



Informatica® Intelligent Cloud Services
October 2025

組織管理

© 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（電子的複写、写真複写、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 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

序文	6
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
 第 1 章 : 管理者について	8
 第 2 章 : 組織	11
組織の設定.....	11
組織の設定.....	12
組織の全般プロパティ.....	13
認証プロパティ.....	14
接続プロパティの保存場所.....	16
フィンガープリント認証のプロパティ.....	16
電子メール通知の設定.....	17
データ統合サービスのプロパティ.....	18
Enterprise Data Catalog 統合プロパティ.....	18
サブ組織.....	19
サブ組織の追加.....	21
サブ組織の削除.....	22
サブ組織の無効化または有効化.....	23
別の組織への切り替え.....	24
サブ組織への親組織のアクセスを拒否.....	24
サブ組織のアドオンコネクタ.....	25
サブ組織でのアセットのエクスポートとインポート.....	25
サブ組織の機能とサービスサポートマトリックス.....	25
追加プロダクション組織とサンドボックス組織.....	26
追加の組織の作成.....	27
 第 3 章 : メータリング	28
Informatica のプロセッシングユニットのメトリック.....	28
IPU メトリックの表示.....	28
IPU スカラ.....	32
IPU メーター.....	33

レートカード.....	35
無効化されたサブ組織および削除されたサブ組織での IPU 使用率.....	37
IPU メトリックレポート.....	38
IPU 消費数警告の設定.....	41
メータリングタグ.....	41
機能ベースのライセンスメトリック.....	43
ライセンスメトリックの表示.....	43
使用状況の詳細の表示.....	48
メータリングの使用状況レポート.....	49
第 4 章 : 全般設定とセキュリティ設定.....	51
ソース管理設定.....	52
サブ組織のソース管理設定.....	53
OAuth を使用したリポジトリアクセス.....	53
オンプレミスリポジトリの操作.....	54
組織のソース管理の有効化.....	54
ソース管理リポジトリ URL の変更.....	56
組織のソース管理の無効化.....	57
リポジトリアクセスの設定.....	57
ソース管理のベストプラクティス.....	58
別のユーザーのチェックアウトの取り消し.....	59
アプリケーション統合プロセスを実行するためのターボモードの設定.....	60
ターボモードでプロセスを実行するための組織の設定.....	60
Secure Agent サービスのローリングアップグレード.....	60
ローリングアップグレードエラーの処理.....	61
Secure Agent サービスの再開スケジュールの設定.....	62
カスタムブランディングの設定.....	62
ロゴおよびファビコンのガイドライン.....	62
組織のカスタムブランディングの設定.....	63
CLAIRE の設定.....	63
通知の設定.....	64
顧客管理対象暗号化キー.....	64
顧客管理対象キーの作成と有効化.....	66
顧客管理対象キーに関するよくある質問.....	66
シークレットマネージャの設定.....	68
AWS Secrets Manager の設定.....	69
Azure Key Vault の設定.....	77
HashiCorp Vault の設定.....	78
シークレットマネージャの有効化と無効化.....	80
サブ組織のシークレットマネージャの設定.....	80
シークレットマネージャを使用するための接続の設定.....	81
セキュリティ設定.....	82
Informatica サポートアクセスの削除.....	83

第 5 章 : 権限	84
権限のルールおよびガイドライン	85
権限の設定	85
第 6 章 : スケジュール	88
ブラックアウト期間の設定	89
繰り返し頻度	89
タイムゾーンとスケジュール	90
夏時間への移行とスケジュール	91
スケジュールの設定	91
スケジュールのエクスポート	92
スケジュール済みタスクのトラブルシューティング	93
第 7 章 : バンドル管理	94
バンドルのタイプ	94
バンドルのインストール	95
バンドルのコピー	96
バンドルのアップグレード	96
バンドルのアンインストール	97
第 8 章 : イベント監視	98
第 9 章 : セキュリティのトラブルシューティング	100
第 10 章 : ライセンス	101
ライセンスのカテゴリ	101
ライセンスのタイプ	102
サブ組織のライセンス	102
サブ組織のライセンスの編集	103
親組織とのライセンスの同期	103
組織タイプの設定	103
ライセンスの有効期限	104
索引	105

序文

「組織管理」を参考にして、Informatica Intelligent Cloud ServicesSMの組織およびサブ組織を設定および保守する方法を学びます。ライセンスの管理とライセンスの使用状況の監視、ソース管理の設定、オブジェクトの権限の設定、スケジュールの作成、バンドルの管理、イベントの監視、およびセキュリティ問題のトラブルシューティングの方法を確認します。

Informatica のリソース

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

Informatica マニュアル

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

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

Informatica Intelligent Cloud Services Web サイト

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

Informatica Intelligent Cloud Services コミュニティ

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

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

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

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

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

Informatica Intelligent Cloud Services マーケットプレイス

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) 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

管理者について

管理者は、Informatica Intelligent Cloud Services にわたる組織管理機能を提供します。

管理者を使用して、組織の以下の側面を管理します。

組織とサブ組織

パスワードの要件、信頼される IP アドレス、接続プロパティの保存、データ統合タスクのタイムゾーンおよび電子メール通知の設定、CLAIRE™推奨の設定、Enterprise Data Catalog の設定など、組織およびサブ組織の設定を行います。サブ組織を作成し、管理します。

組織およびサブ組織の詳細については、[第 2 章, 「組織」 \(ページ 11\)](#)を参照してください。

ライセンス

組織のライセンスを表示し、下位組織のライセンスを管理します。

ライセンスについては、[第 10 章, 「ライセンス」 \(ページ 101\)](#)を参照してください。

メータリング

ジョブ制限、使用状況、Informatica プロセッシングユニット (IPU) のバランスなどのメータリング情報を表示します。

メータリングについては、[第 3 章, 「メータリング」 \(ページ 28\)](#)を参照してください。

エコシステムと SAML のシングルサインオン

Microsoft Azure のシングルサインオン設定を行います。SAML のサードパーティ ID プロバイダのシングルサインオン機能を有効にします。

Microsoft Azure シングルサインオン設定の詳細、および SAML シングルサインオンの有効化と設定に関する詳細については、「[ユーザー管理](#)」を参照してください。

全般設定とセキュリティ設定

プロジェクト、フォルダ、アセットのソース管理を有効化します。一部の Secure Agent サービス用にアップグレードエラー処理とアップグレード再起動スケジュールを設定します。サブ組織に適用する親組織のカスタムブランディング設定を構成します。組織での顧客管理対象暗号化キーの使用を有効化または無効化します。外部シークレットマネージャから接続資格情報を取得するように組織を設定します。

全般設定とセキュリティ設定の詳細については、[第 4 章, 「全般設定とセキュリティ設定」 \(ページ 51\)](#)を参照してください。

ユーザー、ユーザーグループ、およびユーザーロール

ユーザーアカウントを個別に作成および設定して、組織にアクセスできるようにします。同じタスクを実行できるユーザーグループを作成します。ロールを作成および設定して、ユーザーとユーザーグループの特権を定義します。

ユーザー、ユーザーグループ、およびユーザーロールの詳細については、「[ユーザー管理](#)」を参照してください。

許可

ユーザーとユーザーグループが Secure Agent、Secure Agent グループ、接続、およびスケジュールなどのオブジェクトに対して持つ事のできるアクセス権限を設定します。

権限および権限の設定に関する詳細については、[第 5 章、「権限」 \(ページ 84\)](#)を参照してください。

ランタイム環境

Secure Agent をダウンロードし、インストールします。Secure Agent グループを作成し、設定します。

Secure Agent、Secure Agent グループ、および Secure Agent のダウンロードとインストールの詳細については、「[ランタイム環境](#)」を参照してください。

サーバーレスランタイム環境

メンテナンスのオーバーヘッドを削減するために、データ統合によって管理されるランタイム環境を使用します。

注: サーバーレスランタイム環境を使用するには、AWS クラウドプラットフォームでプライベートクラウドを使用する必要があります。

サーバーレスランタイム環境の詳細については、「[ランタイム環境](#)」を参照してください。

Secure Agent サービス

エラスティックサーバー、CIH プロセッサ、データ統合サーバー、EDC 検索エージェント、プロセスサーバーなど、Secure Agent がデータ処理に使用するマイクロサービスを設定します。

Secure Agent サービスとその設定の詳細については、「[Secure Agent サービス](#)」を参照してください。

詳細クラスタ

組織がデータ統合ジョブを処理するために使用できる一時クラスタを管理します。

詳細クラスタの詳細については、[詳細クラスタに関する説明](#)を参照してください。

スケジュール

タスクまたはタスクフローを、指定した時間または一定の間隔で実行するようにスケジュールを作成します。組織でスケジュールされたタスクやジョブが実行出来なくなるブラックアウト期間を定義します。

スケジュールおよび組織のブラックアウト期間に関する詳細については、[第 6 章、「スケジュール」 \(ページ 88\)](#)を参照してください。

アドオンバンドル

データ統合ユーザーがデータ統合プロジェクトで使用できる関連マッピング、マッピングタスク、およびマップレットのセットをインストール、コピー、アップグレード、およびアンインストールします。

アドオンバンドルの管理に関する詳細については、[第 7 章、「バンドル管理」 \(ページ 94\)](#)を参照してください。

データサービスリポジトリ

業界標準メッセージを処理する、追加設定なしで使用できるデータサービスをダウンロードし、それらを使用して、カスタムメッセージを処理するカスタムデータサービスを作成します。

データサービスリポジトリの詳細については、「[データサービスリポジトリ](#)」を参照してください。

イベント監視

アセットおよびセキュリティログを使用して、組織内のアセット、ライセンス、ユーザー、および Secure Agent のイベントを監視します。

アセットおよびセキュリティログの詳細については、[第 8 章, 「イベント監視」 \(ページ 98\)](#)を参照してください。

ファイル転送

組織のファイルサーバーを設定して、ビジネスパートナーのリモートサーバーからファイルを安全に送受信します。接続を設定してから Informatica Intelligent Cloud Services の REST API を使用してパートナーにファイルを送信します。

ファイルサーバーとファイル転送の詳細については、「[ファイル転送](#)」を参照してください。

注: ヘルプに記載されている機能の一部は、組織の Informatica Intelligent Cloud Services ライセンス契約により利用できない場合があります。

第 2 章

組織

組織は、ライセンス、ユーザーアカウント、マッピングやタスクなどのデータ統合アセット、およびジョブとセキュリティに関する情報を格納する Informatica Intelligent Cloud Services リポジトリ内の安全な領域です。1 つ以上の組織にアクセスできる場合があります。

デフォルトでは、無料トライアルを開始するときに作成する組織はプロダクション組織です。

ライセンスに基づき、次の組織にもアクセスできる場合があります。

サブ組織

プロダクション組織の管理者は、1 つ以上のサブ組織を作成できます。サブ組織は、プロダクション組織の子組織です。これらは親組織に自動的にリンクされます。

各サブ組織には、独自のアセット、接続、ランタイム環境、およびユーザーのセットがあります。ただし、親組織は、ランタイム環境とアドオンコネクタをサブ組織と共有できます。親組織の管理者は、サブ組織がこれを禁止していない限り、サブ組織に切り替えることができます。

サブ組織から他の組織を作成することはできません。

追加プロダクション組織とサンドボックス組織

プロダクション組織の管理者は、追加プロダクション組織とサンドボックス組織を作成できます。

これらの組織は、IPU を使用するためプロダクション組織に自動的にリンクされますが、それ以外は完全に独立した組織です。これらは、アセット、接続、ランタイム環境、またはユーザーをプロダクション組織と共有しません。プロダクション組織の管理者は、追加プロダクション組織またはサンドボックス組織に切り替えることはできません。

プロダクション組織が、サブ組織を作成するライセンスを持っている場合、追加プロダクション組織とサンドボックス組織の管理者は、組織のサブ組織を作成できます。

組織の管理者は、組織とそのサブ組織を保持します。Informatica Intelligent Cloud Services に管理者としてログインし、組織の設定、スケジュールの作成と管理、およびアセットとセキュリティに関連するアクティビティの監視を行います。

組織の設定

組織を構成するときは、組織のプロパティ、サブ組織、追加プロダクション組織、ライセンス、ランタイム環境、およびユーザーアカウントを設定します。

会社の組織を設定するには、次の手順を実行します。

1. 組織名や住所、認証情報、通知を受ける電子メールアドレスなどの組織のプロパティを構成します。
2. 組織に適切なライセンスがあることを確認します。

3. 必要に応じて、1 つ以上のサブ組織を作成し、サブ組織のライセンスを設定します。
4. 必要に応じて、追加プロダクション組織とサンドボックス組織を作成します。
5. ランタイム環境と Secure Agents を設定します。
6. ユーザー、ユーザーグループ、およびロールを設定します。

また、組織用に非ネイティブコネクタをダウンロードしてインストールする必要がある場合もあります。例えば、組織内のユーザーが Teradata テーブルからデータを読み取るタスクを作成する場合は、Teradata のアドオンコネクタをダウンロードしてインストールする必要があります。アドオンコネクタのダウンロードとインストールの詳細については、「[接続](#)」を参照してください。

組織の設定

【組織】 ページで、組織またはサブ組織の設定を構成します。**【組織】** ページにアクセスするには、管理者で**【組織】** を選択します。

次の図に、**【組織の設定】** ページを示します。

The screenshot displays the Informatica Administrator interface for the 'Unified_Org' settings page. The left sidebar contains a navigation menu with options like Organization, Licenses, SAML Setup, Metering, Users, Settings, User Groups, User Roles, Runtime Environ..., Serverless Enviro..., Connections, Add-On Connecto..., Schedules, Add-On Bundles, Swagger Files, Logs, and Advanced Clusters. The main content area is titled 'Unified_Org' and has a 'Settings' tab selected. Below the tab, the 'Organization Overview' section is visible, divided into 'General' and 'Address' columns. The 'General' column contains fields for Organization Name (set to 'Unified_Org'), Organization ID (64kL9ooqt0uclJhYAwclia), Environment Type (set to 'Production'), Description, Number of Employees (set to 'Fewer than 10 employees'), and Country (set to 'United States'). The 'Address' column contains fields for Address 1, Address 2, Address 3, City, State, and Zip Code. A 'Save' button is located in the top right corner of the settings area.

次のような設定項目を設定することができます。

- 組織名、説明、従業員数、住所情報などの全般的なプロパティ。
- 認証情報と接続プロパティの保存場所。
- 接続の資格情報とその保存場所。
- フィンガープリント認証の適用。
- 電子メール通知に使用するタイムゾーンや電子メールアドレスなどのデータ統合サービスのプロパティ。
- CLAIRE™の推奨設定。有効にすると、収集されたメタデータに基づいて CLAIRE で推奨する設計時間が指定されます。

- Enterprise Data Catalog サービスの URL、Enterprise Data Catalog からデータを読み取るランタイム環境、Enterprise Data Catalog のユーザー名とパスワードなどの Enterprise Data Catalog 統合プロパティ。

組織の全般プロパティ

組織とサブ組織の全般プロパティを構成できます。全般プロパティには、組織名、ID、説明、住所、従業員の数などの情報が含まれます。組織の履歴情報も全般プロパティに表示されます。

全般プロパティには次のような情報があります。

概要情報

以下の表で、概要プロパティについて説明します。

プロパティ	説明
名前	組織の名前。 組織名を変更した場合、ログアウトしてログインし直すと【組織】メニューに新しい名前が表示されます。
ID	組織の作成時に組織に割り当てられた ID。組織 ID を変更することはできません。
親組織 ID	サブ組織を表示すると、このプロパティには、親組織に割り当てられた ID が表示されます。組織 ID を変更することはできません。
組織のステータス	サブ組織を表示した場合、このプロパティにはサブ組織が有効であるか無効であるかが表示されます。
環境タイプ	組織の環境タイプ（開発、プロダクション、QA、またはサンドボックス）。 Informatica Intelligent Cloud Services は、組織のライセンスに基づいて環境タイプを設定します。場合によっては、値を編集できます。 環境タイプは、次の方法で設定されます。 <ul style="list-style-type: none"> - 無料トライアルを使用して組織を作成する場合、環境タイプは【サンドボックス】です。 - プロダクション組織を新規または追加で作成する場合、環境タイプは【プロダクション】です。 - サンドボックス組織を作成する場合、環境タイプは最初は【サンドボックス】に設定されます。タイプは、開発、QA、またはサンドボックスに設定できます。 環境タイプ間で機能の違いはありません。 注: サブ組織の管理者であるが、その親組織の管理者ではない場合、ユーザーインターフェースでは、環境タイプを、任意のタイプに設定できます（自組織のライセンスで使用できないタイプにも設定可）。請求の問題を避けるために、ライセンスで使用できない環境タイプに変更しないでください。
説明	組織の説明（省略可能）。

プロパティ	説明
従業員数	組織内の従業員数。
このサブ組織への親組織のアクセスを拒否	<p>このオプションをオンにすると、親組織のユーザーは、親組織からサブ組織に切り替えられません。適切な権限を所有する親組織のユーザーは、サブ組織に次の変更のみを加えることができます。</p> <ul style="list-style-type: none"> - サブ組織の有効化および無効化 - サブ組織のライセンスの更新 - 組織の説明や CLAIR の推奨設定などのサブ組織のプロパティの編集 <p>このオプションはサブ組織の【組織】ページに表示されます。このオプションは、サブ組織の管理者がサブ組織にログインすると変更できます。このオプションは、親組織の管理者がサブ組織の組織のプロパティを表示するときは読み取り専用です。</p> <p>このオプションはデフォルトでオフになっています。</p>

住所情報

住所プロパティを使用して、組織の住所、郵便番号、都道府県、および国を指定します。

履歴情報

組織の履歴情報には、組織が作成された日時、組織を作成したユーザー、組織が最後に更新された日時、および組織を最後に更新したユーザーが表示されます。組織に変更を加えると、Informatica Intelligent Cloud Services で履歴情報が更新されます。

認証プロパティ

組織およびサブ組織の認証プロパティを設定できます。認証プロパティは、パスワード制限および IP アドレスフィルタリングを制御します。

ユーザーが匿名ユーザーのパスワードを作成または変更する場合は、パスワード制限が適用されます。パスワードの有効期限日を [Never (なし)] からある日数に変更すると、その日数より古いパスワードを持つユーザーは、次回 Informatica Intelligent Cloud Services にログインするときにパスワードを変更する必要があります。

次の表に、認証プロパティを示します。

プロパティ	説明
パスワードの最小文字数	有効なパスワードに必要なパスワードの最小文字数。4 から 12 文字の範囲でなければなりません。
最小混合文字数	<p>有効なパスワードに必要な文字タイプの最小数。</p> <p>パスワードには、次の文字セットを混在させることができます。</p> <ul style="list-style-type: none"> - 小文字の英字 - 大文字の英字 - 数字 - 特殊文字 <p>例えば、【最小混合文字数】 オプションを 1 に設定した場合、パスワードには 1 つ以上の文字セットが含まれている必要があります。【最小混合文字数】 を 2 に設定した場合は、パスワードに 2 つ以上の文字セットが含まれている必要があります。</p>
パスワードの再利用	ユーザーがパスワードを再利用できるかどうかを制御します。

プロパティ	説明
パスワードの有効期限が切れる	ユーザーがパスワードをリセットしなければならない頻度を設定します。
多要素認証の有効化	<p>ネイティブの人間のユーザーに対して多要素認証を有効にします。</p> <p>多要素認証が有効になっている場合、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と、電子メールで確認コードを受け取ります。それぞれの人間のユーザーの電子メールアドレスは有効である必要があります。</p> <p>【ユーザー】 ページで、ユーザーを人間のユーザーまたは人間以外のユーザーとして分類します。詳細については、「ユーザー管理」を参照してください。</p>
セッションのアイドルタイムアウト	<p>非アクティブによりユーザーのセッションがタイムアウトするまでの時間。Informatica Intelligent Cloud Services は、ユーザーがログアウトする 60 秒前に警告メッセージを表示します。</p> <p>デフォルトは 30 分です。</p>
認証タイプ	<p>ユーザーのログイン後に使用される認証タイプ。デフォルトは [セッション ID] です。</p> <p>[JSON Web トークン (JWT)] を選択した場合は、トークンの有効期限を選択します。デフォルトは 30 分です。</p> <p>認証タイプを変更すると、次のログイン時に新しいタイプが有効になります。この変更は、進行中のセッションには影響を与えません。</p> <p>JWT 認証タイプを使用する前に、トークンの有効期限が切れる前にトークンを更新するようにカスタムスクリプトを変更します。</p> <p>詳細については、JWT Support に関するナレッジベースの記事を参照してください。</p> <p>注:</p> <ul style="list-style-type: none"> - 【認証タイプ】 オプションは、2025 年 11 月 3 日から利用可能になります。 - 組織で B2B Gateway、API マネージャ、または REST V2 コネクタを使用している場合は、JWT 認証タイプを使用しないようにしてください。
信頼済み IP 範囲を使用	<p>IP アドレスフィルタリングを有効にします。</p> <p>IP アドレスフィルタリングは、信頼済み IP アドレス範囲とアカウントパスワードを使用し、未認証のユーザーが組織にアクセスできないようにします。IP アドレスフィルタリングを有効にすると、有効なログインのあるユーザーに、信頼済み IP アドレス範囲内の IP アドレスも必要になります。そうでない場合、そのユーザーは組織にログインできなくなります。</p> <p>このオプションを有効にした場合は、1 つ以上の信頼済み IP アドレス範囲も入力する必要があります。</p> <p>注: 信頼できる IP 範囲が有効になっているときにサーバーレスランタイム環境を作成する場合は、DMZ NAT ゲートウェイの IP アドレスを、信頼できる IP アドレスのリストに追加する必要があります。DMZ NAT ゲートウェイアドレスのリストについては、「ランタイム環境」を参照してください。</p>
許可された信頼済み IP 範囲	<p>組織にアクセスするためのログインに使用可能な信頼済み IP アドレス範囲。Informatica Intelligent Cloud Services では、IP version 4 (IPv4) と IP version 6 (IPv6) での IP アドレス形式がサポートされています。</p> <p>IP アドレスフィルタリングを有効にすると、信頼済み IP アドレス範囲のフィールドが表示されます。追加のアドレス範囲を入力するには、[+] をクリックします。</p> <p>IPv4 ネットワークと IPv6 ネットワークの両方でリソース間のシームレスな通信を確保するには、デュアルスタック構成を有効にします。例えば、仮想マシンが IPv4 または IPv6 のどちらか一方のネットワークタイプを使用し、コネクタをホストするサーバーが別のネットワークタイプを使用している場合は、仮想マシンでデュアルスタックを有効にして、ネットワークタイプに関係なくシームレスな通信を確保できるようにします。</p> <p>注: 無効な IP アドレス範囲を入力した場合、ユーザーは組織にアクセスできません。有効な IP アドレス範囲については、ネットワーク管理者にお問い合わせください。</p>

接続プロパティの保存場所

組織およびサブ組織の接続プロパティを保存する場所を設定できます。接続プロパティの保存場所を指定するには、**【組織】** ページで **【接続の資格情報】** を設定します。

接続プロパティは、次のいずれかの場所に保存できます。

Informatica Cloud

接続プロパティをクラウドに保存すると、接続プロパティが Informatica Intelligent Cloud Services リポジトリに保存され、いつでも利用できるようになります。接続は Informatica Intelligent Cloud Services キー管理サービスによって暗号化されます。

Informatica Intelligent Cloud Services では、標準のバックアップ手順の一環として、接続プロパティを定期的にバックアップします。

ローカルの Secure Agent

ファイアウォール内に存在する接続プロパティが必要な場合は、ローカルな Secure Agent を使用して接続プロパティを格納できます。このオプションを有効にすると、**【接続】** ページにリストされているすべての接続のプロパティがローカルのエージェントに保存されます。

注: FedRAMP の対象となる組織では、ローカル Secure Agent を使用した接続プロパティを保存できません。

このオプションを選択した場合は、1 つの Secure Agent を使用して接続プロパティを保存できます。接続プロパティは次のディレクトリに格納されます。

<Secure Agent のインストールディレクトリ>/apps/Data_Integration_Server/data

ローカルな Secure Agent を使用してプロパティを格納する場合は、タスクを実行し、ユーザーが接続を操作できるように、Secure Agent を実行する必要があります。データの損失を回避するために、接続プロパティを定期的にバックアップします。ベストプラクティスとして、接続プロパティの場所または暗号化キーを変更した後に接続プロパティをバックアップすることをお勧めします。

接続は Informatica Intelligent Cloud Services キー管理サービスによって暗号化されます。Informatica Intelligent Cloud Services は、CBC (Cipher Block Chaining) モードの 256 AES 暗号化を使用して接続を保存します。

AWS Secrets Manager や Azure Key Vault などの外部シークレットマネージャを使用して機密接続資格情報を保存する場合は、接続資格情報のストレージを **【Informatica Cloud】** に設定する必要があります。この操作を行うと、機密資格情報がシークレットマネージャから取得され、他の接続プロパティは Informatica Intelligent Cloud Services リポジトリに保存されます。接続資格情報をローカル Secure Agent に保存している場合は、シークレットマネージャを使用できません。シークレットマネージャの設定の詳細については、「[「シークレットマネージャの設定」 \(ページ 68\)](#)」を参照してください。

接続プロパティを格納する場所を変更できます。これにより、Informatica Intelligent Cloud Services は、接続プロパティを適切な場所に移動します。例えば、ライセンスの有効期限が切れるため、クラウドに接続を格納するように組織を設定するとします。Informatica Intelligent Cloud Services は、ローカルな Secure Agent から Informatica Intelligent Cloud Services へ接続プロパティを移動します。

フィンガープリント認証のプロパティ

Secure Agent の毎回の起動ごとに、指紋認証を適用できます。認証が失敗した場合に、電子メールアラートがトリガされても通常の操作は許可されるようにすることや、エージェントの起動が許可されないようにすることができます。

認証モードを設定するには、**【組織】** ページの **【フィンガープリント認証】** でオプションを設定します。

次のレベルの認証適用を設定できます。

適用および通知なし

フィンガープリントの適用を無効にして、電子メールアドレスを指定しません。

Secure Agent の起動時に認証チェックは実行されません。デフォルトではこのオプションが設定されています。

違反のみを報告

フィンガープリントの適用を無効にして、電子メールアドレスを指定します。電子メールの形式はチェックされますが、電子メールアドレスの有効性は検証されません。「admin@informaticacloud.com」というアドレスからのメールを許可するようにしてください。

Secure Agent の起動時に認証チェックが実行されます。フィンガープリントの不一致があった場合は、電子メール受信者への通知がトリガされますが、エージェントは正常に起動します。

認証一致を適用

フィンガープリントの適用を【オン】に設定し、電子メールアドレスを指定します。電子メールの形式はチェックされますが、電子メールアドレスの有効性は検証されません。

「admin@informaticacloud.com」というアドレスからのメールを許可するようにしてください。

フィンガープリントが一致しない場合は、電子メール受信者に通知が送信され、Secure Agent のログインが起動できなくなります。

注: 適用が有効になっている場合は、電子メールアドレスが要求されます。

フィンガープリントは、Secure Agent の初回起動時に、エージェントのホストマシンのデバイス属性を使用して作成されます。データは匿名化され、ハッシュされて一意のフィンガープリントが生成されます。適用なしから他のレベルの適用に切り替えた場合、Secure Agent は初回起動時にフィンガープリントを生成します。

同じマシンに Secure Agent を再インストールしても、フィンガープリントが変更されることはありません。

次の表に、フィンガープリントの適用によって Secure Agent が起動できない場合に発生するアクションを示します。

アクション	メッセージ
agentcore.log にエラーが記録されます	「内部エラー。エージェント<Secure Agent ID>のフィンガープリントが、以前保存された要求<要求 ID>の値と一致しません。」
電子メール通知が送信されます (電子メールアドレスが指定されている場合)	「組織<組織 ID>の<Secure Agent 名>という名前のエージェントへのログイン中に、フィンガープリントの不一致が発生しました。エージェントが最後にアクティブになったのは<日付 (UTC)>です。」

電子メール通知の設定

電子メール通知の送信先を特定のドメインに制限することができます。承認された電子メールアドレスに対してのみ通知が送信されるようにすることで、機密データが外部に共有される可能性が下がります。

次の電子メール通知設定を構成できます。

電子メールドメインをホワイトリストに登録

電子メールドメインの適用を有効または無効にします。この設定が有効になっている場合、通知は許可されたドメインの電子メールアドレスにのみ送信されます。この設定が無効になっている場合、通知は対象のすべての電子メールアドレスに送信されます。

許可された電子メールドメイン

通知の受信を許可する電子メールドメインを最大 10 件入力できます。電子メールドメインは例えば informatica.com などです。各ドメインを入力した後に Enter を押します。

データ統合サービスのプロパティ

データ統合サービスのプロパティは、データ統合で使用されます。次のプロパティを設定して、ジョブの通知に使用するタイムゾーンと電子メールアドレスを設定します。

以下のデータ統合サービスのプロパティを設定できます。

ジョブのプロパティ

次の表に、ジョブのプロパティを示します。

プロパティ	説明
スケジュールオフセット	標準の予定開始時刻でのサーバーのオーバーロードを防ぐために、予定開始時刻に追加されるわずかな時間。組織には、すべてのスケジュールに適用される単一のスケジュールオフセットがあります。スケジュールオフセットは、手動で開始されたタスクまたはタスクフローの開始時刻には影響しません。スケジュールオフセットは変更できません。スケジュールの詳細には表示されませんが、組織のスケジュールオフセットはすべてのスケジュールに設定した時間範囲に追加されます。これにより、スケジュール済みのタスクが想定どおりの頻度で実行されるようになります。例えば、8:00 a.m.から 12:00 p.m. まで毎時間タスクを実行するようにスケジュールを設定し、組織のスケジュールオフセットを 15 秒とすると、そのスケジュールで、8:00:15、9:00:15、10:00:15、11:00:15、および 12:00:15 にタスクが実行されます。
時間帯	電子メール通知でのジョブ実行タイムスタンプの表示に使用するタイムゾーン。

デフォルトの電子メール通知プロパティ

ジョブの失敗、警告、および成功メッセージに使用するデフォルトの電子メールアドレスを設定するための電子メール通知プロパティを構成します。有効な電子メールアドレスを 1 つ以上入力します。カンマ (,) またはセミコロン (;) を使用して電子メールアドレスを区切ります。

また、タスクレベルで電子メール通知のプロパティを設定することもできます。タスクまたはタスクフローで電子メール通知を設定すると、Informatica Intelligent Cloud Services は、組織に対して設定されたアドレスではなく、タスクまたはタスクフローのアドレスに電子メールを送信します。

Enterprise Data Catalog 統合プロパティ

組織がデータ統合でデータカタログ検出を使用している場合は、組織およびサブ組織に Enterprise Data Catalog 統合プロパティを設定できます。マッピング、同期タスク、およびファイル取り込みとレプリケーションタスクでカタログアセットを使用できるように、Enterprise Data Catalog 統合プロパティを設定します。

組織に設定する Enterprise Data Catalog 統合プロパティは、組織の全ユーザーが実行するデータカタログ検索に適用されます。組織にサブ組織が含まれる場合は、親組織と各サブ組織に異なる Enterprise Data Catalog 統合プロパティを設定できます。

