	Role for creating assets, tasks, and processes. Can configure connections, schedules, and runtime environ...
Monitor	Nov 8, 2018, 12:19 PM	Enabled	Role used for application monitor
Operator	Nov 8, 2018, 1:29 PM	Enabled	Role used for monitoring execution environments
Reporter	Mar 23, 2018, 5:31 PM	Enabled	Role that defines privileges for the reporting team.
Service Consumer	Jan 31, 2019, 2:29 PM	Enabled	Role for running tasks, workflows, and processes.



[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できます。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できます。

[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。

Reporter

Save

Set the privileges for users and groups assigned to the role. Configure privileges separately for each service.

Role Information

Role Name: \* Reporter

Description: Role that defines privileges for the reporting team.

Services: Data Integration

Assets Features

Asset Type	Create	Read	Update	Delete	Run	Set Permission
Business Service Definition	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cloud Content	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Connection	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Masking Task	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fixed-Width File Format	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Folder	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hierarchical Schema	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Intelligent Structure Task	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Linear Taskflow	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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、ロール名を変更できます。

### 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できます。

### 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できます。

### 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できますが、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。

特権がアセットタイプに適用されていない場合、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できます。

### 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できますが、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できます。

アセットと機能特権の詳細については、[「ロールアセットと機能特権」 \(ページ 65\)](#)を参照してください。

## 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へのアクセス権がない場合、アプリケーション統合ビジネスマネージャ、またはアプリケーション統合データビューア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ができません。

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

クロスサービスロールにより、複数のサービスにまたがるアクセス特権を定義します。例えば、デプロイヤーロールを持つユーザーは、API センター、API マネージャ、アプリケーションの統合、アプリケーション統合コンソール、Data Quality、およびデータ取り込みおよびレプリケーションの一部の機能にアクセスできます。

### サービス固有のロール

サービス固有のロールにより、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。例えば、ガバナンスユーザーロールを持つユーザーはデータガバナンス&カタログにアクセスすることはできますが、追加のロールの割り当てがない限り、他のサービスにはアクセスできません。

**注:** システム定義のロール「データローダー管理者」はいずれのユーザーにも割り当てないようにしてください。このロールは、Informatica Data Loader のみで使用されます。

## 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。

次の表に、クロスサービスロールに関する説明を示します。

クロスサービスロール	アクセス権を付与する対象のサービス。	説明
管理者	すべてのサービス	<p>組織管理者のロール。次のような例外を除き、ライセンスを取得したすべてのサービスへの完全なアクセス権を付与します。</p> <ul style="list-style-type: none"> <li>- 組織の顧客管理対象暗号化キーの使用を有効または無効にする特権が付与されることはありません。これらの特権を付与するには、ユーザーに管理者ロールとキー管理者ロールの両方を割り当てます。</li> <li>- すべての MDM サービスへの完全なアクセス権が付与されることはありません。例えば、ユーザーがワークフロー受信トレイにアクセスしたり、MDM ビジネスサービスで階層を作成したりすることはできません。MDM サービスへの完全なアクセス権を付与するには、ユーザーに適切な MDM サービス固有のロールを割り当てます。</li> </ul> <p><b>ヒント:</b> 1 人または 2 人の信頼されたユーザーに管理者ロールを割り当てて、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の割り当てを行うことがベストプラクティスとなります。これらのユーザーは組織の代替の管理者としての役割を果たし、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。</p>
データ統合データプレビュー	<ul style="list-style-type: none"> <li>- データ統合</li> <li>- データプロファイリング</li> <li>- Data Quality</li> <li>- データ検証</li> </ul>	<p>デザイナーがマッピング、タスク、プロファイル、およびテストケースを作成するときにデータをプレビューできるようにする補助的なロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データ統合でのマッピングまたはタスクのデータのプレビュー。</li> <li>- データ統合でのマッピングのデータ品質トランスフォーメーションのデータのプレビュー。</li> <li>- データプロファイリングでのプロファイルのソースオブジェクトデータとプロファイル結果の表示。</li> <li>- データ検証でのテストケースの作成時のデータのプレビュー。</li> </ul> <p><b>注:</b> これは補助的なロールです。ユーザーがデータ統合、データプロファイリング、およびデータ検証にアクセスできるようにするためには、デザイナーロールなどの別のロールとともにこのロールを割り当てます。</p>
データ統合	<ul style="list-style-type: none"> <li>- データ統合</li> <li>- データアクセス管理</li> </ul>	<p>タスクおよびタスクフローを実行し、データアクセスポリシーを実行するためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データ統合でのアセットおよびアセットの詳細の表示。</li> <li>- データ統合でのタスク、タスクフロー、およびテスト実行マッピングの実行。</li> <li>- データ統合でのユーザー自身のデータ統合ジョブおよびジョブの詳細の表示。</li> <li>- データ統合でのユーザー自身のジョブの開始と停止。</li> <li>- データ統合でのセッションログのダウンロード。</li> <li>- データ統合でのデータアクセスポリシーの実行。</li> <li>- データアクセス管理へのアクセス。</li> <li>- データアクセス管理でのデータアクセスポリシーの表示。</li> </ul>

クロスサービスロール	アクセス権を付与する対象のサービス。	説明
デブ ロイ ヤ	<ul style="list-style-type: none"> <li>- API センター</li> <li>- アプリケーションの統合</li> <li>- アプリケーション統合コンソール</li> <li>- データ取り込みおよびレプリケーション</li> <li>- Data Quality</li> <li>- データ検証</li> </ul>	<p>アセットとプロセスをデプロイするユーザーに対するロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- API センターでのアセットの表示とデプロイ、ポリシーの割り当て、組織設定の管理、OAuth 2.0 クライアントの追加（サービスコンシューマロールが割り当てられている場合）。</li> <li>- アプリケーションの統合でのアセットの詳細の表示。</li> <li>- アプリケーション統合コンソールでのアセットのデプロイ、設定の表示、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）のアップロードとデプロイ。</li> <li>- Data Quality でのディクショナリデータを除くアセットの詳細の表示。</li> <li>- データ取り込みおよびレプリケーションでのアプリケーション取り込み、データベース取り込み、およびストリーミング取り込みタスクの表示。</li> <li>- データ検証でのテストケース、テストスイート、およびレポートの表示。</li> <li>- データ検証でのテストケースとテストスイートの実行。</li> </ul>
デザ イナ	<ul style="list-style-type: none"> <li>- 管理者</li> <li>- API センター</li> <li>- アプリケーションの統合</li> <li>- アプリケーション統合コンソール</li> <li>- B2B Gateway</li> <li>- データ取り込みおよびレプリケーション</li> <li>- データ統合</li> <li>- データプロファイリング</li> <li>- Data Quality</li> <li>- データ検証</li> <li>- 統合ハブ</li> <li>- モニタ</li> </ul>	<p>アセット、タスク、およびプロセスを作成するユーザーに対するロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- アセット、タスク、プロセスの作成。CLAIRE Copilot を使用したアセットの作成および要約が含まれます。</li> <li>- 接続、スケジュール、およびランタイム環境の設定。</li> <li>- ジョブと詳細クラスタの監視（一括取り込み内の監視を除く）。</li> <li>- データ検証でのテストケースとテストスイートの表示、作成、および編集。</li> </ul> <p>アプリケーションの統合、B2B Gateway、データ統合、データプロファイリング、Data Quality、およびモニタへの完全なアクセス権を付与します。</p> <p>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は、API センターへの完全なアクセス権を付与します。</p> <p>管理者、API センター、アプリケーション統合コンソール、データ取り込みおよびレプリケーション、統合ハブ、およびデータ検証への部分的なアクセス権を付与します。</p>

クロスサービスロール	アクセス権を付与する対象のサービス。	説明
モニタ	<ul style="list-style-type: none"> <li>- 管理者</li> <li>- API センター</li> <li>- アプリケーションの統合</li> <li>- アプリケーション統合コンソール</li> <li>- B2B Gateway</li> <li>- データ取り込みおよびレプリケーション</li> <li>- データ統合</li> <li>- データプロファイリング</li> <li>- Data Quality</li> <li>- 統合ハブ</li> <li>- モニタ</li> </ul>	<p>ジョブを監視するユーザーに対するロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- API センターアセット、データ統合ジョブ、Data Quality アセット、統合ハブアセット、データ取り込みおよびレプリケーションジョブ、およびアプリケーションの統合プロセスインスタンスの監視。</li> <li>- 管理者での Secure Agent サービスのスケジュールとアップグレード設定の表示。</li> <li>- 管理者でのファイルサーバーの起動と停止、プロキシサーバーの設定、ファイルサーバーの設定の表示。</li> <li>- アプリケーションの統合、B2B Gateway、データ統合、データプロファイリング、および統合ハブでのアセットの詳細の表示。</li> <li>- Data Quality でのディクショナリデータを除くアセットの詳細の表示。</li> <li>- CLAIRE Copilot を使用してアセットを要約します。</li> <li>- アプリケーション統合コンソールでの設定の表示。</li> <li>- API センターでの API 呼び出しログの表示。</li> <li>- データ取り込みおよびレプリケーションでのアプリケーション取り込み、データベース取り込み、およびストリーミング取り込みジョブとジョブの詳細の表示。</li> <li>- モニタでのデータ統合とジョブの詳細の表示。</li> </ul>
オペレータ	<ul style="list-style-type: none"> <li>- アプリケーションの統合</li> <li>- アプリケーション統合コンソール</li> <li>- データプロファイリング</li> <li>- Data Quality</li> <li>- オペレーションインサイト</li> </ul>	<p>プロセスを管理するユーザーに対するロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- アプリケーションの統合およびデータプロファイリングでのアセットの詳細の表示。</li> <li>- アプリケーションの統合でのプロセスインスタンスの管理、一部の運用サーバーのパラメータの変更。</li> <li>- アプリケーション統合コンソールでのプロセスサーバー設定と一部のクラウドサーバー設定の表示と編集。</li> <li>- Data Quality でのディクショナリデータを除くアセットの詳細の表示。</li> <li>- オペレーションインサイトでのクラウドおよびドメインインフラストラクチャと Secure Agent のアラート設定の表示。</li> </ul>
サービスコンシューマ	<ul style="list-style-type: none"> <li>- 管理者</li> <li>- API Portal</li> <li>- アプリケーションの統合</li> <li>- データ統合</li> <li>- Data Quality</li> </ul>	<p>タスクとプロセスを実行するユーザーに対するロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- 管理者での、スケジュール、Swagger ファイル、Secure Agent サービスの設定のアップグレード、ファイルサーバーの起動と停止、プロキシサーバーの設定、その他のファイルサーバー設定の表示。</li> <li>- API Portal を開く。</li> <li>- アプリケーションの統合でのプロセスの呼び出し。</li> <li>- データ統合でのタスクの表示、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。</li> <li>- Data Quality でのディクショナリデータを除くアセットの詳細の表示。</li> </ul> <p>API Portal への完全なアクセス権を付与します。</p>

