



Informatica® Intelligent Cloud Services
July 2025

ファイル転送

© 著作権 Informatica LLC 2021, 2025

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

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

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

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

本マニュアルの情報は、予告なしに変更されることがあります。このドキュメントで問題が見つかった場合は、infa_documentation@informatica.com 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	4
Informatica のリソース.....	4
Informatica マニュアル.....	4
Informatica Intelligent Cloud Services Web サイト.....	4
Informatica Intelligent Cloud Services コミュニティ.....	4
Informatica Intelligent Cloud Services マーケットプレイス.....	5
データ統合のコネクタのドキュメント.....	5
Informatica ナレッジベース.....	5
Informatica Intelligent Cloud Services Trust Center.....	5
Informatica グローバルカスタマサポート.....	5
 第 1 章 : ファイル転送	6
 第 2 章 : ファイルサーバーの構成プロセス	8
始める前に.....	8
 第 3 章 : ファイルサーバー	10
ファイルサーバーの設定.....	10
AS2 サーバーの設定プロパティ.....	10
HTTPS サーバー設定プロパティ.....	16
SFTP サーバー設定プロパティ.....	20
MLLP サーバー設定プロパティ.....	23
プロキシサーバー設定プロパティ.....	24
ファイル統合プロキシサーバーのインストール.....	26
ファイルサーバー.....	27
HTTPS、AS2、SFTP、および MLLP サーバーの停止と開始.....	27
プロキシサーバーの停止と開始.....	27
 第 4 章 : ファイルサーバーのユーザー	28
ファイルサーバーユーザーの設定.....	28
ファイルサーバーユーザーのプロパティ.....	29
ファイルサーバーユーザーの削除.....	32
 第 5 章 : ファイル転送タスク	33
 第 6 章 : グローバル設定	35
 索引	37

序文

ファイル転送を使用して、Informatica Intelligent Cloud ServicesSMとリモートパートナー間でファイルを交換する方法を確認します。ファイルサーバーを構成し、ファイルサーバーのユーザーを作成する方法を確認します。

Informatica のリソース

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

Informatica マニュアル

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

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

Informatica Intelligent Cloud Services Web サイト

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

Informatica Intelligent Cloud Services コミュニティ

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

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

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

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

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

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

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

ファイル転送

ファイルの交換には、B2B Gateway またはデータ統合の REST API sendfiles リソースを使用できます。

リモートパートナーとファイルを交換するには、ファイル統合サービスに関連付けられた組織のファイルサーバーを設定してパートナーのサーバーと安全に通信できるようにします。ファイル統合サービスは、高度なファイル転送プロトコルを実行する Secure Agent のサービスです。

次の種類のファイルサーバーを設定して、リモートパートナーとファイルを交換できます。

AS2 サーバー

AS2 ファイル転送でパートナーからファイルを受信するには、AS2 サーバーを設定してリモート AS2 サーバーからファイルを受信できます。

AS2 ファイルをパートナーのサーバーに送信するには、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。詳細については、データ統合のヘルプの AS2 コネクタのヘルプを参照してください。

例えば、パートナーの AS2 サーバーと EDI メッセージを交換するとします。パートナーからファイルを受信するには、ファイルサーバーを設定してパートナーのサーバーからのファイルを承認します。パートナーのサーバーにファイルを送信するには、パートナーに AS2 接続を設定します。次に、sendfiles REST API リソースを使用して POST 要求を送信する事で、パートナーのサーバーに EDI メッセージを転送します。

HTTPS サーバー

HTTPS ファイル転送でパートナーとファイルを交換するには、HTTPS サーバーを設定し、パートナーがそのサーバーに接続してサーバーとの間でファイルをアップロードおよびダウンロードできるようにします。

SFTP サーバー

SFTP ファイル転送でパートナーとファイルを交換するには、SFTP サーバーを設定し、パートナーがそのサーバーに接続してサーバーとの間でファイルをアップロードおよびダウンロードできるようにします。

MLLP サーバー

Minimal Lower Layer Protocol (MLLP) プロトコルは、HL7 メッセージなどの医療業界のメッセージを転送するために使用されます。HL7 は、医療情報システムのメッセージング仕様です。MLLP プロトコルで医療業界のメッセージを転送するには、MLLP サーバーを設定し、パートナーがそのサーバーに接続してサーバーとの間でファイルをアップロードおよびダウンロードできるようにします。