以下の表に、Enterprise Data Catalog 統合プロパティを示します。

プロパティ	説明
カタログ URL	Enterprise Data Catalog サービスの URL。次の形式を使用します。 <code>http://<完全修飾ホスト名>:<ポート></code> URL の最後に「/ldmcatalog」を追加しないでください。
ランタイム環境	Enterprise Data Catalog からのデータの読み取りに使用する Secure Agent グループの名前。 選択したグループのエージェントは、Enterprise Data Catalog と通信できる必要があります。このため、Enterprise Data Catalog ホストがエージェントマシンと同じネットワーク内に存在するか、通信用の適切なポートが開かれている必要があります。
ユーザー名	Secure Agent が Enterprise Data Catalog にアクセスするために使用する Enterprise Data Catalog ユーザーアカウント。 このユーザーアカウントは、Enterprise Data Catalog 内のオブジェクトを表示および検索し、Enterprise Data Catalog REST API を使用して機能を実行する権限を持っている必要があります。
パスワード	Enterprise Data Catalog ユーザーアカウントのパスワード。
データカタログを表示	データ統合 のデータ統合ページを表示および非表示にします。

サブ組織

組織に適切なライセンスがある場合は、組織内に 1 つ以上のサブ組織を作成できます。企業内のさまざまなビジネス環境を表すサブ組織を作成します。例えば、組織内のさまざまなクライアントや部門を表すサブ組織を作成できます。

プロダクション組織、追加プロダクション組織、またはサンドボックス組織からサブ組織を作成できます。

サブ組織を作成すると、サブ組織を作成するために使用する組織が親組織になります。各サブ組織の親組織は 1 つのみで、別のサブ組織を含めることはできません。

注: サブ組織は、親組織と同じ POD（デプロイメントポイント）に存在している必要があります。CI/CD（継続的統合/継続的デプロイメント）指向のアプローチでは、すべてのサブ組織が機能リリースを同時に受け取るため、同じメンテナンス期間中に問題やダウンタイムが発生する可能性があります。

組織のライセンスは、作成できるサブ組織の数を制御します。この数を増やすには、Informatica グローバルカスタマサポートにお問い合わせください。

サブ組織の作成には、次の利点があります。

サブ組織のライセンスは、個別に管理するか、親組織のライセンスと自動的に同期できます。

各サブ組織は、サブ組織を作成するためのライセンスとバンドルライセンスを除く、親組織からのすべての機能、コネクタ、およびカスタムライセンスを継承します。

組織のライセンスに基づいて、次のいずれかの方法でサブ組織のライセンスを管理することができます。

- サブ組織のライセンスを個別に管理する。親組織の管理者は、それぞれのサブ組織のライセンスの有効期限を無効化、有効化、および変更することができます。1 つのサブ組織を変更した場合でも、他のサブ組織に影響が及ぶことはありません。

- サブ組織のライセンスを親ライセンスと自動同期させる。

ユーザーとアセットを個別に管理できます。

各サブ組織には、ユーザーとアセットの独自のセットがあります。

サブ組織で作成するユーザーは、サブ組織に固有のもので、親組織や他のサブ組織にはログインできません。親組織の管理者と、サブ組織のアクセス特権を持つ親組織のユーザーのみが、親組織およびすべてのサブ組織にアクセスできます。

マッピングやタスクなどのアセットも組織内で固有のもので、アセットは、サブ組織間、または親組織と任意のサブ組織間では共有されません。組織間でアセットを移行する場合は、片方の組織からアセットをエクスポートし、別の組織にインポートします。

ランタイム環境を共有できます。

親組織の管理者は、Secure Agent グループをサブ組織と共有できます。Secure Agent グループを共有すると、サブ組織のユーザーは、グループ内の Secure Agent でジョブを実行できます。

親組織またはサブ組織のユーザーは、その組織またはサブ組織に属する Secure Agent のみを使用できます。サブ組織のユーザーは、親組織に属する Secure Agent を使用することはできません。

注: グループ内のすべてのエージェントでデータ統合サーバーのサービスのみを実行する場合は、Secure Agent グループを共有します。共有 Secure Agent グループで他のエージェントサービスのジョブを実行することはできません。

共有 Secure Agent グループの詳細については、「ランタイム環境」を参照してください。

バンドルを使用してリソースを共有できます。

バンドルデプロイメント機能を使用すると、バンドルを親組織からサブ組織にシームレスにプッシュできます。これにより、組織構造全体にリソースと機能がスムーズかつ効率的に分散されます。

バンドルの詳細については、「[第 7 章、「バンドル管理」 \(ページ 94\)](#)」を参照してください。

集計された IPU 消費メトリックを表示できます。

各サブ組織の IPU (Informatica Processing Unit) 消費メトリックは集計され、それぞれの親組織にロールアップされます。この統合により、リソースがどのように利用されているかについての明確な概要を取得することができます。消費データは、主要なプロダクション組織に到達するまで、組織階層内で統合およびロールアップされます。

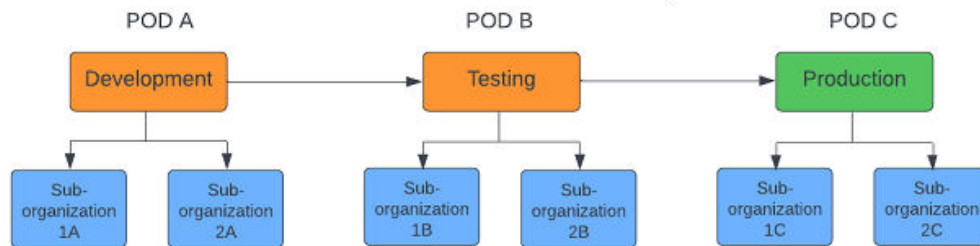
ログインせずに組織間を切り替えることができます。

サブ組織を表示する特権を持つ親組織のユーザーは、ログアウトせずに組織間を切り替えたり、Informatica Intelligent Cloud Services にログインし直したりすることができます。

サブ組織の例

CI/CD のベストプラクティスを遵守するには、開発、テスト、プロダクションなど、ビジネスのさまざまな領域を表す個別のサブ組織を作成する必要があります。これを実現するには、最初に開発、テスト、プロダクション用に個別の親組織を作成します。POD または組織が使用できなくなった場合に機能が停止することを防ぐために、各親組織は異なる POD 上にあることが理想的です。各親組織の下に、さまざまなクライアントまたは部門を表すサブ組織を作成します。

次の図に、推奨される階層を示します。



この階層を使用すると、開発からテストに移行し、プロダクションで終了する、環境間の更新と改善の段階的なフローが保証されます。この方法で環境を分離すると、意図しない変更が他のワークフローステージに影響を与える可能性を減らすことができます。

OEM（Original Equipment Manufacturer）の場合、サブ組織は個々のクライアントを表します。この構造により、OEM はライセンスの制御と監視を維持できる一方で、個々のクライアントは開発、テスト、プロダクションプロセスを管理できます。

企業の場合、サブ組織はさまざまな部門を表します。この構造により、管理上の監視が簡素化され、部門によって設定されたアセット、プロセス、その他のリソースに親組織がアクセスできるようになります。

サブ組織の追加

サブ組織を追加するには、新しいサブ組織を作成するか、既存の組織をリンクします。

次のいずれかの方法でサブ組織を追加できます。

サブ組織の作成。

親組織にする組織にログインし、サブ組織を作成します。新しいサブ組織は、親組織に自動的にリンクされます。

既存の組織のリンク。

リンク元の組織が親組織になり、リンク先の組織がサブ組織になります。

サブ組織の作成

親組織の管理者はサブ組織を作成できます。

サブ組織を作成するには、管理者ロールが割り当てられたネイティブユーザー、または「サブ組織 - 作成」および「サブ組織 - 表示」特権を持つネイティブユーザーである必要があります。

サブ組織を作成するには、次の手順を実行します。

1. 親組織にする組織にログインします。
2. 管理者を開いて【組織】を選択します。
3. 【サブ組織】タブを開き、【新しいサブ組織】をクリックします。
4. サブ組織のプロパティを入力し、【保存】をクリックします。

サブ組織を作成したら、ライセンスを確認し、他の人が使用できるようにランタイム環境、ユーザーアカウント、および接続を構成します。

組織のリンク

既存の組織をリンクすることで、サブ組織を作成できます。リンク元の組織が親組織になり、リンク先の組織がサブ組織になります。

組織をリンクするには、リンクする組織の組織 ID が必要になります。この情報は、**【組織】** ページで確認できます。

注: 親組織が持っていないライセンスを持つサブ組織をリンクすると、サブ組織はそのライセンスを失います。次のすべての条件が該当する場合に、組織をリンクできます。

- ユーザーアカウントと組織があること。
- 組織は別の組織の親でもサブ組織でもありません。
- 親組織の管理者であること、およびサブ組織を作成するためのライセンスが親組織にあること。
- サブ組織としてリンクする組織に、サブ組織を作成するためのライセンスがないこと。

後から組織をリンク解除できます。

組織をリンクするには:

1. 親組織にする組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** タブを開き、**【サブ組織をリンク】** をクリックします。
4. **【サブ組織をリンク】** ダイアログボックスで、次の情報を入力します。
 - リンクする組織の組織 ID。
 - サブ組織として設定する組織の管理者のユーザー名とパスワード。
5. 組織をリンクするには、**【サブ組織をリンク】** をクリックします。
組織が **【サブ組織】** ページに表示されます。

サブ組織の削除

サブ組織を削除するには、組織のリンクを解除するか、サブ組織を削除します。

次のいずれかの方法でサブ組織を削除できます。

親組織からの既存サブ組織のリンク解除。

リンクされていないサブ組織は、スタンドアロン組織になります。スタンドアロン組織は、別の親組織にリンクすることや元の親組織に再リンクすることができます。リンクされていない組織について、サブ組織を作成するためのライセンスを取得すると、それを別のサブ組織の親組織にすることができます。

サブ組織の削除。

サブ組織を削除すると、その組織に関連付けられているすべてのアセットとデータが削除されます。使用量ベースのライセンスをお持ちの場合、サブ組織は削除後も現在の請求期間中に引き続き IPU を消費します。詳細については、「[「無効化されたサブ組織および削除されたサブ組織での IPU 使用率」 \(ページ 37\)](#)」を参照してください。

サブ組織のリンク解除

親組織からサブ組織のリンクを解除することができます。組織のリンクを解除した後は、別の親組織にリンクする予定がある場合を除いて、リンク解除した組織を必要なライセンスで更新します。

次のすべての条件に当てはまる場合は、サブ組織のリンクを解除できます。

- リンク解除するサブ組織に対する管理者アカウントを持っていること。
- 親組織の管理者であること、およびサブ組織を作成するためのライセンスが親組織にあること。
- リンクを解除するサブ組織内のアセットは、Secure Agent グループの共有をランタイム環境として使用しません。サブ組織内の任意のアセットが Secure Agent グループの共有をランタイム環境として使用している場合は、サブ組織のリンクを解除する前に、別のランタイム環境を使用するようにアセットを更新します。

注: この条件はアプリケーション取り込みとレプリケーションとデータベース取り込みとレプリケーションには適用されません。これは、アプリケーション取り込みとレプリケーションとデータベース取り込みとレプリケーションは共有ランタイム環境をサポートしていないためです。

サブ組織のリンクを解除するには:

1. 親組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** タブを開きます。
4. リンクを解除するサブ組織の **【アクション】** メニューを展開し、**【リンク解除】** を選択します。
5. **【リンク解除】** ダイアログボックスで、管理者ロールを持つサブ組織内のユーザーのユーザー名とパスワードを入力します。
6. **【リンク解除】** をクリックします。
サブ組織が、親組織からリンク解除されます。

サブ組織の削除

サブ組織を削除できます。サブ組織を削除すると、関連付けられたすべてのデータが完全に削除されます。使用量ベースのライセンスをお持ちの場合、サブ組織のメタリング情報は親組織に保持されます。

親組織の管理者であれば、サブ組織を削除できます。

1. 親組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** タブを開きます。
4. リンクを解除するサブ組織の **【アクション】** メニューを展開し、**【削除】** を選択します。

注: 使用量ベースのライセンスをお持ちの場合、サブ組織は削除が完了した請求期間が終了するまで引き続き IPU を消費します。詳細については、「[「無効化されたサブ組織および削除されたサブ組織での IPU 使用率」 \(ページ 37\)](#)」を参照してください。

サブ組織の無効化または有効化

親組織の管理者である場合は、サブ組織を無効または有効にできます。

サブ組織の作成時に、デフォルトでサブ組織は有効化されます。サブ組織と別個の使用許諾契約がある場合や、使用許諾契約の有効期限が切れた場合、サブ組織を無効にすることがあります。サブ組織は、無効化後に再度有効にできます。

サブ組織は、サブ組織の管理者がサブ組織への親組織のアクセスをブロックしている場合も、無効または有効にできます。

次のアクションを実行できます。

サブ組織の無効化

サブ組織を無効にすると、その組織は残りますが、サブ組織のユーザーはサブ組織にログインできない、または REST API を介してサブ組織にアクセスします。サブ組織内のスケジュールされたジョブは実行されません。

使用量ベースのライセンスをお持ちの場合は、サブ組織を無効にしてもそのサブ組織は引き続き IPU を消費します。詳細については、「[「無効化されたサブ組織および削除されたサブ組織での IPU 使用率」 \(ページ 37\)](#)」を参照してください。

サブ組織の有効化

サブ組織を有効にすると、サブ組織のユーザーはサブ組織にログインでき、自分のユーザーロールに基づいてアセットにアクセスし、タスクを実行できます。適切な権限を持つユーザーは、REST API を介してサブ組織にアクセスできます。スケジュールされたジョブは、スケジュールに従って再開されます。

サブ組織を **【組織】** ページの **【サブ組織】** タブで無効または有効にします。サブ組織の **【アクション】** メニューで、**【無効】** または **【有効】** を選択します。

別の組織への切り替え

親組織の管理者またはサブ組織の表示権限を持つ親組織のユーザーの場合は、これらの組織間で切り替えることができます。Informatica Intelligent Cloud Services をログアウトして、もう一度ログインする必要はありません。

注: 親組織から下位組織に切り替えると、下位組織で次の操作を実行できなくなります。

- データ転送タスクの作成またはインポート
- 動的マッピングタスクの作成またはインポート
- タスクフローの作成、検証、パブリッシュ、および実行
- タスクフローのエクスポートとインポート

別の組織に切り替えるには:

- ▶ 右上隅の **【組織】** メニューから、表示する組織を選択します。

サブ組織への親組織のアクセスを拒否

サブ組織の管理者である場合は、サブ組織への親組織のアクセスを拒否できます。

サブ組織へのアクセスを拒否すると、親組織のユーザーは、親組織からサブ組織に切り替えられません。適切な権限を所有する親組織のユーザーは、サブ組織に次の変更のみを加えることができます。

- サブ組織の有効化および無効化
- サブ組織のライセンスの更新
- 組織の説明や CLAIRE の推奨設定などのサブ組織のプロパティの編集

親組織のサブ組織へのアクセスを拒否するには、管理者としてサブ組織にログインします。**【組織】** ページで、**【このサブ組織への親組織のアクセスを拒否】** オプションを有効にします。

サブ組織のアドオンコネクタ

サブ組織でアドオンコネクタを使用するには、親組織にコネクタをインストールする必要があります。サブ組織にアドオンコネクタをインストールすることはできません。

サブ組織は、親組織からすべてのコネクタライセンスを継承します。サブ組織で特定のコネクタを使用しない場合は、サブ組織のコネクタライセンスを無効にします。サブ組織のライセンスの編集と無効化に関する詳細については、[「サブ組織のライセンスの編集」](#) (ページ 103) を参照してください。

サブ組織でのアセットのエクスポートとインポート

サブ組織では、次の方法でアセットをエクスポートおよびインポートします。

- サブ組織にログインして、サブ組織からアセットをエクスポートおよびインポートします。
- 親組織の管理者は親組織にログインし、サブ組織に切り替えて、データ統合アセットをインポートまたはエクスポートできます。

注: この条件は、タスクフローとアプリケーション統合アセットには適用されません。

サブ組織の機能とサービスサポートマトリックス

サブ組織の機能は、Informatica サービスによって異なります。

次の表に、各サービスの機能を示します。

サービス	ライセンス機能	メータリング機能	バンドル	共有 Secure Agent	アセットアクセス
クラウドデータ統合 (CDI)	親組織には、サブ組織を作成するためのライセンスがあります。	親組織は、機能ベースのライセンスを使用する必要があります。	使用可能	サポート	サポートされていません。
クラウドアプリケーション統合 (CAI)	親組織には、サブ組織を作成するためのライセンスがあります。	親組織は、機能ベースのライセンスを使用する必要があります。	使用可能	サポートされていません	サポートされていません
Cloud データガバナンスとデータカタログ (CDGC)	親組織には、サブ組織を作成するためのライセンスがあります。	親組織は、機能ベースのライセンスを使用する必要があります。	該当なし	サポートされていません	サポートされていません
Master Data Management (MDM)	親組織には、サブ組織を作成するためのライセンスがあります。	親組織は、機能ベースのライセンスを使用する必要があります。	該当なし	サポートされていません	サポート
Cloud データ品質 (CDQ)	親組織には、サブ組織を作成するためのライセンスがあります。	親組織は、機能ベースのライセンスを使用する必要があります。	使用可能	サポート	サポートされていません。

追加プロダクション組織とサンドボックス組織

組織に適切なライセンスがある場合は、プロダクション組織から追加プロダクション組織とサンドボックス組織を作成できます。これらの組織は、アセットやユーザーごとに別の組織を用意しつつ、すべての IPU の使用状況をプロダクション組織から管理する場合に作成します。追加プロダクション組織とサンドボックス組織は、プロダクション組織に自動的にリンクされます。

以下のタイプの組織を作成できます。

追加プロダクション組織

これは別個のプロダクション組織です。これは、プロダクション組織と同じように機能します。ただし、追加プロダクション組織から、さらに追加プロダクション組織やサンドボックス組織を作成することはできません。

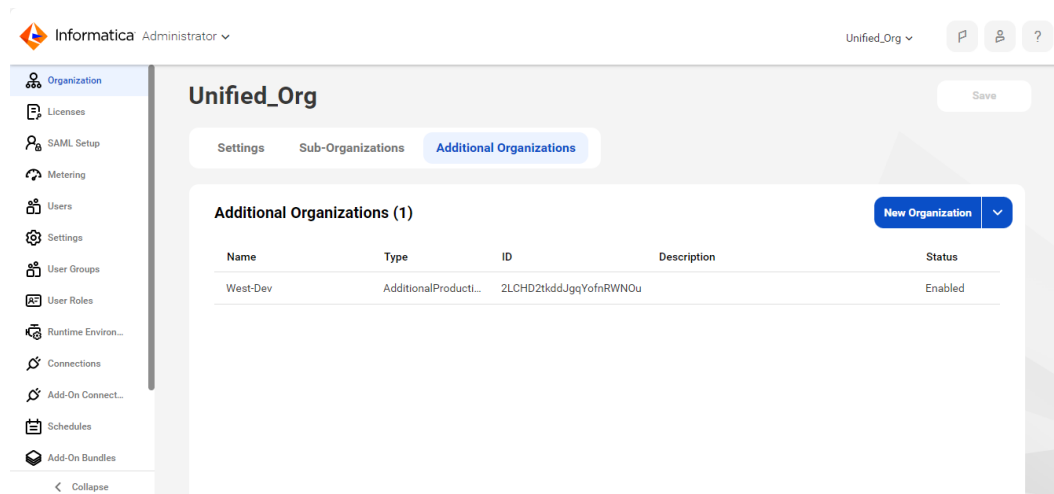
サンドボックス組織

これは、アセットの開発とテストに通常使用される組織です。サンドボックス組織と追加プロダクション組織との間に、機能上の違いはありません。

追加プロダクション組織とサンドボックス組織は、プロダクション組織からは相互に完全に独立しています。これらが、アセット、接続、ランタイム環境、またはユーザーを共有することはありません。ただし、これらの間でアセットをエクスポートおよびインポートすることはできます。

作成する追加プロダクション組織とサンドボックス組織は、プロダクション組織からすべてのライセンスとエディションを継承します。プロダクション組織が、サブ組織を作成するライセンスを持っている場合、追加プロダクション組織とサンドボックス組織の管理者は、組織のサブ組織を作成できます。

追加プロダクション組織とサンドボックス組織は、プロダクション組織の【組織】ページにある【追加組織】タブに表示されます。次の画像は、【追加組織】タブを示しています。



追加プロダクション組織またはサンドボックス組織を作成するときは、組織名と組織管理者のユーザー名を入力する必要があります。このユーザーアカウントを使用して新しい組織にログインし、他のユーザーやアセットを追加できます。

追加プロダクション組織またはサンドボックス組織を作成した後、これらを無効にしたり削除したりすることはできません。また、プロダクション組織からリンクを解除することもできません。これを行う必要がある場合は、Informatica グローバルカスタマサポートにお問い合わせください。

追加の組織の作成

【組織】 ページの【追加組織】 タブで、追加プロダクション組織またはサンドボックス組織を作成します。

注: 追加プロダクション組織またはサンドボックス組織を作成すると、組織に対して追加の IPU 料金が発生する場合があります。

追加の組織を作成するには、管理者ロールを持つネイティブユーザーであるか、「AdditionalOrg 作成」および「AdditionalOrg 表示」 特権を持つネイティブユーザーである必要があります。

追加の組織を作成するには、次の手順を実行します。

1. プロダクション組織にログインします。
2. 管理者を開いて【組織】 を選択します。
3. 【追加組織】 タブを開きます。
4. 【新しい組織】 をクリックし、【追加プロダクション組織】 または【サンドボックス組織】 を選択します。
5. 【新しい組織】 ページで、新しい組織の管理者のユーザー名と組織名を入力します。
ユーザー名は一意にする必要があります。これは、有効な電子メールアドレスにするか、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します。
6. 必要に応じて、説明、従業員数、および住所情報を入力します。
7. 【保存】 をクリックします。

【追加組織】 タブに新しい組織が表示され、ステータスが【有効】 になります。Informatica Intelligent Cloud Services から、新しい組織管理者向けのウェルカムメールが電子メールアドレスに送信されます。

8. プロダクション組織からログアウトします。
9. ウェルカムメールにある【アカウントの確認】 リンクをクリックし、プロンプトに従って、新しい組織管理者のアカウントをアクティブ化します。

アカウントのアクティブ化が完了したら、Informatica Intelligent Cloud Services により、新しい組織へのログインが実行されます。

新しい組織にログインした後は、他のユーザーを追加して、ランタイム環境、接続、およびアセットを作成できます。

第 3 章

メータリング

組織およびサブ組織のメータリング情報を表示できます。メータリング情報は【メータリング】ページに表示されます。

【メータリング】ページの情報は、組織の使用許諾契約に応じて異なります。

- 使用量ベースのライセンスを持っている場合、【メータリング】ページには、現在の請求サイクルに購入、消費した Informatica プロセッシングユニット（IPU）の数と、残りの IPU 数を含むダッシュボードが表示されます。各サービスに対する使用済みの IPU の数を示すメーターを表示することもできます。
- 機能ベースのライセンスを持っている場合、【メータリング】ページには、組織が使用したコンピューティングリソースの量および残りのコンピューティングリソースの量が表示されます。また、ページには、組織のライセンスを通じて設定された使用制限が表示されます。IPU は機能ベースのライセンスには適用されないため、このページには IPU に関する情報は表示されません。【メータリング】ページには、ライセンスに基づいて、ダッシュボードまたはテーブルとして情報が表示されます。

Informatica のプロセッシングユニットのメトリック

組織でインテリジェントクラウドデータ管理機能を利用している場合、ライセンスは Informatica Intelligent Cloud Services の使用量に基づきます。

Informatica プロセッシングユニット（IPU）は、Informatica Intelligent Cloud Services のスカラ（コンピューティングユニットや処理済みのイベント数など）の使用に対する前払いに使用されるクレジットの単位です。【メータリング】ページで IPU のバランスと使用状況を監視できます。

管理者ロールを持つユーザーは、組織が 25、50、75、95、および 100%という IPU 消費率のしきい値を超えた場合に、電子メールで通知を受け取ります。

IPU メトリックの表示

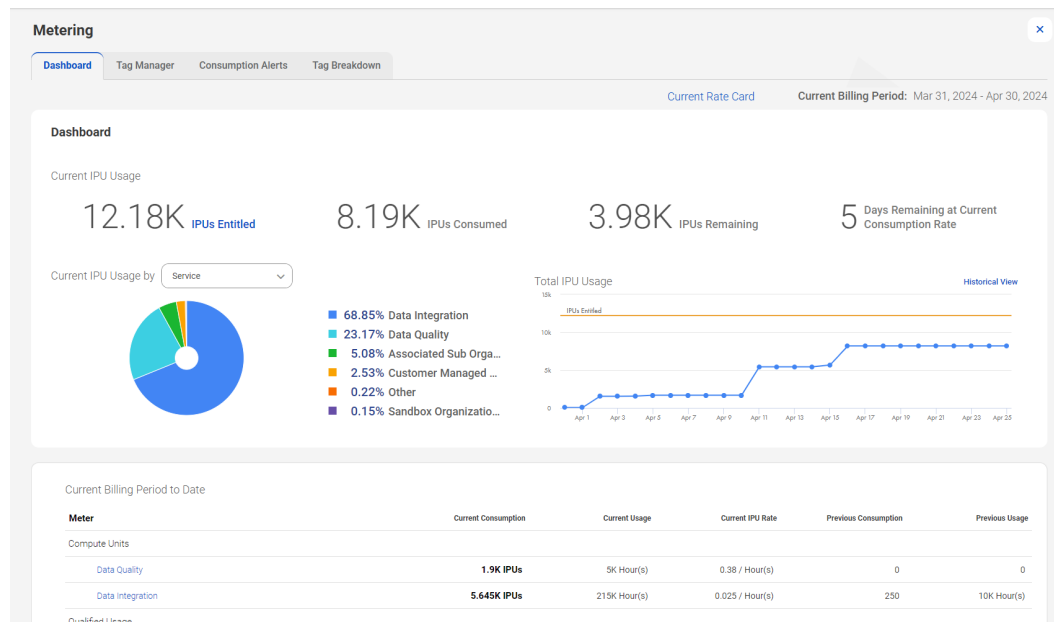
【メータリング】ページで IPU メトリックを表示します。【メータリング】ページには、ダッシュボードビューに IPU 情報が表示されます。

ダッシュボードには、ログインしている組織と、サブ組織、追加のプロダクション組織、サンドボックス組織などのリンクされた組織の IPU 使用率が表示されます。

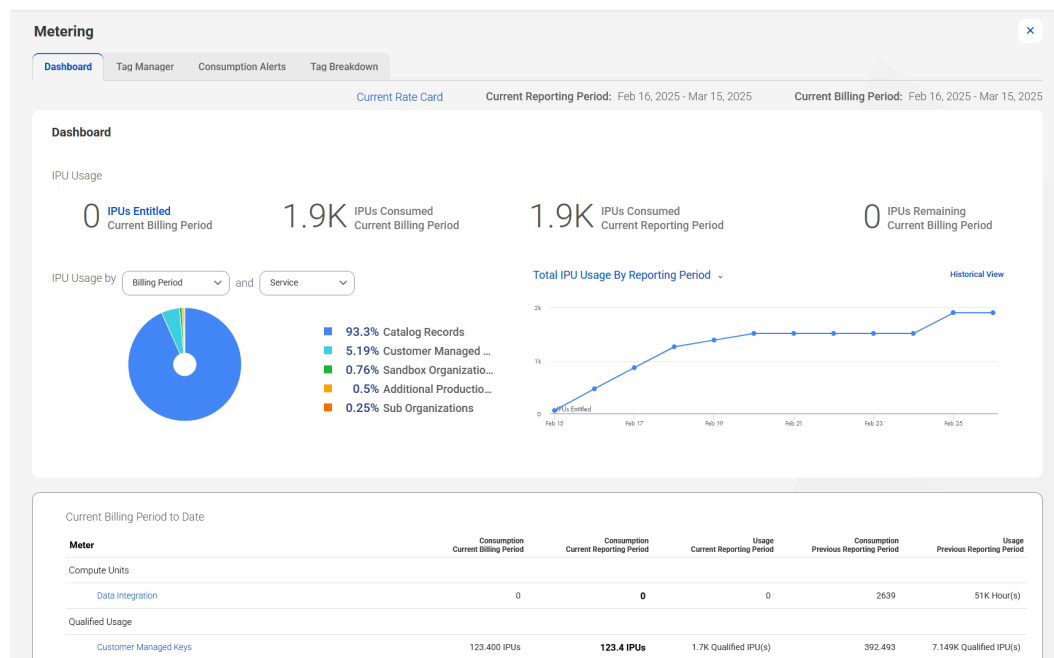
【メータリング】ページのビューには、請求期間と、該当する場合はレポート期間に基づいたメトリックが表示されます。請求期間とレポート期間は、契約期間とは異なります。請求期間とレポート期間は協定世界時（UTC）に基づくため、現在の請求期間と現在のレポート期間は、タイムゾーンと比較して過去または将来の日付として表示される場合があることに注意してください。

【メータリング】ページからレポートをダウンロードすることができます。ダウンロードできるデータの詳細については、[「IPU メトリックレポート」](#)（ページ 38）を参照してください。

次の図は、月単位の請求期間が設定されているアカウントのメータリングダッシュボードを示しています。



次の画像に、年次請求期間が設定されているアカウントのメータリングダッシュボードを示します。



注: [メータリング] ページには、小数点以下3桁に四捨五入された IPU 使用状況メトリックが表示されます。詳細なダウンロードレポートには、正確なメトリックが保存されます。

IPU の請求期間

IPU の請求期間は、月次または年次に設定することができます。月次請求に表示される【メータリング】ページの内容は、年次請求のページとは若干異なります。

月次請求

請求期間が月次の場合は、IPU 情報を請求期間ごとに表示することができます。メータリング 1.0 モデルでは、月次請求が使用されます。

月次請求のメータリングダッシュボードには、次のパネルが表示されます。

現在の IPU 使用量

【現在の IPU 使用率】パネルには、次の情報が表示されます。

- 現在の請求期間の、権限が与えられている IPU の合計数、使用された IPU の合計数、残りの IPU の合計数。
- 現在の使用量に基づく、IPU バランスがなくなるまでの残りの推定日数。
- 請求期間の IPU 使用率。使用率は、メーター、プロジェクト、またはフォルダ別に表示できます。プロジェクトまたはフォルダ別に使用率を表示する場合は、アセットの場所ごとに過去の使用率を表示するというオプションがあります。
- 1 日あたりの IPU の総使用率を示すグラフ。

IPU 使用量に関する履歴情報を表示するには、【履歴ビュー】をクリックし、含める請求期間の数を選択します。

現在の請求期間

【現在の請求期間】パネルには、ほぼすべてのメーターに関する次のような情報が表示されます。

- IPU レート。
- 現在の請求期間と以前の請求期間に消費された IPU。
- 現在の請求期間と前の請求期間のコンピューティングユニット、データボリューム、処理された行などのスカラに基づく使用率。

メーターの詳細を表示するには、メーター名をクリックします。詳細ページには、IPU およびスカラごとの現在の使用率、選択した数の請求期間における IPU 使用率を示す使用履歴グラフ、および日付ごとの詳しい使用率情報が表示されます。