## 管理者ロール

管理者サービスへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、管理者へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	組織の顧客管理対象暗号化キーの使用を有効または無効にする特権を除く、管理者への完全なアクセス権を付与します。この権限を許可するには、ユーザーに管理者ロールとキー管理者ロールの両方を割り当てます。
デザイナー*	ユーザーが管理者で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 接続、ランタイム環境、スケジュール、Swagger ファイル、および詳細設定項目の設定。</li><li>- アドオンコネクタのインストール、およびアドオンバンドルのインストールとアンインストール。</li><li>- Secure Agent サービスのアップグレード設定の表示。</li><li>- ファイルサーバーの起動と停止、プロキシサーバーの設定、および他のファイルサーバー設定の表示。</li></ul>
エラスティック RTE Dev Ops エンジニア	ユーザーがエラスティックランタイム環境を管理できるようにします。ユーザーは次のタスクを実行できます。 <ul style="list-style-type: none"><li>- エラスティックランタイム環境をデプロイする。</li><li>- Informatica のアーティファクトリからエラスティックランタイム環境イメージに関する情報を取得する。</li><li>- イメージのプルに必要なトークンに対して操作を実行する。</li></ul>
キー管理者	ユーザーが、 <b>[設定]</b> ページの <b>[セキュリティ]</b> タブで、組織の顧客管理対象暗号化キーの使用を有効または無効にすることができますようにします。このロールを、管理者ロールも持つユーザーに割り当てます。ユーザーにどちらのロールもない場合、 <b>[セキュリティ]</b> タブは表示されません。  顧客管理対象暗号化キーの詳細については、「 <i>組織の管理</i> 」を参照してください。
モニタ*	ユーザーが管理者で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 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の表示。</li><li>- ファイルサーバーの起動と停止、プロキシサーバーの設定、および他のファイルサーバー設定の表示。</li></ul>
サービスコンシューマ*	ユーザーが管理者で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 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の表示。</li><li>- ファイルサーバーの起動と停止、プロキシサーバーの設定、および他のファイルサーバー設定の表示。</li></ul>
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## API センターのロール

API センターへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、API センターへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	API センターへの完全なアクセス権を付与します。
API ポリシーマネージャ	ユーザーがポリシーを定義できるようにします。ユーザーが API センターの次のようなページにアクセスできるようにします。 <ul style="list-style-type: none"><li>- エクスプローラ（読み取り専用）</li><li>- ポリシー</li></ul>
デプロイヤー*	サービスコンシューマロールが割り当てられている場合、ユーザーは API センターでアセットの表示とデプロイ、ポリシーの割り当て、組織設定の管理、OAuth 2.0 クライアントの追加を行うことができます。ユーザーが次のようなページにアクセスできるようにします。 <ul style="list-style-type: none"><li>- エクスプローラ（読み取り専用）</li><li>- API コンソール</li><li>- 設定</li></ul> <b>注:</b> これらの特権を付与するには、デプロイヤー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る必要があります。
デザイナー*	サービスコンシューマロールが割り当てられている場合は、すべてのアセット特権への完全なアクセス権が付与され、ユーザーは API センターでポリシーを割り当てることができます。ユーザーが次のようなページにアクセスできるようにします。 <ul style="list-style-type: none"><li>- 新しいアセット</li><li>- エクスプローラ</li></ul> <b>注:</b> これらの特権を付与するには、デザイナー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る必要があります。
モニタ*	ユーザーが API センターアセットを監視できるようにします。ユーザーが次のようなページにアクセスできるようにします。 <ul style="list-style-type: none"><li>- エクスプローラ（読み取り専用）</li><li>- API モニタ</li></ul>
サービスコンシューマ*	デザイナーまたはデプロイヤーロールも割り当てられている場合に、ユーザーが API センターにアクセスできるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」（ <a href="#">ページ 43</a> ）を参照してください。	

API センターのロールの詳細については、API センターのヘルプを参照してください。

## API マネージャのロール

API マネージャへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、API マネージャへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	API マネージャへの完全なアクセス権を付与します。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」(ページ 43)を参照してください。	

API マネージャへのさまざまなレベルのアクセス権を付与するには、カスタムロールを作成します。詳細については、API マネージャのヘルプを参照してください。

## API Portal のロール

API Portal へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、API Portal へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	API Portal への完全なアクセス権を付与します。
サービスコンシューマ*	ユーザーが API Portal を開くことができるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」(ページ 43)を参照してください。	



## 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ロール

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へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、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へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	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への完全なアクセス権を付与します。実行特権を持ちます。
アプリケーション統合ビジネスマネージャ	ビジネス活動を監視するためのロール。このロールを持つユーザーは、アセットおよびプロセスインスタンスに関する情報を表示できますが、変更することはできません。 ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アプリケーションの統合でのフォルダとアセットのリストとアセットの詳細の表示。</li><li>- アプリケーション統合コンソールの [プロセス]、[API]、および [接続] ページへのアクセス。</li></ul>
アプリケーション統合データビューア	ユーザーが、アプリケーション統合コンソールで詳細なログを表示できるようにするための補足的なロール。このロールは、他の 1 つ以上のロールとともに割り当てます。例えば、デザイナー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できるようにする場合は、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ー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。 <b>注:</b> ログレベルが [詳細] に設定されている場合、ユーザーはアーティファクトの詳細なログを表示できます。
デプロイヤー*	ユーザーが、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で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アプリケーションの統合でのアセットの詳細の表示。</li><li>- アプリケーション統合コンソールの [プロセス]、[ログ]、[サーバー設定]、[デプロイ済みアセット]、および [リソース] ページでのアセットのデプロイと設定の表示。</li><li>- 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) の、アプリケーション統合コンソールでのアップロードとデプロイ。</li></ul> 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ます。
デザイナー*	アプリケーションの統合への完全なアクセス権を付与します。 ユーザーが、アプリケーション統合コンソールの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るようにします。
モニタ*	ユーザーが、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で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アプリケーションの統合でのアセットの詳細の表示。</li><li>- アプリケーション統合コンソールでの設定の表示。</li></ul>
オペレータ*	ユーザーが、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で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アプリケーションの統合でのアセットの詳細の表示。</li><li>- アプリケーション統合コンソールでのプロセスサーバー設定と一部のクラウドサーバー設定の表示と編集。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、テナントの詳細を表示することはできません。</li></ul>

ロール	説明
サービスコンシューマ*	ユーザーが、API を介してアプリケーションの統合を実行できるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## B2B Gateway のロール

B2B Gateway へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、B2B Gateway へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	B2B Gateway への完全なアクセス権を付与します。
デザイナー*	B2B Gateway への完全なアクセス権を付与します。
モニタ*	ユーザーがアセットの詳細を表示できるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## B2B パートナーポータルロール

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。

**注:** B2B パートナーポータルの外部取引パートナーには、システム定義のロールはありません。したがって、それらのパートナーにはカスタムロールを作成する必要があります。

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思われる名前を付けます。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思われる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 64) 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。

## Business 360 コンソールのロール

Business 360 コンソールへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、Business 360 コンソールへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	Business 360 コンソールへの完全なアクセス権を付与します。ユーザーがソリューションのアップグレードを実行できるようにします。 <b>注:</b> Business 360 コンソールへの完全なアクセス権を付与するには、ユーザーに、管理者、デザイナー、および MDM デザイナーのユーザーロールを割り当てます。ユーザーが Business 360 コンソールで設定タスクのみを実行できるようにするには、ユーザーに、管理者ロール、またはデザイナーと MDM デザイナーの両方のロールを割り当てます。
Business 360 プロセス実行者	カスタムユーザーロールを持つユーザーが Business 360 コンソールおよびビジネスアプリケーションでタスクを実行するために必要なロール。ユーザーが、Business 360 コンソールでビジネスエンティティを更新できるようにします。 ユーザーがビジネスアプリケーションで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- レコードとカスタムレポートの保存。</li><li>- 階層の表示、作成、更新、削除。</li><li>- レコード、関連レコード、および階層データのインポート。</li><li>- [ワークフロー受信ボックス] ページへのアクセス。</li></ul>
デザイナー*	ユーザーが、データ統合や Data Quality などの他のサービスとの統合を必要とするタスクを Business 360 コンソールで実行できるようにします。 ユーザーが Business 360 コンソールで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 参照データアセットを除く MDM SaaS アセットの作成。</li><li>- データモデルとソースシステムの定義。</li><li>- 受信や送信などのジョブの定義と監視。</li><li>- データ品質、照合とマージ、存続性、ビジネスイベント、およびグローバル設定項目の設定。</li></ul> ユーザーが参照データアセットを定義することはできません。
ジョブ実行者	ユーザーが、Business 360 コンソールで受信ジョブと送信ジョブを実行できるようにします。 <b>注:</b> このロールは、ユーザーがファイルのインポートなどのタスクを実行するときにビジネスアプリケーションが実行するジョブを実行する場合には必要ありません。
MDM デザイナー	ユーザーが Business 360 コンソールで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- MDM SaaS アセットの作成。</li><li>- データモデルとソースシステムの定義。</li><li>- 受信や送信などのジョブの定義と監視。</li><li>- データ品質、照合とマージ、存続性、ビジネスイベント、およびグローバル設定項目の設定。</li><li>- アセットのエクスポートおよびインポート（ユーザーにデザイナーロールもある場合）。</li></ul>
* 複数のサービスへのアクセス権が付与されます。詳細については、 <a href="#">「クロスサービスロール」</a> （ページ 43）を参照してください。	

Business 360 コンソールのロールの詳細については、Business 360 コンソールのヘルプを参照してください。

## CLAIRE GPT ロール

CLAIRE GPT へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、CLAIRE GPT へのアクセス権を提供するシステム定義のユーザーロールとその説明を示します。

ロール	説明
CLAIRE GPT ユーザー	CLAIRE GPT のすべての機能への完全なアクセス権を提供します。

CLAIRE GPT ユーザーロールの詳細については、「CLAIRE GPT のヘルプ」を参照してください。

## PowerCenter 用クラウドデータ統合（CDI-PC）のロール

CDI-PC サービスへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、CDI-PC へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
ドメイン管理	CDI-PC への完全なアクセス権を付与します。

## Customer 360 SaaS のロール

MDM - Customer 360 SaaS へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、MDM - Customer 360 SaaS へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
Customer 360 アナリスト	レコードを作成するためのロール。ユーザーが、MDM - Customer 360 SaaS でレコードを作成、編集、および削除できるようにします。 Customer 360 アナリストがレコードを作成または編集するとこの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 データスチュワード	レコードと階層を作成するためのロール。ユーザーが、Customer 360 SaaS で次のようなタスクを含む任意のタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 承認なしでのレコードの作成、編集、および削除。</li><li>- ジョブの実行。</li><li>- 顧客レコードの確認と承認。</li></ul>
Customer 360 マネージャ	レコードを管理するためのロール。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 顧客レコードの確認と承認または却下。</li><li>- 承認なしでのレコードの作成、編集、および削除。</li></ul>
MDM ビジネスユーザー	ユーザーが、Customer 360 SaaS 内のレコードを表示できるようにします（作成または編集はできません）。