プロキシサーバー

1 つまたは複数のファイル統合プロキシサーバーを demilitarized zone（非武装ゾーン）（DMZ）内にインストールして設定できます。パートナーのサーバーは、組織のファイルサーバーと直接通信する代わりに、プロキシサーバーと通信できます。複数のファイルサーバーが同じファイル統合プロキシサーバーを使用できます。

プロキシサーバーは Windows オペレーティングシステムと Linux オペレーティングシステムにインストールできます。

組織とファイルを交換するリモートパートナーごとに、ファイルサーバーユーザーアカウントを作成します。ファイルサーバーユーザーのプロトコルアクセシビリティを定義します（つまり、AS2、HTTPS、SFTP、またはこれらのサーバーの組み合わせ）。各ファイルサーバーユーザーに、ホームディレクトリが作成されるか割り当てられます。ネットワーク共有場所をユーザーのホームディレクトリに定義でき、そのユーザーに対してフォルダレベルおよびファイルレベルの権限を定義できます。

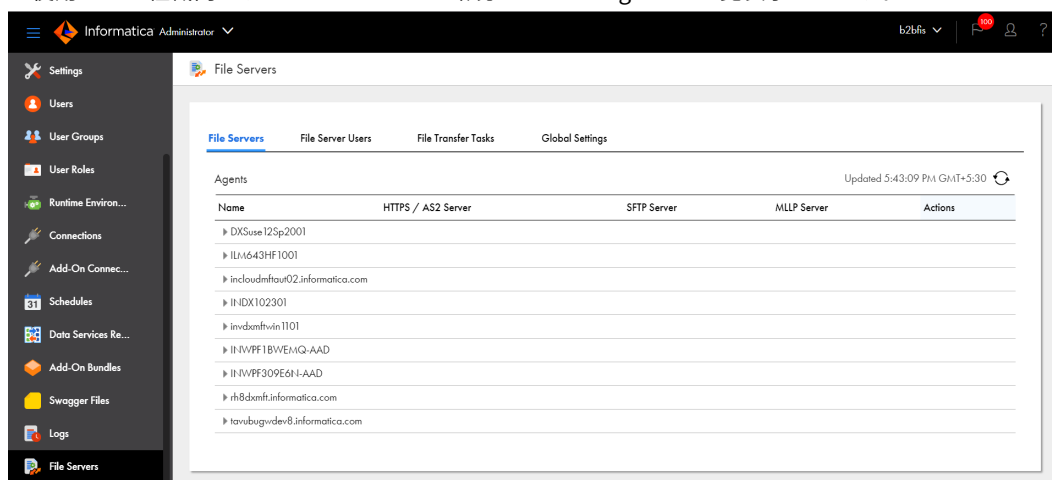
モニタの **【ファイル転送ログ】** ページでファイル転送ジョブを監視できます。ファイル転送ジョブの監視の詳細については、モニタのヘルプを参照してください。

第 2 章

ファイルサーバーの構成プロセス

リモートパートナーと Informatica Intelligent Cloud Services 組織との間でファイルを交換するようにファイルサーバー、ファイルサーバーユーザー、グローバル設定を設定します。

ファイル統合サービスを使用する Secure Agent ごとにファイルサーバーを設定できます。管理者の【ファイルサーバー】ページでファイルサーバーを設定します。【ファイルサーバー】ページに、ファイル統合サービスを使用できる組織内のすべてのランタイム環境と Secure Agent が一覧表示されます。



外部パートナーがお客様の組織とファイルを交換できるようになる事には、以下のタスクが含まれます。

- ファイルサーバープロパティを設定します。AS2、HTTPS、SFTP、および MLLP サーバーを設定できます。
- オプションで、1 つ以上のプロキシサーバーをパートナーのファイルサーバーと組織のファイルサーバーとの間の仲介としてインストールおよび設定します。
- リモートパートナーのサーバーユーザーがお客様のサーバーとファイルを交換できるように設定します。
- ファイルを交換するデフォルトフォルダを指定します。

始める前に

ファイルサーバーを設定する前に、適切なライセンスがある事、およびパートナーとパブリックキーを交換している事を確認します。

組織がリモートサーバーとファイルを交換できるようにするには、次のタスクを完了します。

1. パートナーにパブリックキーを送信します。

2. パートナーのパブリックキーを受信します。
3. パートナーのパブリックキーを自分のトラストストアにインポートします。
4. ファイルサーバーを設定します。

注:

- Secure Agent でファイル統合サービスが実行中であることを確認します。Secure Agent サービスのステータスの確認については、「Secure Agent サービス」を参照してください。
- ファイルサーバー上で権限を作成、読み取り、更新、削除、および設定するための十分な特権があることを確認してください。