年次請求

請求期間が年次の場合は、それぞれの請求期間、または各月のレポート期間ごとに IPU 情報を表示することができます。Flex IPU メータリングモデルでは、年次請求が使用されます。

年次請求のメータリングダッシュボードには、次のパネルが表示されます。

IPU 使用率

【IPU 使用率】パネルには、次の情報が表示されます。

- 現在の請求期間の、権限が与えられている IPU の合計数、使用された IPU の合計数、残りの IPU の合計数。
- 現在のレポート期間に使用された IPU の合計数。レポート期間は当月です。
- 請求期間またはレポート期間の IPU 使用率。使用率は、メーター、プロジェクト、またはフォルダ別に表示できます。プロジェクトまたはフォルダ別に使用率を表示する場合は、アセットの場所ごとに過去の使用率を表示するというオプションがあります。

- 請求期間またはレポート期間における 1 日あたりの IPU の総使用率を示すグラフ。

IPU 使用量に関する履歴情報を表示するには、**【履歴ビュー】** をクリックし、含めるレポート期間の数を選択します。

現在の請求期間

【現在の請求期間】 パネルには、ほぼすべてのメーターに関する次のような情報が表示されます。

- 現在の請求期間に使用された IPU の数。
- 現在のレポート期間と前のレポート期間に使用された IPU の数。
- 現在のレポート期間と前のレポート期間のコンピューティングユニット、データボリューム、処理された行などのスカラに基づく使用率。

各メーターの詳細を表示するには、メーター名をクリックします。詳細ページには、IPU およびスカラごとの現在の使用率、選択した数のレポート期間における IPU 使用率を示す使用履歴グラフ、およびレポート期間ごとの詳しい IPU 使用率情報が表示されます。

複数の組織の IPU メトリック

サブ組織、サンドボックス組織、および追加のプロダクション組織の IPU 使用率情報を表示できます。

メータリングダッシュボードの **【現在の請求期間】** パネルでは、組織のメーターに関する次のような情報を確認できます。

メーター	説明
サンドボックス組織	ログインしている組織に直接リンクされているサンドボックス組織の合計 IPU 使用率と消費率がスカラごとに表示されます。 各サンドボックス組織の詳細を示す詳細ページへのリンクが含まれています。
サブ組織	ログインしている組織に直接リンクされているサブ組織の合計 IPU 使用率と消費率がスカラごとに表示されます。 各サブ組織の詳細を示す詳細ページへのリンクが含まれています。
追加のプロダクション組織	ログインしている組織に直接リンクされている追加のプロダクション組織の合計 IPU 使用率と消費率がスカラごとに表示されます。 追加の各プロダクション組織の詳細を示す詳細ページへのリンクが含まれています。
関連するサブ組織の IPU 使用率	プロダクション組織にログインすると、サンドボックスまたは追加のプロダクション組織のすべてのサブ組織の合計 IPU 使用率と、サブ組織あたりの 6IPU のレートが表示されます。

例えば、プロダクション組織に 2 つのサンドボックス組織と 1 つの追加のプロダクション組織があるとしします。サンドボックス組織と追加のプロダクション組織には、それぞれサブ組織があります。

プロダクション組織にログインすると、次のようなメータリング情報が表示されます。

- プロダクション組織の IPU 使用率、スカラ別の消費率、および詳細なメータリングデータ。
- 2 つのサンドボックス組織の IPU 使用率とスカラ別の消費率の合計。
- 追加プロダクション組織の IPU 使用率とスカラ別の消費率。
- サンドボックス組織および追加のプロダクション組織のサブ組織の合計 IPU 使用率。

サンドボックス組織の 1 つにログインすると、次のようなメータリング情報が表示されます。

- サンドボックス組織の IPU 使用率、スカラ別の消費率、および詳細なメータリングデータ。

- サンドボックス組織のサブ組織におけるスカラ別の IPU 使用率と消費率。

注: リンクされた組織のその日の最初の IPU 使用率がプロダクション組織の **【メータリング】** ページに反映されるまでには、最大 10 分の遅れが発生する可能性があります。

IPU スカラ

IPU はスカラ値に基づいています。各サービスには適切なスカラが使用されます。

例えば、データ統合の使用量はコンピューティングユニットで測定され、Cloud 統合ハブの使用量は、処理済みのイベント数によって測定されます。

次の表に、プライマリスカラとその測定単位を示します。

スカラ値	測定単位	説明
API 呼び出し	100 万件の API 呼び出し	カスタム API 呼び出しの数。
コンピューティングユニット	時間	使用または消費された処理容量。
接続	番号	接続数。 組織がシークレットマネージャを使用して接続資格情報を保存する場合、この数値は、シークレットマネージャから資格情報を取得するように構成された接続の数を表します。
データボリューム	ギガバイト	転送または変換されたデータの量、あるいは組み込まれたデータの量。
処理済みのイベント数	イベント	中間ストレージレイヤにアクセスするデータのインバウンドインスタンスとアウトバウンドインスタンス。
処理されたオブジェクト	オブジェクト (1,000 件単位)	PowerCenter アセットの評価中および Cloud データ統合アセットへの変換中に処理されたオブジェクトの数。
組織	Number	追加プロダクション組織、サブ組織、およびサンドボックス組織の数。 サブ組織を削除した場合、この数には次の請求期間が始まるまでに削除したサブ組織が含まれます。
修飾の使用率	修飾 IPU	組織で使用されている合計 IPU のうち、顧客管理対象キーを有効にしている IPU の割合。 この値は、毎日リセットされるのではなく、請求期間の終了時にリセットされます。
クエリ	1000 件のクエリ	送信されたクエリの数。
保存されているレコード数	レコード	保存されたレコード数。 この値は、毎日リセットされるのではなく、請求期間の終了時にリセットされます。
処理済みの行数	100 万行	基になるデータベースログから処理された行数。
タスクフローの実行	実行	タスクフローの実行回数。

IPU メーター

IPU メーターは、インテリジェントクラウドデータ管理に含まれるサービスと機能です。

次の表に、IPU メーターと適用可能なスカラを示します。

メーター	スカラ値
アドレス検証 - バッチ（認証済みの検証と提案を含む） - ジオコーディング	処理済みの行数
詳細データ統合	コンピューティングユニット
高度なサーバーレスとの詳細データ統合	コンピューティングユニット
詳細データ品質	コンピューティングユニット
高度なサーバーレスとの詳細データ品質	コンピューティングユニット
API 管理	API 呼び出し
アプリケーションの統合	コンピューティングユニット/API 呼び出し 注: Turbo モードで実行されているプロセスの IPU メーターは、メータリングダッシュボードの【API 呼び出し】セクションの【アプリケーション統合】リンクに表示されます。アプリケーション統合の API 呼び出しメーターは、1,000 コール単位で測定されます。 標準モードで実行されているプロセスの IPU メーターは、メータリングダッシュボードの【コンピューティングユニット】セクションの【アプリケーション統合】リンクに表示されます。
高度なサーバーレスとのアプリケーション統合	コンピューティングユニット/API 呼び出し 注: Turbo モードで実行されているプロセスの IPU メーターは、メータリングダッシュボードの【API 呼び出し】セクションの【高度なサーバーレスとのアプリケーション統合】リンクに表示されます。アプリケーション統合の API 呼び出しメーターは、1,000 コール単位で測定されます。 標準モードで実行されているプロセスの IPU メーターは、メータリングダッシュボードの【コンピューティングユニット】セクションの【高度なサーバーレスとのアプリケーション統合】リンクに表示されます。
B2B Gateway	コンピューティングユニット
B2B & 業界ソリューション	コンピューティングユニット
PowerCenter 用 Cloud データ統合	コンピューティングユニット
PowerCenter 用 Cloud データ統合 - 変更データキャプチャ	処理済みの行数
PowerCenter 用 Cloud データ統合 - プッシュダウンの最適化	処理済みの行数

メーター	スカラ値
顧客管理対象キー	修飾の使用率
データアクセス管理 - ポリシープッシュダウン	1日あたりの保存されているアセット数
データアクセス管理 - クエリ	API 呼び出し
データアクセス管理 - 処理済みの行数	処理済みの行数
データガバナンス&カタログ - カタログレコード	保存されているレコード数
データガバナンス&カタログ - ガバナンスレコード	保存されているレコード数
データガバナンス&カタログ - メタデータレコード消費数	API 呼び出し
データガバナンス&カタログ - カタログソースの実行	コンピューティングユニット
データガバナンス&カタログ - サーバーレスでのカタログソースの実行	コンピューティングユニット
データ統合	コンピューティングユニット
データ統合 - 変更データキャプチャ	処理済みの行数
高度なサーバーレスとのデータ統合	コンピューティングユニット
データマーケットプレイスレコード	保存されているレコード数
データマスキング	コンピューティングユニット
データ品質	コンピューティングユニット
高度なサーバーレスとの Data Quality	コンピューティングユニット
業種別ソリューション	コンピューティングユニット
INFACore	コンピューティングユニット
統合ハブ	処理済みのイベント数
一括取り込みアプリケーション（アプリケーション取り込みとレプリケーション用）	データボリューム
一括取り込みアプリケーション - 変更データキャプチャ（アプリケーション取り込みおよびレプリケーション用）	処理済みの行数
一括取り込みデータベース（データベース取り込みとレプリケーション用）	データボリューム
一括取り込みデータベース: 変更データキャプチャ（データベース取り込みおよびレプリケーション用）	処理済みの行数

メーター	スカラ値
一括取り込みファイル（ファイル取り込みとレプリケーション用）	データボリューム
一括取り込みストリーミング（ストリーミング取り込みとレプリケーション用）	データボリューム
MDM データ取り込みとレプリケーション（ストリーミング取り込みとレプリケーション用）	データボリューム
PC2CDI モダナイゼーションサービスの評価	処理されたオブジェクト
PC2CDI モダナイゼーションサービスの変換	処理されたオブジェクト
追加のプロダクション組織	組織
サンドボックス組織	Organizations
Secret Manager	接続
SQL ELT	処理済みの行数
サブ組織	Organizations
タスクフローの実行	タスクフローの実行
関連するサブ組織の IPU 使用率	Organizations

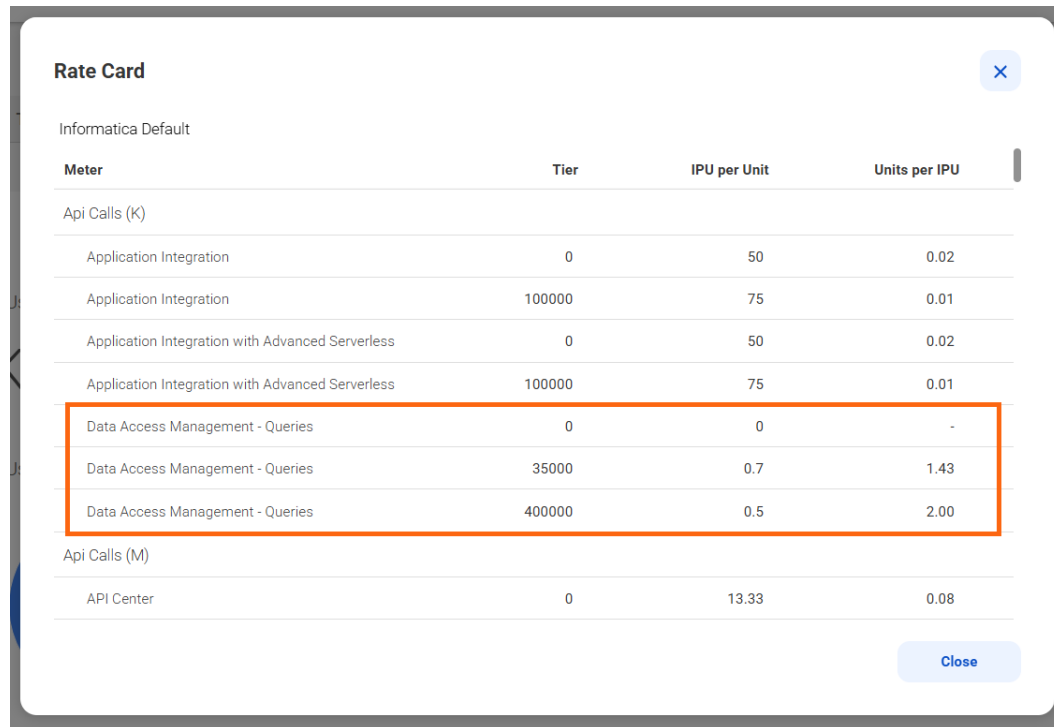
レートカード

レートカードには、それぞれのメーターと層の現在の IPU レートが一覧表示されます。

注: このセクションのサンプルのレートカードには、組織の現在の IPU レートが反映されていない可能性があります。

段階的なレートของमीเตอร์

層のあるमीターには、層ごとの IPU レートが表示されます。次の画像に、[Data Access Management - クエリ] ミーターの層ごとの IPU レートを含むサンプルレートカードを示します。



Meter	Tier	IPU per Unit	Units per IPU
Informatica Default			
Api Calls (K)			
Application Integration	0	50	0.02
Application Integration	100000	75	0.01
Application Integration with Advanced Serverless	0	50	0.02
Application Integration with Advanced Serverless	100000	75	0.01
Data Access Management - Queries	0	0	-
Data Access Management - Queries	35000	0.7	1.43
Data Access Management - Queries	400000	0.5	2.00
Api Calls (M)			
API Center	0	13.33	0.08

この例では、[Data Access Management - クエリ] ミーターの IPU レートは、以下の方法で計算されます。

- 最大 35,000 件のクエリを無料で実行できます。
- クエリ 35,001 件から 400,000 件までは、クエリごとに 0.7IPU のコストがかかります。
- 400,000 件を超えるクエリは、クエリごとに 0.5 IPU のコストがかかります。

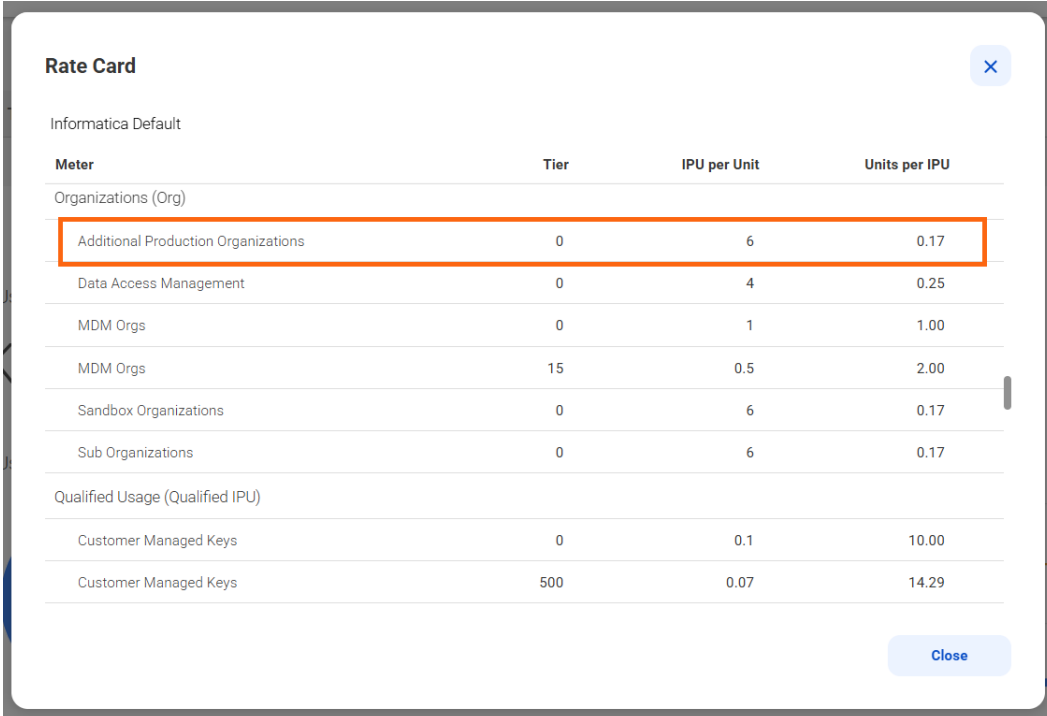
例えば、請求期間に 450,000 件のクエリを実行した場合、次の式を使用して合計 IPU を計算できます。

$$(35,000 * 0) + (365,000 * 0.7) + (50,000 * 0.5) = 305,500.5 \text{ IPU}$$

次の請求期間が始まると、クエリ数はゼロにリセットされます。

定額レートのメーター

層のないメーターには、定額 IPU レートが表示されます。次の画像に、追加のプロダクション組織のメーターの IPU レートを含むサンプルレートカードを示します。



Meter	Tier	IPU per Unit	Units per IPU
Organizations (Org)			
Additional Production Organizations	0	6	0.17
Data Access Management	0	4	0.25
MDM Orgs	0	1	1.00
MDM Orgs	15	0.5	2.00
Sandbox Organizations	0	6	0.17
Sub Organizations	0	6	0.17
Qualified Usage (Qualified IPU)			
Customer Managed Keys	0	0.1	10.00
Customer Managed Keys	500	0.07	14.29

追加のプロダクション組織のメーターには層がないため、追加のプロダクション組織ごとに、請求期間あたり 6 IPU の定額レートが設定されています。

無効化されたサブ組織および削除されたサブ組織での IPU 使用率

サブ組織は、「サブ組織」メーターの「組織」スカラ値にカウントされます。サブ組織も、他のメーターとスカラ値に基づいて IPU を使用します。

無効化されたサブ組織および削除されたサブ組織については、IPU の消費量に関する次のルールに注意してください。

無効化されたサブ組織

サブ組織を無効にした場合でも、そのサブ組織は次のスカラを使用するメーターの IPU を引き続き消費します。

- 保存されたレコード
- Organizations
- 修飾の使用率

削除されたサブ組織

Informatica グローバルカスタマサポートがサブ組織の削除プロセスを完了すると、サブ組織は現在の請求期間に 6 つの IPU を消費し、それ以降の請求期間では IPU を消費なくなります。Administrator でサブ組織を削除しても、Informatica グローバルカスタマサポートが削除プロセスを完了するためのチケットを開いていない場合、サブ組織は引き続き組織のスカラ値にカウントされ、IPU の消費を続けます。

サブ組織が削除された後も、親組織のメータリングページには、サブ組織のメータリングデータが履歴ビューに引き続き表示されます。

IPU メトリックレポート

IPU 使用率のサマリ、アセットの場所別の IPU 使用率、または特定のメーターに関する詳細を含むレポートをダウンロードできます。

次のタイプのレポートをダウンロードできます。

IPU 使用率履歴レポート

IPU 使用率サマリレポートには、プロダクション組織とそのサブ組織、追加のプロダクション組織、およびサンドボックス組織の IPU 使用率のサマリが含まれます。レポートには、選択した請求期間またはレポート期間のデータが含まれます。レポートには、各メーターの月ごとの次のデータが含まれます。

- スカラ使用率
- IPU 使用量
- 組織 ID と組織名

[IPU 使用率の履歴] ページから IPU サマリレポートをダウンロードします。

IPU メタデータ内訳レポート

IPU メタデータ内訳レポートには、選択した請求期間またはレポート期間の IPU 使用量が、プロジェクトとフォルダ別、またはメータリングタグ別の内訳で表示されます。このレポートには、次のような使用状況が表示されます。

- プロダクション組織およびそのリンクされた組織の製品メーターの使用状況。
注: この使用状況は、メーターによってはプロジェクト属性を持たない場合があります。プロジェクト属性を持つメーターの詳細については、「REST API リファレンス」を参照してください。
- 組織を直接リンクするための定期的な IPU コスト。

注: この使用状況は、プロジェクト属性には関連付けられていません。

[タグの内訳] タブまたは **[アセット別の IPU 使用率のメタデータ]** ページから IPU メタデータ内訳レポートをダウンロードします。

テーブルビューレポート

テーブルビューレポートには、IPU メーターの詳細ページのテーブルに現在表示されている情報が含まれます。レポートには、データをリクエストしたときに所属していた組織からの情報のみが含まれます。IPU メーターの詳細ページからテーブルビューレポートをダウンロードします。

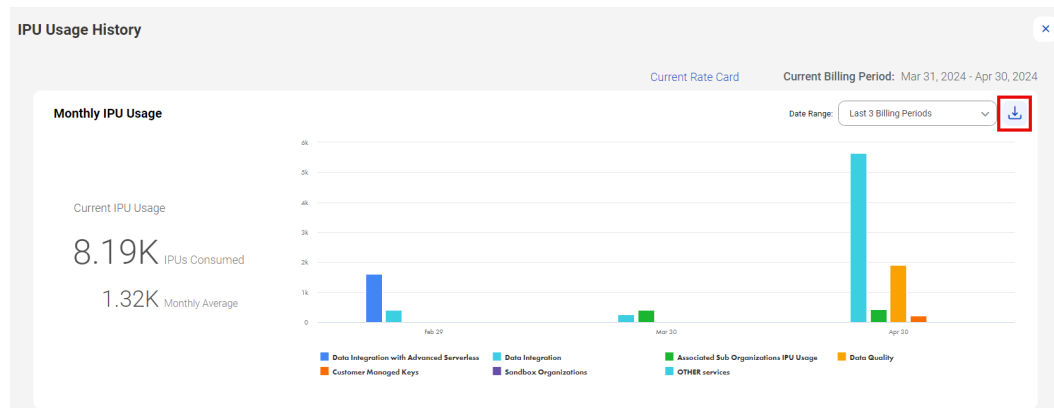
詳細なサービスレポート

一部のメーターでは、特定の日付範囲のサービスの詳細を含むレポートをダウンロードできます。レポートには、データをリクエストしたときに所属していた組織からの情報のみが含まれます。IPU メーターの詳細ページから詳細サービスレポートをダウンロードします。

アセットの内訳レポート

アセットの内訳レポートには、IPU メーターのアセットの内訳タブに表示される情報が表示されます。レポートには、データをリクエストしたときに所属していた組織からの情報のみが含まれます。IPU メーターの詳細ページのアセットの内訳タブから、アセットの内訳レポートをダウンロードします。

レポートをダウンロードするには、[ダウンロード] アイコンをクリックします。次の図は、[IPU 使用率の履歴] ページの [ダウンロード] アイコンを示しています。



IPU 使用率の履歴レポートのダウンロード

[IPU 使用率の履歴] ページからサマリレポートをダウンロードします。

1. [メータリング] ページで [履歴ビュー] をクリックします。
2. レポートに含める請求期間を選択します。最大で過去 13 回の請求期間を選択できます。
3. [ダウンロード] アイコンをクリックします。
4. [エクスポート] をクリックします。

IPU メタデータの内訳レポートのダウンロード

アセットの場所やメータリングタグなどのメタデータごとの内訳を示した IPU 使用率レポートをダウンロードします。

1. [メータリング] ページで、[タグの内訳] タブまたは [アセット別の IPU 使用率のメタデータ] ページに移動します。
2. IPU 使用率をプロジェクトとフォルダごとに表示するか、メータリングタグごとに表示するかを選択します。
3. レポートに含める請求期間を選択します。最大で過去 13 回の請求期間を選択できます。
4. [ダウンロード] アイコンをクリックします。

注: すべてのメーターにプロジェクトとフォルダの情報が含まれているわけではありません。Informatica Intelligent Cloud Services でメータリングデータが処理される前にアセットを削除した場合、アセットのメータリングデータにもプロジェクトとフォルダは含まれません。ユーザーインターフェースとダウンロードしたレポートには、プロジェクトとフォルダの情報のないアセットが 1 行に表示されます。この行のプロジェクトの値は空白です。

IPU メーターレポートのダウンロード

メーターの詳細ページで特定のメーターのレポートをダウンロードします。概要テーブルまたはアセットの内訳テーブルに基づくレポートをダウンロードできます。一部のメーターについては、詳細なサービスレポートをダウンロードすることができます。

1. [メータリング] ページの [現在の請求期間] 領域で、メーター名をクリックします。
2. ダウンロードするレポートのタイプに応じて、[概要] タブまたは [アセットの内訳] タブに移動します。
3. レポートに含める請求期間を選択します。

4. **【ダウンロード】** アイコンをクリックします。
5. 詳細なサービスレポートをダウンロードするオプションが利用可能な場合、**【ダウンロード】** アイコンをクリックすると**【メータリングの使用状況レポート】** ダイアログボックスが表示されます。次のいずれかの手順に従います。
 - テーブルビューレポートを選択し、**【エクスポート】** をクリックします。
 - 詳細なサービスレポートを選択し、レポートの日付範囲を選択して、**【エクスポート】** をクリックします。

注: すべてのメーターに、アセット名、アセットタイプ、プロジェクト、フォルダなどのアセット情報が含まれているわけではありません。Informatica Intelligent Cloud Services でメータリングデータが処理される前にアセットを削除した場合、アセットのメータリングデータにもこの情報は含まれません。この情報を使用できない場合、**【アセットの内訳】** タブのアセット名、アセットタイプ、プロジェクト、およびフォルダは空白になります。アセット情報を使用できない場合、ダウンロードしたレポートではアセット情報が *NULL* になります。

データ統合の詳細レポート

データ統合の詳細レポートは、指定された期間内に組織が実行したジョブに対するメータリングの使用状況の詳細を提供します。

データ統合の詳細レポートには、次のフィールドを含めることができます。

フィールド	説明
タスク ID	タスクを識別するための一意の ID。
タスク名	ジョブの名前。
タスクオブジェクト名	ジョブで使用されるオブジェクトの名前。 レプリケーションタスクと同期タスクに適用されます。
タスクタイプ	タスクのタイプ（マッピングタスクやレプリケーションタスクなど）。
タスク実行 ID	ジョブの実行 ID。
プロジェクト名	タスクが含まれるプロジェクト。
フォルダ名	タスクが含まれるフォルダ。タスクがプロジェクトの直下にある場合、このフィールドは空白です。
組織 ID	組織の一意の ID。
環境 ID	ランタイム環境のフェデレーション ID。
環境	ランタイム環境の名前。
使用されるコア	ジョブで使用されるコアの数。
割り当てられた SCU:	要求されたサーバーレスコンピューティングユニット。 サーバーレスレポートに適用されます。
開始時刻	ジョブが開始された時刻。協定世界時（UTC）が使用されます。
終了時刻	ジョブが終了した時刻。協定世界時（UTC）を使用します。

フィールド	説明
ステータス	ジョブのステータス。
測定値	変更データキャプチャおよび SQL ELT レポート用に処理された行数。 サーバーレスレポート用に消費されたサーバーレスコンピューティングユニット。 他のすべてのレポートで消費されたコンピューティング時間。
監査時間	タスクによってメータリング用に報告された時間。
OBM タスク時間	実際の処理時間。 Salesforce OBMSG に適用されます。

IPU 消費数警告の設定

Informatica Intelligent Cloud Services 内または電子メールで警告を設定して、組織が設定した IPU 数に達したときに通知を受け取ることができます。

組織の管理者は、組織が設定した数の IPU を消費したときに警告を受け取るように選択できます。プロダクション組織は、**[組織]** タブまたは **[タグ]** タブでしきい値を設定できます。サブ組織には、**[タグ]** タブで自分のサブ組織の IPU 警告としきい値を表示および設定するためのアクセス権のみが割り当てられます。消費数警告を受け取るのは管理者のみです。

1. **[メータリング]** ページの **[消費数警告]** タブで、**[組織の消費数警告を有効にする]** を選択して、消費数警告のメトリックを設定します。
2. 警告のしきい値の設定方法を選択します。
 - **IPU 絶対値:** メトリックを整数で設定します。
 - **IPU パーセンテージ値:** メトリックをパーセンテージで設定します。

あるメトリックから別のメトリックに切り替える場合、以前の消費しきい値は削除され、新しい値を入力する必要があります。絶対値を使用して警告を設定する場合、その数を、権限が与えられている IPU の数より大きくすることはできません。

3. **[消費しきい値]** フィールドに、警告を受信する基準となる、消費した IPU の数またはパーセンテージを入力します。これらの値は、**[消費数警告を有効にする]** チェックボックスをオフにして警告を無効にした場合でも、参照用として維持されます。
4. 警告は、**[タグ]** タブでプロジェクトレベルまたはフォルダレベルで設定できます。**[タグ]** タブには、現在ログインしている組織のプロジェクトとフォルダが表示されます。

警告を設定すると、組織の管理者はサービス内および電子メールで警告を受け取ります。また、組織が自社の設定に加えて IPU の 25%、50%、75%、95%、100% を消費した場合も、従来どおり標準の警告を受け取ります。

[IPU 絶対値] フィールドまたは **[IPU パーセンテージ値]** フィールドで設定した値よりも多くの IPU を消費した場合、システムは次の請求期間まで警告を送信しません。

メータリングタグ

メータリングタグは、クラウドリソースの整理と監視に役立つアセットプロパティです。メータリングタグを使用して、さまざまな部門、プロジェクト、またはイニシアチブにわたる IPU 使用率を追跡します。

アセットにメータリングタグを割り当てた後、**[メータリング]** ページの **[タグの内訳]** タブで、メータリングタグごとの IPU 使用率を確認できます。組織でメータリングタグを作成すると、メータリングタグは階層内のすべての組織に適用されます。

メータリングタグは次のサービスで使用できます。

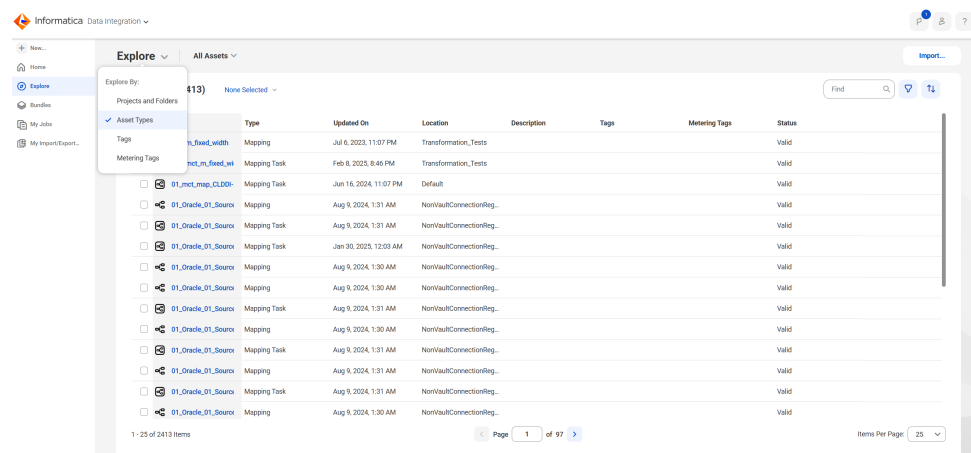
- データ取り込みおよびレプリケーション
- データ統合
- Data Quality
- データプロファイリング