Customer 360 SaaS のロールの詳細については、MDM - Customer 360 SaaS のヘルプを参照してください。

## データガバナンス&カタログのロール

データガバナンス&カタログへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、データガバナンス&カタログへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者	データガバナンス&カタログでアセットをエクスポートするためのロール。
データアクセス所有者	データアクセス管理ページでデータアクセスアセットを表示および管理するロール。
ガバナンス管理者*	データガバナンス&カタログおよびメタデータコマンドセンターでアセットを管理するためのロール。ユーザーがデータガバナンス&カタログで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アセットのエクスポートとインポート。</li><li>- 変更の承認への参加。</li><li>- データアクセス管理ページの表示。</li><li>- データ品質ルールオカレンスに対して失敗した行の最新のプレビューの表示。</li></ul>
ガバナンス所有者*	データガバナンス&カタログでアセットを管理するためのロール。ユーザーがデータガバナンス&カタログで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アセットのエクスポートとインポート。</li><li>- 変更の承認への参加。</li><li>- データ品質ルールオカレンスに対して失敗した行の最新のプレビューの表示。</li></ul>
ガバナンスユーザー*	データガバナンス&カタログでアセットをエクスポートするためのロール。ユーザーがデータガバナンス&カタログでアセットをエクスポートできるようにします。また、ユーザーがデータアクセス管理ページを表示できるようにもします。
<p>*データマーケットプレイスおよびメタデータコマンドセンターへのアクセスも提供します。詳細については、「<a href="#">データマーケットプレイスのロール</a>」(ページ 55)および「<a href="#">メタデータコマンドセンターのロール</a>」(ページ 60)を参照してください。</p> <p>カタログ化およびガバナンスのタスクを実行するには、管理者がメタデータコマンドセンターでアクセスポリシーを作成し、これらのユーザーロールに割り当てる必要があります。詳細については、メタデータコマンドセンターのヘルプの「管理」を参照してください。</p>	

データガバナンス&カタログのロールの詳細については、データガバナンス&カタログのヘルプを参照してください。

## データ取り込みおよびレプリケーションロール

データ取り込みおよびレプリケーションへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、データ取り込みおよびレプリケーションへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	データ取り込みおよびレプリケーションへの完全なアクセス権を付与します。
デプロイヤー*	ユーザーが、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るようにします。
デザイナー*	ユーザーが、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、および設定できるようにします。また、ユーザーが <i>CLAIRE Copilot</i> を使用してアセットを作成および要約できるようにします。
モニタ*	ユーザーが、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るようにします。また、ユーザーが <i>CLAIRE Copilot</i> を使用してアセットを要約できるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 ( <a href="#">ページ 43</a> ) を参照してください。	

## データ統合ロール

データ統合へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、データ統合へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	データ統合への完全なアクセス権を付与します。
データ統合プレビューア*	ユーザーがデータ統合で次のようなタスクを実行できるようにする補足的なロール。 <ul style="list-style-type: none"><li>- 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の選択時のデータのプレビュー。</li><li>- マッピングで選択したデータ品質トランスフォーメーション実行時のデータのプレビュー。</li></ul> ユーザーがデータ統合にアクセスできるようにするためには、このロールをデザイナーロールなどの別のロールとともに割り当てます。
データ統合タスク実行者*	タスクとタスクフローを実行するためのロール。ユーザーがデータ統合で次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- アセットとアセットの詳細の表示。</li><li>- タスクとタスクフローの実行と、マッピングのテスト実行。</li><li>- ユーザー自身のデータ統合ジョブとジョブの詳細の表示。</li><li>- ユーザー自身のジョブの開始と停止。</li><li>- セッションログのダウンロード。</li></ul>
デザイナー*	データ統合への完全なアクセス権を付与します。

ロール	説明
モニタ*	ユーザーが、データ統合でアセットの詳細を表示できるようにします。また、ユーザーが CLAIRe Copilot を使用してアセットを要約できるようにします。
サービスコンシューマ*	ユーザーが、データ統合でタスクの表示、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ようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」(ページ 43)を参照してください。	

## データマーケットプレイスのロール

データマーケットプレイスへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。システム定義のロールをデータマーケットプレイスユーザーに割り当てることができます。

次の表に、データマーケットプレイスへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
Data Marketplace 管理者	管理タスクを実行するためのロール。データマーケットプレイスへの完全なアクセス権を付与します。
Data Marketplace カテゴリ所有者	<p>カテゴリに対する権限を持つユーザーのためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- ユーザーのカテゴリ内でのデータコレクションの作成および一括作成。</li> <li>- ユーザーのカテゴリ内でのデータコレクションのデータアセットの追加と削除。</li> <li>- データコレクションのためのデータオーダーの承認と却下。</li> <li>- ユーザーが担当するカテゴリに関するデータコレクション要求の承認または却下。</li> <li>- データ内の配信ターゲットのユーザーカテゴリ内のコレクションへの追加と編集。</li> <li>- ユーザーカテゴリ内のデータコレクションへのバリエーションのリンクと削除。</li> <li>- ユーザーカテゴリ内のデータコレクションの削除。</li> <li>- ユーザーがアクセス可能なコンテキストと照らし合わせた、ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- パブリッシュされたデータコレクションの検索。</li> <li>- コレクションの比較。</li> <li>- データコレクションへのデータアセットの追加および一括追加。</li> <li>- オーダーの作成と、データコレクション要求の発行。</li> <li>- カテゴリの作成、一括作成、変更、および削除。</li> <li>- ユーザーカテゴリ内のデータコレクションの利用規約の追加と削除。</li> <li>- 公開ディスカッションチャンネルへの参加。</li> <li>- ユーザーがアクセス可能なプライベートチャンネルへのコメント。</li> </ul>



ロール	説明
Data Marketplace データコレクションオーナー	<p>データコレクションに対する権限を持つユーザーのためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データコレクションの作成、一括作成、変更、および削除。</li> <li>- ユーザーが所有するデータコレクションの表示。</li> <li>- ユーザーが所有するデータコレクションへの利用規約とデータアセットの追加および一括追加。</li> <li>- ユーザーが所有するデータコレクションからの利用規約とデータアセットの削除。</li> <li>- パブリッシュされたデータコレクションの検索。</li> <li>- コレクションの比較。</li> <li>- ユーザーが所有するデータコレクション内の配信ターゲットの追加と編集。</li> <li>- ユーザーがアクセス可能なコンテキストと照らし合わせた、ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- コレクションに対するオーダーの作成と、コレクションまたはカテゴリに対するデータコレクション要求の発行。</li> <li>- ユーザーが所有するデータコレクションに対して発生したデータコレクション要求の完了と却下。</li> <li>- データコレクションアクセス要求の承認と却下。</li> <li>- バリエーションのリンク。</li> <li>- 公開ディスカッションチャンネルへの参加。</li> <li>- ユーザーがアクセス可能なプライベートチャンネルへのコメント。</li> </ul>
Data Marketplace データコレクションテクニカルオーナー	<p>データコレクションに対する技術的な権限を持つユーザーのためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データコレクションのオーダーの表示。</li> <li>- データコレクションへの配信ターゲットの追加と編集。</li> <li>- 取り消しの要求と、データコレクションへのアクセスの取り消し。</li> <li>- データコレクション内のデータアセットおよび利用規約の追加と削除。</li> <li>- ユーザーがアクセス可能なコンテキストと照らし合わせた、ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- パブリッシュされたデータコレクションの検索。</li> <li>- コレクションの比較。</li> <li>- コレクションに対するオーダーの作成と、コレクションおよびカテゴリに対するデータコレクション要求の発行。</li> <li>- 「利用規約 - データコレクション」リレーションおよび「配信ターゲット - データコレクション」リレーションの一括作成。</li> <li>- データ利用者がオーダーしたデータの配信。</li> <li>- 公開ディスカッションチャンネルへの参加。</li> <li>- ユーザーがアクセス可能なプライベートチャンネルへのコメント。</li> </ul>
Data Marketplace 配信オーナー	<p>データコレクションを配信するための配信オプションを管理するためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データコレクションの検索と比較。</li> <li>- ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- 配信オプションと配信ターゲットの作成。</li> <li>- 配信形式、配信方法、配信テンプレート、「配信ターゲット - データコレクション」リレーションの一括作成。</li> <li>- コンシューマアクセスの取り消しの要求、コンシューマアクセスの取り消し、ユーザーが責任を負う配信オプションを持つデータコレクションのデータオーダーの履行。</li> <li>- ユーザーがアクセス可能なパブリックおよびプライベートのディスカッションチャンネルへの参加。</li> </ul>



ロール	説明
Data Marketplace テクニカル管理者	<p>技術的な管理タスクを実行するためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データオーダーの表示、データコレクションへの配信ターゲットの追加。</li> <li>- データユーザーへの要求されたデータコレクションの配信。</li> <li>- データコレクションの検索と比較。</li> <li>- ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- データアセット、配信ターゲット、および利用規約のデータコレクションへの追加。</li> <li>- データ要素、データアセット、およびコンシューマアクセスの一括作成。</li> <li>- データ要素とデータアセットの削除。</li> <li>- オブジェクトのラベルの変更。</li> <li>- データ配信の形式と方法の設定。</li> <li>- データを配信するためのデフォルトの配信ターゲットの設定。</li> <li>- データガバナンス&amp;カタログからのアセットのインポート。</li> <li>- 一般的な「利用規約」メッセージの設定と、新しい利用規約の作成。</li> <li>- コストセンターの作成。</li> <li>- 取り消しの要求と、コンシューマアクセスの取り消し。</li> <li>- コストセンター、配信形式、配信方法、配信テンプレート、「利用規約 - データコレクション」リレーション、「配信ターゲット - データコレクション」リレーションの一括作成。</li> <li>- スター付き所有者の設定。</li> <li>- ユーザーがアクセス可能なパブリックおよびプライベートのディスカッションチャンネルへの参加。</li> <li>- データマーケットプレイスユーザーインターフェースのカスタマイズ。</li> </ul>
Data Marketplace ユーザー	<p>データコレクションを使用するためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データコレクションの並べ替えと比較。</li> <li>- パブリッシュされたデータコレクションの検索。</li> <li>- 要求および配信されたデータコレクションの表示。</li> <li>- データコレクションの詳細の表示。</li> <li>- ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- コレクションおよびカテゴリに関するデータコレクション要求の作成とキャンセル。</li> <li>- パブリックおよびプライベートのディスカッションチャンネルへの参加。</li> </ul>
ガバナンス管理者	<p>データコレクションを使用するためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データコレクションの並べ替えと比較。</li> <li>- パブリッシュされたデータコレクションの検索。</li> <li>- 要求および配信されたデータコレクションの表示。</li> <li>- データコレクションの詳細の表示。</li> <li>- ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- コレクションおよびカテゴリに関するデータコレクション要求の作成とキャンセル。</li> <li>- パブリックおよびプライベートのディスカッションチャンネルへの参加。</li> </ul>
ガバナンスユーザー	<p>データコレクションを使用するためのロール。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- データコレクションの並べ替えと比較。</li> <li>- パブリッシュされたデータコレクションの検索。</li> <li>- 要求および配信されたデータコレクションの表示。</li> <li>- データコレクションの詳細の表示。</li> <li>- ユーザーがアクセス可能なデータコレクションの評価。</li> <li>- コレクションおよびカテゴリに関するデータコレクション要求の作成とキャンセル。</li> <li>- パブリックおよびプライベートのディスカッションチャンネルへの参加。</li> </ul>

データマーケットプレイスのロールの詳細については、データマーケットプレイスのヘルプを参照してください。

## データプロファイリングロール

データプロファイリングへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、データプロファイリングへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	データプロファイリングへの完全なアクセス権を付与します。
データ統合プレビューア*	ユーザーが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表示するときに、ソースオブジェクトデータをプレビューできるようにする補足的なロール。 ユーザーが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は、このロールをデザイナーロールなどの別のロールとともに割り当てます。
デザイナー*	データプロファイリングへの完全なアクセス権を付与します。
モニタ*	ユーザーが、データプロファイリングでアセットの詳細を表示できるようにします。
オペレータ*	ユーザーが、データプロファイリングでアセットの詳細を表示できるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## データ品質のロール