第 3 章

ファイルサーバー

ファイルサーバーを設定し、リモートパートナーとファイルを交換します。

以下のサーバーを設定する事ができます。

- AS2 サーバー。パートナーから AS2 ファイル転送でファイルを受信します。
- HTTPS サーバー。パートナーはサーバーに接続し、ファイルをアップロードおよびダウンロードします。
- SFTP サーバー。パートナーはサーバーに接続し、ファイルをアップロードおよびダウンロードします。
- MLLP サーバー。パートナーはサーバーに接続し、医療業界のメッセージを転送します。
- プロキシサーバー。パートナーのファイルサーバーと組織のファイルサーバーとの間を仲介します。

ファイルサーバーの設定

ファイルサーバーのプロパティを設定し、サーバーとリモートパートナーとの間でファイルを交換します。

1. Administrator で、**【ファイルサーバー】** を選択します。
2. **【ファイルサーバー】** タブで、リモートサーバーとのファイルの交換に使用するファイル統合サービスを実行する Secure Agent を選択します。
3. **【エージェント用のファイルサーバー】** ページで、設定するサーバーのタイプ（HTTPS サーバー、AS2 サーバー、SFTP サーバー、またはプロキシサーバー）のタブを選択します。
4. ファイルサーバーのプロパティを設定し、**【保存】** をクリックします。

AS2 サーバーの設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、AS2 サーバーを設定してリモート AS2 サーバーからファイルを受信できます。

AS2 サーバープロパティを **【エージェント用のファイルサーバー】** ページの **【AS2 サーバー】** タブで設定します。

以下のタイプのプロパティを設定します。

- 全般
- SSL
- リスナ

- メッセージのセキュリティ
- MDN (Message Disposition Notification)
- アップロード制限

全般プロパティ

以下の表に、全般的な AS2 サーバーのプロパティを示します。

プロパティ	説明
AS2 の有効化サーバー	AS2 サーバーを有効にするかどうか。 有効にしない場合、AS2 サーバーでファイルを受信出来ません。 デフォルトでは無効になっています。
AS2 サーバー ID	送信者が使用する名前または ID。ID に関する次のルールに注意してください。 - 値は大文字と小文字が区別されます。 - ID には最大 128 文字の ASCII 文字、特殊文字、スペースを含めることができます。
ポート	AS2 サーバーのポート番号。 デフォルトは 15400 です。
ローカルアドレス	AS2 サーバーのローカルアドレス。
SSL の有効化	リモート AS2 サーバーとの通信で SSL 暗号化を使用するかどうか。 デフォルトでは無効になっています。

SSL プロパティ

以下の表に、SSL のプロパティを示します。

プロパティ	説明
SSL プロトコル	HTTPS 接続を保護するために SSL と TLS のどちらのプロトコルを使用するか。 次のいずれかの値を選択します。 - TLS 送信を保護するために、SSL の新しいバージョンである Transport Layer Security が使用されます。 - SSL。送信を保護するために、従来の Secure Socket Layer プロトコルが使用されます。 デフォルトは SSL です。
SSL プロトコル 有効	許容する TLS と SSL のバージョンをカンマで区切って指定します。 サポートされているバージョンは次のとおりです。 - TLS: TLSv1.2 および TLSv1.3 - SSL: SSLv2Hello および SSLv3 値が未指定の場合、選択したプロトコルのすべてのバージョンが有効になります。

プロパティ	説明
クライアント認証	<p>クライアントにサーバーとの認証に使用する証明書が必要かどうか。</p> <p>次のいずれかの値を選択します。</p> <ul style="list-style-type: none"> - なし。SSL 接続が証明書を確認せずに実行され、ユーザーはパスワードを使用して認証されます。送信された情報のいずれかで証明書が必要となる場合、接続に失敗します。 - 必須。有効な証明書が使用可能にならないと、SSL 接続ではユーザーを接続または認証しません。 - オプション。SSL 接続で有効な証明書を検索しますが、証明書がない場合は引き続きパスワード認証を行います。
キーストアの場合	<p>クライアントがファイル統合サービスとの通信の認証に使用するプライベートキーおよび関連する証明書を格納するキーストアの場合。</p> <p>パスとファイル名を指定します。</p>
キーストアのパスワード	キーストアにアクセスするためのパスワード。
キーストアタイプ	<p>プライベートキーストアのタイプ。</p> <p>以下の値を使用します。</p> <ul style="list-style-type: none"> - JKS - PKCS12
キーエイリアス	MDN の署名に使用するプライベートキーのキーエイリアスまたは証明書。
トラストストアの場合	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
トラストストアのパスワード	トラストストアにアクセスするためのパスワード。
トラストストアのタイプ	<p>トラストストアのタイプ。</p> <p>以下の値を使用します。</p> <ul style="list-style-type: none"> - JKS - PKCS12