メータリングタグの設定

メータリングタグを作成し、それらのタグをアセットに関連付けて、さまざまな部門、プロジェクト、またはイニシエート間での IPU の使用量を整理および追跡します。

メータリングタグを設定するには、メータリングタグを作成してから、アセットに関連付ける必要があります。

1. メータリングタグを作成するには、次の手順を実行します。
 - a. **[Administrator]** の **[メータリング]** ページで、**[タグマネージャ]** タブをクリックします。
 - b. **[メータリングタグ]** セクションで、**[追加]** ボタンをクリックしてタグを作成します。
 - c. **[タグ名]** フィールドと **[タグ値]** フィールドにタグ名とタグ値を入力します。タグ名ごとに複数のタグ値を作成することができます。
 - d. または、**[アドホックタグ値を許可]** を使用して、組織内のユーザーがこのタグ名に対して新しいタグ値を作成できるようにします。
 - e. **[複数値のタグ付けを許可]** を使用すると、同じタグ名から複数のタグ値を使用してアセットにタグを付けることができます。
 - f. これらのメータリングタグ設定を保存するには、**[保存]** をクリックします。タグは、保存後に編集することができます。
2. メータリングタグをアセットに関連付けるには、次の手順を実行します。
 - a. サービスの **[参照]** ページで、**[参照元]** > **[アセットタイプ]** の順に移動します。次の図は、データ統合の **[参照]** ページで **[アセットタイプ]** にアクセスするための場所を示しています。



- b. アセットの **[アクション]** メニューで、**[プロパティ]** をクリックします。
- c. **[メータリングタグ]** プロンプトを使用して、このアセットをメータリングタグに関連付けます。

Administrator の **[タグの内訳]** タブには、特定のメータリングタグに関連付けたアセットの IPU 使用率の内訳が表示されます。

注: 部門、プロジェクト、またはイニシアチブに割り当てたタグを更新すると、変更が翌日に反映されます。タグを削除してキャッシュをクリアすると、タグは表示されなくなります。

機能ベースのライセンスメトリック

組織に機能ベースのライセンスがある場合、**[メータリング]** ページには、ライセンスに基づいた情報が表示されます。

[メータリング] ページには、ライセンスされた機能に応じて次のビューが表示されます。

ダッシュボードビュー

適切なライセンスがある場合、**[メータリング]** ページのダッシュボードビューに情報が表示されます。

「今月のメトリック概要」領域には、その月の残りの合計コンピューティングリソースと各メータータイプが表示されます。組織のエディションに応じて、組織に適用されるすべてのメーターの表を表示することもできます。

それぞれのメータータイプの詳細領域には、残りのリソース量、1日あたりの平均リソース使用量、残りの使用日数など、その月のメーター情報が表示されます。メータータイプの詳細を表示するには、組織またはサブ組織、日付範囲、およびランタイム環境ごとの使用状況を示す詳しいグラフを表示できます。

ライセンスメトリックビュー

ダッシュボードビューの表示に必要なライセンスがない場合は、**[メータリング]** ページにはライセンスメトリックのテーブルが表示されます。このテーブルには、組織に適用されるすべてのメーターの概要メトリックが一覧表示され、その内容は組織のエディションに応じて異なります。

ダッシュボードビューの概要領域から、すべてのメーターの「**ライセンスメトリック**」ビューに移動することもできます。

注: 機能ベースのライセンスは、IPU ベースのライセンスとは異なります。IPU は機能ベースのライセンスには使用されません。組織で IPU を使用している場合は、「[「Informatica のプロセッシングユニットのメトリック」 \(ページ 28\)](#)」を参照してください。

ライセンスメトリックの表示

組織で使用されているすべてのメーターの表を表示できます。一部のメーターでは、メーターの使用状況を示すレポートをダウンロードできます。**[メータリング]** ページのライセンスメトリックビューからテーブルを表示し、レポートをダウンロードします。

ダッシュボードビューからライセンスメトリックビューを開くには、**[メトリックサマリ - 今月]** 領域の**[すべてのメーター]** をクリックします。ダッシュボードビューの表示に必要なライセンスがない場合は、**[メータリング]** ページを開くとライセンスメトリックビューが表示されます。

ライセンスメトリックビューに表示されるメーターは、組織が使用しているエディションによって決まります。また、組織にはカスタムメーターも割り当てられる場合があります。メータリング情報はすべてのエディションで使用できない場合があります。

組織で複数のエディションを使用している場合、またはカスタムメーターを使用している場合、1つのメーターが異なる制限で複数回表示されることがあります。この場合、最新の制限が適用されます。例えば、あるエディションの同期ジョブが1日500個に制限され、別のエディションの同期ジョブが1日に100個に制限されている場合、1日のジョブは500個に制限されます。**[有効]** カラムに適用した制限が表示されます。

ライセンスメトリックビューには、メーターごとに以下の情報が表示されます。

プロパティ	説明
エディション	メーターに関連付けられているエディションの名前。
サービス	メーターが適用されるサービス。
メータリング	メーターの名前。例えば、1日あたりの同期ジョブの数、マッピングジョブによって処理された1か月あたりの行数、またはレプリケーションジョブの総数です。一括取り込みの場合、このカラムには次の取り込みタイプが表示されます: ファイル取り込みとレプリケーション、アプリケーション取り込みとレプリケーション、データベース取り込みとレプリケーション、アプリケーション取り込みとレプリケーション - 変更データキャプチャ、データベース取り込みとレプリケーション - 変更データキャプチャ、およびストリーミング取り込みとレプリケーション。
制限	ジョブまたは処理した行の最大数などの制限数。 この制限は親組織と各サブ組織に適用されます。例えば、1日あたりのジョブが100個に制限された場合、親組織が実行できるジョブは1日100個、各サブ組織が実行できるジョブも1日100個になります。 このフィールドに-1が表示された場合、制限はありません。
使用中	使用された実際のユニット数。組織またはサブ組織でメータリング期間に実行されるジョブ数または使用される計算時間などがあります。
使用済みの割合	組織またはサブ組織でメータリング期間に使用されたユニットの割合。
有効	組織またはサブ組織でメーターが有効かどうかを示します。

メーター定義

[メータリング] ページの「ライセンスメトリック」ビューに表示されるメーターは、組織が使用しているエディションによって決まります。

次の表に、エディションに基づいて効力がある可能性があるメーターについて説明します。

メーター	定義
詳細データ統合	詳細モードのマッピングに対する、時間単位で測定されるコンピューティングユニット。
高度なサーバーレスとの詳細データ統合	詳細モードのマッピングに対する、時間単位で測定されるサーバーレスコンピューティングユニット。
詳細データ品質	詳細モードのマッピングのデータ品質アセットに対する、時間単位で測定されるコンピューティングユニット。
高度なサーバーレスとの詳細データ品質	詳細モードのマッピングのデータ品質アセットに対する、時間単位で測定されるサーバーレスコンピューティングユニット。
処理された CDI 行	詳細モード外でマッピングによって処理された行数。

メーター	定義
CDI-E コンピューティングの時間数	非推奨。このメーターは、詳細データ統合メーターに置き換えられました。
日次/月間受信 API 要求最大	日次または月間の API アクセス要求の数。
Data Governance and Catalog - カタログレコード	カタログに保存されている技術アセットの数。
Data Governance and Catalog - ガバナンスレコード	カタログに保存されているガバナンスアセットの数。
Data Governance and Catalog - メタデータレコード消費数	カタログレコードを消費するために行われた公開 API 呼び出しの数。
Data Governance and Catalog - カタログソースの実行	Secure Agent でのカタログソース同期ジョブの実行用のコンピューティングユニット（時間単位）。
Data Governance and Catalog - サーバーレスでのカタログソースの実行	Informatica マネージドインフラストラクチャでのカタログソース同期ジョブの実行用のコンピューティングユニット（時間単位）。
高度なサーバーレスとのデータ統合	詳細モード外のマッピングに対する、時間単位で測定されるサーバーレスコンピューティングユニット。
データマーケットプレイスレコード	30 日間に作成されたデータコレクションと注文の数。
Data Quality	詳細モード外のマッピングの Data Quality アセットに関する、時間単位で測定されるコンピューティングユニット。
高度なサーバーレスとの Data Quality	詳細モード外のマッピングの Data Quality アセットに関する、時間単位で測定されるサーバーレスコンピューティングユニット。
一括取り込みメーター	<p>一括取り込みアプリケーション、一括取り込みデータベース、一括取り込みファイル、および一括取り込みストリーミングの場合は、アプリケーション取り込みとレプリケーション、データベース取り込みとレプリケーション、ファイル取り込みとレプリケーション、またはストリーミング取り込みとレプリケーションジョブによって 1 か月の間に取り込まれたギガバイト（GB）の数。</p> <p>一括取り込みアプリケーション - 変更データキャプチャと一括取り込みデータベース - 変更データキャプチャの場合は、取り込まれた行数。</p> <p>MDM データの取り込みとレプリケーションの場合は、MDM SaaS からリアルタイムイベントをパブリッシュする MDM ユーザーが実行したストリーミング取り込みとレプリケーションタスクによって取り込まれたギガバイト（GB）の数。</p>
タスクフローの実行	日次または月間のタスクフロー実行数。
日次/月間の PowerCenter ジョブの数	日次または月間の PowerCenter ジョブの数。
日次/月間のマッピングジョブの数	日次または月間のマッピングジョブの数。*
日次/月間のマスキングジョブの数	日次または月間のマスキングジョブの数。

メーター	定義
日次/月間のレプリケーションジョブの数	日次または月間のレプリケーションジョブの数。
日次/月間の PowerCenter ジョブが処理した行数	日次または月間の PowerCenter ジョブが処理した行数。
日次/月間のマッピングジョブが処理した行数	日次または月間のマッピングジョブが処理した行数。*
日次/月間のマスキングジョブが処理した行数	日次または月間のマスキングジョブが処理した行数。
日次/月間のレプリケーションジョブが処理した行数	日次または月間のレプリケーションジョブが処理した行数。
日次/月間の同期ジョブが処理した行数	日次または月間の同期ジョブが処理した行数。
日次の状態同期ジョブの数	日次の状態同期ジョブの数。 状態同期ジョブには、REST API を介して実行する fetchState ジョブおよび loadState ジョブが含まれます。
サブ組織の数	サブ組織の数。サブ組織を削除した場合、このメーターには削除したサブ組織が含まれます。
日次/月間の同期ジョブの数	日次または月間の同期ジョブの数。
ユーザー管理作成要求数	ユーザー管理作成要求数。 ユーザー管理作成要求には、ユーザー、ユーザーグループ、カスタムロールの作成のための要求が含まれます。
サーバーレス CDI コンピューティングの時間数	非推奨。詳細モード外のマッピングに関する、時間単位で測定されるサーバーレスコンピューティングユニット。
サーバーレス CDI-E コンピューティングの時間数	非推奨。詳細モードのマッピングに関する、時間単位で測定されるサーバーレスコンピューティングユニット。
使用されたサーバーレスユニットの総数	非推奨。タスクの実行に使用されたサーバーレスコンピューティングユニットの総数。
エラスティッククラスタのノードが使用した計算時間の合計	非推奨。このメーターは、詳細データ統合メーターに置き換えられました。
PowerCenter ジョブの総数	PowerCenter ジョブの総数。
エージェントの総数	停止したエージェントを含む、Secure Agents の合計数。 Informatica Cloud Hosted Agent は含みません。
接続の総数	接続の総数。
フォルダの総数	フォルダの総数。
マッピングジョブの総数	マッピングジョブの総数。*
マスキングジョブの総数	マスキングジョブの総数。

メーター	定義
プロジェクトの総数	プロジェクトの総数。
レプリケーションジョブの総数	レプリケーションジョブの総数。
PowerCenter ジョブが処理した行の総数	PowerCenter ジョブが処理した行の総数。
マッピングジョブが処理した行の総数	マッピングジョブで処理された行の総数。
マスキングジョブが処理した行の総数	マスキングジョブが処理した行の総数。
レプリケーションジョブが処理した行の総数	レプリケーションジョブが処理した行の総数。
同期ジョブが処理した行の総数	同期ジョブが処理した行の総数。
同期ジョブの総数	同期ジョブの総数。

Data Quality アセットとデータプロファイリングアセットのガイドライン

トランスフォーメーションが Data Quality アセットを読み取る、詳細モード外のマッピングを実行すると、マッピングのトランザクションが Data Quality メーターに記録されます。トランスフォーメーションが Data Quality アセットを読み取る、詳細モードのマッピングを実行すると、マッピングのトランザクションが Data Quality エラスティックメーターに記録されます。

データ統合サーバーでプロファイルを実行すると、プロファイルのトランザクションが Data Quality メーターに記録されます。詳細クラスターでプロファイルを実行すると、プロファイルのトランザクションが Data Quality エラスティックメーターに記録されます。

マッピング内のトランスフォーメーションの出力データをプレビューできます。Data Quality アセットを読み取るトランスフォーメーションでデータをプレビューする場合、Informatica は次の方法でコストを計算します。

- トランスフォーメーションを含むマッピングが詳細モード外で実行されると、Data Quality のコンピューティング時間が消費されます。
- トランスフォーメーションを含むマッピングが詳細モードで実行されると、Data Quality エラスティックのコンピューティング時間が消費されます。

サーバーレスコンピューティングユニットのメータリング

使用されているサーバーレスコンピューティングユニットの合計を表示すると、メーターには、組織がタスクの実行に使用しているサーバーレスコンピューティングユニットの数に基づいた値が表示されます。

サーバーレスランタイム環境がタスクを実行すると、環境では、タスクが要求するコンピューティングユニットの数に基づいて、リソースを使用して仮想マシンが作成されます。

最小タスク時間は 2 分です。タスクが 2 分未満で完了する場合、サーバーレスランタイム環境は 2 分のコンピューティングユニットを使用します。2 分が経過すると、コンピューティングユニットは 1 秒単位で使用されます。

ジョブをキャンセルすると、使用されるコンピューティングユニットの数は、次のうちの大きい方の値になります。

- キャンセルされる前にジョブが実行されていた時間
- 2 分

詳細クラスタのガイドライン

詳細モードのマッピングを実行すると、サーバーレスランタイム環境は、タスクが要求するサーバーレスコンピューティングユニットの数に基づいたリソースを持つ 1 つのワーカーノードを含む詳細クラスタを作成します。別のタスクを実行すると、環境では、アイドル状態のワーカーノードが再利用されるか、ワーカーノードをクラスタに追加して追加のリソースが予約されます。

タスクの実行を開始するとメータリングが開始され、タスクが完了すると終了します。メータリングには、ジョブをコンパイルする時間やクラスタを開始する時間は含まれません。

ジョブのコンパイルに失敗した場合、クラスタの開始に失敗した場合、またはクラスタの開始前にジョブをキャンセルした場合など、クラスタが作成される前にジョブが失敗した場合、メータリングは有効になりません。

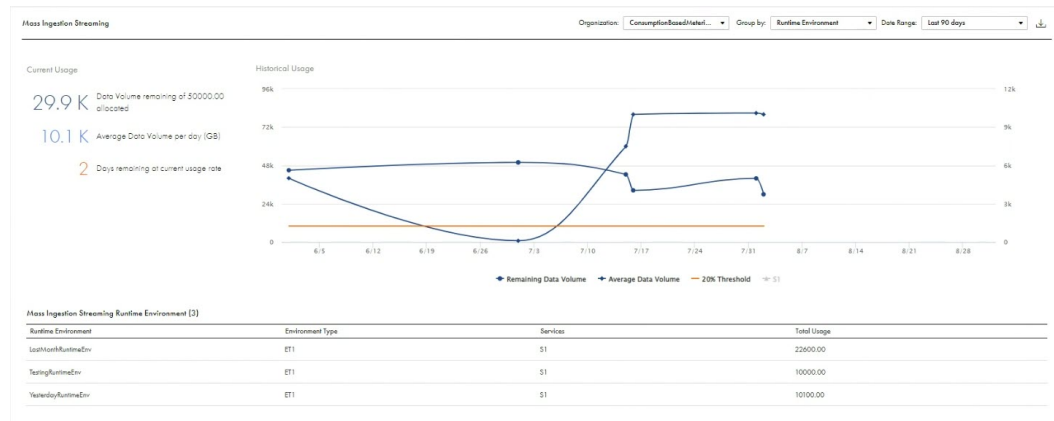
使用状況の詳細の表示

詳細なメータリング統計を表示できます。詳細な統計を表示するには、**【メータリング】** ページのダッシュボードビューで、関連するグラフの **【詳細グラフ】** をクリックします。

次のメーターでは、詳細なメータリング統計を利用できます。

- アプリケーション統合
- 高度なサーバーレスとのアプリケーション統合
- カタログレコード
- CDI-E コンピューティングの時間数
- サーバーレス CDI-E コンピューティングの時間数
- サーバーレス CDI コンピューティングの時間数
- データ品質
- Data Quality エラスティック
- 高度なサーバーレスとの Data Quality
- 高度なサーバーレスとの Data Quality エラスティック
- ガバナンスレコード
- 一括取り込みアプリケーション
- 一括取り込みアプリケーション - 変更データキャプチャ
- 一括取り込みデータベース
- 一括取り込みデータベース - 変更データキャプチャ
- 一括取り込みファイルの Microsoft SQL Server および Azure SQL Database ターゲット
- 一括取り込みストリーミング
- MDM データ取り込みとレプリケーション
- PC2CDI モダナイゼーションサービスの評価
- PC2CDI モダナイゼーションサービスの変換

次の図に、過去 90 日間の各ランタイム環境の合計使用量を示す詳細ページの例を示します。



ビューは、次の方法でカスタマイズできます。

- 組織にサブ組織がある場合は、親組織またはサブ組織の使用状況の詳細を表示できます。削除したサブ組織の使用状況の詳細を表示することはできません。
- グループ化は変更できます。例えば、ランタイム環境ごとにグループ化して各ランタイム環境の合計使用量を確認したり、完全なテーブルを表示して日付ごとの使用量を確認したりすることができます。
- 現在の月、先月、過去 90 日間、過去 6 か月または 13 か月などの、報告期間を定義するための日付範囲は変更できます。

メータリングの使用状況レポート

組織でアプリケーション統合、データ取り込みおよびレプリケーションサービス、詳細クラスタ、PowerCenter 用クラウドデータ統合（CDI-PC）を使用して PowerCenter アセットをモダナイズしている場合、またはサーバーレスランタイム環境を使用している場合は、メータリングの使用状況レポートをダウンロードできます。

メータリングの使用状況レポートには、次の情報が含まれます。

- アプリケーション統合の場合、レポートには、プロセス、ガイド、および OData API の実行の詳細が含まれます。アプリケーション統合の高度なサーバーレスランタイム環境の場合、レポートにはプロセスとガイドの実行の詳細が含まれます。
ターボモードで実行されるプロセス、サブプロセス、ガイド、および OData API のレポートを表示およびダウンロードするには、**【アプリケーション統合】** をクリックし、メータリングダッシュボードの **【API 呼び出し】** セクションにある **【高度なサーバーレスを使用したアプリケーション統合】** リンクをクリックします。
- 標準モードで実行されるプロセス、ガイド、および OData API のレポートを表示およびダウンロードするには、**【アプリケーション統合】** をクリックし、メータリングダッシュボードの **【コンピューティングユニット】** セクションにある **【高度なサーバーレスを使用したアプリケーション統合】** リンクをクリックします。
- アプリケーション取り込みとレプリケーションとデータベース取り込みとレプリケーションの場合は、取り込みジョブのロードタイプによってレポートの内容が異なります。初期ロードを実行するジョブの場合、レポートには、取り込まれたデータ量が GB 単位で含まれます。増分ロードを実行するジョブの場合、レポートには処理されたレコード数または行数が表示されます。初期ロードと増分ロードを組み合わせて実行するジョブの場合は、両方のレポートが含まれます。
- ファイル取り込みとレプリケーションの場合は、ファイル取り込みとレプリケーションタスクによって取り込まれたデータの量に関する詳細がレポートに表示されます。

- ストリーミング取り込みとレプリケーションの場合は、ストリーミング取り込みとレプリケーションジョブによって取り込まれたデータの量に関する詳細がレポートに表示されます。
- 詳細クラスタの場合、レポートには、クラスタノードのコンピューティング時間に関する詳細が含まれます。
- PowerCenter 用クラウドデータ統合（CDI-PC）の場合、レポートには、評価または変換ジョブが実行された日時、組織 ID、ジョブの詳細、評価または変換中に処理されたオブジェクトの数などの詳細が表示されます。
- サーバーレスランタイム環境の場合、レポートには、タスクを実行するために要求および使用されたサーバーレスコンピューティングユニットの数に関する詳細が含まれます。

メータリング使用状況レポートには、開始日の午前 0:00（UTC）から終了日の午後 11:59（UTC）までの IPU 使用率が含まれます。

組織でアプリケーション取り込みとレプリケーション、データベース取り込みとレプリケーション、ファイル取り込みとレプリケーション、ストリーミング取り込みとレプリケーション、詳細クラスタ、またはサーバーレスランタイム環境を使用していない場合、メータリングの使用状況レポートは使用できません。

【詳しいグラフ】からのメータリングの使用状況レポートのダウンロード

【メータリング】ページの【詳しいグラフ】ビューからメータリングの使用状況レポートをダウンロードします。

1. 管理者で【メータリング】を選択します。
2. ダウンロードするメータリングの使用状況レポートの【詳しいグラフ】をクリックします。
3. 表示する組織と日付範囲を選択します。
選択した内容に応じてレポートデータが調整されます。
4. ダウンロードアイコンをクリックします。
5. 【エクスポート】をクリックします。

第 4 章

全般設定とセキュリティ設定

【設定】 ページで全般設定、通知設定、およびセキュリティ設定を構成できます。

組織のライセンスに基づいて、次のような設定を行うことができます。

ソース管理設定

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に、組織のソース管理を設定できます。組織のグローバルソース管理リポジトリへの接続を設定します。リポジトリへの読み取り/書き込み、または読み取り専用アクセスを設定できます。また、プロジェクトレベルのソース管理を有効にして、ユーザーがソース管理リポジトリを特定のプロジェクトにリンクできるようにすることもできます。

詳細については、[「ソース管理設定」 \(ページ 52\)](#)を参照してください。

Secure Agent サービスのアップグレード設定

ローリングアップグレードをサポートするサービスのアップグレード中にエラーが発生した場合、そのサービスのアップグレードを続行するか停止するかを指定できます。詳細については、[「Secure Agent サービスのローリングアップグレード」 \(ページ 60\)](#)を参照してください。

マイナーアップグレード後に再起動する必要があるサービスの再起動スケジュールを設定できます。再起動スケジュールの再開を設定するには、アップグレードを実行する曜日と時刻を選択します。詳細については、[「Secure Agent サービスの再開スケジュールの設定」 \(ページ 62\)](#)を参照してください。

カスタムブランディング設定

親組織のカスタムブランディング設定を構成し、サブ組織に適用できます。各サブ組織のカスタムブランディング設定を、要件に応じて設定することもできます。カスタムブランディング設定には、ロゴ、カラーテーマ、ファビコンが含まれます。

カスタムブランディング設定を構成すると、Reference 360 サービスには、指定したロゴとファビコンが表示されます。

詳細については、[「カスタムブランディングの設定」 \(ページ 62\)](#)を参照してください。

通知の設定

組織のユーザーが電子メール通知を受け取るかどうかを設定できます。新しいユーザーのデフォルトの動作を設定し、すべてのユーザーに対する設定を上書きすることができます。

詳細については、[「通知の設定」 \(ページ 64\)](#)を参照してください。

顧客管理対象暗号化キーの設定

Informatica のマスタキーを使用する代わりに、独自のマスタキーを使用して、組織の暗号化キーを暗号化できます。

独自のマスタキーを作成して使用するには、まずクラウドプロバイダのキー管理サービスでキーをプロビジョニングし、Informatica Intelligent Cloud Services でアカウント間アクセスを有効にします。次に、**【セキュリティ】** タブの **【顧客管理対象キーの有効化】** オプションを有効化し、キープロパティを入力します。

詳細については、「[顧客管理対象暗号化キー](#)」 (ページ 64)を参照してください。

シークレットマネージャの設定

AWS Secrets Manager や Azure Key Vault などの外部シークレットマネージャから機密接続資格情報を取得するように組織を設定できます。組織のシークレットマネージャを設定するには、**[セキュリティ]** タブで **[シークレットマネージャを有効にする]** オプションを選択し、接続の詳細を入力します。

詳細については、「[シークレットマネージャの設定](#)」 (ページ 68)を参照してください。

ソース管理設定

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に、組織のソース管理を設定できます。ソース管理を設定すると、クラウドでホストされた Git リポジトリ、またはオンプレミスの Git リポジトリにオブジェクトのバージョンを保存できます。ソース管理は **[設定]** ページで設定します。

Informatica Intelligent Cloud Services でソース管理を使用するには、適切なライセンスが必要です。

次の表に、使用できるソース管理リポジトリのリストを示します。

リポジトリ	セルフホスト	クラウドホスト
Atlassian Bitbucket	サポート	データ統合アセットでのみサポートされます
GitHub	サポート	サポート
GitLab	サポート	サポート
Microsoft Azure DevOps	-	サポート

注: 組織が FedRAMP の対象である場合、クラウドでホストされる Bitbucket またはクラウドでホストされる GitLab を使用することはできません。

組織のソース管理を設定すると、ユーザーはソース管理をオブジェクトに適用できます。オブジェクトは自動的にチェックインされません。ユーザーは、ソース管理を個別のアセットまたはプロジェクトまたはフォルダ内のすべてのアセットに適用できます。ソース管理のプロジェクト、フォルダ、およびアセットへの適用の詳細については、該当する Informatica Intelligent Cloud Services サービスのヘルプシステムを参照してください。

ソース管理の設定時に、組織のグローバルソース管理リポジトリへの接続を設定します。組織のソース管理は、次の方法で設定できます。

グローバルソース管理リポジトリへの読み取り/書き込みアクセスを設定します。

読み取り/書き込みアクセスを設定すると、組織内のユーザーは、オブジェクトのチェックインおよびチェックアウト、オブジェクトのバージョンのプル、オブジェクトを前のバージョンに戻すことができます。ユーザーは、ソース管理オブジェクトを変更するには、それらをチェックアウトする必要があります。ユーザーはオブジェクトを排他的にチェックアウトするため、ユーザーは別のユーザーによってチェックアウトされているオブジェクトを変更することはできません。ユーザーは、ソース管理されていないオブジェクトはチェックアウトせずに変更できます。

読み取り/書き込みアクセスは、プロジェクトおよびアセットを開発する組織用に設定することがあります。

グローバルソース管理リポジトリへの読み取り専用アクセスを設定します。

読み取り専用アクセスを設定すると、組織内のユーザーは、ソース管理オブジェクトのバージョンをリポジトリからプルできます。しかし、ユーザーはオブジェクトのチェックアウトまたはチェックインをすることはできません。ユーザーは、組織内のプロジェクト、フォルダ、およびアセットをチェックアウトせずに、それらに変更を加えることができます。

読み取り専用アクセスは、テストまたは本番組織に設定し、ユーザーがアセットの最新バージョンをテストまたは実行できるようにすることがあります。

リポジトリアクセスタイプを変更できます。しかし、読み取り/書き込みから読み取り専用に変更するには、まずオブジェクトがチェックアウトされていないことを確認する必要があります。チェックアウトされているオブジェクトがある場合、Informatica Intelligent Cloud Services ではリポジトリアクセスタイプの読み取り/書き込みから読み取り専用への変更は許可されません。

警告: 読み取り専用アクセスを設定すると、ユーザーは、ソース管理オブジェクトを上書きできます。例えば、ユーザー John が最新バージョンのソース管理マッピングをプルし、変更するとします。別のユーザーが後でこのマッピングの任意のバージョンをプルした場合、John の変更は失われます。オブジェクトの権限およびユーザー権限は、ユーザーが誤って組織内のソース管理アセットを上書きするのを防止するように、注意深く設定します。

プロジェクトレベルのリポジトリの有効化

ユーザーがグローバルリポジトリ内のブランチを指定するか、プロジェクトごとに異なるリポジトリを指定できるようにすることができます。プロジェクトに異なるリポジトリブランチを使用すると、組織内のチーム間での並列開発とコラボレーションが可能になります。

また、リポジトリ URL を変更することもできます。これを実行するには、まずすべてのソース管理アセットのリンクを解除します。ソース管理アセットがある場合、Informatica Intelligent Cloud Services では、リポジトリ URL の変更は許可されません。

設定した後でソース管理を無効にする場合、ソース管理からすべてのオブジェクトのリンクを解除してから、組織のソース管理を無効にします。

管理者ロールまたは「チェックアウトの取り消しを強制」特権を持つユーザーロールを持っている場合は、別のユーザーによってチェックアウトされたオブジェクトのリンクを解除できます。

サブ組織のソース管理設定

サブ組織のソース管理は、サブ組織の【設定】ページで設定します。ベストプラクティスとして、各サブ組織は、その組織用のソース管理リポジトリを使用する必要があります。さらに、サブ組織用のソース管理リポジトリは、その親組織のソース管理リポジトリと別である必要があります。

個別のソース管理リポジトリを管理することで、1つの組織内のユーザーが、別の組織のアセットを誤って上書きしたり変更したりすること起きないようにします。

親組織の管理者がサブ組織のソース管理操作を実行できるようにする場合、親組織の管理者の Git ユーザーアカウントが、サブ組織のソース管理リポジトリへのアクセス権を持つように設定します。

OAuth を使用したリポジトリアクセス

ソース管理リポジトリがクラウドでホストされている場合は、個人アクセストークンの代わりに OAuth 認証を使用してリポジトリへのアクセスを提供するように組織を設定できます。OAuth 認証は【設定】ページで設定します。

GitHub リポジトリを使用する場合は、Informatica Intelligent Cloud Services が組織の GitHub リポジトリに対してソース管理操作を実行できるようにする GitHub アクセサアプリケーションがリポジトリにインストールされている必要があります。このアプリケーションがリポジトリにインストールされていない場合は、【設定】ページからインストールできます。

オンプレミスリポジトリの操作

ソース管理リポジトリがオンプレミスの場合、Secure Agent は Secure Agent マシンにリポジトリのローカルコピーを作成します。Secure Agent は、ローカルリポジトリでソース管理操作を実行してから、それらをリモートリポジトリにプッシュします。

オンプレミスリポジトリを使用する場合は、Secure Agent マシンにリポジトリのローカルコピーとその後のすべてのバージョン管理操作のための十分なスペースがあることを確認してください。

Secure Agent は、ユーザーがアセットのチェックインなどのソース管理操作を初めて実行するときに、ローカルリポジトリを作成します。ローカルリポジトリの作成する時に、Informatica Intelligent Cloud Services アセットを格納するブランチをコピーします。他のブランチはコピーされません。ユーザーがソース管理操作を実行するたびに、エージェントは、操作をサポートするために変更に関する情報をリモートリポジトリから取得します。

デフォルトでは、Secure Agent は、Secure Agent マシンの次のディレクトリにローカルリポジトリを作成します。

```
<Secure Agent インストールディレクトリ>/apps/GitRepoConnectApp/data/git_repository/<クライアント URL>/<組織 ID>/<ブランチ>/<リモートリポジトリ名>
```

Secure Agent の詳細ページで GitRepoConnectApp サービスの **git_local_repository_path** プロパティを編集することで、ローカルリポジトリディレクトリを変更できます。このプロパティの値の変更に関する詳細については、「*Secure Agent サービス*」を参照してください。

組織のソース管理の有効化

組織のソース管理を有効にするには、**【設定】** ページでグローバルソース管理リポジトリへのアクセスタイプと接続を設定します。構成する設定は、リポジトリのタイプに応じて異なります。