Data Quality へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、Data Quality へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	Data Quality への完全なアクセス権を付与します。
デプロイヤー*	ユーザーが、Data Quality のディクショナリデータを除くアセットの詳細を表示できるようにします。
デザイナー*	Data Quality への完全なアクセス権を付与します。
モニタ*	ユーザーが、Data Quality のディクショナリデータを除くアセットの詳細を表示できるようにします。
オペレータ*	ユーザーが、Data Quality のディクショナリデータを除くアセットの詳細を表示できるようにします。

ロール	説明
サービスコンシューマ*	ユーザーが、Data Quality のディクショナリデータを除くアセットの詳細を表示できるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## 統合ハブのロール

Cloud 統合ハブへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、Cloud 統合ハブへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	Cloud 統合ハブへの完全なアクセス権を付与します。
デザイナー*	ユーザーが、Cloud 統合ハブアセットを作成、表示、編集、削除、および実行できるようにします。 プロビジョニングの実行、システムプロパティの設定、または Cloud 統合ハブアセットの権限の設定を行う特権が付与されることはありません。
モニタ*	ユーザーが、Cloud 統合ハブでアセットの詳細を表示できるようにします。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

Cloud 統合ハブのロールの詳細については、Cloud 統合ハブのヘルプを参照してください。

## メタデータコマンドセンターのロール

メタデータコマンドセンターへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールまたはカスタムロールを割り当てることができます。

次の表に、メタデータコマンドセンターへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	メタデータコマンドセンターでアップグレードを実行し、カタログソース設定を更新するためのロール。メタデータコマンドセンターでタスクを実行するには、ガバナンス管理者ロールを使用することをお勧めします。
ガバナンス管理者**	データガバナンス&カタログおよびメタデータコマンドセンターでアセットと操作を管理するためのロール。ユーザーがメタデータコマンドセンターで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- カatalogソース設定に対する権限の実行と設定。</li><li>- メタデータアクセス制御、アセットグループ、アセットページのカスタマイズ、カスタム属性、データ分類、IDMC メタデータ設定、リネージュ設定、参照データ、システム設定、およびワークフロー設定を管理します。</li><li>- ジョブの監視。</li><li>- アクセス制御、アセットグループ、アセットページのカスタマイズ、カスタム属性、データ分類、IDMC メタデータ設定、リネージュ設定、参照データ、システム設定、およびワークフロー設定を表示します。</li></ul>
<p>* 複数のサービスへのアクセス権が付与されます。詳細については、「<a href="#">クロスサービスロール</a>」 (<a href="#">ページ 43</a>)を参照してください。</p> <p>** データアクセス管理、データガバナンス&amp;カタログ、およびデータマーケットプレイスへのアクセスも提供します。詳細については、「<a href="#">データガバナンス&amp;カタログのロール</a>」 (<a href="#">ページ 53</a>)を参照してください。</p> <p>カタログ化およびガバナンスのタスクを実行するには、管理者がメタデータコマンドセンターでアクセスポリシーを作成し、これらのユーザーロールに割り当てる必要があります。詳細については、メタデータコマンドセンターのヘルプの「管理」を参照してください。</p>	

メタデータコマンドセンターのロールの詳細については、メタデータコマンドセンターのヘルプを参照してください。

## モニタロール

モニタへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、モニタへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	モニタへの完全なアクセス権を付与します。
デザイナー*	モニタへの完全なアクセス権を付与します。

ロール	説明
モニタ*	ユーザーが、モニタでデータ統合ジョブとジョブの詳細を表示できるようにします。 ユーザーがエクスポートジョブまたはインポートジョブを表示することはできません。
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## オペレーションインサイトロール

オペレーションインサイトへのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、オペレーションインサイトへのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
管理者*	オペレーションインサイトへの完全なアクセス権を付与します。
オペレータ*	ユーザーがオペレーションインサイトで次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"> <li>- クラウドとドメインのインフラストラクチャの表示。</li> <li>- Secure Agent のアラート設定の表示。</li> </ul>
* 複数のサービスへのアクセス権が付与されます。詳細については、「 <a href="#">クロスサービスロール</a> 」 (ページ 43) を参照してください。	

## Product 360 SaaS のロール

MDM - Product 360 SaaS へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、MDM - Product 360 SaaS へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
Product 360 マネージャ	レコードを管理するためのロール。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"> <li>- レコードの確認と承認。</li> <li>- 承認なしでのレコードの作成、編集、および削除。</li> </ul>
Product 360 読み取り専用	レコードを表示するためのロール。ユーザーが、Product 360 SaaS 内のレコードを表示できるようにします（編集はできません）。

Product 360 SaaS のロールの詳細については、MDM - Product 360 SaaS のヘルプを参照してください。

## Reference 360 のロール

MDM - Reference 360 へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。システム定義のロールを Reference 360 ユーザーに割り当てることができます。

次の表に、MDM - Reference 360 へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
Reference360 管理者	Reference 360 のための管理ロール。ユーザーが、Reference 360 環境を設定できるようにします。
Reference 360 ビジネスアナリスト	アセットを分析するためのロール。ユーザーはアセットを表示および分析できますが、アセットに対する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	参照データに対する各分野のエキスパートのためのロール。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 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の作成と管理。</li><li>- 他のユーザーが提案した変更の承認。</li><li>- 承認のための独自の変更の送信と、承認なしでの変更の直接パブリッシュ。</li></ul>
Reference 360 プランナ	階層を作成および管理するためのロール。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 階層アセットの作成、階層モデルの定義、階層リレーションのインポート。</li><li>- 不要になった階層の削除。</li><li>- 階層の他のユーザーへのプランナステークホルダーロールの割り当て。</li></ul>
Reference 360 プライマリオーナー	参照データ構造を作成および定義するためのロール。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 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の作成と定義。</li><li>- コードリストの削除。</li><li>- コードリスト内のコード値の変更の提案。この変更についてはビジネススチュワードの承認を受ける必要があります。</li><li>- ステークホルダーロールを使用した、コードリストと参照データセットへのユーザーのアクセス権の割り当て。</li></ul>
Reference 360 ステークホルダー	コード値の変更を提案するためのロール。ユーザーが変更を提案できるようにします（提案された変更についてはビジネススチュワードの承認を受ける必要があります）。
Reference 360 ユーザー	制限付きのアクセスロール。デフォルトでは、このロールを持つユーザーはいずれのアセットにもアクセスできません。ユーザーがコードリストやクロスウォークなどの特定のアセットにアクセスできるようにするには、このロールをアセットのステークホルダーロールとともに割り当てます。

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

## Supplier 360 SaaS のロール

MDM - Supplier 360 SaaS へのアクセス権を付与するには、ユーザーに適切なロールを割り当てます。ユーザーには、システム定義のロールを割り当てるか、カスタムロールを作成することができます。

次の表に、MDM - Supplier 360 SaaS へのアクセス権を付与する、システム定義のロールに関する説明を示します。

ロール	説明
Supplier 360 アナリスト	レコードを分析するためのロール。ユーザーが、Supplier 360 SaaS でレコードを作成、読み取り、編集、および削除できるようにします。Supplier 360 アナリストがレコードを作成または編集すると、この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 商品マネージャ	商品の評価タスクを管理するためのロール。作成者特権と承認者特権を持ちます。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 商品評価タスクの要求と拒否。</li><li>- 承認ワークフローでの商品評価タスクの実行。</li><li>- レコードの作成、読み取り、編集、および削除。</li></ul>
Supplier 360 契約マネージャ	契約評価タスクを管理するためのロール。作成者特権と承認者特権を持ちます。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 契約評価タスクの要求と拒否。</li><li>- 承認ワークフローでの契約評価タスクへの対応。</li><li>- レコードの作成、読み取り、編集、および削除。</li></ul>
Supplier 360 クレジットマネージャ	信用評価タスクを管理するためのロール。作成者特権と承認者特権を持ちます。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 信用評価タスクの要求と拒否。</li><li>- 承認ワークフローでの信用評価タスクへの対応。</li><li>- レコードの作成、読み取り、編集、および削除。</li></ul>
Supplier 360 データスチュワード	レコードを管理するためのロール。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 承認の有無にかかわらず、レコードの作成、読み取り、編集、および削除。</li><li>- ジョブの実行。</li><li>- レコードの確認と承認。</li><li>- レコードの照合、マージ、およびマージ解除。</li></ul>
Supplier 360 読み取り専用	Supplier 360 SaaS のレコードを表示するためのロール。ユーザーがレコードを表示できるようにします（作成または編集はできません）。
Supplier 360 リスクマネージャ	リスク評価タスクを管理するためのロール。作成者特権と承認者特権を持ちます。ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- リスク評価タスクの要求と拒否。</li><li>- 承認ワークフローでのリスク評価タスクへの対応。</li><li>- レコードの作成、読み取り、編集、および削除。</li></ul>
Supplier 360 タスク管理者	評価タスクを管理するためのロール。作成者特権と承認者特権を持ちます。ユーザーが、拒否されたすべての評価タスクを表示できるようにします。

Supplier 360 SaaS のロールの詳細については、MDM - Supplier 360 SaaS のヘルプを参照してください。

# 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の設定ができて、データ統合タスクの作成、編集、または実行ができないカスタム管理ロールを作成したい場合などもあります。

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 によってカスタムロールに追加の特権が付与されることはありません。

**注:** ロールを作成、更新、または削除する特権をカスタムロールに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。

## ロールアセットと機能特権

すべてのロールは、一連のアセットまたは機能特権に関連付けられています。これらの特権により、ユーザーはアセットやサービス機能进行操作しながら特定の機能を実行できます。カスタムロールを作成するときに、アセットと機能特権を割り当てます。

アセット特権により、さまざまな種類のアセットに対する CRUD、実行、および権限の設定特権を付与します。例えば、マッピングの作成特権をロールに割り当てると、そのロールを持つユーザーはマッピングを作成、表示、および更新できるようになります。

次の表に、アセット特権に関する説明を示します。

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。 読み取り特権と更新特権が自動的に付与されます。
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。 読み取り特権が自動的に付与されます。
削除	選択したタイプのアセットを削除します。

特権	説明
実行	<p>選択したタイプのアセットを実行します。</p> <p>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できます。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、および再起動できます。</p> <p>Cloud 統合ハブサービスの場合、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できます。</p>
権限の設定	<p>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。</p> <p>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。</p>

機能特権により、サービスの特定の機能を使用する権限を制御します。例えば、Data Quality の「データレビュー - ディクショナリ」特権により、ユーザーはディクショナリの内容の表示が許可されます。

カスタムロールを作成するときに、ロールの詳細ページでアセットと機能特権を割り当てます。ロールの詳細ページの詳細については、[「ロールの詳細」 \(ページ 41\)](#)を参照してください。

システム定義のロールに関連付けられたアセットおよび機能特権を変更することはできません。

## 管理者のアセット特権と機能特権

管理者のアセット特権と機能特権を使用して、管理者での作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、アセットと機能特権を有効にすることができます。

### 管理者のアセット特権

次の表に、管理者のアセット特権を示します。

アセット特権	説明
接続	ユーザーが接続に対する権限を作成、読み取り、更新、削除、または設定できるようにします。
エラスティック構成	ユーザーが詳細設定を作成、読み取り、更新、削除、または実行できるようにします。
フォルダ	ユーザーがプロジェクトフォルダに対する権限を作成、読み取り、更新、削除、または設定できるようにします。
グループ	ユーザーがユーザーグループを作成、読み取り、更新、または削除できるようにします。
OAuth クライアント	<p>ユーザーが OAuth 2.0 クライアントを作成、読み取り、更新、または削除できるようにします。</p> <p>OAuth 2.0 クライアントの作成と管理の詳細については、API センターのヘルプを参照してください。</p>
組織	ユーザーが組織情報の読み取りおよび更新できるようにします。
特権	ユーザーが各ロールに関連付けられたアセット特権および機能特権を表示できるようにします。