1. 管理者の **【設定】** ページで、[ソース管理] 領域の **【編集】** をクリックします。

2. **【ソース管理の有効化】** オプションを有効にします。

3. 必要に応じて、**【プロジェクトレベルソース制御の有効化】** 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、ユーザーはグローバルリポジトリ内のブランチ、またはプロジェクトレベルで使用する別のリポジトリを指定することができます。

4. ソース管理リポジトリへのアクセスタイプを設定します。

- 読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。
- 読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。

5. クラウドでホストされているリポジトリへのアクセスを設定するには、次の情報を入力します。

オプション	説明
プラットフォーム	プラットフォームタイプ。 【クラウド】 を選択します。

オプション	説明
リポジトリのタイプ	<p>組織で使用するバージョン管理システム。次のいずれかのクラウドホストシステムを使用することができます。</p> <ul style="list-style-type: none"> • GitHub • Microsoft Azure DevOps • Atlassian Bitbucket（データ統合用） • GitLab
グローバル Git リポジトリの URL	<p>リポジトリ URL。以下に例を示します。 https://github.com/MyGitUser/MyRepositoryName.git リポジトリ URL は HTTPS プロトコルを使用する必要があります。 ヒント: リポジトリのクローンオプションを選択することで、リポジトリの URL を見つけることができます。</p>
グローバル Git ブランチ名	<p>Informatica Intelligent Cloud Services オブジェクトを格納するブランチの名前。指定するブランチは、リポジトリにすでに存在する必要があります。 ブランチ名を入力しない場合は、Informatica Intelligent Cloud Services では、リモートリポジトリのデフォルトのブランチの名前に基づいて、ブランチ名が「master」または「main」に設定されます。</p>
Git への OAuth アクセスを許可	<p>OAuth を使用してリポジトリにアクセスするには、このオプションを有効にします。 GitHub リポジトリを使用する場合は、Informatica Intelligent Cloud Services のアクセスを許可する Git アクセスアプリケーションを組織のリポジトリにインストールする必要があります。このアプリケーションをインストールするには、[Github に Git アクセスアプリをインストール] をクリックします。</p>

6. オンプレミスリポジトリへのアクセスを設定するには、次の情報を入力します。

オプション	説明
プラットフォーム	プラットフォームタイプ。[オンプレミス] を選択します。
グローバル Git リポジトリの URL	<p>リポジトリ URL。以下に例を示します。 https://gitlab.example.com/MyGitUser/MyRepositoryName.git リポジトリ URL は HTTPS プロトコルを使用する必要があります。 ヒント: リポジトリのクローンオプションを選択することで、リポジトリの URL を見つけることができます。</p>
グローバル Git ブランチ名	<p>Informatica Intelligent Cloud Services オブジェクトを格納するブランチの名前。指定するブランチは、リポジトリにすでに存在する必要があります。 ブランチ名を入力しない場合は、Informatica Intelligent Cloud Services では、リモートリポジトリのデフォルトのブランチの名前に基づいて、ブランチ名が「master」または「main」に設定されます。</p>
ランタイム環境	<p>Git リポジトリへの接続に使用されるランタイム環境。 このリポジトリは、選択したランタイム環境のすべてのエージェントがアクセスする必要があります。</p>

オンプレミスリポジトリへの OAuth アクセスを設定することはできません。

7. **【保存】** をクリックします。

Informatica Intelligent Cloud Services は、リポジトリ接続を確認するためのソース管理資格情報の入力を求めるプロンプトを表示します。Informatica Intelligent Cloud Services はこの情報を保存しません。

接続が有効であり、リポジトリへの読み取り/書き込みアクセスを設定した場合、Informatica Intelligent Cloud Services はこのリポジトリに小さな readme ファイルを書き込み、これがリポジトリにオブジェクトをプッシュできることを確認します。

ソース管理の有効化後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を入力する必要があります。ユーザーは、自分の資格情報を入力するまでは、**【参照】** ページのソース管理カラムを表示できず、ソース管理アクションを実行できません。ソース管理資格情報を入力するには、**【ユーザー】** アイコンを Informatica Intelligent Cloud Services ウィンドウの右上隅でクリックし、**【設定】** を選択します。

ソース管理リポジトリ URL の変更

ソース管理リポジトリ URL を変更するには、まず組織内のすべてのオブジェクトをリンク解除し、新規リポジトリ URL を管理者の **【設定】** ページで入力します。URL の変更後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を更新する必要があります。

1. そのリポジトリを使用する各 Informatica Intelligent Cloud Services サービスで、すべてのオブジェクトをソース管理からリンク解除します。
2. 管理者で、**【設定】** ページを開き、[ソース管理] 領域の **【編集】** をクリックします。
3. **【ソース管理の有効化】** オプションが有効になっていることを確認します。
4. ソース管理リポジトリへのアクセスタイプを設定します。
 - 読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。
 - 読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。
5. プラットフォームと、Informatica Intelligent Cloud Services オブジェクトを格納するブランチの名前を確認します。クラウドでホストされているリポジトリの場合は、OAuth アクセス設定も確認します。
6. 新規リポジトリ URL を次のように入力します。

`https://github.com/MyGitUser/MyRepositoryName.git`

ヒント: リポジトリの URL は、リポジトリのタイプに基づいて次の方法で見つけることができます。

リポジトリ	URL を見つける方法
Atlassian Bitbucket (セルフホストおよびクラウドホスト)	リポジトリを開き、 【クローン】 を選択します。
GitHub (クラウドホスト)	リポジトリを開き、 【クローンまたはダウンロード】 > 【HTTPS でクローン】 を選択します。
GitHub Enterprise (セルフホステッド)	リポジトリを開き、 【コード】 > 【HTTPS でクローン】 を選択します。

リポジトリ	URLを見つける方法
GitLab（セルフマネージドおよびクラウドホスト）	リポジトリを開き、 【コード】 > 【HTTPSでクローン】 を選択します。
Microsoft Azure DevOps（クラウドホスト）	リポジトリを開き、 【クローン】 を選択します。

リポジトリ URL は HTTPS プロトコルを使用する必要があります。

7. **【保存】** をクリックします。

Informatica Intelligent Cloud Services は、リポジトリ接続を確認するためのソース管理資格情報の入力を求めるプロンプトを表示します。Informatica Intelligent Cloud Services はこの情報を保存しません。

接続が有効であり、リポジトリへの読み取り/書き込みアクセスを設定した場合、Informatica Intelligent Cloud Services はこのリポジトリに小さな readme ファイルを書き込み、これがリポジトリにオブジェクトをプッシュできることを確認します。

ソース管理リポジトリ URL の変更後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を更新する必要があります。ソース管理資格情報を更新するには、**【ユーザー】** アイコンを Informatica Intelligent Cloud Services ウィンドウの右上隅でクリックし、**【設定】** を選択します。

組織のソース管理の無効化

組織のソース管理を無効にできます。ソース管理を無効にすると、組織とソース管理リポジトリの間のリンクが解除されます。ソース管理リポジトリ内のオブジェクトは削除されません。

読み取り書き込みに関する組織のソース管理を無効にする前に、すべてのアセットをリンク解除する必要があります。

- そのリポジトリを使用する各 Informatica Intelligent Cloud Services サービスで、すべてのオブジェクトをソース管理からリンク解除します。
- 管理者で、ソース管理を無効にします。
 - 管理者で、**【設定】** ページを開きます。
 - 【ソース管理】** 領域の **【編集】** をクリックします。
 - 【ソース管理の有効化】** オプションを無効にします。
 - 【保存】** をクリックします。
- オプションとして、組織内のユーザーがユーザー設定で自分のソース管理資格情報を削除できるようにします。
 - Informatica Intelligent Cloud Services ウィンドウの右上隅で、**【ユーザー】** アイコンをクリックし、**【設定】** を選択します。
 - ソース管理資格情報をクリアします。
 - 【保存】** をクリックします。

リポジトリアクセスの設定

ソース管理されているオブジェクトを操作するには、Informatica Intelligent Cloud Services でリポジトリ資格情報を指定します。

資格情報には、使用するリポジトリサービスに応じて、個人用アクセストークンまたはアプリパスワードを含めることができます。組織のリポジトリが OAuth アクセス用に設定されている場合は、パーソナルアクセストークンやアプリケーションのパスワードを提供する代わりに OAuth アクセスを有効にすることもできます。

個人用アクセストークンとアプリパスワードは、プライベートリポジトリを完全に制御できるように設定する必要があります。個人用アクセストークンの生成については、GitHub、GitLab、または Azure DevOps Git のヘルプを参照してください。アプリパスワードの生成については、Bitbucket のヘルプを参照してください。

リポジトリへのアクセスを設定するには、次の手順を実行します。

1. ツールバーの **【ユーザー】** アイコンをクリックし、**【設定】** を選択します。
2. **【ソースコード管理資格情報】** セクションで、次のいずれかのタスクを実行します。
 - リポジトリの資格情報を入力します。
 - リポジトリへの OAuth アクセスを有効にします。
アクセスを承認していない場合は、GitHub と Azure DevOps の Git リポジトリに Git アクセスアプリが表示されます。Informatica Intelligent Cloud Services へのアクセスを承認する場合に選択します。
3. **【保存】** をクリックします。

ソース管理のベストプラクティス

組織がソース管理を効果的に設定して使用できるようにするには、次のガイドラインをベストプラクティスとして使用します。

設定のガイドライン

組織のソース管理を設定するときは、次のガイドラインに従います。

- 開発、テスト、ステージング、本番には別々の組織を使用します。
異なる組織を管理するときは、環境間を独立させ、1つの環境に対する変更が、他の環境に影響しないようにします。例えば、テスト環境内のアセットへの変更が、誤って本番環境にデプロイされることがないようにします。
- ソース管理リポジトリへの読み取り/書き込みアクセスを持つ開発組織を設定し、ソース管理リポジトリへの読み取り専用アクセスを持つ非開発組織を設定します。
そうすることで、開発組織内のユーザーのみが、アセットに変更を加えられます。また、非開発環境内のユーザーが、誤って変更をソース管理リポジトリにプッシュすることを防止できます。
- 特定のソース管理リポジトリにプッシュする開発組織は1つのみにしてください。
開発組織用の独立したリポジトリを管理することで、ある組織内のユーザーが別の組織のアセットを誤って変更したり上書きしたりする事故が起きないようにします。独立したリポジトリを管理すると、別の組織からのアセット ID 参照の競合も回避できます。
- 組織のソース管理を有効にするときは、空のリポジトリを選択します。
Informatica Intelligent Cloud Services はアセットを Git リポジトリ内の Explore フォルダに保存するため、リポジトリに Explore という名前のフォルダが含まれないようにします。
- ソース管理の資格情報を、複数の Informatica Intelligent Cloud Services ユーザー間で共有しないようにします。
個別の資格情報によってセキュリティが維持され、特定の変更を加えたユーザーが誰かを追跡するのが簡単になります。さらに、各ユーザーは、GitHub 内に自分の制限を持ちます。

開発ガイドライン

アセットを開発し操作するときは、次のガイドラインに従います。

依存関係の管理に関するガイドライン

依存関係を持つアセットを管理するには、次のガイドラインに従います。

- アセットをリポジトリからプルする前に、接続およびランタイム環境を作成します。
必要な接続およびランタイム環境がターゲット組織内にあるときは、タスクをリポジトリからプルした直後に実行できます。
- マッピングやコンポーネントなどの再利用可能なアセットが、使用前にリポジトリ内にあることを確認します。
Informatica Intelligent Cloud Services は、マッピングタスクなどのアセットが依存するマッピングが組織内がない場合、アセットの保存を許可しません。

アセットのチェックインおよびチェックアウトに関するガイドライン

アセットをチェックインおよびチェックアウトするときは、次のガイドラインに従います。

- アセットの名前を変更または移動する場合は、アセットの第 1 レベルの依存アセットをチェックアウトし、それらを同じチェックインに含めます。
例えば、マッピングタスクが使用するマッピングの名前を変更する必要があり、そのマッピングタスクがタスクフローで使用されている場合は、マッピングとマッピングタスクをチェックアウトします。タスクフローをチェックアウトする必要はありません。マッピングの名前を変更した後に、マッピングとマッピングタスクを 1 回のチェックインアクションでチェックインします。
- アセットのチェックイン時にコメントを入力します。
アセットのチェックイン時に、リリースタグ名を **【サマリ】** フィールドに入力し、より説明的なコメントを **【説明】** フィールドに入力することがあります。これを実行すると、Informatica Intelligent Cloud Services の **【Git Summary (Git サマリ)】** フィールドに、アセットに関連付けられたリリースタグが表示されます。
- 複数のアセットを同時にチェックインするときは、アセット数を 800 件以下に制限します。
800 件を超えるアセットを同時にチェックインすると、Informatica Intelligent Cloud Services と Git リポジトリサービスとの間のパフォーマンスが低下する可能性があります。

別のユーザーのチェックアウトの取り消し

管理者ロールがある場合、またはユーザーロールに管理者サービスへのチェックアウトの取り消しを強制する機能がある場合、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取り消すことができます。ユーザーがオブジェクトをチェックアウトして、休暇を取る場合、または組織を離れる場合、別のユーザーによりチェックアウトされたオブジェクトのチェックアウトを取り消す必要がある場合があります。

チェックアウトを取り消すと、オブジェクトはソース管理リポジトリにある最後のバージョンに戻ります。オブジェクトのバージョン履歴には、チェックアウトやチェックアウトアクションを取り消した記録は残りません。後で変更したバージョンが必要になる可能性がある場合、チェックアウトを取り消す前にオブジェクトのコピーを作成します。

取り消しアクションは元に戻せません。プロジェクトまたはフォルダのチェックアウトを取り消すと、そのプロジェクトまたはフォルダのロックは解除されますが、プロジェクトまたはフォルダ内にあるオブジェクトはロックされたままになります。

1. ユーザーがオブジェクトをチェックアウトしたサービスを開きます。
2. **【エクスプローラ】** ページで、オブジェクトに移動します。

3. オブジェクトが含まれている行で、**【アクション】** をクリックし、**【チェックアウトの取り消し】** を選択します。

取り消しアクションによってロックが解除されるため、オブジェクトはチェックアウトできる状態になります。

注: オブジェクトがチェックアウトされた後に移動または名前が変更された場合、チェックアウトを取り消すとオブジェクトの名前と場所はチェックアウトされる前の名前と場所に戻されます。

アプリケーション統合プロセスを実行するためのターボモードの設定

使用量ベースのライセンスを持ち、2025 年 4 月 30 日より前に作成された組織の場合、アプリケーション統合プロセスをターボモードで実行するように設定できます。

ターボモードは、組織内の Secure Agent またはサーバーレスランタイム環境で実行されるすべてのプロセスに対して設定できます。ターボモードは、高スループット、パフォーマンスの向上、および低遅延を提供します。プロセスがターボモードで実行されている場合、スカラー値は **【1,000 件の API 呼び出し】** となり、これはプロセスとサブプロセスの呼び出し回数によって決定されます。

2025 年 4 月 30 日以降に作成された組織では、すべてのプロセスがターボモードでのみ実行されます。

注: ターボモードで実行されるプロセスを中断して再起動することはできません。

ターボモードでプロセスを実行するための組織の設定

2025 年 4 月 30 日より前に作成された組織では、アプリケーション統合プロセスをターボモードで実行するように設定できます。これらの組織では、ターボモードは、新しいジョブに対して、または組織内で実行されるすべての既存のジョブと新しいジョブに対して有効または無効にすることができます。

1. 管理者の **【設定】** ページで、**【アプリケーション統合の設定】** セクションの **【ターボモードの有効化】** オプションを有効にします。

【ターボモードの有効化】 フィールドが表示されます。

注: **【ターボモードの有効化】** オプションは、2025 年 4 月 30 日以降に作成された組織では編集できません。

2. **【ターボモードの有効化】** フィールドで、次のいずれかのオプションを選択します。

- **新しいジョブ。** 新しいジョブに対してのみターボモードが有効になります。
- **既存のジョブと新しいジョブ。** すべての既存ジョブと新規ジョブに対してターボモードが有効になります。

注: Secure Agent でターボモードを有効にした後は、設定が有効になるまでに少なくとも 20 分はかかります。

Secure Agent サービスのローリングアップグレード

一部の Secure Agent サービスは、ローリングアップグレードをサポートしています。ローリングアップグレードでは、Secure Agent グループ内のエージェントで実行されているサービスは、順次アップグレードされます。

す。そのため、あるエージェント上でサービスがアップグレードされる間、そのサービスはグループ内の他のエージェント上で使用可能であり続けます。

次の Secure Agent サービスは、ローリングアップグレードをサポートしています。

- プロセスサーバー

Secure Agent グループ内のエージェントで実行されているその他のサービスは、各エージェント上で同時にアップグレードされます。そのため、そのグループ内のエージェントがアップグレードされている間は、サービスを使用できません。グループ内のすべてのエージェントが正常にアップグレードされると、使用できるようになります。

例

組織では、次のランタイム環境を使用しています。

- Secure Agent グループ A:

エージェント A1 はデータ統合サーバーおよびプロセスサーバーを実行します。

エージェント A2 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

- Secure Agent グループ B:

エージェント B1 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

エージェント B2 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

組織がアップグレードされるときに、Secure Agent グループ A および B は同時にアップグレードされます。各 Secure Agent グループ内で、プロセスサーバーは順次アップグレードされます。そのため、プロセスサーバーがエージェント A1 および B1 でアップグレードされる間、エージェント A2 および B2 で実行され続けます。エージェント A1 および B1 でのアップグレードが完了すると、プロセスサーバーはエージェント A2 および B2 でアップグレードされます。

データ統合サーバーと一括取り込みはローリングアップグレードをサポートしていません。グループ A および B で、データ統合サーバーは各エージェントで同時にアップグレードされます。グループ B で、一括取り込みはエージェント B1 および B2 で同時にアップグレードされます。

ローリングアップグレードエラーの処理

ローリングアップグレードをサポートするサービスのアップグレード中にエラーが発生した場合、そのサービスのアップグレードを続行するか停止するかを指定できます。エラー処理動作を **【設定】** ページで設定します。

以下のいずれかのオプションを選択することができます。

エラーが発生した場合、エラーにフラグを設定して、アップグレードを続行する

サービスのアップグレード中にエラーが発生した場合、サービスはエラーが発生したエージェントのエラーで停止します。そのアップグレードは、グループ内の別のエージェント上で続行されます。

警告: このオプションを有効にし、グループ内のすべてのエージェント上でエラーが発生した場合、そのサービスは Secure Agent グループでの実行を停止します。これがジョブの中断の原因になる場合があります。

エラーが発生した場合、アップグレードを停止する

サービスのアップグレード中にエラーが発生した場合、サービスはエラーが発生したエージェントのエラーで停止します。まだアップグレードされていないグループ内の他のすべてのエージェントに対してサービスのアップグレードが停止します。まだアップグレードされていないエージェントは、そのサービスの以前のバージョンで実行し続けます。

これがデフォルトのオプションです。

エラー処理動作を設定するには、**【編集】** を [Secure Agent サービスのアップグレード設定] 領域でクリックし、適切なオプションを選択し、**【保存】** をクリックします。

Secure Agent サービスの再開スケジュールの設定

プロセスサーバーなどの一部の Secure Agent サービスには、アップグレード後に再開する必要があるものがあります。これらのサービスは、月間アップグレードやパッチリリースなどのマイナーアップグレード後に再開スケジュールを設定できます。再開スケジュールを【設定】ページで設定します。

再開スケジュールを設定するときは、サービスを再開する曜日と時刻を選択します。例えば、毎週日曜日の 00:00 GMT の再開をスケジュールできます。

プロセスサーバーサービスの再起動スケジュールを設定できます。再起動スケジュールを設定するには、次の手順を実行します。

1. Administrator で【設定】を選択します。
2. 【Secure Agent サービスのアップグレード設定】領域で【編集】をクリックします。
3. 日時を選択します。
4. 【保存】をクリックします。

再起動スケジュールを設定しない場合、デフォルトでは、ポイントオブデプロイメント（POD）がアップグレードされてから 7 日後にプロセスサーバーサービスが自動的に再起動されます。

カスタムブランディングの設定

Informatica のデフォルト設定の代わりに、カスタムロゴ、カラーテーマ、およびファビコンを使用してブランディング設定をカスタマイズできます。カスタムブランディングは、【設定】ページで設定します。

カスタムブランディングの設定は、次のサービスに適用されます。

- データガバナンス&カタログ
- データマーケットプレイス
- メタデータコマンドセンター
- MDM - Customer 360 SaaS
- MDM - Product 360 SaaS
- MDM - Reference 360
- MDM - Supplier 360 SaaS
- Multidomain MDM SaaS

ブランディング設定をカスタマイズするには、適切なライセンスが必要です。

ロゴおよびファビコンのガイドライン

組織のロゴとファビコンをアップロードする際は、次のガイドラインを使用してください。

- ロゴおよびファビコンの画像のファイルサイズは 1 MB 未満でなければなりません。
- ロゴ画像の最大サイズは 80 x 325 ピクセルでなければなりません。推奨サイズは 48 x 325 ピクセルです。
- ロゴ画像をアップロードする際、画像は枠内に配置されます。ズームコントロールオプションを使用して、画像が枠内に収まるように画像のサイズを変更してください。
- ファビコン画像の最大サイズは 196 x 196 ピクセルでなければなりません。推奨サイズは 32 x 32 ピクセルです。

- カスタムロゴには PNG、JPG、および GIF 形式を使用し、ファビコンには PNG 形式を使用します。

組織のカスタムブランディングの設定

【設定】 ページで、ロゴやファビコンをアップロードして、カラーテーマを選択できます。

1. 管理者の **【設定】** ページで、**【カスタムブランディング】** 領域の **【編集】** をクリックします。
2. **【カスタムブランディングの有効化】** を選択します。
3. サブ組織が、親組織からブランディング設定を継承するようにするには、**【サブ組織はカスタムブランディングを継承する】** を選択します。
4. ロゴ画像を更新するには、**【アップロード】** をクリックし、ロゴファイルを選択します。ロゴのガイドラインの詳細については、[「ロゴおよびファビコンのガイドライン」 \(ページ 62\)](#) を参照してください。
5. ファビコン画像を更新するには、**【アップロード】** をクリックし、ファビコンファイルを選択します。ファビコンのガイドラインの詳細については、[「ロゴおよびファビコンのガイドライン」 \(ページ 62\)](#) を参照してください。
6. ロゴとファビコンに合うカラーテーマを選択します。自分でテーマを作成することもできます。
7. カスタムブランディング設定を適用する前に、**【プレビュー】** セクションで変更をプレビューして確認します。
8. **【保存】** をクリックします。

CLAIRE の設定

組織の CLAIRE 設定を構成して、CLAIRE GPT、マッピングに関する CLAIRE の推奨事項、および米国以外の POD ユーザー向けの追加の CLAIRE 機能を有効または無効にすることができます。

次のような設定項目を設定することができます。

CLAIRE 生成 AI サービス

CLAIRE 生成 AI サービスを有効にすると、組織内のユーザーは CLAIRE GPT を使用して、自然言語プロンプトを通じてデータを検出、分析、検索することができます。

デフォルトでは、CLAIRE 生成 AI サービスは無効になっています。CLAIRE 生成 AI サービスは、必要に応じて有効または無効にすることができます。

CLAIRE GPT の詳細については、「CLAIRE GPT のヘルプ」を参照してください。

CLAIRE の推奨事項

CLAIRE の推奨を有効にすると、ご自身の会社のアセットまたはその他の Informatica Intelligent Cloud Services 組織のアセットのメタデータの分析に基づいたマッピングデザインに対する製品内の推奨事項が許可されます。CLAIRE エンジンによって収集され処理されたメタデータは匿名です。

デフォルトでは、CLAIRE の推奨事項は有効になっています。CLAIRE の推奨を無効にすると、会社内のすべてのユーザーに対して推奨が無効になります。会社では推奨をいつでも有効または無効にする事ができます。

サブ組織の CLAIRE の推奨は、サブ組織内から有効および無効にします。

CLAIRE の推奨事項を有効にすると、データ統合ユーザーは Mapping Designer での個々のマッピングの推奨を無効にすることができます。

組織で詳細な統合を使用している場合は、CLAIRE の推奨事項を有効にすると、次の機能が有効になります。

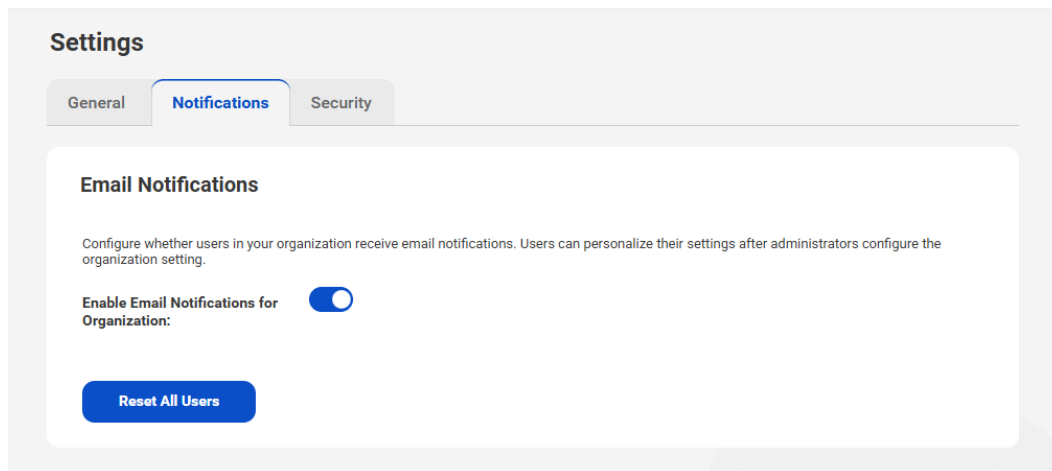
- CLAIRE を利用した設定、CLAIRE インサイト、および詳細クラスタに対する CLAIRE の推奨事項
- CLAIRE を利用したランタイムストラテジと、詳細モードのマッピングに基づくマッピングタスクに対する CLAIRE チューニング
- 詳細モードでマッピングを実行するジョブに対する CLAIRE の推奨事項

通知の設定

【設定】 ページの **【通知】** タブで、組織内のユーザーが電子メール通知を受信するかどうかを設定できます。

デフォルトでは、ユーザーはすべての電子メール通知を受信します。組織のデフォルトを変更し、すべてのユーザーを組織のデフォルト設定にリセットすることができます。組織のデフォルト設定は、新しいユーザーおよび設定をカスタマイズしていないユーザーに適用されます。

組織のデフォルトを設定するには、**【組織の電子メール通知の有効化】** プロパティを設定します。次の図は、組織に対して電子メール通知が有効になっている状態の **【通知】** タブを示しています。



注: すべてのユーザーは、電子メール通知が有効になっているかどうかを確認し、ユーザー設定で設定をパーソナライズすることができます。

顧客管理対象暗号化キー

独自のマスタキーを使用して、組織の暗号化キーを暗号化できます。

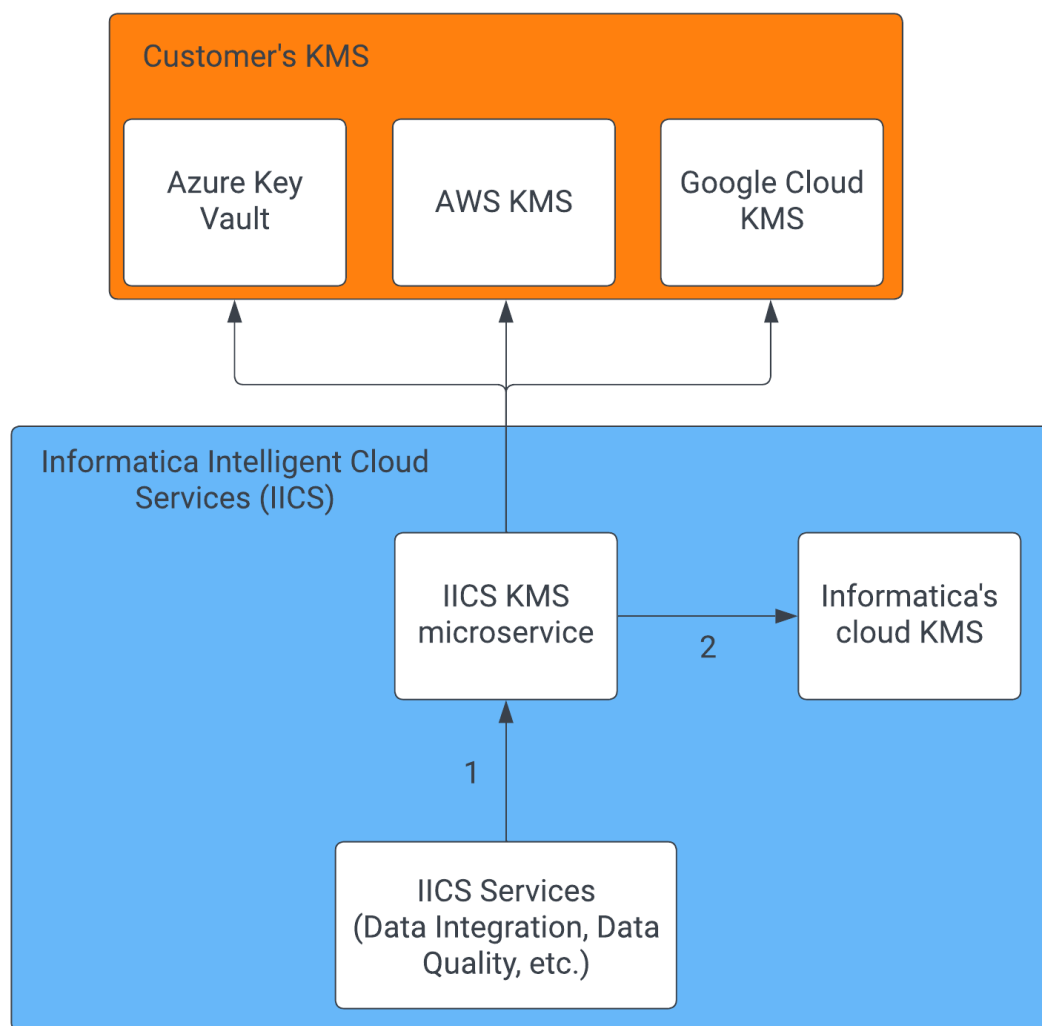
デフォルトでは、Informatica Intelligent Cloud Services は、Informatica Intelligent Cloud Services キー管理サービス（KMS）で生成および保存された組織固有の暗号化キーを使用して、クラウド内にある組織の機密データを保護します。不正アクセスを防ぐために、キーはクラウドプロバイダの KMS に保存されているマスタキーを使用して暗号化されます。マスタキーは Informatica の KMS アカウントでプロビジョニングされ、POD によって異なります。

必要に応じて、顧客管理対象キー（CMK）を作成できます。CMK を作成した場合、CMK へのアクセスはその作成者が管理します。ただし、Informatica Intelligent Cloud Services が組織の機密データを暗号化および復号化できるように、CMK へのアクセス権を付与する必要があります。

CMK を作成すると、次のメリットがあります。

- データへのアクセスを制限して制御できます。
- データ侵害が発生した場合に、データの復号化を制限できます。
- KMS でキーマテリアルを作成して保持できます。キーがクラウドサービスプロバイダに一切公開されません。
- ライフサイクル全体を通じて、自らキーを完全に管理できます。いつでもアクセスを取り消したり、キーを削除したりできます。

次の図は、Informatica Intelligent Cloud Services が CMK とインタフェースする方法を示しています。



1. Informatica Intelligent Cloud Services は、依存せずに Informatica Intelligent Cloud Services KMS とインタフェースします。
2. 顧客管理対象でないキーは、Informatica のクラウド KMS に送られます。

次のクラウドプロバイダのキー管理サービスを使用すると、CMK を作成して有効化することができます。

- Amazon Web Services

- Microsoft Azure
- Google Cloud

注: CMK を作成する場合、KMS と Informatica Intelligent Cloud Services POD は同じクラウドプロバイダを使用する必要があります。例えば、Informatica Intelligent Cloud Services POD が AWS の USW1 である場合、AWS KMS に CMK を保存する必要があります。Google Cloud KMS または Azure Key Vault に保存することはできません。

顧客管理対象キーの作成と有効化

顧客管理対象キーを作成して有効化するには、KMS でキーをプロビジョニングしてから、管理者で顧客管理対象キーを有効化します。

注: CMK を作成して有効化するための実行手順は、クラウドプロバイダーによって異なります。具体的な手順については、次の H2L 記事を参照してください。

- [Enable Customer Managed Keys for your Organization on Amazon Web Services](#)
- [Enable Customer Managed Keys for your Organization on Microsoft Azure](#)
- [Enable Customer Managed Keys for your Organization on Google Cloud](#)

一般的には、次の手順を実行します。

1. クラウド KMS でキーをプロビジョニングし、Informatica Intelligent Cloud Services でアカウント間アクセスを有効にします。
2. 管理者で、**【設定】** ページの **【セキュリティ】** タブを開き、**【顧客管理対象キーの有効化】** オプションを有効化し、キープロパティを入力します。

注: この手順を実行するには、Admin ロールと Key Admin ロールの両方を持つユーザーアカウントを使用して Informatica Intelligent Cloud Services にログインする必要があります。

キーのプロパティを設定したら、キーをテストできます。キーがアクティブになるまでに最大 24 時間かかる場合があります。

CMK を作成して有効化した後は、**【セキュリティ】** タブの **【顧客管理対象キーの有効化】** オプションを無効にすることで、いつでも取り消すことができます。これを行うと、Informatica のマスタキーを使用するように戻ります。

顧客管理対象キーに関するよくある質問

組織に適切なライセンスがあるのに、**【設定】** ページに **【セキュリティ】** タブが表示されません。なぜですか？

Admin ロールと Key Admin ロールの両方を持つユーザーアカウントを使用して Informatica Intelligent Cloud Services にログインしてください。いずれかのロールがない場合、**【セキュリティ】** タブは表示されません。

ユーザーロールの詳細については、「*ユーザー管理*」を参照してください。

【設定】 ページで **【管理対象キーのテスト】** をクリックすると、テストが失敗しました。どうすればよいですか？

キーのテスト中にエラーが発生した場合は、次のチェックを実行します。

- 管理者の **【設定】** ページでのキーの設定が、クラウド KMS の CMK の設定と一致していることを確認します。
- クラウド KMS で、CMK のステータスがアクティブであることを確認します。

- クラウド KMS で、CMK に対する権限がキーへの Informatica 暗号化アクセスを許可していることを確認します。

エラーが解決しない場合は、Informatica グローバルカスタマサポートにお問い合わせください。

KMS で CMK がローテーションされるとどうなりますか？

クラウド KMS でキーを手動またはスケジュールでローテーションできます。キーをローテーションすると、新しいバージョンのキーが作成されます。キーの古いバージョンはクラウド KMS に残り、復号化にのみ使用されます。

Informatica Intelligent Cloud Services は、Azure Key Vault と Google Cloud KMS でのキーのローテーションを検出します。CMK がローテーションされると、Informatica Intelligent Cloud Services は古い CMK を使用して組織のキーを復号化し、新しい CMK を使用してそれらを暗号化します。

Informatica Intelligent Cloud Services は、AWS KMS でのキーのローテーションを検出することはできません。AWS KMS を使用する場合は、Informatica Intelligent Cloud Services で顧客管理対象キーを無効にしてから、再度有効にする必要があります。この操作を行うには、次の手順を実行します。

1. 管理者の【設定】ページで、【セキュリティ】タブをクリックして、【キー ARN】と【ロール ARN】をメモします。
2. 【顧客管理対象キーの有効化】オプションを無効化します。
3. 【顧客管理対象キーの有効化】オプションを有効化し、キー ARN とロール ARN を再入力して、【保存】アイコンをクリックします。

KMS で CMK を更新する必要がある場合はどうすればよいですか？

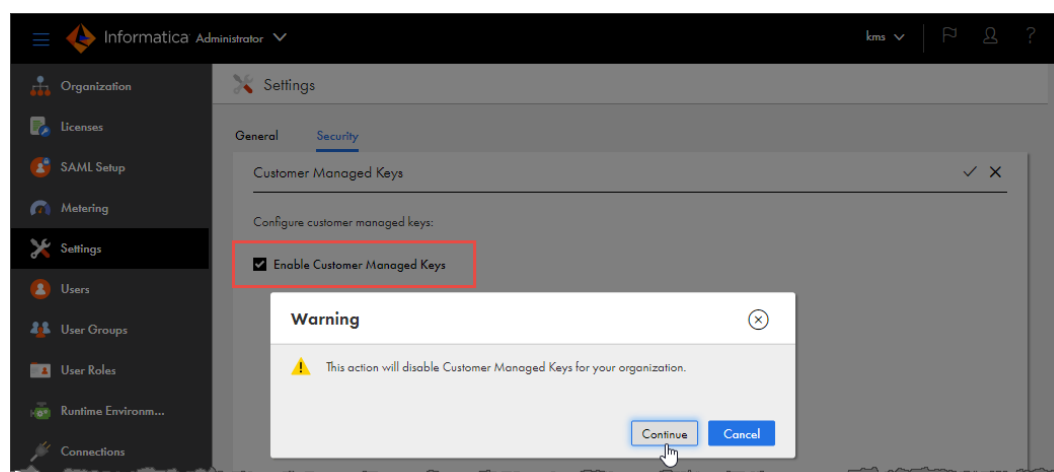
CMK を更新する必要がある場合は、まずクラウド KMS で新しい CMK をプロビジョニングします。次に、管理者の【設定】ページで、キーの詳細を更新します。

注: 管理者でキーの詳細を更新するまでは、クラウド KMS の古いバージョンの CMK をアクティブなままにしておきます。

【設定】ページでキーの詳細を更新したら、クラウド KMS の古いバージョンの CMK を削除できます。

Informatica にキー暗号化の管理を任せる場合はどうすればよいですか？

キーの暗号化の管理を Informatica に任せる場合は、管理者の【設定】ページで【顧客管理対象キーの有効化】オプションを無効化できます。



これを行うときは、クラウド KMS で現在のバージョンの CMK をアクティブなままにしておきます。CMK がアクティブでない場合、顧客管理対象キーの無効化は失敗します。

このオプションを無効化すると、組織の暗号化キーは、Informatica が管理する暗号化キーを使用して再び暗号化されます。Informatica 暗号化キーがアクティブになるまでに最大 10 分かかる場合があります。

管理者で **【顧客管理対象キーの有効化】** オプションを無効化した後、クラウド KMS で CMK を無効化または削除できます。

CMK への Informatica のアクセスを一時的に取り消したい場合はどうすればよいですか？

CMK への Informatica のアクセスを一時的に取り消す場合は、クラウド KMS でキーを無効化できます。

CMK を無効にすると、Informatica Intelligent Cloud Services は組織の暗号化されたデータの暗号化を解除できなくなり、そのデータを使用するジョブは、クラウド KMS で CMK を再アクティブ化するまではすべて失敗します。

侵害された疑いがある場合、CMK を交換するにはどうすればよいですか？

CMK を交換する場合は、クラウド KMS でキーを削除して、新しいキーを作成します。

警告: クラウド KMS で CMK を削除すると、Informatica Intelligent Cloud Services の暗号化されたデータが完全に失われ、そのデータを使用するジョブが失敗する原因となります。

CMK を交換する必要がある場合は、次の手順を実行して、暗号化されたデータへのアクセスが失われず、ジョブが失敗することがないようにします。

1. 管理者で **【設定】** ページを開き、**【セキュリティ】** タブをクリックして、**【顧客管理対象キーの有効化】** オプションを無効化します。
2. クラウド KMS で、CMK を削除します。
3. クラウド KMS で、新しい CMK を作成します。
4. 管理者の **【設定】** ページで、**【顧客管理対象キーの有効化】** オプションを再度有効にし、新しい CMK の詳細を入力します。

暗号化されたデータに Informatica からアクセスしてほしくない場合、CMK を削除してかまいませんか？

警告: クラウド KMS で CMK を削除すると、Informatica Intelligent Cloud Services の暗号化されたデータが完全に失われ、そのデータを使用するジョブが失敗する原因となります。

Informatica Intelligent Cloud Services の暗号化されたデータに Informatica からアクセスすることをやめさせる場合は、クラウド KMS で CMK を削除できます。

シークレットマネージャの設定

資格情報を Informatica Intelligent Cloud Services リポジトリに保存するのではなく、外部シークレットマネージャから機密接続資格情報を取得するように組織を設定できます。シークレットマネージャは、シークレットコンテナまたは Key Vault とも呼ばれます。

シークレットマネージャを使用すると、次のような利点があります。

- パスワード、OAuth トークン、API 共有シークレットなどの機密接続資格情報を完全に制御できます。
- アプリケーションごとではなく、複数の環境にまたがってシークレットを管理できます。
- Informatica Intelligent Cloud Services の接続、マッピング、またはタスクに影響を与えることなく、スケジュールに従ってシークレットをローテーションできます。

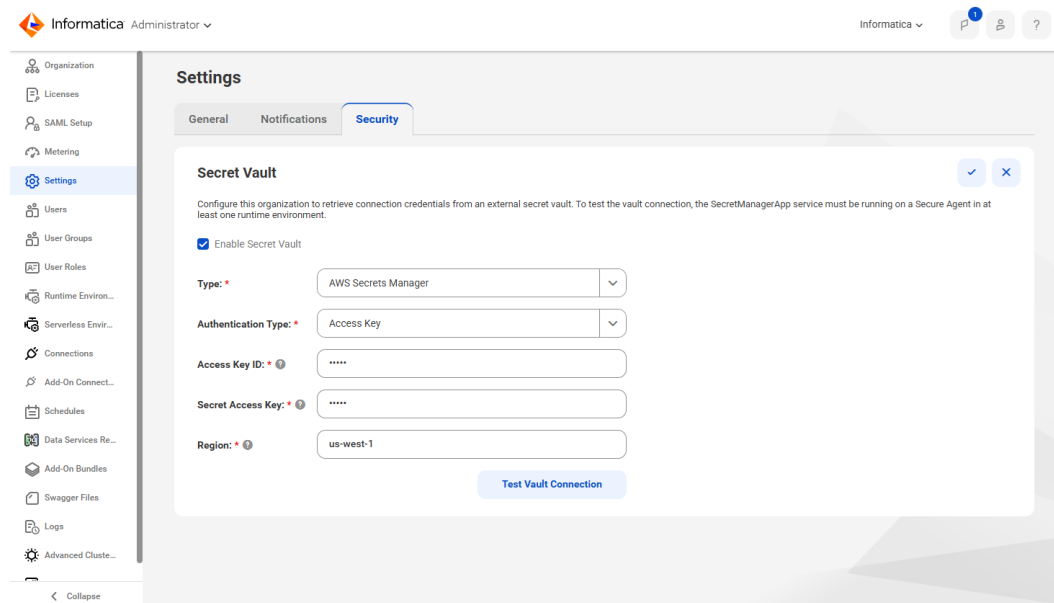
組織でシークレットマネージャの使用を有効にすると、Secure Agent はシークレットマネージャから機密接続資格情報に動的にアクセスできるようになります。組織またはサブ組織ごとに 1 つのシークレットマネージャを設定できます。

次のいずれかのシークレットマネージャを使用できます。

- AWS Secrets Manager
- Azure Key Vault
- HashiCorp Vault (HCP クラウドホスト)

AWS Secrets Manager を使用した場合、Secure Agent はロールベースの認証、インスタンスプロファイル認証、またはアクセスキー認証を使用して AWS Secrets Manager にアクセスできます。

次の図に示すように、**【設定】** ページの **【セキュリティ】** タブでシークレットマネージャを使用するように組織またはサブ組織を設定します。



シークレットマネージャを使用するように組織を設定するには、管理者ロール、または SMS 接続管理および SMS 接続表示の機能特権と、管理者サービスにアクセスするための十分な特権が必要です。また、接続資格情報をクラウドに保存するように組織を設定する必要があります。組織が接続資格情報をローカル Secure Agent に保存している場合は、シークレットマネージャを使用できません。

シークレットマネージャを使用するように組織を設定した後、シークレットマネージャから資格情報を取得するように接続を設定できます。

AWS Secrets Manager の設定

AWS Secrets Manager は、データベース資格情報、API キー、およびアプリケーションに必要なその他のシークレットなどの機密情報を安全に保存、管理、取得するために役立つフルマネージドの AWS サービスです。接続プロパティに認証情報を直接入力する代わりに、AWS Secrets Manager から機密性の高い接続資格情報を取得するように組織を設定することができます。

Secure Agent は、次のいずれかの認証方法を使用して Secrets Manager にアクセスします。

- ロールベースの認証。ロールベースの認証を使用する場合は、Secure Agent が使用する IAM ロールを設定する必要があります。

- インスタンスプロファイル認証。インスタンスプロファイル認証を使用する場合は、Secure Agent をホストする AWS リソースへのインスタンスプロファイルを設定してアクセスする必要があります。
- アクセスキー認証

シークレットをホストする AWS アカウントと、Secure Agent をホストするアカウントが異なる場合は、両方のアカウントでアカウント間アクセスを設定する必要もあります。

AWS Secrets Manager からシークレットを取得するように組織を設定するには、Administrator でシークレット Vault を有効にし、シークレットマネージャとして AWS Secrets Manager を選択して、接続プロパティを設定します。次に、Secrets Manager から機密性の高い資格情報を取得するように接続を設定することができます。

AWS Secrets Manager の IAM ロール設定

ロールベースの認証を使用して AWS Secrets Manager にアクセスする場合は、Secure Agent がシークレットへのアクセスに使用する IAM ロールに適切なポリシーと権限が割り当てられていることを確認する必要があります。また、ロールを EC2 インスタンスにアタッチする必要もあります。

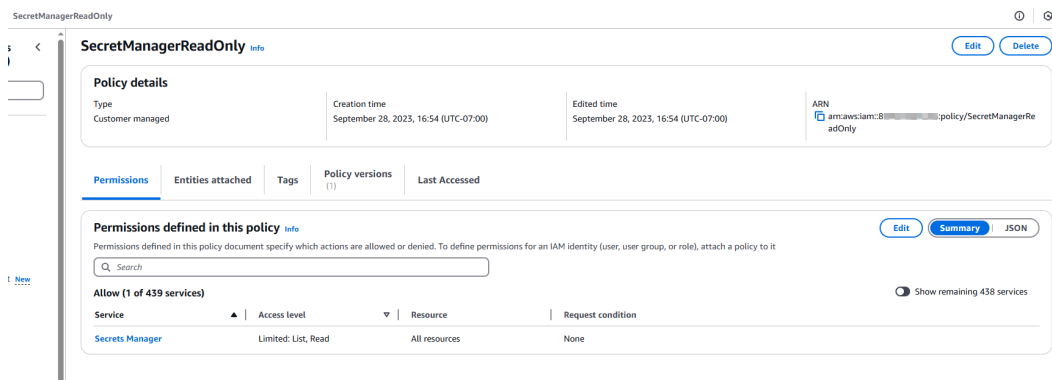
IAM ロールを設定するには、最初に適切な権限を持つポリシーを定義し、そのポリシーをロールに割り当ててから、ロールの信頼ポリシーを更新します。

手順 1.IAM ポリシーの作成と適切な権限の割り当て。

次のポリシーを設定します。

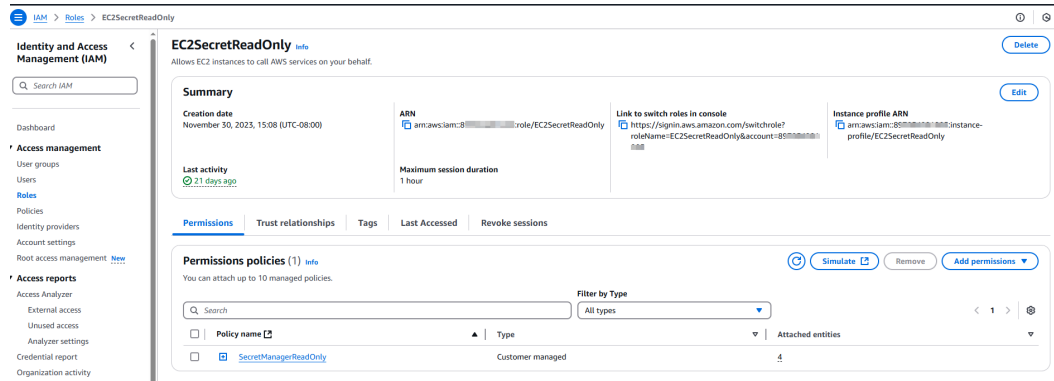
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*"
    }
  ]
}
```

ポリシーは、シークレットマネージャからのシークレットの一覧表示および読み取りが許可されている必要があります。次の画像に、必要な最小限のポリシーを示します。



手順 2. IAM ロールへのポリシーの割り当て。

作成したポリシーを、Secure Agent がシークレットにアクセスするために使用するロールに割り当てます（次の画像を参照）。



手順 3. IAM ロールの信頼ポリシーの更新。

ポリシーを割り当てた後に、IAM ロールの信頼ポリシーを更新して、ロールにアクセスできる AWS リソースを定義します。この操作を行うには、任意の EC2 VM インスタンスにロールへのアクセスを許可するか、EC2 インスタンスのロールによる、シークレットの読み取り権限を持つロールの引き受けを許可します。

IAM ロールが EC2 インスタンスのロールと同じロールである場合は、ロール自体を引き受けることができます。

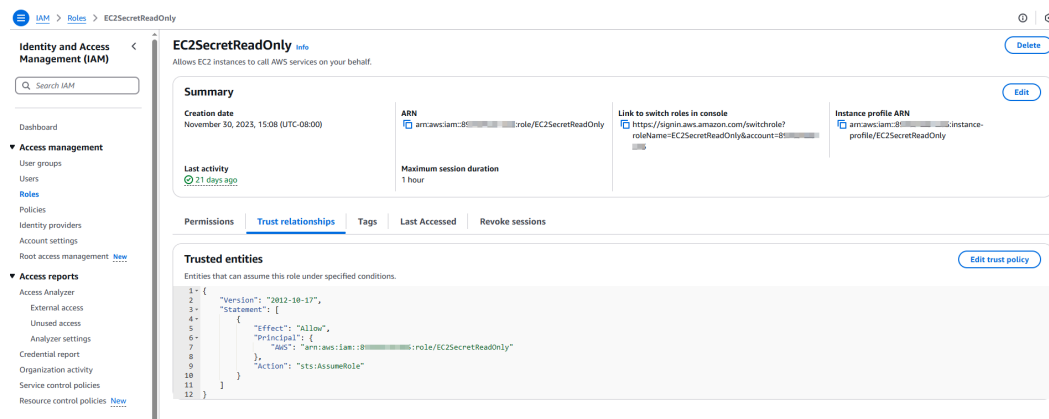
任意の EC2 VM インスタンスによるロールへのアクセスを許可するには、次の信頼ポリシーを設定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

EC2 インスタンスのロールによる、シークレットの読み取り権限を持つロールの引き受けを許可するには、次の信頼ポリシーを設定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<account ID>:role/<EC2 instance's role>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

次の画像に、信頼ポリシーを示します。

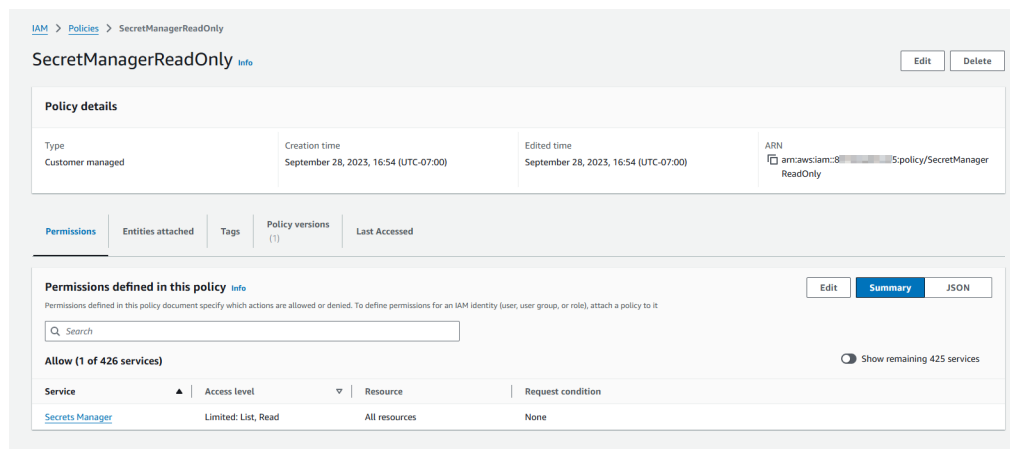


IAM ロールへのポリシーの割り当てと EC2 インスタンスへの IAM ロールのアタッチの詳細については、AWS のマニュアルを参照してください。

AWS Secrets Manager のインスタンスプロファイル設定

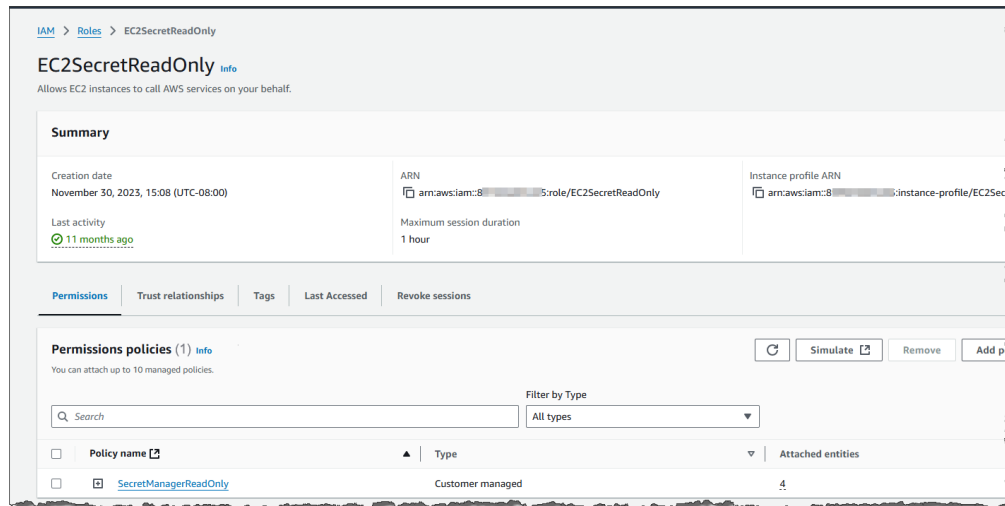
インスタンスプロファイル認証を使用して AWS Secrets Manager にアクセスする場合は、シークレットを読み取ることができる IAM ポリシーを作成し、このポリシーを持つロールを作成してから、Secure Agent をホストする AWS リソースにインスタンスプロファイルをアタッチする必要があります。

1. AWS マネジメントコンソールにログインします。
2. IAM コンソールに移動します。
3. **【アクセス管理】** で、**【ポリシー】** を選択します。
4. **【ポリシーの作成】** をクリックします。
5. 次の図に示すように、**【すべてのリストアクション】** および **【すべての読み取りアクション】** アクセスレベルを持つ IAM ポリシーを作成します。



6. **【アクセス管理】** で、**【ロール】** を選択します。
7. **【ロールの作成】** をクリックします。
8. **【信頼できるエンティティの選択】** ページで、信頼できるエンティティタイプとして **【AWS サービス】**、ユースケースとして **【EC2】** を選択し、**【次へ】** をクリックします。
9. **【権限の追加】** ページで、作成したポリシーを選択し、**【次へ】** をクリックします。

10. 次の図に示すように、ロール名を入力し、権限ポリシーを確認して、ロールを作成します。



11. EC2 ダッシュボードに移動し、Secure Agent をホストする EC2 インスタンスを選択します。
12. **【詳細】** をクリックします。
13. **【IAM インスタンスプロファイル】** で、作成した IAM ロールを選択して、EC2 インスタンスを起動します。

AWS Secrets Manager のアカウント間アクセス設定

シークレットをホストする AWS アカウントと、Secure Agent をホストするアカウントが異なる場合は、両方のアカウントでアカウント間アクセスを設定する必要があります。

シークレットマネージャを使用するように接続を設定する場合は、接続のランタイム環境を選択します。ランタイム環境に、AWS アカウント内でホストされている Secure Agent が含まれており、このアカウントがシークレットをホストするアカウントと異なる場合は、アカウント間アクセスを設定する必要があります。Secure Agent がシークレットにアクセスできるように、アカウント間アクセスを設定します。

注: アカウント間アクセスを設定するには、シークレットをホストするリソースが、組織でシークレットマネージャを使用できるよう設定したときに選択したリージョンと同じリージョンにある必要があります。組織でシークレットマネージャを使用できるように設定する方法の詳細については、[「シークレットマネージャの有効化と無効化」](#) (ページ 80) を参照してください。

手順 1. シークレットをホストするアカウントを設定します。

シークレットをホストするアカウントを設定するには、カスタママネージド KMS キーを作成し、そのキーを使用してシークレットを暗号化して、シークレットにリソースポリシーをアタッチする必要があります。アカウント間アクセスに AWS マネージドキーを使用することはできません。

以下の手順を実行します。

1. 次の手順を実行して、KMS キーを作成します。
 - a. AWS マネジメントコンソールにログインし、「Key Management Service」または「KMS」を検索します。
 - b. **【顧客管理対象キー】** に移動します。

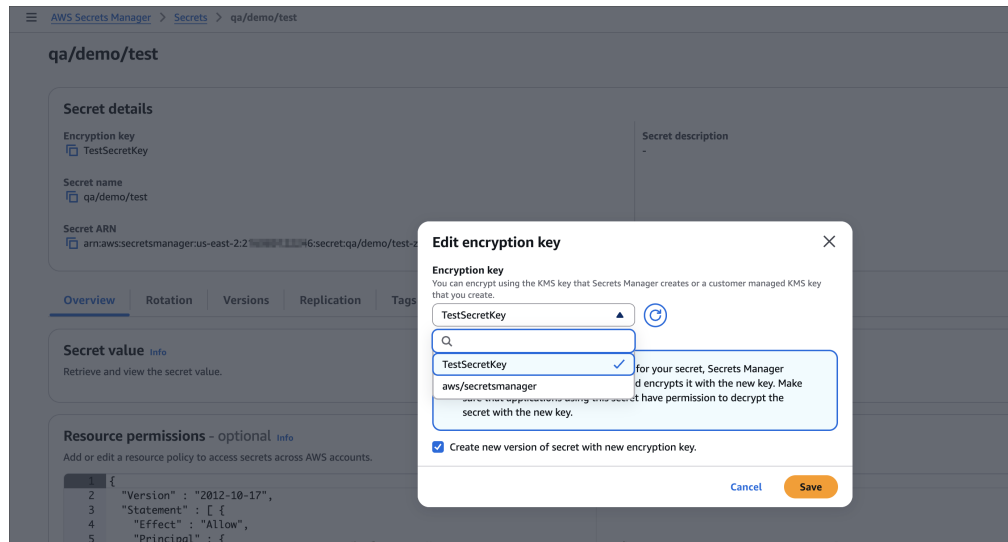
- c. 次のプロパティを持つ新しいカスタマネージドキーを作成します。

プロパティ	値
キータイプ	対称
キーの用途	暗号化と復号
キー管理者	キーを管理する IAM ユーザーまたはロールを選択します。
キーユーザー	キーを使用してシークレットの暗号化と復号を行う IAM ユーザーまたはロールを選択します。

- d. Secure Agent をホストするアカウントの IAM ロールへのアクセスを許可するように、次のキーポリシーを設定します。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::<Secure Agent account>:role/EC2SecretReadOnly"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

2. 次の図に示すように、カスタマネージドキーを使用してこのアカウントのシークレットを暗号化し、[保存] をクリックします。



3. 次のリソースポリシーをシークレットにアタッチします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<Secure Agent account>:role/<application_role>"
      },
    },
  ],
}
```

```

    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
  }
]
}

```

手順 2. Secure Agent をホストするアカウントを設定します。

Secure Agent をホストするアカウントを設定するには、エージェントが使用するロールに ID ポリシーをアタッチし、エージェントをホストするアカウントが、シークレットをホストするアカウントから KMS キーを取得できることを確認します。

エージェントがシークレットにアクセスするために使用するロールに、次の ID ポリシーをアタッチします。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "<secret ARN of secrets account>"
    },
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "<KMS key ARN of secrets account>"
    }
  ]
}

```

エージェントをホストするアカウントが KMS キーを取得できることを確認するには、エージェントをホストするアカウントの EC2 インスタンスから次のコマンドを実行します。

```
aws secretsmanager get-secret-value --secret-id '<secret ARN>'
```

アカウント間アクセスの設定の詳細については、AWS のドキュメントの [Access AWS Secrets Manager secrets from a different account](#) を参照してください。

AWS Secrets Manager のシークレット名

AWS Secrets Manager は、シークレット名に制限を適用します。

AWS Secrets Manager では、シークレット名に英数字と次の特殊文字のみを含めることができます。