アセット特権	説明
プロジェクト	ユーザーがプロジェクトに対する権限を作成、読み取り、更新、削除、または設定できるようにします。
ロール	ユーザーがユーザーのロールと Administrator の <b>【ユーザーロール】</b> ページを表示できるようにします。
スケジュール	ユーザーがプロジェクトスケジュールに対する権限を作成、読み取り、更新、削除、または設定できるようにします。
スケジューラブラックアウト	ユーザーがスケジュールブラックアウト期間を作成、読み取り、更新、または削除できるようにします。
スケジューラジョブ	ユーザーが、スケジュールに従ったアセットの実行、アセットのスケジュール情報の表示、アセットのスケジュールの更新、またはアセットからのスケジュールの削除を行うことができるようにします。
Secure Agent	ユーザーが Secure Agent に対する権限を作成、読み取り、更新、削除、または設定できるようにします。
Secure Agent グループ	ユーザーが Secure Agent グループに対する権限を作成、読み取り、更新、削除、または設定できるようにします。
ユーザー	ユーザーがユーザーアカウントを作成、読み取り、更新、および削除できるようにします。

## 管理者の機能特権

次の表に、管理者の機能特権を示します。

機能特権	説明
AdditionalOrg 作成特権	AdditionalOrg 表示特権も付与されている場合に、ユーザーが追加のプロダクション組織およびサンドボックス組織を作成できるようにします。
AdditionalOrg 表示特権	ユーザーがプロダクション組織から追加のプロダクション組織とサンドボックス組織を表示できるようにします。 この特権は、追加のプロダクション組織およびサンドボックス組織を作成するために必要です。
アセット - チェックイン/チェックアウト	ユーザーがソース管理リポジトリにアセットをチェックインおよびチェックアウトできるようにします。
アセット - エクスポート	ユーザーが組織からアセットをエクスポートできるようにします。
アセット - インポート	ユーザーが組織にアセットをインポートできるようにします。
アセット - プルバージョン	ユーザーがソース管理リポジトリからアセットをプルできるようにします。
アセット - ソース管理ログ	ユーザーがソース管理ログを表示できるようにします。
監査ログ - 表示	ユーザーが監査ログを表示できるようにします。
バンドル - 作成	「バンドル - 表示」特権も付与されている場合に、ユーザーがバンドルを作成できるようにします。

機能特権	説明
バンドル - 削除	「バンドル - 表示」特権も付与されている場合に、ユーザーがバンドルを削除できるようにします。
バンドル - インストール	「バンドル - 表示」特権も付与されている場合に、ユーザーがバンドルをインストールして組織で使用できるようにします。
バンドル - パブリッシュ	「バンドル - 表示」特権も付与されている場合に、ユーザーがバンドルをパブリッシュできるようにします。
バンドル - 更新	「バンドル - 表示」特権も付与されている場合に、ユーザーがバンドルを更新できるようにします。
バンドル - 表示	ユーザーがバンドルを表示できるようにします。 この特権は、バンドルの作成、削除、インストール、パブリッシュ、および更新に必要です。
カスタムリポジトリソース制御の設定	ソース制御の設定特権も付与されている場合に、ユーザーがプロジェクトレベルのソース管理リポジトリに対してプロジェクト固有のリポジトリ URL およびブランチ名を設定できるようにします。
ソース制御の設定	ユーザーがプロジェクト、フォルダ、およびアセットのバージョン管理を有効にするためのソース管理を設定できるようにします。
コネクタ - 表示	ユーザーが組織で利用可能なコネクタを表示し、Administrator で <b>【アドオンコネクタ】</b> ページを表示できるようにします。
チェックアウトの取り消しを強制	別のユーザーがチェックアウトしたオブジェクトのチェックアウトをユーザーが取り消すことができるようにします。
エラスティックランタイム環境 - イメージの取得	ユーザーが Informatica のアーティファクトリからエラスティックランタイム環境イメージに関する情報を取得する API を実行できるようにします。ユーザーは、エラスティックランタイム環境をデプロイするクラスティンストラスクリプトを実行するために、この権限を持っている必要があります。
エラスティックランタイム環境 - トークンの管理	ユーザーが Informatica のアーティファクトリからエラスティックランタイム環境イメージをプルするために必要なトークンに対して操作を実行できるようにします。ユーザーは、エラスティックランタイム環境をデプロイするクラスティンストラスクリプトを実行するために、この権限を持っている必要があります。
KMS ビュー管理対象キー	ユーザーが <b>【設定】</b> ページの <b>【セキュリティ】</b> タブで <b>【顧客管理対象キー】</b> 領域を表示できるようにします。
請求の管理	データ統合-PayGo のユーザーが自身の支払い情報を管理できるようにします。 データ統合-Free とデータ統合-PayGo の詳細については、 <a href="#">「Introducing Informatica Cloud Data Integration-Free and PayGo」</a> を参照してください。
キーのローテーション設定を管理	顧客がプラットフォーム REST API バージョン 3 キーリソースを通じて組織のキーローテーションを管理できるようにします。 v3 キーリソースの詳細は、『 <i>REST API リファレンス</i> 』を参照してください。
ユーザー通知の管理	管理者は、組織内のすべてのユーザーの通知設定を設定することができます。

機能特権	説明
ratecard.view	ユーザーが [メータリング] ページで組織の現在の料金表を表示できるようにします。
SMS 接続管理	ユーザーが組織のシークレットマネージャの使用を有効化または無効化したり、シークレットマネージャの設定を構成および更新したりできるようにします。
SMS 接続表示	ユーザーが [設定] ページの [セキュリティ] タブで [シークレット Vault] 領域を表示できるようにします。
サブ組織 - 作成	「サブ組織 - 表示」特権も付与されている場合に、ユーザーがサブ組織を作成できるようにします。
サブ組織 - 削除	「サブ組織 - 表示」特権も付与されている場合に、ユーザーがサブ組織を削除できるようにします。
サブ組織 - 更新	「サブ組織 - 表示」特権も付与されている場合に、ユーザーがサブ組織設定を編集できるようにします。
サブ組織 - リンク	「サブ組織 - 表示」特権も付与されている場合に、ユーザーがサブ組織をリンクできるようにします。
サブ組織 - ライセンスの管理	「サブ組織 - 表示」特権も付与されている場合に、ユーザーが組織のサブ組織のライセンスを管理できるようにします。
サブ組織 - リンク解除	「サブ組織 - 表示」特権も付与されている場合に、ユーザーが親組織からサブ組織のリンクを解除できるようにします。
組織 - 表示	ユーザーがサブ組織を表示し、親組織からサブ組織に切り替えることができます。 この特権は、サブ組織の作成、削除、更新、リンク、ライセンスの管理、およびリンク解除を行うために必要です。
SDI のアップグレード	ユーザーがデータ統合-Free の組織をデータ統合-PayGo 組織にアップグレードできるようにします。 データ統合-Free とデータ統合-PayGo の詳細については、 <a href="#">「Introducing Informatica Cloud Data Integration-Free and PayGo」</a> を参照してください。

## アプリケーションの統合機能特権

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に対するカスタムロールを作成するときに、アプリケーションの統合の機能特権を割り当てます。

**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。この操作を行うには、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 特権を選択します。

次の表に、アプリケーションの統合の機能特権に関する説明を示します。

機能特権	説明
管理	<p>ユーザーに、設計時と実行時における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への完全な管理アクセス権を付与します。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- サービスの管理と開始。</li> <li>- 実行中のサービスの停止。</li> <li>- デプロイされたプロセスのインスタンスとログの表示。</li> <li>- 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。</li> <li>- デプロイされたカタログの管理。</li> <li>- 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。</li> <li>- プロセスサーバーのメトリックの表示。</li> <li>- プロセス API をアクティブ化および非アクティブ化します。</li> <li>- リスナーベースの接続でイベントソースを表示、開始、および停止します。</li> </ul> <p><b>注:</b> この特権により、ユーザーに組織管理特権が付与されることはありません。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。</p>
コンソール管理	<p>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権を付与します。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- デプロイされたプロセスのインスタンスの表示。</li> <li>- 実行中のサービスの停止。</li> <li>- デプロイされたプロセス開発者 BPR とカタログの表示。</li> <li>- 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。</li> <li>- プロセスサーバーのメトリックの表示。</li> <li>- プロセス API をアクティブ化および非アクティブ化します。</li> <li>- リスナーベースの接続でイベントソースを表示、開始、および停止します。</li> </ul> <p>この特権では、ユーザーは BPR ファイルを展開できません。</p>
データビューア	<p>ユーザーがアプリケーション統合コンソールの詳細なログにアクセスできるようにします。</p> <p>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。通常は、開発者にこのロールを割り当てる必要はありません。</p> <p><b>注:</b> 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。</p>
開発	<p>ユーザーがプロセスをデバッグできるようにします。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- サービスの開始。</li> <li>- アプリケーション統合コンソールの [詳細プロセスインスタンス] ページの表示。</li> <li>- プロセスインスタンスの管理。</li> <li>- プロセス API をアクティブ化および非アクティブ化します。</li> <li>- リスナーベースの接続でイベントソースを表示、開始、および停止します。</li> </ul>
監視	<p>ユーザーが、詳細なログを除くアプリケーション統合コンソールのすべての部分を表示できるようにします。ユーザーが次のようなタスクを実行できるようにします。</p> <ul style="list-style-type: none"> <li>- プロセス API をアクティブ化および非アクティブ化します。</li> <li>- リスナーベースの接続でイベントソースを表示、開始、および停止します。</li> </ul>
アプリケーション統合アセットのパブリッシュ	<p>ユーザーが、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できるようにします。</p>

機能特権	説明
アプリケーション統合コンソールの表示	ユーザーに、アプリケーション統合コンソールへのアクセス権を付与します。 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、この特権に開発特権を割り当てます。
アプリケーション統合デザイナーの表示	ユーザーに、アプリケーションの統合へのアクセス権を付与します。 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、この特権に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。

## データガバナンス&カタログの機能特権

データガバナンス&カタログの機能特権を使用して、ユーザーがデータガバナンス&カタログの操作中に特定の機能にアクセスできるようにします。カスタムロールを作成するときに、この機能特権を有効にすることができます。

次の表に、データガバナンス&カタログの機能特権とその説明を示します。

特徴	説明
データガバナンス&カタログアプリケーションへのアクセス	データガバナンス&カタログへのアクセス権を付与する場合はこの機能を有効にします。 無効にすると、データガバナンス&カタログにアクセスしてガバナンスタスクを実行することはできなくなります。
エクスポート	ユーザーがデータガバナンス&カタログからアセットをエクスポートできるようにします。
強制削除	ユーザーに次の特権を付与します。 <ul style="list-style-type: none"> <li>- 受信リレーションを持つアセットを削除する</li> <li>- 階層内のすべての子アセットを含むアセットを一括インポートで削除する</li> </ul>
インポート	ユーザーが、事前定義されたテンプレートをダウンロードし、ビジネスアセットをデータガバナンス&カタログにインポートできるようにします。この特権を有効にした場合は、アセットをインポートするための次のアセット特権を追加でユーザーに付与する必要があります。 <ul style="list-style-type: none"> <li>- ビジネスアセット。作成特権と更新特権</li> <li>- テクニカルアセット。更新特権</li> </ul>
チケットの管理	ユーザーに次の特権を付与します。 <ul style="list-style-type: none"> <li>- アセットのステークホルダーにならずにチケットを解決またはキャンセルする。</li> <li>- アセットのステークホルダーにならずに手動チケットの通知を受け取る。</li> </ul>
ワークフロータスクの管理	ユーザーがワークフロータスクを管理できるようにします。
変更の承認への参加	ユーザーに次の特権を付与します。 <ul style="list-style-type: none"> <li>- データガバナンス&amp;カタログのワークフロー承認への参加。</li> </ul> <p>この特権を付与するロールは、ユーザーがワークフロータスクを作成または変更したときに、メタデータコマンドセンターの <b>【ロール】</b> に表示されます。</p> <ul style="list-style-type: none"> <li>- データガバナンス&amp;カタログのアセットへの関係者の追加。</li> <li>- メタデータコマンドセンターでのワークフローの設定。</li> </ul>