```
/ _ + = . @ - "
```

シークレット名の詳細については、AWS Secrets Manager のマニュアルを参照してください。

AWS Secrets Manager 接続プロパティ

シークレットマネージャとして AWS Secrets Manager を選択した場合は、認証タイプやリージョンなどの接続プロパティを設定します。接続プロパティは、認証タイプによって異なります。

ロールベースの認証

ロールベースの認証を使用して Secrets Manager にアクセスする場合は、次のプロパティを設定します。

プロパティ	説明
タイプ	シークレットマネージャのタイプ。[AWS Secrets Manager] を選択します。
認証タイプ	Secure Agent が Secrets Manager にアクセスするために使用する認証タイプ。ロールベースの認証の場合は、[ロールベースのアクセス] を選択します。
IAM ロール	Secure Agent がシークレットにアクセスするために使用する IAM ロールの Amazon Resource Name (ARN)。通常、形式は次のようになります。 <code>arn:aws:iam::<アカウント>:role/<パス付きのロール名></code> 注: IAM ロールは、「 AWS Secrets Manager の IAM ロール設定 」(ページ 70)に記載されているように設定する必要があります。Secure Agent をホストする AWS リソースは、このロールにアクセスできる必要があります。
外部 ID	IAM ロールを引き受けるには外部 ID が必要です。 サーバーレスエージェントの場合は必須です。
リージョン	Secrets Manager シークレットがホストされている地域のリージョンコード (us-east-2 など)。US East (Ohio)のような完全なリージョン名は入力しないようにしてください。
STS エンドポイント	リージョナルエンドポイントまたは手動で設定したエンドポイントを使用している場合は、STS エンドポイントの URL。 例えば、サービスエンドポイントが米国西部(北カリフォルニア)の場合は、次の値を入力します。 <code>https://secretsmanager.us-west-1.amazonaws.com</code> 指定されていない場合、グローバルエンドポイント <code>https://sts.amazonaws.com</code> が使用されます。
STS エンドポイントのリージョン	us-west-1 などのサービスエンドポイントが配置されているリージョン。 STS エンドポイントのリージョンが Secrets Manager のリージョンと異なる場合は、このプロパティに値を入力します。指定されていない場合、STS エンドポイントのリージョンは Secrets Manager のリージョンと同じであるとみなされます。

インスタンスプロファイル認証

インスタンスプロファイル認証を使用してシークレットマネージャにアクセスする場合は、次のプロパティを設定します。

プロパティ	説明
タイプ	シークレットマネージャのタイプ。[AWS Secrets Manager] を選択します。
認証タイプ	Secure Agent が Secrets Manager にアクセスするために使用する認証タイプ。インスタンスプロファイル認証の場合は、[インスタンスプロファイル] を選択します。
地域	Secrets Manager シークレットがホストされている地域のリージョンコード (us-east-2 など)。 US East (Ohio)のような完全なリージョン名は入力しないようにしてください。

アクセスキー認証

アクセスキーを使用して Secrets Manager にアクセスする場合は、次のプロパティを設定します。

プロパティ	説明
タイプ	シークレットマネージャのタイプ。[AWS Secrets Manager] を選択します。
認証タイプ	Secure Agent が Secrets Manager にアクセスするために使用する認証タイプ。アクセスキー認証の場合は、[アクセスキー] を選択します。
アクセスキー ID	Secure Agent がシークレットにアクセスするために使用する AWS アクセスキー ID (例: AKIAIOSFODNN7EXAMPLE)。 アクセスキー ID は、GetSecretValue および ListSecrets 権限を持つアクセスポリシーが割り当てられた IAM ロールに関連付ける必要があります。 アクセスキー ID とシークレットアクセスキーを入力する必要があります。
シークレットアクセスキー	Secure Agent がシークレットにアクセスするために使用する AWS シークレットアクセスキー (例: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)。 アクセスキー ID とシークレットアクセスキーを入力する必要があります。
リージョン	Secrets Manager シークレットがホストされている地域のリージョンコード (us-east-2 など)。 US East (Ohio)のような完全なリージョン名は入力しないようにしてください。

AWS Secrets Manager のプロパティの詳細については、AWS のドキュメントを参照してください。

Azure Key Vault の設定

Azure Key Vault は、クラウドアプリケーションとサービスで使用する暗号化キー、シークレット、および証明書を保護するように設計された、Microsoft Azure によって提供されるクラウドサービスです。これは、組織がトークン、パスワード、API キー、暗号化キー、およびその他の機密情報へのアクセスを安全に保存および制御するために役立ちます。接続プロパティに資格情報を直接入力する代わりに、Azure Key Vault から機密性の高い接続資格情報を取得するように組織を設定することができます。

Azure Key Vault からシークレットを取得するように組織を設定するには、Administrator でシークレット Vault を有効にし、シークレットマネージャとして Azure Key Vault を選択して、接続プロパティを設定します。次に、Azure Key Vault から機密性の高い資格情報を取得するように接続を構成することができます。

Azure Key Vault シークレット名

Azure Key Vault では、シークレット名に英数字とダッシュのみを含めることができます。

シークレットの名前と形式の詳細については、Azure Key Vault のドキュメントを参照してください。

Azure Key Vault 接続プロパティ

シークレットマネージャとして Azure Key Vault を選択した場合は、クライアント ID、クライアントシークレット、テナント ID などの接続プロパティを設定します。

以下のプロパティを設定します。

プロパティ	説明
タイプ	シークレットマネージャのタイプ。[Azure Key Vault] を選択します。
クライアント ID	Secure Agent が Key Vault に接続するために使用するアプリケーション（クライアント）ID。 クライアント ID は、アプリの登録時に Azure AD によって割り当てられた一意のアプリケーション（クライアント）ID です。 ヒント: アプリケーション（クライアント）ID は、Azure サブスクリプションの [Azure Active Directory] > [エンタープライズアプリケーション] > [アプリケーション（クライアント）ID] で確認できます。 指定するアプリケーション（クライアント）には、シークレットの取得およびリストに対する権限が必要です。
クライアントシークレット	Secure Agent が Key Vault へのアクセスを要求するときに ID を証明するために使用するシークレット文字列。
テナント ID	Key Vault への要求の認証に使用する Azure Active Directory（テナント）ID。
Vault URI	接続の資格情報を格納する Key Vault の URI。
オーソリティホスト	オーソリティホストエンドポイントの URL。指定されていない場合、グローバルエンドポイント https://login.microsoftonline.com が使用されます。

Azure Key Vault のプロパティの詳細については、Azure のドキュメントを参照してください。

HashiCorp Vault の設定

HashiCorp Vault は、シークレットを管理し、機密データを保護するために設計されたツールです。アプリケーションで使用されるトークン、パスワード、証明書、暗号化キー、およびその他のシークレットへのアクセスを保存、管理、制御するための安全な方法を提供します。接続プロパティに資格情報を直接入力する代わりに、HashiCorp Vault から機密性の高い接続資格情報を取得するように組織を設定することができます。

Vault からシークレットを取得するように組織を設定するには、Administrator でシークレット Vault を有効にし、シークレットマネージャとして HashiCorp Vault を選択して、接続プロパティを設定します。次に、Vault から機密性の高い資格情報を取得するように接続を設定することができます。

HashiCorp Vault 認証

Informatica Intelligent Cloud Services は、AppRole 認証を使用して HashiCorp Vault で認証します。認証が成功すると、Vault は Informatica Intelligent Cloud Services にクライアントトークンを発行します。このトークンには、AppRole にアタッチされているポリシーが含まれています。

トークンには次のいずれかのタイプを指定できます。

- バッチトークン。バッチトークンの有効期間は短時間で固定されており、更新することはできません。実行時間の長いジョブには推奨されません。
- サービストークン。サービストークンは、実行時間の長いジョブに適しており、更新して有効期間を延ばすことができます。Vault はデフォルトでサービストークンを発行します。

サービストークンの有効期間は長く、更新可能であるため、Informatica Intelligent Cloud Services にサービストークンを発行するように HashiCorp Vault AppRole を設定する必要があります。Vault がバッチトークンを発行し、トークンの有効期限が切れた場合、Secure Agent は Vault に接続してシークレットを取得することができません。

クライアントトークンの詳細については、HashiCorp Vault のドキュメントを参照してください。

HashiCorp Vault のシークレット形式

HashiCorp Vault では、シークレットの形式はシークレットエンジンのバージョンに応じて異なります。

Vault では、シークレットは、シークレットエンジンのバージョンに基づいて、次のいずれかの形式にする必要があります。

シークレットエンジンのバージョン	形式
シークレットエンジン v1	secret/<secret_path>:<key>
シークレットエンジン v2	secret/data/<secret_path>:<key>

注: シークレットパスとキーを区切るためにコロンが使用されるため、Informatica Intelligent Cloud Services ではパスにコロンを含むキーは処理されません。

シークレットの名前と形式の詳細については、HashiCorp Vault のドキュメントを参照してください。

HashiCorp Vault の接続プロパティ

シークレットマネージャとして HashiCorp Vault を選択した場合は、ロール ID、シークレット ID、Vault URI などの接続プロパティを設定します。

以下のプロパティを設定します。

プロパティ	説明
タイプ	シークレットマネージャのタイプ。【HashiCorp Vault】を選択します。
ロール ID	Secure Agent が Vault での認証に使用する AppRole の ID。 AppRole には、シークレットの読み取り権限と一覧表示権限が必要です。
シークレット ID	Secure Agent が Vault での認証に使用する AppRole のシークレット ID。
Vault URI	接続の資格情報が格納されている Key Vault の URI。例: <code>https://my-hashicorp-vault-12343a56.a1b2345c.z1.hashicorp.cloud:8200</code>

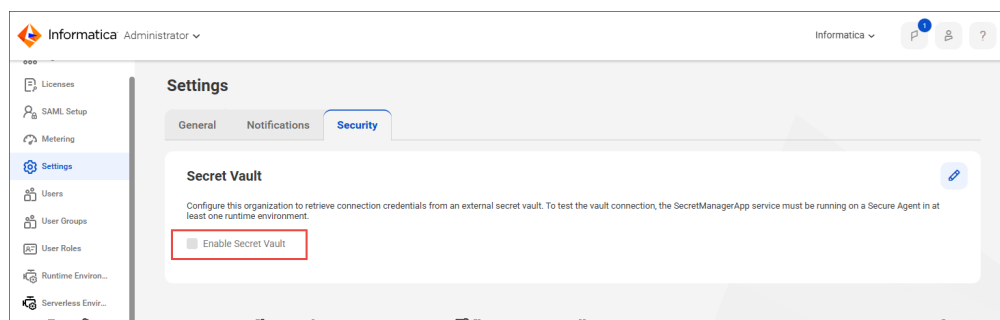
プロパティ	説明
名前空間	キーコンテナ内の名前空間(使用される場合)。
AppRole パス	AppRole 認証方法が有効にされたカスタムパス。指定されていない場合、値はデフォルトのパス <code>approle</code> であるとみなされます。

HashiCorp Vault のプロパティの詳細については、HashiCorp のマニュアルを参照してください。

シークレットマネージャの有効化と無効化

【設定】 ページの **【セキュリティ】** タブで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ます。

1. 【設定】 ページで、**【セキュリティ】** タブを開きます。
2. 編集（鉛筆）アイコンをクリックします。
3. 次の図に示すように、**【シークレットコンテナを有効にする】** を選択します。



4. 使用するシークレットマネージャ（AWS Secrets Manager、Azure Key Vault、または HashiCorp Vault）を選択します。
5. Vault URI、認証タイプ、リージョンなどの接続の詳細を入力します。
6. 接続をテストします。

接続をテストするときは、ランタイム環境を選択する必要があります。ランタイム環境内のすべての Secure Agent はローカルマシンまたは VM にインストールされており、SecretManagerApp サービスが各エージェントで実行されている必要があります。ホステッドエージェントとサーバーレスエージェントは、外部シークレットマネージャに接続できません。

接続が成功した後に、シークレットマネージャを使用するように接続を設定できます。

シークレットマネージャの使用を無効にするには、**【シークレットコンテナを有効にする】** オプションをオフにします。ただし、最初にすべての接続で **【シークレットコンテナの使用】** オプションを無効にする必要があります。

サブ組織のシークレットマネージャの設定

サブ組織のシークレットマネージャを設定できます。この操作を行うには、サブ組織にログインし、シークレットマネージャを有効にします。

サブ組織のシークレットマネージャを有効にする場合は、SecretManagerApp サービスがサブ組織のネイティブな Secure Agent で実行されていることを確認してください。SecretManagerApp サービスが、親組織から共有された Secure Agent で実行されている場合は、親組織に設定されたシークレットマネージャにのみ接続することができます。サブ組織に設定されているシークレットマネージャに接続することはできません。

SecretManagerApp Secure Agent サービスの詳細については、「Secure Agent サービス」を参照してください。

シークレットマネージャを使用するための接続の設定

機密資格情報を持つ接続を設定して、シークレットマネージャからこれらの資格情報を取得できます。

注: 外部シークレットマネージャから機密情報である接続資格情報を取得するように設定されている一部の組織では、ユーザーは管理者で接続を作成する必要があります。これらの組織のユーザーは、データ統合で接続の作成や編集を行うことはできません。

1. **【接続】** ページを開きます。
2. 以下のいずれかのアクションを実行します。
 - 接続を作成するには、**【新しい接続】** をクリックし、接続の詳細を入力します。
 - 接続を編集するには、接続名をクリックしてから **【編集】** をクリックします。
3. **【接続プロパティ】** 領域で、**【シークレットコンテナの使用】** を選択します。
4. シークレットマネージャに保存するそれぞれのプロパティの横にあるオプションを有効にし、対応するフィールドにシークレット名を含めたパスを入力します。シークレットが JSON オブジェクトの場合は、シークレットキーも含める必要があります。

次の表は、シークレットの形式に応じて入力する値を示しています。

シークレットの形式	入力する値の形式
次のような JSON オブジェクト <pre>{ "engine": "mysql", "username": "tsmith", "password": "Hello123", "host": "my-database-endpoint.us-west-2.rds.amazonaws.com", "dbname": "myDatabase", "port": "1234" }</pre>	<secret_path>:<key> または、AWS Secrets Manager を使用する場合は、シークレットの完全な ARN を次の形式で入力できます*。 arn:aws:secretsmanager:<region>:<account_ID>:secret:<secret_name>-<6_random_characters>:<secret_path>
次のような単純な値 --name "MyPassword" --value "Hello123"	<secret_path> または、AWS Secrets Manager を使用する場合は、シークレットの完全な ARN を次の形式で入力できます*。 arn:aws:secretsmanager:<region>:<account_ID>:secret:<secret_name>-<6_random_characters>
* AWS Secrets Manager を使用しており、Secure Agent をホストするアカウントがシークレットをホストするアカウントと異なる場合は、シークレットの完全な ARN を入力する必要があります。	

例えば、リレーショナル接続を設定し、データベースのパスワードを HashiCorp Vault に保存するとします。シークレットへのパスは secret/data/MyCredentials で、シークレットキーは MyPassword です。HashiCorp Vault からパスワードを取得するには、**【シークレットコンテナの使用】** を選択し、**【パスワード】** フィールドの横にあるオプションを有効にして、**【パスワード】** フィールドに「secret/data/MyCredentials:MyPassword」と入力します。

次の図は、接続の詳細を示しています。

5. 接続で使用するランタイム環境を選択します。

ランタイム環境内のすべての Secure Agent はローカルマシンまたは VM にインストールされており、シークレットマネージャにアクセスできる必要があります。さらに、SecretManagerApp サービスが各エージェントで実行されている必要があります。

6. 接続固有のプロパティを設定します。
7. 接続をテストするには、**【テスト接続】** をクリックします。
8. **【保存】** をクリックします。

接続の設定の詳細については、「[接続](#)」を参照してください。

セキュリティ設定

管理者は、**【設定】** ページの **【セキュリティ】** タブで、Informatica の従業員が組織の詳細を表示できるかどうかを制御できます。

Informatica サポートアクセスを削除すると、サポートケースの解決が遅れる可能性があります。Informatica サポートアクセスを削除する場合は、次のようなことに注意してください。

- サポートチケットを提出するときに、関連するサービスとタスクのログ、または組織のアセットを手動でアップロードする必要がある場合があります。
- Informatica サポートは、新しいリリースやその他のメンテナンスイベント中にジョブを監視して、潜在的な影響を評価することはできません。
- Informatica サポートとトラブルシューティングを行う際には、画面を共有する必要がある場合があります。
- Informatica は、今後のリリースが組織にどのような影響を与えるかについて通知することはできません。

Informatica サポートアクセスの削除

Informatica のサポートアクセスを削除して、アセットとセキュリティをより詳細に制御することができます。アクセスを削除すると、Informatica がサポートケースを解決できるように、アクセスを一時的に有効にすることができます。

1. 管理者で、**【設定】** ページに移動します。
2. **【Informatica グローバルサポートアクセス】** セクションで、**【Informatica グローバルサポートアクセスを無効にする】** を選択します。このチェックボックスには管理者のみがアクセスできます。

一時的なアクセス権を付与して、サポートケースのトラブルシューティング中に Informatica のサポートが組織のデータを表示できるようにすることができます。Informatica サポートアクセスを一時的に有効にするには、**【アクセスを一時的に有効にする】** を選択し、アクセスを再度削除する日時を入力します。

第 5 章

権限

権限によって、Secure Agent、Secure Agent グループ、接続、スケジュール、またはアセットに対するユーザーのアクセス権が決まります。また、オブジェクトに対する追加またはカスタムのセキュリティを追加します。権限によって、オブジェクトに対する権限の読み取り、更新、削除、実行、および変更が可能なユーザーおよびグループが定義されます。

ユーザーアカウント、または管理者がメンバとなっているグループに割り当てられたロールには、オブジェクトタイプに対する権限の設定特権が必要です。例えば、Secure Agent の権限を構成するには、Secure Agent に対する権限の設定特権を持つロールが割り当てられる必要があります。

オブジェクトの権限を構成するには、オブジェクトに移動して適切な権限を設定します。例えば、開発チームのユーザーグループのユーザーだけが開発データフォルダのアセットにアクセスできるようにします。フォルダに移動し、権限を編集し、フォルダに開発チームのユーザーグループの権限を付与します。

権限は、オブジェクトのコピーではなく、設定したオブジェクトに適用されます。したがって、アセットをコピーまたはエクスポートする場合、その権限はアセットと一緒にコピーまたはエクスポートされません。例えば、ユーザー `rjones` が実行権限を持っているマッピングタスクをエクスポートします。マッピングタスクをインポートすると、インポートされたマッピングには割り当てられた権限がありません。したがって、マッピングタスクを実行する特権を持つユーザーは、インポートされたタスクを実行できます。

オブジェクトに対して次の権限を構成できます。

権限	説明
読み取り	オブジェクトを開いて表示します。 オブジェクトがソース管理されている場合、この権限を持つユーザーまたはグループは、オブジェクトをソース管理リポジトリからプルまたはチェックアウトできます。操作を実行するには、統合ハブ接続にアクセスするための読み取り権限が必要です。 タスクを選択すると、この権限によって、ユーザーまたはグループが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	オブジェクトを編集します。 オブジェクトがソース管理されている場合、この権限によって、ユーザーまたはグループは、オブジェクトをチェックイン、チェックアウト、プル、リンク解除、またはロールバックできます。 読み取り権限が必要です（自動的に付与される）。
削除	オブジェクトを削除します。
実行	オブジェクトを実行します。 マッピング、タスク、タスクフロー、および Cloud 統合ハブアセットに適用されます。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、および再起動します。
権限の変更	オブジェクトに割り当てられている権限を変更します。

注: これらの権限は、Informatica Intelligent Cloud Services 内で制御されます。Windows や Linux で Secure Agent を起動、停止、または設定する場合の権限のような、オペレーティングシステムの権限を制御するものではありません。

権限のルールおよびガイドライン

権限には、次の規則とガイドラインを使用します。

- オブジェクトの権限を構成するときに、権限を付与するユーザーまたはグループに、そのオブジェクトタイプに対する適切な特権を持つロールが割り当てられていることを確認します。
- 例えば、ユーザーに特定のフォルダに対するサービスコンシューマロールの更新特権があっても、サービスコンシューマロールにはフォルダの更新特権がないため、ユーザーはフォルダを更新できません。
- アセットを編集するには、アセット内で使用されているすべてのアセットに対する読み取り権限がユーザーに与えられている必要があります。例えば、同期タスクに対する読み取りおよび更新の権限をユーザーに割り当てた場合、そのユーザーにタスクで使用されている接続、マップレット、スケジュール、および保存されたクエリに対する読み取り権限もあることを確認します。
- マッピングタスクを実行するサブスクリプションまたはパブリケーションを実行するには、マッピングタスクを含むプロジェクトとフォルダに対する更新特権がユーザーに割り当てられている必要があります。
- ユーザーがタスクを編集すると、読み取り権限のないアセットは表示されません。予期しない結果を回避するには、ユーザーが適切な読み取り権限を付与されるまで、すべての変更をキャンセルし、タスクの編集を回避する必要があります。
- タスクフローを構成する場合、ユーザーは、タスクフローに追加するすべてのタスクに対する実行権限を必要とします。
- タスクフローを編集するには、タスクフローのすべてのタスクに対して実行権限が必要です。すべてのタスクに対して実行権限がない場合、ユーザーはタスクフローに変更を保存できません。
- タスクフローを実行するには、ユーザーにタスクフローに対する読み取り権限と実行権限が必要です。
- ジョブを監視したり、実行中のジョブを停止したりするには、ユーザーはマッピング、タスク、またはタスクフローの実行権限を必要とします。
- 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。

権限の設定

オブジェクトタイプに対する権限の設定特権を持つロールが割り当てられている場合は、オブジェクトの権限を構成できます。例えば、フォルダの権限を構成するには、フォルダの権限の設定特権を持つロールが割り当てられている必要があります。

1. 権限を構成するオブジェクトに移動します。



例:

- Secure Agent または Secure Agent グループの権限を構成するには、管理者で **【ランタイム環境】** を選択します。
 - 接続の権限を構成するには、管理者で **【接続】** を選択します。
 - マッピングの権限を構成するには、データ統合でマッピングを含むプロジェクトとフォルダを開きます。
2. オブジェクトを含む行で、**【アクション】** をクリックして **【権限】** を選択するか、**【権限の変更】** アイコンをクリックします。

【権限】 ダイアログボックスには、オブジェクトに対する権限を持つユーザーとグループが一覧表示されます。

【権限】 ダイアログボックスにユーザーまたはグループが一覧表示されない場合は、そのオブジェクトに対して権限が構成されていません。オブジェクトタイプに対して適切な特権を持つユーザーは、オブジェクトにアクセスできます。

次の図は、マッピングの **【権限】** ダイアログボックスを示しています。


Permissions: m_FilterAndSortCustRecords  

Users and Groups with permissions on the asset are listed here. Other Users have no access to the asset. If no Users or Groups are listed, then this asset has no permissions restrictions.

Users Groups

<input type="checkbox"/>	User Name	First Name	Last Name	Read	Update	Delete	Execute	Change Per...
<input type="checkbox"/>	jsmith	John	Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	jrandolp	Jane	Randolph	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add **Remove**

 **Save** **Cancel**

3. オブジェクトに対するユーザー権限を構成するには:
- a. **【ユーザー】** を選択します。
 - b. ユーザーが **【ユーザー】** の一覧に表示されていない場合は、**【追加】** をクリックし、ユーザーを選択します。
 - c. ユーザーに対する適切な権限を有効または無効にします。
- 注:** オブジェクトに対するユーザー権限を付与すると、Informatica Intelligent Cloud Services によって管理者もオブジェクトに対するアクセス権限を持つユーザーとして追加されます。これにより、権限を構成するときにオブジェクトへのアクセスが失われるのを防ぎます。
4. オブジェクトに対するユーザーグループの権限を構成するには:
- a. **【グループ】** を選択します。
 - b. グループが **【グループ】** の一覧に表示されていない場合は、**【追加】** をクリックし、グループを選択します。
 - c. グループに対する適切な権限を有効または無効にします。

注: オブジェクトに対するグループの権限を付与すると、Informatica Intelligent Cloud Services によって管理者もオブジェクトに対するアクセス権限を持つユーザーとして追加されます。これにより、権限を構成するときにオブジェクトへのアクセスが失われるのを防ぎます。

5. オブジェクトの権限の制限をすべて削除するには、**【権限】** ダイアログボックスからすべてのユーザーとグループを削除します。

すべてのユーザーとグループを削除すると、そのオブジェクトタイプに対して適切な特権を持つすべてのユーザーがオブジェクトにアクセスできるようになります。

6. **【保存】** をクリックします。

第 6 章

スケジュール

タスクまたはタスクフローを、指定した時間または一定の間隔で実行するようにスケジュールを作成できます。また、スケジュールされたタスクまたはジョブが実行されないブラックアウト期間を定義することもできます。

プロジェクトスケジュールで作成、読み取り、更新、削除、または権限の設定を行うには、Administrator アセット特権のスケジュール権限が必要です。スケジュールを作成し、**Administrator** の管理者ページでブラックアウト期間を設定します。スケジュールを作成した後に、データ統合でデータ統合。

スケジュールを作成するときは、日付と時刻を指定します。関連付けられたアセットを午前 12:00 から午後 11:55 の間の一日中実行するようにスケジュールすることができます。Informatica Intelligent Cloud Services によって、開始時刻、終了時刻などのすべての時間設定に短いスケジュールオフセットが追加される場合があります。その結果、スケジュールされたタスクとタスクフローは、予想よりも後で開始される場合があります。たとえば、正午まで 1 時間ごとに実行するようにスケジュールを設定し、組織のスケジュールオフセットが 10 秒であるとしします。Informatica Intelligent Cloud Services では、スケジュールの終了時刻が午後 12:00:10 に延長されます。1 時間ごとの最後のタスクまたはタスクフローは午後 12:00:10 に開始されます。組織のスケジュールオフセットを確認するには、データ統合サービスの **【スケジュールオフセット】** 組織プロパティを確認してください。

スケジュールでは次のタスクを実行できます。

スケジュールとタスクまたはタスクフローの関連付け

タスクまたはタスクフローにスケジュールを関連付けるには、タスクまたはタスクフローを編集します。例えば、スケジュールをマッピングタスクに関連付けるには、データ統合でマッピングタスクを編集し、**【スケジュール】** ページでスケジュールを選択します。

スケジュールを含むタスクまたはタスクフローをコピーすると、そのスケジュールは新しいアセットに関連付けられません。スケジュールを新しいアセットに関連付けるには、アセットを編集します。

スケジュール済みタスクの監視

モニタの **【すべてのジョブ】** ページからスケジュールされたタスクを監視することができます。スケジュールされたタスクは、**【マイジョブ】** ページには表示されません。

スケジュールのエクスポート

組織からスケジュールをエクスポートして、別の組織にインポートできます。**【スケジュール】** ページでスケジュールをエクスポートします。スケジュールがタスクまたはタスクフローに関連付けられている場合、タスクまたはタスクフローはエクスポートファイルに含まれません。

スケジュールの削除

管理者の **【スケジュール】** ページでスケジュールを削除します。

注: タスクまたはタスクフローで使用されているスケジュールを削除することはできません。スケジュールを削除する前に、すべてのタスクとタスクフローからスケジュールを削除します。

ブラックアウト期間の設定

ブラックアウト期間を設定すると、指定した期間中は組織内のすべてのスケジュールされたタスクおよびタスクフローが実行できなくなります。スケジュールされたデータ統合およびデータ取り込みおよびレプリケーションファイルのパブリケーションおよびファイルサブスクリプションが期間中に実行されない、ブラックアウト期間を設定できます。

組織またはサブ組織ごとに1つのブラックアウト期間を設定できます。親組織に設定したブラックアウト期間は、サブ組織には影響しません。

タスクがブラックアウト期間中に実行されるようにスケジュールされている場合、タスクインスタンスはブラックアウト期間中に開始されず、ブラックアウト期間が終了しても自動的に再開されません。ブラックアウト期間の後、タスクインスタンスはスケジュールに従って再開されます。ブラックアウト期間の開始時にタスクがすでに実行されている場合、そのタスクは停止されません。

ブラックアウト期間を設定するには、管理者で **【スケジュール】** を選択し、**【ブラックアウト期間】** をクリックします。ブラックアウト期間が **【スケジュール】** ページに表示されます。

繰り返し頻度

繰り返し頻度では、タスクを実行する頻度を決定します。繰り返し頻度は、N 分ごと、毎時、毎日、毎週、隔週、または毎月を設定できます。

以下の表に、繰り返し頻度のオプションを示します。

オプション	説明
繰り返ししない	タスクをスケジュールどおりに実行しますが、繰り返ししません。
N 分ごと	指定した時間（分単位）に基づく間隔でタスクを実行します。以下のオプションを設定することができます。 <ul style="list-style-type: none">- 繰り返し頻度。頻度を分単位で選択します。オプションは、5、10、15、20、30、45 です。- 日。タスクを実行する曜日。1 つ以上の曜日を選択できます。- 時間範囲。タスクを開始する時間。[終日] を選択するか、時間範囲を設定します。時間範囲は 00 時 00 分から 23 時 55 分で設定できます。- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。
n 時間ごと	スケジュールの開始時刻に基づき、タスクを 1 時間間隔で実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none">- 繰り返し頻度。頻度を時間単位で選択します。オプションは、1、2、3、4、6、8、12 です。- 日。タスクを実行する曜日。1 つ以上の曜日を選択できます。- 時間範囲。タスクを開始する時間。[終日] を選択するか、時間範囲を設定します。時間範囲は 00 時 00 分から 23 時 55 分で設定できます。- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。

オプション	説明
日次	<p>毎日スケジュールで設定した開始時刻にタスクを実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> - 繰り返し頻度。タスクを実行する頻度。[毎日] または [すべての平日] を選択します。 - 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。
週次	<p>スケジュールの開始時刻に基づき、1 週間間隔でタスクを実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> - 日。タスクを実行する曜日。1 つ以上の曜日を選択できます。 - 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。 <p>曜日を指定しない場合、タスクは開始日と同じ曜日に定期的に行われます。</p>
隔週	<p>スケジュールの開始時刻に基づき、タスクを 2 週間隔で実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> - 日。タスクを実行する曜日。1 つ以上の曜日を選択できます。少なくとも 1 つの日を選択する必要があります。 - 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。 <p>午後 5:00 に開始する隔週スケジュールを火曜日に設定し、タスクを 2 週間隔で月曜日に実行する場合、このスケジュールのタスク実行は次の月曜日に開始します。</p>
月次	<p>スケジュールの開始時刻に基づき、1 カ月間隔でタスクを実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> - 日付。タスクを実行する日付。次のいずれかのオプションを設定できます。 <ul style="list-style-type: none"> - 1～28 の間で正確な日付を選択します。月の後半のある曜日にタスクを実行する場合は、<n> <day of the week> オプションを使用します。 - <n> <day of the week> を選択します。<n> のオプションは、[第 1]、[第 2]、[第 3]、[第 4]、[最終] です。<day of the week> のオプションは、[日]、[日曜日] - [土曜日] です。 <p>ヒント: [日付] オプションでは、月の初日または最終日にタスクを実行するように設定できます。</p> - 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。

タイムゾーンとスケジュール

Informatica Intelligent Cloud Services は、時間を世界協定時刻（UTC）で保存します。ログインすると、Informatica Intelligent Cloud Services で時間が変換され、ユーザープロファイルに関連付けられたタイムゾーンで表示されます。

スケジュールを作成するときに、使用するスケジューラのタイムゾーンを選択します。自分のタイムゾーンまたは組織のタイムゾーンとは異なるタイムゾーンを選択できます。

夏時間への移行とスケジュール

Informatica Intelligent Cloud Services は、隔週のタスクを除くすべてのタスクに夏時間の変更を適用します。

夏時間を有効にすると、午前 2 時 00 分 – 午前 2 時 59 分に実行するようにスケジュールされたタスクは、時刻が午前 2 時 00 分から午前 3 時 00 分に変更される日は実行されません。タスクが隔週で午前 2 時に実行するようにスケジュールされている場合は、時刻が変更される日の午前 3 時にそのタスクが実行され、次回は午前 2 時に実行されます。

夏時間により、標準時が開始されるときに午前 1 時 00 分 – 午前 1 時 59 分に実行するようにスケジュールされたタスクが再実行されることはありません。例えば、毎日午前 1 時半に実行するようにスケジュールされたタスクがあるとします。時刻が午前 2 時から午前 1 時に変更されても、このタスクが午前 1 時半に再実行されることはありません。

ヒント: Informatica Intelligent Cloud Services で午前 2 時前後の時刻変更時にスケジュールされた実行がスキップされないようにするため、午前 12:59 から午前 3:01 の間はジョブの実行をスケジュールしないでください。

スケジュールの設定

【スケジュール】 ページでスケジュールを設定します。マッピングタスクと同期タスクの場合、タスクを設定するときに新しいスケジュールを作成することもできます。スケジュールは、1 回だけ実行するように設定したり、指定した間隔で無期限に、または指定した終了時刻まで実行するように設定したりすることができます。

1. 管理者で **【スケジュール】** を選択します。
2. スケジュールを作成するには、**【新しいスケジュール】** をクリックします。
スケジュールを編集するには、スケジュールを含む行の編集アイコンをクリックします。
3. 以下のプロパティを設定します。

プロパティ	説明
スケジュール名	スケジュールの名前。 各スケジュール名は組織内で一意である必要があります。スケジュール名には、英数字、スペース、および次の特殊文字を含めることができます。 _ . + - 最大長は 255 文字です。名前の大文字と小文字は区別されません。
説明	スケジュールの説明。 最大長は 255 文字です。

プロパティ	説明
開始	<p>スケジュールを開始する日付と時刻。</p> <p>日付の形式は MM/DD/YYYY です。時刻は 24 時間形式です。</p> <p>〔カレンダー〕 ボタンをクリックし、開始日付を選択します。開始日時は、一定間隔で繰り返すタスクおよびタスクフロージョブの繰り返し頻度に影響することがあります。</p> <p>例えば、開始日が 11 月 10 日で、繰り返し頻度が毎月の場合、スケジュールは毎月 10 日に関連付けられたアセットを実行します。開始時刻を 3 時 10 分、繰り返し頻度を 1 時間にした場合、アセットは毎時 10 分に実行されます。</p> <p>デフォルトは、スケジュールを作成するユーザーの現在の日付、現在の時刻、およびタイムゾーンです。</p>
タイムゾーン	<p>使用するスケジュールのタイムゾーンを選択します。タイムゾーンは、組織のタイムゾーンやユーザーのタイムゾーンとは異なるものにすることができます。</p>
繰り返す	<p>スケジュールの繰り返し頻度。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"> - 繰り返さない - N 分ごと - n 時間ごと - 日次 - 週次 - 隔週 - 月次 <p>デフォルトは〔繰り返さない〕です。</p>

4. **〔保存〕** をクリックします。

スケジュールのエクスポート

組織からスケジュールをエクスポートし、それらのスケジュールを他の組織にインポートできます。スケジュールに関連付けられているアセットは、エクスポートファイルには含まれません。**〔スケジュール〕** ページでスケジュールをエクスポートします。

1. 管理者で **〔スケジュール〕** を選択します。
2. **〔エクスポート〕** をクリックします。
3. **〔スケジュールのエクスポート〕** ダイアログボックスで、エクスポートするスケジュールを選択します。
4. オプションとして、エクスポートジョブ名を更新します。
デフォルトでは、ジョブ名は SchedulesExport_<日付>です。
5. **〔エクスポート〕** をクリックします。

管理者によって、スケジュールをエクスポートするためのエクスポートジョブが作成されます。

6. エクスポートジョブのステータスを確認し、エクスポートファイルをダウンロードするには、モニタで **〔インポート/エクスポートログ〕** ページを開き、**〔エクスポート〕** タブをクリックします。

エクスポートジョブを含む行で、またはジョブの詳細ページでエクスポートファイルをダウンロードできます。

データ統合など、別のサービスの **〔エクスプローラ〕** ページでスケジュールをインポートできます。アセットのインポートについて詳しくは、そのサービスのヘルプを参照してください。

スケジュールをインポートした後、それらをターゲット組織のアセットに関連付けることができます。

スケジュール済みタスクのトラブルシューティング

タスクがスケジュールされた時間に実行されません。

スケジュールがタスクを開始しようとしたときに、タスクの別のインスタンスがすでに実行されている場合、タスクはタスクがスケジュールされた時間に実行されません。例えば、5 分ごとに実行するようにタスクをスケジュールしたとします。最初のタスクは 12 pm に開始しますが、12:06 pm まで完了しません。最初のインスタンスが完了しないため、タスクの 2 番目のインスタンスは 12:05 pm に実行されません。データ統合は次のタスクを午後 12:10 に開始します。

この問題を解決するには、次のタスクの実行が開始される前にタスクが完了するように、スケジュールを変更します。

第 7 章

バンドル管理

バンドルは Informatica Intelligent Cloud Services プロジェクトの生産性の向上と品質の向上に使用できる関連アセットのセットです。データ統合ユーザーはバンドルを設計、作成、およびパブリッシュします。管理者はバンドルを管理します。

組織の管理者である場合は、次の操作を実行してバンドルを管理できます。

バンドルをインストールする。

バンドル設計者が参照として使用するように構成した公開、非公開、または非表示バンドルをインストールできます。バンドルは **【参照】** ページのアドオンバンドルプロジェクトにインストールされます。組織のユーザーはバンドル内のアセットを使用できますが、編集することはできません。

バンドルをコピーする。

バンドル設計者がコピー用に構成した公開、非公開、または非表示バンドルをコピーできます。バンドルをコピーするときに、バンドルの内容をコピーするフォルダを選択します。バンドルを複数回コピーし、その内容を毎回別のプロジェクトまたはフォルダに保存することができます。バンドルをコピーすると、組織内のユーザーはアセットを編集できます。

バンドルをアップグレードする。

バンドルをインストールし、新しいバージョンのバンドルが使用できるようになると、バンドルをアップグレードして最新バージョンを入手できます。

バンドルをアンインストールする。

インストール済みのバンドルが組織で不要になった場合は、アンインストールすることができます。

インストール済み、または組織で使用可能なバンドルを表示するには、管理者で **【アドオンバンドル】** を選択します。**【アドオンバンドル】** ページには、インストール済みバンドル、コピーされたバンドル、インストールまたはコピーに使用可能なバンドルに関する情報が表示されます。

バンドルの作成または公開の詳細については、データ統合サービスのヘルプの「アセット管理」を参照してください。

バンドルのタイプ

バンドルの作成時に、バンドルタイプを指定します。バンドルタイプにより、バンドルを使用できるユーザーおよびバンドルをパブリッシュする方法を指定します。

以下のタイプのバンドルを作成できます。

公開バンドル

公開バンドルは、すべての組織とサブ組織で利用できます。公開バンドルを作成する場合、承認のためにバンドルを Informatica に送信します。バンドルが承認されると、Informatica により、すべての組織でバンドルが使用できるようになります。

非公開 バンドル

非公開バンドルは親組織とサブ組織のみで使用できます。親組織で非公開バンドルを作成し、そのバンドルをサブ組織にパブリッシュします。パブリッシュされた非公開バンドルはサブ組織の **【アドオンバンドル】** ページに表示されます。Informatica がプライベートバンドルのレビューを行うことはありません。

プッシュされたバンドルにサブ組織の既存タスクと互換性がないオブジェクトの変更が含まれている場合は、サブ組織のタスクが無効になるか、タスクが削除されることがあります。

組織にサブ組織がない場合、プライベートバンドルを作成することはできません。

非表示 バンドル

非表示バンドルは、他のバンドルを作成するための参照として使用されます。非表示バンドルをインストールするには、アクセスコードが必要です。

バンドルのインストール

バンドル設計者が参照として使用するように構成した公開、非公開、または非表示バンドルをインストールできます。**【アドオンバンドル】** ページの **【使用可能なバンドル】** タブでバンドルをインストールします。

非表示バンドルをインストールする前に、バンドルのアクセスコードを取得します。組織内で作成されたバンドルのアクセスコードを取得するには、データ統合で **【バンドル】** ページを開き、バンドル名をクリックして **【アクセスコードのコピー】** をクリックします。組織の外部で作成されたバンドルのアクセスコードを取得するには、バンドルパブリッシャに問い合わせてください。

1. 管理者で、**【アドオンバンドル】** を選択します。

2. **【使用可能なバンドル】** をクリックします。

【使用可能なバンドル】 タブには、インストールまたはコピーに使用できる公開および非公開バンドルが一覧表示されます。

3. インストールするバンドルが非表示バンドルの場合は、**【検索】** フィールドにバンドルのアクセスコードを入力します。

4. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。

5. **【許可】** フィールドが **【参照】** または **【参照とコピー】** に設定されていることを確認します。

コピー専用で構成されたバンドルをインストールすることはできません。

6. **【インストール】** をクリックします。

データ統合でバンドルがアドオンバンドルプロジェクトに追加され、アセットが使用できる状態になります。また、バンドルは管理者の **【アドオンバンドル】** ページにある **【インストール済みバンドル】** タブに一覧表示されます。

バンドルのコピー

バンドル設計者がコピー用に構成した公開、非公開、または非表示バンドルをコピーできます。**【アドオンバンドル】** ページの**「使用可能なバンドル」** タブでバンドルをコピーします。バンドルをコピーするたびに、**「コピーされたバンドル」** タブにイベントが記録されます。

非表示バンドルをコピーする前に、バンドルのアクセスコードを取得してください。組織内で作成されたバンドルのアクセスコードを取得するには、データ統合で**【バンドル】** ページを開き、バンドル名をクリックして**【アクセスコードのコピー】** をクリックします。組織の外部で作成されたバンドルのアクセスコードを取得するには、バンドルパブリッシャに問い合わせてください。

1. 管理者で、**【アドオンバンドル】** を選択します。
2. **【使用可能なバンドル】** をクリックします。
「使用可能なバンドル」タブには、インストールまたはコピーに使用できる公開および非公開バンドルが一覧表示されます。
3. コピーするバンドルが非表示バンドルの場合は、**【検索】** フィールドにバンドルのアクセスコードを入力します。
4. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。
5. **【許可】** フィールドが**【コピー】** または**【参照とコピー】** に設定されていることを確認します。
参照のみとして使用するように構成されているバンドルをコピーすることはできません。
6. **【バンドルの内容を次の場所にコピー...】** をクリックします。
7. **【参照】** ダイアログボックスで、バンドルの内容をコピーするデータ統合プロジェクトまたはフォルダを選択します。
8. **【選択】** をクリックします。
バンドル内のアセットが、選択したプロジェクトまたはフォルダにコピーされます。

バンドルのアップグレード

更新バージョンが入手可能になった時点で、インストール済みバンドルをアップグレードできます。バンドルステータスは、**【アドオンバンドル】** ページの**「インストール済みバンドル」** タブで確認できます。

1. 管理者で、**【アドオンバンドル】** を選択します。
2. **【インストール済みバンドル】** をクリックします。
「バンドルステータス」列は、バンドルが最新かどうか、またはアップグレードが利用可能かどうかを示します。
3. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。
4. **【アップグレード】** をクリックします。

バンドルのアンインストール

組織内のユーザーがバンドルを必要としなくなった場合は、アンインストールします。[アドオンバンドル] ページの [インストール済みバンドル] タブでバンドルをアンインストールします。

注: バンドルをアンインストールすると、組織のすべてのバンドルアセットが削除されます。バンドル内のアセットを使用するタスクを保持する場合は、タスクでそのアセットを削除してからバンドルをアンインストールします。

1. 管理者で、[アドオンバンドル] を選択します。
2. [インストール済みバンドル] をクリックします。
3. バンドル名をクリックして、[バンドルの詳細] ページを開きます。
4. [Uninstall (アンインストール)] をクリックします。

バンドルをアンインストールすると、[使用可能なバンドル] タブに一覧表示されます。

第 8 章

イベント監視

アセットログとセキュリティログを使用して、組織内のアセット、ライセンス、ユーザー、および Secure Agent のイベントを監視できます。ログを表示するには、「監査ログ-表示」特権を持つロールを割り当てる必要があります。

次のログを使用してイベントを監視できます。

アセットログ

次の情報が表示されます。

- 各アセットが作成、更新、コピー、または削除されたときや、アセットを変更したユーザー名など、アセットのイベント。
- ライセンスが追加、削除、または変更されたときなど、ライセンスに関連するイベント。

アセットログを開くには、管理者を開いて **【ログ】** を選択し、ページ上部の **【アセットログ】** を選択します。

セキュリティログ

次の情報が表示されます。

- 組織内のユーザーが Informatica Intelligent Cloud Services にログインまたはログアウトしたときなど、ユーザーの認証イベント。
- 各エージェントが作成または更新されたとき、組織情報が更新されたとき、エージェントまたは組織を変更したユーザーの名前など、Secure Agent および組織のイベント。

セキュリティログを開くには、管理者を開いて **【ログ】** を選択し、ページ上部の **【セキュリティログ】** を選択します。

次の図は、アセットログを示しています。

Asset Logs

View asset or security logs. You can search or sort.

Asset Logs (142)

Find

User Name	Updated On	Object Name	Object Type	Event
ltroy	Jul 13, 2017, 12:48:03 PM	m_BostonCustomers_PassThru	MAPPING	COPY
ajones	Jul 13, 2017, 11:28:11 AM	rt_LACustomers	SAAS_DRS	CREATE
ltroy	Jul 13, 2017, 9:39:55 AM	tf_BostonCustomers	TASKFLOW	UPDATE_PERMISSION
ltroy	Jul 12, 2017, 11:25:52 AM	tf_BostonCustomers	TASKFLOW	UPDATE
dsmith	Jul 11, 2017, 3:58:42 PM	KG_Mapping	MAPPING	UPDATE
dsmith	Jul 11, 2017, 3:58:17 PM	KG_Mapplet1	SAAS_CUSTOM_FUNC	CREATE
dsmith	Jul 11, 2017, 3:56:57 PM	KG_Mapplet1	CUSTOM_FUNC	CREATE
ajones	Jul 11, 2017, 3:55:27 PM	Accounts_by_State_New	DTEMPLATE	CREATE
ajones	Jul 11, 2017, 3:27:54 PM	Accounts_by_State_New	MAPPING	COPY
ajones	Jul 11, 2017, 3:27:07 PM	Accounts_by_State_New	MAPPING	UPDATE

1 - 25 of 142

< 1 of 6 >

25

アセットログには、過去 90 日間のイベントが表示されます。セキュリティログには、過去 400 日間のイベントが表示されます。

ログに表示されるプロパティは、次の方法でカスタマイズできます。

- 列を非表示にするには、列見出し領域を右クリックし、非表示にする列をオフにします。
- ログイベントをソートするには、ソート基準にするプロパティの列見出しをクリックします。ソート順序を逆転させるには、列見出しをもう一度クリックします。
- 特定のイベントのログを検索するには、検索文字列を【検索】フィールドに入力します。オブジェクト名またはイベントタイプを検索できます。

第 9 章

セキュリティのトラブルシューティング

次のセキュリティ違反エラーを受信しました。

There may have been a security violation while accessing the site. Verify that there are no malicious scripts running in your browser. This error also appears when you submit the form multiple times through a browser reload.

このエラーは、ページのオプションをクリックしたときに、そのページが前回のクリックによるロードを実行中であるときに発生します。データ統合に戻るには、[こちら] のリンクをクリックしてください。

接続、レプリケーションタスクなどのオブジェクトに関する詳細を表示しようとする、[オブジェクトが見つかりません] ページが表示されます。

オブジェクトは最近削除されました。オブジェクトが存在しないと、[オブジェクトが見つかりません] ページが表示されます。ページを更新して、現在のオブジェクトを表示します。

タスクを実行しようとする、[アクセスが拒否されました] ページが表示されます。

使用しているユーザーアカウントでの実行許可がないタスクを実行しようとする、[アクセスが拒否されました] ページが表示されます。タスクを実行するための適切なロールまたはアセットの権限がない可能性があります。タスクを実行する必要がある場合は、組織の管理者にユーザーアカウントの確認を依頼してください。

セキュリティスキャンの結果、エラスティックランタイム環境に「脆弱な SSL/TLS キー交換」の脆弱性があることが判明しました。

この脆弱性を解決するには、次の手順を実行します。

1. 管理者で、[ランタイム環境] を選択します。
2. リストからエラスティックランタイム環境を選択します。
3. [サーバー設定] タブを選択します。
4. [サービス設定] サブタブで、[JRE_OPTS] を検索します。
見つかったエントリに Service=Data_Integration_Server、Type=TOMCAT_JRE、Name=JRE_OPTS が含まれていることを確認します。
5. エントリを編集し、値を-Djdk.tls.ephemeralDHKeySize=2048 に設定します
6. 変更を保存します。

第 10 章

ライセンス

ライセンスによって組織の Informatica Intelligent Cloud Services サブスクリプションレベルが決まり、Informatica Intelligent Cloud Services の機能、コネクタ、およびバンドルへアクセスできるようになります。

管理者は、組織に設定されたライセンスの確認、ライセンスの有効期限の確認、および下位組織のライセンスの管理ができます。

ライセンスされたジョブの制限と使用量のメトリックを確認することもできます。メトリックの確認については、[第 3 章, 「メータリング」 \(ページ 28\)](#)を参照してください。

ライセンスのカテゴリ

ライセンスは、エディションライセンス、コネクタライセンス、およびカスタムライセンスに分類されます。

次のライセンスカテゴリを利用できます。

エディションライセンス

エディションライセンスは、機能ベースまたは使用量ベースとなります。機能ベースのエディションライセンスは、データ統合マッピングタスク、ビジネスサービスコンポーネント、きめ細かいセキュリティなどの Informatica Intelligent Cloud Services 機能へのアクセスを提供します。インテリジェントクラウドデータ管理機能のライセンスなどの使用量ベースのエディションライセンスは、前払い式の消費モデルを使用して Informatica Intelligent Cloud Services へのアクセスを提供します。

コネクタライセンス

コネクタライセンスは、Amazon Redshift、Microsoft SQL Server、Oracle などのエンティティへの接続を提供します。

カスタムライセンス

カスタムライセンスは、エディションに含まれていないライセンスです。機能、パッケージ、またはバンドルへのアクセスを提供します。エディションライセンスにも含まれている機能へのアクセスを提供するカスタムライセンスを組織で使用している場合、カスタムライセンスの使用条件は、エディションライセンスの条件を上書きします。

ライセンスのタイプ

組織を作成すると、Informatica Intelligent Cloud Services でライセンスされている各エディションのライセンスタイプを組織に割り当てます。

Informatica Intelligent Cloud Services では、以下のタイプのライセンスを使用します。

トライアル

30 日間無料でエディションを使用できます。トライアル期間の終了時に、エディションをサブスクライブできます。トライアルサブスクリプションでは、ライセンスに関連付けられている機能、コネクタ、およびパッケージへのアクセスが制限される場合があります。

サブスクリプション

契約期間中は、ライセンスされているエディションを使用することができます。契約期間の終わりに近づくと、Informatica Intelligent Cloud Services から契約が間もなく終了することが通知されます。エディションの使用を続けるには、契約を更新します。

無料サブスクリプション

同期タスクは、無料で使用できます。無料サブスクリプションでは、同期タスクの機能へのアクセスが制限される場合があります。

サブ組織のライセンス

サブ組織には、親組織によって保持されるライセンスがあります。親組織に属していないライセンスをサブ組織が必要とする場合は、Informatica グローバルカスタマサポートに連絡して、親組織のライセンスを取得します。

サブ組織を作成すると、各サブ組織は親組織からカスタムライセンスとしてライセンスを継承します。サブ組織は、次のライセンスを除くすべてのライセンスを継承します。

- サブ組織を作成するためのライセンス
- バンドルライセンスサブ組織でバンドルを使用するには、サブ組織のユーザーがバンドルをインストールする必要があります。

組織がインテリジェントクラウドデータ管理ライセンスを持っている場合、サブ組織でもこのライセンスを利用できます。親組織とサブ組織は、Informatica プロセッシングユニット (IPU) のバランスを共有します。

サブ組織のライセンスは、次の方法で管理できます。

ライセンスの個別管理

ライセンスを個別に管理すると、親組織の管理者は、継承されたライセンスの有効期限の無効化、有効化、および短縮を行うことができます。各サブ組織のライセンスを個別に管理します。サブ組織の管理者はライセンスを表示できますが、変更はできません。

これがデフォルトのオプションです。

サブ組織のライセンスの親組織との自動同期

適切なライセンスを所有している場合、サブ組織のライセンスを親組織と自動的に同期できます。このライセンスを有効にすると、ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ライセンスの同期は、組織に多数のサブ組織があり、サブ組織が同じライセンスを所有しているときに有効にすることがあります。

ライセンスの同期が組織に対して有効でない場合、サブ組織のライセンスを個別に管理する必要があります。

注: 親組織が持っていないライセンスを持つサブ組織をリンクすると、サブ組織はそのライセンスを失います。

サブ組織のライセンスの編集

親組織の管理者であり、親組織とサブ組織との間のライセンス同期が有効でない場合、サブ組織のライセンスを編集できます。サブ組織のライセンスは、親組織内またはサブ組織内から編集できます。

1. 親組織にログインします。
2. 親組織内からライセンスを編集するには:
 - a. 管理者を開いて **【組織】** を選択します。
 - b. **【サブ組織】** をクリックします。
 - c. ライセンスを編集するサブ組織を選択します。
 - d. **【ライセンス】** をクリックします。
3. サブ組織内からライセンスを編集するには:
 - a. 右上隅の **【組織】** メニューから、ライセンスを編集するサブ組織を選択します。
 - b. 管理者を開いて **【ライセンス】** を選択します。
4. 機能を有効にするにはライセンスを選択し、機能を無効にするにはライセンスの選択を解除します。
5. 必要に応じて、有効期限を変更します。

すべてのライセンスには有効期限が必要です。元の有効期限を過ぎたライセンスを延長することはできません。
6. **【保存】** をクリックします。

親組織とのライセンスの同期

サブ組織のライセンスを親組織と自動的に同期できます。ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ライセンスの同期を有効にするには、Informatica グローバルカスタマサポートに問い合わせ、この機能のライセンスを要求してください。ライセンスが親組織に対して有効になると、ライセンスのサブ組織との同期が自動的に発生します。親組織の管理者は、ライセンスを同期させるために、何か操作をする必要はありません。

注: この機能のライセンスが有効になると、サブ組織のライセンスを個別に編集することはできません。

この機能のライセンスが有効になり、サブ組織を無効にすると、サブ組織はライセンス設定を失います。サブ組織を再度有効にした場合、サブ組織はすべてのライセンス設定を親組織から継承します。

親組織とサブ組織との間のライセンス同期は、サブ組織のライセンスメーターカウントには影響しません。

組織タイプの設定

【ライセンス】 ページを表示すると、組織のライセンスに関する詳細や、組織タイプなどのその他の詳細を確認できます。組織タイプは、組織がトライアル組織、プロダクション組織、またはサンドボックス組織のいずれであるかを表します。親組織の管理者である場合は、それぞれのサブ組織の組織タイプを設定する必要があります。

組織タイプは、親組織の管理者がサブ組織の **【ライセンス】** ページを表示することで編集できます。サブ組織のユーザーまたは親組織では編集できません。

親組織の管理者の場合は、親組織内またはサブ組織内からサブ組織の組織タイプを設定できます。組織タイプは設定後に変更できます。

1. 親組織にログインします。
2. 親組織内から組織タイプを編集する手順
 - a. 管理者を開いて【組織】を選択します。
 - b. 【サブ組織】をクリックします。
 - c. タイプを設定するサブ組織を選択します。
 - d. 【ライセンス】をクリックします。
 - e. 【サブ組織の詳細】領域の【タイプ】リストで、組織タイプを選択します。
3. サブ組織内から組織タイプを編集する手順
 - a. 右上隅の【組織】メニューから、タイプを設定するサブ組織を選択します。
 - b. 管理者を開いて【ライセンス】を選択します。
 - c. 【サブ組織の詳細】領域の【タイプ】リストで、組織タイプを選択します。
4. 【保存】をクリックします。

ライセンスの有効期限

ライセンスの有効期限が切れると、ライセンスに関連付けられている機能、コネクタ、またはパッケージにアクセスできなくなります。ライセンスに関連付けられているスケジュール済みのジョブも無効になります。組織のすべてのライセンスの有効期限が切れると、Informatica Intelligent Cloud Services にログインできなくなります。

管理者の【ライセンス】ページでライセンスの有効期限を確認することができます。ライセンスを延長するには、Informatica グローバルカスタマサポートにお問い合わせください。ライセンスを延長すると、関連付けられている機能、コネクタ、およびパッケージにアクセスし、スケジュール済みのジョブの処理を再開できます。

索引

A

Administrator サービス
概要 [8](#)
AWS Secrets Manager
シークレット名 [75](#)
設定 [69](#)
Azure DevOps ユーザー 資格情報 [57](#)
Azure Key Vault
シークレット名 [78](#)
設定 [77](#)

B

Bitbucket ユーザー 資格情報 [57](#)

C

CLAIRE
設定 [63](#)
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](#)

E

Enterprise Data Catalog
Informatica Intelligent Cloud Services との統合 [18](#)

G

GitHub ユーザー 資格情報 [57](#)

H

HashiCorp Vault
シークレット形式 [79](#)
設定 [78](#)
認証方法 [79](#)

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](#)
IPU メーター [28](#), [33](#)
IPU 使用率
レポート [38](#)

IPU 使用率 (続く)
監視 [28](#)
請求期間 [30](#)
無効化されたサブ組織および削除されたサブ組織 [37](#)
IP アドレスフィルタリング
設定 [14](#)

K

Key Vault、[参照項目](#)シークレットマネージャ

S

Secure Agent
接続プロパティの保存 [16](#)
Secure Agent サービス
アップグレード設定 [51](#)
ローリングアップグレード [61](#)
ローリングアップグレードエラーの処理 [61](#)
再開スケジュールの設定 [62](#)

W

Web サイト [6](#)

あ

アセットログ
最大ログエントリ [18](#)
表示 [98](#)
アップグレード通知 [7](#)
アドオンバンドル
バンドルを参照してください。 [94](#)
アプリケーションの統合
メータリングの使用状況レポート [49](#)
アプリケーション取り込みとレプリケーション
メータリングの使用状況レポート [49](#)

い

イベント
監視 [98](#)

か

ガイドライン
ロゴおよびファビコン [62](#)
カスタムブランディング
設定 [51](#)
組織の設定 [62](#), [63](#)

さ

サーバーレスランタイム環境

サーバーレスコンピューティングユニット [47](#)

メータリングの使用状況レポート [49](#)

サブ組織

ライセンスの同期 [103](#)

CLAIRE の設定 [63](#)

Enterprise Data Catalog 統合プロパティ [18](#)

アセットのエクスポートとインポート [25](#)

アドオンコネクタ [25](#)

カスタムブランディングの設定 [63](#)

シークレットマネージャの設定 [51](#)

スケジュールオフセット [18](#)

ソース管理の無効化 [57](#)

ソース管理の有効化 [54](#)

ソース管理リポジトリの変更 [56](#)

ソース管理設定 [51](#), [53](#)

データ統合サービスのプロパティ [18](#)

プロパティ [12](#)

メータリング [28](#)

ライセンス [102](#)

ライセンスの編集 [103](#)

ライセンスの有効期限 [104](#)

既存サブ組織の削除 [23](#)

既存組織のリンク [22](#)

顧客管理対象キーの設定 [51](#)

作成 [21](#)

作成する理由 [19](#)

削除 [22](#)

親組織からのリンク解除 [23](#)

親組織のアクセスを拒否 [24](#)

接続プロパティの保存 [16](#)

全般プロパティ [13](#)

組織タイプ [103](#)

追加 [21](#)

認証プロパティ [14](#)

別の組織への切り替え [24](#)

無効化および有効化 [23](#)

無効化と IPU 使用率 [37](#)

例 [19](#)

し

シークレットコンテナ、参照項目シークレットマネージャ

シークレットマネージャ

AWS Secrets Manager の IAM ロール設定 [70](#)

AWS Secrets Manager のアカウント間アクセス設定 [73](#)

AWS Secrets Manager のインスタンスプロファイル設定 [72](#)

AWS Secrets Manager 接続プロパティ [76](#)

Azure Key Vault 接続プロパティ [78](#)

HashiCorp Vault の接続プロパティ [79](#)

サブ組織の制限事項 [80](#)

接続設定 [81](#)

組織に対する無効化 [80](#)

組織に対する有効化 [80](#)

組織の設定 [68](#)

システムステータス [7](#)

ジョブの使用状況

監視 [43](#)

ジョブの制限数

監視 [43](#)

す

スカラ

IPU メーター [32](#)

スケジュール

Secure Agent サービスの再開 [62](#)

インポート [92](#)

エクスポート [92](#)

スケジュールオフセット [18](#)

スケジュール済みタスクの監視 [88](#)

タイムゾーン [90](#)

タスクまたはタスクフローとの関連付け [88](#)

ブラックアウト期間の設定 [89](#)

夏時間 [91](#)

繰り返し頻度 [89](#)

削除 [88](#)

設定 [91](#)

説明 [88](#)

ステータス

Informatica Intelligent Cloud Services [7](#)

ストリーミング取り込みとレプリケーション

メータリングの使用状況レポート [49](#)

せ

セキュリティ

トラブルシューティング [100](#)

セキュリティログ

最大ログエントリ [18](#)

表示 [98](#)

セッションのアイドルタイムアウト

設定 [14](#)

そ

ソース管理

OAuth を使用したアクセスの設定 [53](#)

オンプレミスリポジトリ [54](#)

サブ組織の設定 [53](#)

チェックアウトの取り消し [59](#)

ベストプラクティス [58](#)

リポジトリ URL の変更 [56](#)

リポジトリへのアクセスの設定 [57](#)

リポジトリへの読み取り/書き込みアクセスの設定 [52](#)

リポジトリへの読み取り専用アクセスの設定 [52](#)

開発ガイドライン [58](#)

設定 [51](#)

設定のガイドライン [58](#)

組織の設定 [52](#)

組織の無効化 [57](#)

組織の有効化 [54](#)

た

タイムゾーン

説明 [90](#)

て

データベース取り込みとレプリケーション

ファイル取り込みとレプリケーション

メータリングの使用状況レポート [49](#)

メータリングの使用状況レポート [49](#)

データ取り込みおよびレプリケーションサービス
メータリングの使用状況レポート [49](#)
データ統合のデータカタログページ
表示と非表示 [18](#)

と

トラブルシューティング
セキュリティ [100](#)

は

パスワード
再利用 [14](#)
最小混合文字数 [14](#)
最小長 [14](#)
有効期限 [14](#)
バンドル
アップグレード [96](#)
アンインストール [97](#)
インストール [95](#)
コピー [96](#)
管理 [94](#)
表示 [94](#)

ふ

フィンガープリント認証
組織 [16](#)
ブラックアウト期間
組織用の設定 [89](#)

め

メータリング
IPU スカラ [32](#)

メータリング (続く)
IPU メーター [28](#), [33](#)
IPU メトリックの表示 [28](#)
IPU 使用率レポート [38](#)
IPU 使用量の表示 [28](#)
サーバーレスコンピューティングユニット [47](#)
すべてのメーターの表示 [43](#)
メーター定義 [44](#)
ライセンスメトリックの表示 [43](#)
使用状況のグラフの表示 [48](#)
使用状況の詳細の表示 [48](#)
使用状況レポート [49](#)
組織とサブ組織 [28](#)
メータリングの使用状況レポート
情報 [49](#)
メンテナンスの停止 [7](#)

ら

ライセンス
サブ組織 [102](#)
サブ組織タイプの設定 [103](#)
サブ組織のライセンスの編集 [103](#)
タイプ [102](#)
管理 [101](#)
有効期限 [104](#)
ライセンスメーター [43](#)
ライセンスメトリック
表示 [43](#)

ろ

ログインの拒否
トラブルシューティング [100](#)