特徴	説明
データのプレビュー	ユーザーが、データガバナンス&カタログでデータ品質ルールオカレンスに対して失敗した行の最新のプレビューを表示できるようにします。
参考データの表示	ユーザーが【参照データ】タブで、ビジネス用語、メトリック、手動データ要素、およびデータ要素の参照データを表示できるようにします。

## データ取り込みおよびレプリケーションの最小アセットと機能特権

データ取り込みおよびレプリケーションデータベースのカスタムロールの作成時に、データ取り込みおよびレプリケーションデータベースのアセットと機能特権を割り当てます。

データベース取り込みとレプリケーションタスクを作成、表示、または編集するには、最低限必要な特権を含むユーザーロールを割り当てます。これらの特権を含む管理者やデザイナー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。

### 最低限のアセット特権

次の表に、最低限必要なアセット特権を示します。

サービス	アセットタイプ	アセット特権
データ取り込みおよびレプリケーション	データベース取り込みタスク	作成、読み取り、更新
管理者	接続	読み取り
管理者	Secure Agent グループ	読み取り

### 最低限の機能特権

次の表に、最低限必要な機能特権を示します。

サービス	機能特権
管理者	コネクタ - 表示



## データ統合のアセット特権と機能特権

データ統合のアセット特権と機能特権を使用して、データ統合での作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、アセット特権と機能特権を有効にすることができます。

### データ統合のアセット特権

次の表に、データ統合のアセット特権を示します。

アセット特権	説明
API コレクション	ユーザーが API コレクションに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
Azure データ同期タスク	この特権は使用されません。
ビジネスサービス定義	ユーザーがビジネスサービスに対する権限を作成、読み取り、更新、削除、および設定できるようにします。
データローダータスク	ユーザーがデータローダータスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
データマスキングタスク	ユーザーがデータマスキングタスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
データ転送タスク	ユーザーがデータ転送タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
動的マッピングタスク	ユーザーが動的マッピングタスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
ファイルリсна	ユーザーがファイルリснаに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
固定長ファイル形式	ユーザーが固定長ファイル形式に対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
階層スキーマ	ユーザーが階層スキーマに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
業種別データサービス	ユーザーがデータサービスリポジトリからのデータサービスに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。また、ユーザーが業種別データサービスカスタマイザ、階層マッパー、マッピング内のデータサービストランスフォーメーションなどのアセットでそれらを使用できるようにします。
インテリジェント構造タスク	ユーザーがインテリジェント構造モデルに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
リニアタスクフロー	ユーザーがリニアタスクフローに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
マッピング	ユーザーがマッピングに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。 マッピングを実行するには、マッピングとマッピングタスクに対する実行権限がユーザーに割り当てられている必要があります。

アセット特権	説明
マッピングタスク	ユーザーがマッピングタスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。 マッピングタスクを実行するには、マッピングとマッピングタスクに対する実行権限がユーザーに割り当てられている必要があります。
マップレット	ユーザーがマップレットに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
PowerCenter タスク	ユーザーが PowerCenter タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
レプリケーションタスク	ユーザーがレプリケーションタスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
保存済みクエリ	ユーザーが保存済みクエリに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
Sequence Generator	ユーザーが共有シーケンスに対する権限を作成、読み取り、更新、削除、および設定できるようにします。
Swagger	ユーザーが Swagger ファイルを作成、読み取り、更新、および削除できるようにします。
同期タスク	ユーザーが同期タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
タスクフロー	ユーザーがタスクフローに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
ユーザー定義関数	ユーザーがユーザー定義関数に対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。

## データ統合の機能特権

次の表に、データ統合の機能特権を示します。

機能特権	説明
CDI エラーログへのアクセス	ユーザーが、 <b>[すべてのジョブ]</b> 、 <b>[実行中のジョブ]</b> 、 <b>[マイジョブ]</b> の各ページ、およびジョブの詳細からエラー行ファイルをプレビューできるようにします。
データ統合 Copilot にアクセス	ユーザーが、データ統合とデータ取り込みおよびレプリケーションに CLAIRE Copilot を使用できるようにします。ユーザーが CLAIRE Copilot で実行できるタスクは、ユーザーのアセット特権に応じて異なります。例えば、CLAIRE Copilot でマッピングを作成するには、ユーザーはデータ統合でマッピングを作成する特権を持っている必要があります。CLAIRE Copilot でデータベース取り込みとレプリケーションタスクを作成するには、ユーザーはデータ取り込みおよびレプリケーションでデータベース取り込みとレプリケーションタスクを作成する特権を持っている必要があります。
データ - プレビュー	ユーザーがマッピング内のデータのプレビューと、SQL ELT の最適化データベースプレビュージョブの実行をできるようにします。

機能特権	説明
前処理および後処理コマンドの無効化	ユーザーが前処理コマンドと後処理コマンドを編集できないようにします。既存のコマンドは引き続き実行されますが、編集することはできません。
IICS Discovery 用 EDC	ユーザーがデータカタログ検出を使用して Enterprise Data Catalog からオブジェクトを検索し、それらのオブジェクトをマッピングや一部のタイプのタスクで使用できるようにします。 <b>注:</b> ユーザーがデータカタログの検出を実行できるようにするには、 <b>【組織】</b> ページで Enterprise Data Catalog の統合プロパティを設定する必要があります。

## データマーケットプレイスの機能特権

データマーケットプレイスサービスのユーザーロールで使用可能な Informatica Intelligent Cloud Services 管理者の機能特権を表示します。

次の表に、データマーケットプレイスの機能特権とその説明を示します。

## データプロファイリングの機能特権

データプロファイリングの機能特権を使用して、データプロファイリングアセットでの作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、アセット特権と機能特権を有効にすることができます。

次の表に、データプロファイリングの機能特権とその説明を示します。

特権	説明
データプロファイリング	データプロファイリングタスクに対する権限を作成、読み取り、更新、削除、実行、および設定します。
データプロファイリング - カラムの比較	プロファイル実行でカラムを比較します。
データプロファイリング - データプロファイリング実行の比較	複数のプロファイル実行を比較します。
データプロファイリング - データプロファイリング結果 - 表示*	<ul style="list-style-type: none"> <li>- データプロファイリングタスクを作成したユーザーを含むすべてのユーザーのデータプロファイリングタスクのプロファイリング結果を表示します。</li> <li>- データガバナンス&amp;カタログのスコアカードにある有効な行と無効な行を、<b>成功した行のプレビュー</b>と<b>失敗した行のプレビュー</b>を使用して表示します。</li> </ul>
データプロファイリング - ドリルダウン*	データプロファイリングタスクの作成時にドリルダウンオプションを表示して選択します。
データプロファイリング - データプロファイリング結果のエクスポート	プロファイリング結果を Microsoft Excel ファイルにエクスポートします。
データプロファイリング - ルールの管理	データプロファイリングタスクのルールを追加または削除します。

特権	説明
データプロファイリング - クエリ - 作成	クエリを作成します。
データプロファイリング - クエリ - 送信	クエリを実行してクエリ結果を表示します。
データ統合 - データプレビュー	【データプレビュー】領域にソースオブジェクトデータを表示します。
データプロファイリング 機密データ - 表示	特定のユーザーロールの機密情報を非表示にします。【機密データ - 表示】特権が設定されている場合、【カラムの比較】タブの最小値、最大値、および最も頻度の高い値の情報を表示することはできません。
データプロファイリング データ値ストレージの無効化	プロファイリングウェアハウスに最小値、最大値、および最も頻度の高い値を格納しません。【データ値ストレージの無効化】機能を設定すると、機密情報はプロファイル結果およびソースシステムに保存されなくなります。機密データを表示する権限が割り当てられている場合や、【値の頻度ペアの最大数】オプションでプロファイルタスクを設定した場合も、値は保存されません。デフォルトでは、この機能は無効になっています。この機能を無効にすると、値は適切に格納されます。
<p>* ドリルダウンを実行し、データガバナンス&amp;カタログのスコアカードで【成功した行のプレビュー】と【失敗した行のプレビュー】を表示するには、次の特権が必要です。</p> <ul style="list-style-type: none"> <li>- データプロファイリング - クエリ - 作成</li> <li>- データプロファイリング - クエリ - 送信</li> <li>- データプロファイリング - データプロファイリング結果 - 表示</li> <li>- データプロファイリング 機密データ - 表示</li> </ul>	

次の表に、異なるユーザーロールに対して設定されている場合の【データ値ストレージの無効化】機能および【機密データ - 表示】機能の動作を示します。

機能	カスタム ロール	管理者またはデ ザイナ	結果
データ値ストレージの無効化	非アクティブ	アクティブ	機密情報は保存されません。
	アクティブ	非アクティブ	機密情報は保存されません。
機密データ - 表示	非アクティブ	アクティブ	機密情報が表示されます。
	アクティブ	非アクティブ	機密情報が表示されます。

注: 【データ値ストレージの無効化】機能をアクティブにすると、機密情報はデータプロファイリングまたはソースシステムに保存されなくなります。

## データ品質の機能特権

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にすることができます。

Data Quality の機能特権は、管理者ロールとデザイナーロールに対してデフォルトで有効になっています。

次の表に、Data Quality の機能特権に関する説明を示します。

機能特権	説明
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内容を表示できるようにします。 <ul style="list-style-type: none"><li>- ユーザーが <b>【エクスプローラ】</b> ページからディクショナリを開いたとき。</li><li>- 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。</li></ul>
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します。 <b>注:</b> データ品質アセットでテストを実行するには、このロールとともにデータ品質のマッピングの <b>【実行】</b> 特権が必要です。
例外データ - 削除	ユーザーが、例外管理ジョブに関連付けられた例外データを例外データストアから削除できるようにします。例外管理ジョブは、Data Quality、データプロファイリング、またはデータ統合の <b>【マイジョブ】</b> ページにあります。
例外データ - 表示	ユーザーが、例外管理ジョブによって特定された例外レコードをダウンロードできるようにします。例外管理ジョブは、Data Quality、データプロファイリング、またはデータ統合の <b>【マイジョブ】</b> ページにあります。

**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場合は、**【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] 特権のない状態でディクショナリを開くと、Data Quality に、データを表示するために必要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。

## ドメイン管理サービスのアセット特権と機能特権

ドメイン管理サービスのアセット特権と機能特権を使用して、CDI-PC での作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、アセット特権と機能特権を有効にすることができます。

**重要:** Secure Agent および Secure Agent グループアセットに対する読み取りアクセス権をユーザーのロールに割り当てる必要があります。この操作を行うには、管理者サービスを選択し、アセットに読み取り特権を割り当てます。

## ドメイン登録のアセット特権

次の表に、ドメイン登録のアセット特権とその説明を示します。

アセット特権	説明
読み取り	ユーザーが、登録済みのドメインとドメインの詳細を表示できるようにします。
作成	ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 登録済みのドメインとドメインの詳細の表示。</li><li>- ドメインの登録。</li><li>- ドメインの登録解除。</li><li>- 登録の再試行。</li><li>- ドメインの詳細の編集。</li><li>- ドメインの調整。</li></ul> 作成特権には、読み取り特権および更新特権が含まれます。
更新	ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 登録済みのドメインとドメインの詳細の表示。</li><li>- ドメインの登録解除。</li><li>- 登録の再試行。</li><li>- ドメインの詳細の編集。</li><li>- ドメインの調整。</li></ul> 更新特権には、読み取り特権が含まれます。
削除	ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"><li>- 登録済みのドメインとドメインの詳細の表示。</li><li>- 登録解除されたドメインの削除。</li></ul> 削除特権には、読み取り特権が含まれます。

## ドメイン登録の機能特権

次の表に、ドメイン登録の機能特権とその説明を示します。

ドメイン登録の機能特権	説明
ドメインの更新	ユーザーがドメインを更新できるようにします。

## ヒューマンタスクのアセットと機能特権

ヒューマンタスクアセットの機能特権を使用して、ヒューマンタスクアセットの操作中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、アセットと機能特権を有効にすることができます。

### ヒューマンタスクアセットの特権

次の表に、ヒューマンタスクのアセット特権を示します。

アセット特権	説明
ヒューマンタスクアセット	ユーザーが次のアクションを実行できるようにします。 <ul style="list-style-type: none"><li>- ヒューマンタスクアセットの作成、読み取り、更新、または削除。</li><li>- ヒューマンタスクを生成するヒューマンタスクステップを含むプロセスの実行。</li><li>- ヒューマンタスクアセットへのアクセスを許可するための、他のユーザーロールへの権限の割り当て。</li></ul>

### ヒューマンタスクの機能特権

次の表に、ヒューマンタスクの機能特権を示します。

機能特権	説明
開発	ユーザーが、ヒューマンタスクアセットを作成および編集し、アプリケーションの統合プロセスでヒューマンタスクステップを使用できるようにします。
ヒューマンタスクアプリケーションの表示	ユーザーが、ヒューマンタスクサービスを表示およびヒューマンタスクサービスにアクセスできるようにします。
タスクの表示	ユーザーが、ヒューマンタスクサービスのヒューマンタスクインボックスにアクセスできるようにします。

## メタデータコマンドセンターの機能特権

メタデータコマンドセンターの機能特権を使用して、メタデータコマンドセンターでの作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、この機能特権を有効にすることができます。

次の表に、メタデータコマンドセンターの機能特権とその説明を示します。

特徴	説明
メタデータコマンドセンターアプリケーションへのアクセス	メタデータコマンドセンターへのアクセス権を付与します。無効にすると、ユーザーはメタデータコマンドセンターにアクセスできなくなります。
カスタム属性の管理	ユーザーがデータガバナンス&カタログに表示されるアセットリレーション、事前定義された属性、およびアセットタイプのカスタム属性を管理できるようにします。
カスタム属性の表示	ユーザーがデータガバナンス&カタログでアセットタイプの属性を表示できるようにします。

特徴	説明
データ分類の管理	ユーザーがデータ分類包含ルールを作成および管理できるようにします。
データ分類の表示	メタデータコマンドセンターで機能を有効にしてカタログソースジョブを実行した後に、ユーザーがデータガバナンス&カタログでデータ分類を表示できるようにします。
ルックアップテーブルの管理	ユーザーがデータ分類で使えるルックアップテーブルをインポートおよびパブリッシュできるようにします。
ルックアップテーブルの表示	ユーザーがメタデータコマンドセンターのルックアップテーブルを表示できるようにします。
ジョブの監視	ユーザーがジョブを監視できるようにします。
リネージュ設定の管理	ユーザーが次のようなタスクを実行できるようにします。 <ul style="list-style-type: none"> <li>- 1 つ以上のカタログソースへの接続を割り当てまたは割り当て解除します。</li> <li>- カatalogソースをリンクしてリネージュを生成します。</li> </ul>
リネージュ設定の表示	ユーザーが [リネージュ] タブからデータリネージュを表示できるようにします。
アクセス制御の管理	ユーザーがステークホルダーロールとアクセスポリシーを作成および管理できるようにします。また、ユーザーが保存された検索条件やダッシュボードを共有したり、他のユーザーのデフォルトのダッシュボードを設定したりすることもできるようにします。
アクセス制御の表示	ユーザーがアクセスポリシーを表示できるようにします。
アセットグループの管理	ユーザーがアセットグループを作成、更新、または削除できるようにします。
アセットグループの表示	ユーザーがアセットグループを表示できるようにします。
ワークフローの管理	ユーザーがワークフローを作成または変更できるようにします。
ワークフローの表示	ユーザーがワークフローを表示できるようにします。
Workflow Designer	ユーザーが新しいワークフローを設計できるようにします。
システム設定の管理	ユーザーがシステム設定を変更できるようにします。
システム設定の表示	ユーザーが [参照 ID] タブを表示できるようにします。
アセットページのカスタマイズの管理	ユーザーがページのレイアウトの作成、更新、および削除やアセットのパネルのプレビューを行うことができるようにします。ユーザーがロール、ユーザーグループ、または組織内のすべてのユーザーに基づいて、他のユーザーにデフォルトのレイアウトを割り当てられるようにします。
アセットページのカスタマイズの表示	ユーザーがページのレイアウトを表示できるようにします。
IDMC メタデータ設定の管理	ユーザーがデータ統合タスクおよびアプリケーションの統合オブジェクトのメタデータをカタログと同期できるようにします。
IDMC メタデータ設定の表示	ユーザーが IDMC メタデータを表示できるようにします。



特徴	説明
アップグレードの管理	ユーザーが最新バージョンのデータガバナンス&カタログへのアップグレードを開始できるようにします。
スーパー管理者	ユーザーがガバナンス管理者ロール以外の固有の管理者機能へのアクセスを行うことができるようにします。

## モニタの機能特権

モニタの機能特権を使用して、モニタでの作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、この機能特権を有効にすることができます。

次の表に、モニタの機能特権を示します。

機能特権	説明
ジョブの結果 - 表示	ユーザーが、 <b>[すべてのジョブ]</b> 、 <b>[実行中のジョブ]</b> 、および <b>[マイジョブ]</b> ページでジョブの結果を表示できるようにします。
ログ - 表示およびダウンロード	ユーザーがジョブログファイルを表示およびダウンロードできるようにします。

## オペレーションインサイトの機能特権

オペレーションインサイトの機能特権を使用して、オペレーションインサイトでの作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、この機能特権を有効にすることができます。

次の表に、オペレーションインサイトの機能特権とその説明を示します。

特徴	説明
アノマリーアラートの設定 - 変更	ユーザーが PowerCenter プロジェクトの CLAIRE アラートを作成および変更できるようにします。
データ統合ジョブアラート	ユーザーが <b>[データ統合アラート]</b> ページの表示と、データ統合ジョブのアラートの作成および変更を行うことができるようにします。
ドメインインフラストラクチャ - 変更	ユーザーがドメインの登録、編集、および登録解除、 <b>[インフラストラクチャアラート]</b> ページの表示を行うことができるようにします。
ドメインインフラストラクチャアラートの設定 - 変更	ユーザーが <b>[インフラストラクチャアラート]</b> ページでドメインアラートを変更できるようにします。
ドメインジョブの分析 - 表示	ユーザーが PowerCenter、Data Engineering、および Data Quality の <b>[ドメイン]</b> ページを表示できるようにします。
ドメインプロジェクト - 変更	ユーザーが PowerCenter プロジェクトを作成および編集できるようにします。また、ユーザーが Data Engineering Integration と Data Quality のプロジェクトを表示することもできるようにします。

特徴	説明
インフラストラクチャ - 変更	ユーザーがドメインマップを編集できるようにします。
インフラストラクチャ - 表示	ユーザーにオペレーションインサイトへのアクセスを提供し、ユーザーが <b>【ホーム】</b> ページを表示できるようにします。また、ユーザーが <b>【すべてのインフラストラクチャ】</b> ページの <b>【Secure Agent とグループ】</b> タブを表示できるようにします。 ユーザーが <b>【インフラストラクチャアラート】</b> ページと <b>【PowerCenter アラート】</b> ページを表示できるようにします。
ジョブアラートの設定 - 変更	ユーザーが PowerCenter ジョブのアラートを作成および変更できるようにします。
一括取り込みジョブアラート	ユーザーがデータ取り込みおよびレプリケーションジョブのアラートを表示、作成、および変更できるようにします。
オペレーションインサイト - 表示	ユーザーが次のパネルとページを表示できるようにします。 <ul style="list-style-type: none"> <li>- <b>【ホーム】</b> ページの <b>【ロードされた行】</b> パネル。</li> <li>- <b>【すべてのインフラストラクチャ】</b> ページの <b>【ドメイン】</b> タブ。</li> <li>- <b>【PowerCenter】</b>、<b>【Data Engineering Integration】</b>、および <b>【Data Quality】</b> ページ。</li> <li>- <b>【PowerCenter】</b> ページの推奨事項。</li> <li>- <b>【PowerCenter アラート】</b> ページのアラート設定。</li> <li>- <b>【受信したアラート】</b> ページ。</li> </ul> また、ユーザーが割り当てられたプロジェクトを表示したり、プロジェクトの CLAIR アラートを表示したりすることもできるようにします。
Secure Agent ランタイムアラートの設定 - 変更	ユーザーが <b>【インフラストラクチャアラート】</b> ページで Secure Agent アラートを編集できるようにします。

## ワークベンチサービスのアセット特権と機能特権

ワークベンチサービスのアセット特権と機能特権を使用して、PowerCenter 用クラウドデータ統合 (CDI-PC) での作業中にユーザーが特定の機能にアクセスできるようにします。カスタムロールを作成するときに、アセット特権と機能特権を有効にすることができます。

### ワークベンチサービスのアセット特権

次の表に、ワークベンチサービスのアセット特権とその説明を示します。

アセット特権	説明
アセスメントリポイント設定	ユーザーがアセットリポイント設定タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
アセスメントタスク	ユーザーが PowerCenter リポジトリアセスメントタスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
一括更新タスク	ユーザーがアセットメタデータ一括更新タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
接続マップ設定	ユーザーが接続マップ設定タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。

アセット特権	説明
変換プロパティ設定	ユーザーが変換プロパティ設定タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
変換タスク	ユーザーがアセット変換タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。
パラメータファイル変換タスク	ユーザーがパラメータファイル変換タスクに対する権限を作成、読み取り、更新、削除、実行、および設定できるようにします。

## ワークベンチサービスの機能特権

次の表に、ワークベンチサービスの機能特権とその説明を示します。

機能特権	説明
アーティファクトのダウンロード	ユーザーがアセスメントジョブ、変換ジョブ、または一括更新ジョブから生成されたファイルをダウンロードできるようにします。
リポジトリの評価	リポジトリを評価できます。 <b>注:</b> アセスメントジョブを実行するには、管理者ロールがユーザーに割り当てられていることを確認してください。
評価結果の表示	評価結果にアクセスできます。
設定の表示	ユーザーが設定を表示できるようにします。
ジョブを表示	ユーザーがアセスメントジョブ、変換ジョブ、パラメータファイル変換ジョブ、および一括更新ジョブの詳細を表示できるようにします。
タスクの表示	ユーザーがアセスメントタスク、変換タスク、パラメータファイル変換タスク、および一括更新タスクの詳細を表示できるようにします。

## 第 7 章

# ユーザー設定

ユーザー設定では、電子メール通知の受信方法の設定やソースコードの資格情報の設定を行うことができます。

ユーザー設定にアクセスするには、ツールバーの【ユーザー】アイコンをクリックしてから、【設定】を選択します。ユーザー設定ページには、次のようなセクションがあります。

### 通知の設定

【通知の設定】セクションには、アセットの関係者の変更やアセットに対する新しいコメントなど、通知をトリガするイベントのカテゴリが一覧表示されます。デフォルトでは、イベントが発生するたびに電子メール通知が届きます。イベント通知は無効にすることができ、一部の通知カテゴリでは、指定した間隔でイベントを要約した電子メールを受信するように選択することができます。

### ソースコード管理資格情報

【ソースコード管理資格情報】セクションでは、リポジトリの資格情報を設定して、ソース管理を操作できます。

詳細については、「[組織管理](#)」を参照してください。

## 通知カテゴリおよびサブカテゴリ

通知をトリガする各イベントは、【管理】などのカテゴリと【関係者の変更】などのサブカテゴリに属します。それぞれのカテゴリとサブカテゴリの設定を構成することができます。

### 管理

次の表に、【管理】カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
関係者の変更	アセットの関係者の変更（関係者の削除や所有権の移転を含む）

### アセットの変更

次の表に、【アセットの変更】カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
アセットの変更	アセット、カタログソース、または関係に対する変更

## コラボレーション

次の表に、[コラボレーション] カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
認証	アセットの認証ステータスの変更
コメント	アセットに対する新しいコメント
メンション	他のユーザーがスレッドであなたをタグ付けしました
評価数	アセットの評価の変更
共有	他のユーザーが保存済み検索をあなたと共有した

## 重要な通知

次の表に、[重要な通知] カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
重要な管理アラート	組織、ネットワーク要件、Secure Agent、またはサービスの可用性を維持するために管理者が注意する必要があるその他の運用上の変更に関連する更新
重要なイベントアラート	今後のリリースとサービスメンテナンス
事前通知	ユーザーの対応が必要な機能またはリリースの影響

注: [重要な操作] カテゴリの通知を無効にすると、変更が有効になるまでに最大 10 営業日かかる場合があります。

## データ品質

次の表に、[データ品質] カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
データオブザーバビリティ	ソースデータの異常に対してデータオブザーバビリティが生成するイベント
データ品質	データ品質ルールオカレンスに対するデータ品質スコアの変更（障害や異常を含む）

## チケットとワークフロー

次の表に、[チケットとワークフロー] カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
アクセス	データへのアクセスの変更
オーダー	注文に対して生成されたイベント

サブカテゴリ	説明
要求	データマーケットプレイスでのデータ収集要求に対して生成されたイベント
タスク	あなたが完了する必要があるタスクに関するリマインダー
チケット	チケットに対して生成されたイベント
ワークフローの進行状況	ワークフローに対して生成されたイベント

## ユーザージョブ

次の表に、[ユーザージョブ] カテゴリのサブカテゴリに関する説明を示します。

サブカテゴリ	説明
エクスポートジョブ	エクスポートジョブに対して生成されたイベント
インポートジョブ	インポートジョブに対して生成されたイベント

## 第 8 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なら、管理者または他の資格あるユーザーによって、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ー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ー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、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する必要があります。
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 9 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。

プロフィー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、**[プロフィール]** を選択します。
2. **[プロフィール]** 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、プロフィールに表示されます。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。

## 第 10 章

# 組織へのユーザーの招待

適切なロールが割り当てられている場合は、ランタイム環境またはプライマリクラウドデータウェアハウスの設定時にユーザーを組織に招待できます。ユーザーを組織に招待して、ランタイム環境の設定やクラウドデータウェアハウスへの接続を手伝ってもらうことができますようにします。

組織に参加するようにユーザーを招待するには、**【友人や同僚を招待して手伝ってもらう】** をクリックします。ユーザーの招待を行うには、管理者ロールが割り当てられているか、デザイナーロールと、「読み取りロール」および「ユーザーの作成」管理者アセット特権を持つカスタムロールが割り当てられている必要があります。招待するユーザーには、管理者ロールまたはデザイナーロールを割り当てる必要があります。

**【友人や同僚を招待して手伝ってもらう】** オプションが表示されない場合、またはユーザーに別のロールを割り当てる場合は、管理者の **【ユーザー】** ページでユーザーを追加します。

1. **【友人や同僚に手伝ってもらう】** をクリックします。
2. 招待するユーザーの名、姓、電子メールアドレス、ユーザー名、およびロールを入力します。  
ユーザー名は、組織内で一意である必要があります。ユーザーを招待した後にユーザー名を変更することはできません。
3. **【OK】** をクリックします。  
招待したユーザーには、組織に参加するためのリンクが記載されたメールが送信されます。

## 第 11 章

# 通知

Informatica Intelligent Cloud Services では、ジョブステータスの更新、ライセンスの有効期限、およびワークフローの進行状況などの特定のイベントに関する通知を受信します。これらの通知については、通知トレイでの表示や **【通知】** ページでの管理、電子メールでのアラートを受信を行うことができます。

ツールバーの **【通知】** アイコンには、未読の通知の数が表示されます。アイコンをクリックすると、通知トレイに最新の未読の通知を表示することができます。一部のサービスでは、トレイをフィルタリングして、現在のサービスからの通知のみを表示できます。

通知は **【通知】** ページで表示および管理することができます。**【通知】** ページにアクセスするには、通知トレイの **【アクション】** メニューから **【すべての未読の通知を表示】** を選択します。通知は、サービス、カテゴリ、サブカテゴリ、ステータス、および受信日でフィルタリングできます。

通知アラートを電子メールで受信するには、ユーザー設定でオプションを設定します。詳細については、[第 7 章, 「ユーザー設定」 \(ページ 84\)](#) を参照してください。

# 索引

## C

Cloud アプリケーション統合コミュニティ  
URL [6](#)  
Cloud 開発者コミュニティ  
URL [6](#)

## I

Informatica Intelligent Cloud Services  
Web サイト [6](#)  
Informatica グローバルカスタマサポート  
連絡先情報 [7](#)

## J

JWT アクセストークン [24](#)

## M

Microsoft Azure  
シングルサインオン設定プロパティ [10](#)

## O

OAuth  
REST API 呼び出しでの JWT アクセストークンの使用 [24](#)

## S

SAML のシングルサインオン  
ID プロバイダ設定のプロパティ [20](#)  
JWT アクセストークンの使用 [24](#)  
SAML グループマッピングのプロパティ [23](#)  
SAML ロールマッピングのプロパティ [23](#)  
SAML 承認によるユーザー管理 [15](#)  
SAML 属性マッピングのプロパティ [21](#)  
SAML 認証によるユーザー管理 [14](#)  
SCIM 2.0 の使用 [16](#)  
Secure Agent の登録 [14](#)  
SSO 設定のプロパティ [19](#)  
サービスプロバイダメタデータ [24](#)  
サービスプロバイダ設定 [21](#)  
ユーザーの作成 [14](#), [15](#)  
ユーザーの削除 [14](#), [15](#)  
ユーザー資格情報のストレージ [14](#), [15](#)  
概要 [12](#)  
信頼済み IP 範囲 [14](#)  
制限 [14](#)  
設定の概要 [18](#)  
設定手順 [18](#)

SAML のシングルサインオン (続く)  
追加の属性マッピングプロパティ [21](#)  
認証と承認からの切り替え [15](#)  
認証と承認への切り替え [16](#)  
認証のみからの切り替え [16](#)  
認証のみへの切り替え [15](#)  
要件 [13](#)

## W

Web サイト [6](#)

## あ

アセット  
特権の割り当て [41](#)  
アップグレード通知 [7](#)

## え

エコシステムのシングルサインオン  
構成プロパティ [10](#)

## さ

サービス  
ユーザーグループへの割り当て [37](#)

## し

システムステータス [7](#)

## す

スケジュール  
ユーザーのスケジュール済みジョブの再割り当て [35](#)  
ステータス  
Informatica Intelligent Cloud Services [7](#)

## せ

セキュリティの質問  
編集 [89](#)

## た

タイムゾーン  
ユーザープロファイルの変更 [89](#)

## は

パスワード  
変更 [89](#)

## ふ

プロフィール  
編集 [89](#)

## め

メンテナンスの停止 [7](#)

## ゆ

ユーザ  
定義 [8](#)

ユーザー

アプリケーション統合の匿名ユーザー [27](#)  
グループの割り当て [28](#)  
サービスの割り当ておよび割り当て解除 [33](#)  
スケジュール済みジョブの再割り当て [35](#)  
デフォルトのサービスの設定 [33](#)  
ユーザーグループへの割り当て [37](#)

ユーザー統計 [27](#)

リセット [34](#)

ロールの割り当て [28](#)

ログイン日時のダウンロード [27](#)

ロック解除 [34](#)

概要 [26](#)

構成例 [87](#)

作成 [32](#)

削除 [35](#)

招待 [90](#)

詳細 [28](#)

認証方法 [9](#)

編集 [28](#)

無効化 [34](#)

ユーザーグループ

メンバの追加と削除 [37](#)

ユーザーへの割り当て [28](#)

ロールの割り当て [37](#)

概要 [36](#)

構成例 [87](#)

作成 [38](#)

削除 [39](#)

詳細 [37](#)

定義 [8](#)

編集 [37](#)

名前の変更 [37](#), [39](#)

ユーザープロフィール

編集 [89](#)

## ろ

ロール

Administrator のロール [46](#)

API センターのロール [47](#)

API ポータルのロール [48](#)

API マネージャのロール [48](#)

B2B ゲートウェイのロール [50](#)

B2B パートナーポータルのロール [50](#)

Business 360 コンソールのロール [51](#)

CDI-PC のロール [52](#)

CLAIRE GPT ロール [52](#)

Customer 360 のロール [52](#)

Data Marketplace のロール [55](#)

Monitor のロール [60](#)

Product 360 のロール [61](#)

Reference 360 のロール [62](#)

Supplier 360 のロール [63](#)

アセットと機能特権 [65](#)

アプリケーション統合コンソールのロール [49](#)

アプリケーション統合のロール [49](#)

オペレーションインサイトのロール [61](#)

オペレータロール [43](#)

カスタム [40](#), [64](#)

クローン作成 [64](#)

クロスサービス [43](#)

サービスコンシューマロール [43](#)

システム定義 [40](#), [42](#)

データガバナンス&カタログのロール [53](#)

データプロファイリングのロール [58](#)

データ統合データプレビューアロール [43](#)

データ統合のロール [54](#)

データ品質のロール [58](#)

デザイナロール [43](#)

デブロイヤロール [43](#)

メタデータコマンドセンターのロール [60](#)

モニタロール [43](#)

ユーザーグループへの割り当て [37](#)

ユーザーへの割り当て [28](#)

ユーザー設定の例 [87](#)

一括取り込みのロール [54](#)

概要 [40](#)

管理者ロール [43](#)

作成 [64](#)

削除 [65](#)

詳細 [41](#)

定義 [8](#)

統合ハブのロール [59](#)

特権の割り当て [41](#)

名前の変更 [65](#)

有効および無効 [40](#)