リスナのプロパティ

AS2 サーバーには複数のサーバーリスナを追加できます。サーバーリスナを使用して、AS2 サーバーに特定のポート番号とローカルアドレスを設定します。サーバーリスナをリストに追加するには、**[リスナの追加]** をクリックします。

次の表に、リスナを追加する際のプロパティを示します。

プロパティ	説明
名前	サーバーリスナの名前。
ポート	リスナが監視するサーバーのポート番号。
ローカルアドレス	サーバーリスナのローカルアドレス。

プロパティ	説明
SSL の有効化	AS2 リスナと通信するために SSL over HTTPS 接続を有効にするかどうか。 無効にした場合、HTTPS ではなく HTTP を使用して AS2 リスナとの接続を確立します。 デフォルトでは無効になっています。
SSL プロトコル	SSL を有効にした場合に適用されます。HTTPS 接続を保護するために SSL と TLS のどちらのプロトコルを使用するか。 次のいずれかの値を選択します。 - TLS 送信を保護するために、SSL の新しいバージョンである Transport Layer Security が使用されます。 - SSL。送信を保護するために、従来の Secure Socket Layer プロトコルが使用されます。
SSL プロトコル 有効	SSL を有効にした場合に適用されます。許容する TLS と SSL のバージョンをカンマで区切って指定します。 サポートされているバージョンは次のとおりです。 - TLS: TLSv1.2 および TLSv1.3 - SSL: SSLv2Hello および SSLv3 値を指定しないと、選択したプロトコルのすべてのバージョンが有効になります。
クライアント認証	クライアントにサーバーとの認証に使用する証明書が必要かどうか。 次のいずれかの値を選択します。 - なし。SSL 接続が証明書を確認せずに実行され、ユーザーはパスワードを使用して認証されます。送信された情報のいずれかで証明書が必要となる場合、接続に失敗します。 - 必須。有効な証明書が使用可能にならないと、SSL 接続ではユーザーを接続または認証しません。 - オプション。SSL 接続で有効な証明書を検索しますが、証明書がない場合は引き続きパスワード認証を行います。
キーストアの場所	クライアントがファイル統合サービスとの通信の認証に使用するプライベートキーおよび関連する証明書を格納するキーストアの場所。 パスとファイル名を指定します。
キーストアのパスワード	キーストアにアクセスするためのパスワード。
キーストアタイプ	プライベートキーストアのタイプ。 次のいずれかの値を使用します。 - JKS - PKCS12
キーエイリアス	キーストアのキーに割り当てられた一意の名前。
トラストストアの場所	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
トラストストアのパスワード	トラストストアにアクセスするためのパスワード。
トラストストアのタイプ	トラストストアのタイプ。 次のいずれかの値を使用します。 - JKS (Java キーストア) - PKCS12 (Public-Key Cryptography Standards)

メッセージのセキュリティプロパティ

以下の表に、基本的なメッセージのセキュリティプロパティを示します。

プロパティ	説明
暗号化が必要	ファイル統合サービスが受信するファイルを暗号化する必要があるかどうか。 デフォルトでは有効になっています。
署名が必要	リモート AS2 サーバーのファイルにデジタル署名を含める必要があるかどうか。署名が必要な場合、ファイル統合サービスは署名がないメッセージを却下します。 デフォルトでは有効になっています。
認証	ユーザーが認証を受ける必要があるかどうか。 デフォルトでは無効になっています。
暗号化証明書のエイリアス	受信メッセージの復号化に使用するキーエイリアスまたは証明書。エイリアスは、キーストアの証明書を参照します。 AS2 メッセージを送信するすべてのパートナーは、この証明書のパブリックパートを持っている必要があります。

MDN プロパティ

以下の表に、受信メッセージのプロパティを示します。

プロパティ	説明
MDN 署名証明書のエイリアス	AS2 サーバーが受信メッセージに署名するために使用するプライベートキーを指すエイリアス。プライベートキーは、デフォルトのプライベートキーストアにあります。
非同期 MDN の自動承認	受信確認を自動または手動で送信するかどうか。
非同期 MDN のプロキシを有効化	プロキシサーバーが非同期 MDN に対して有効かどうかを決定します。 デフォルトでは無効になっています。
プロキシタイプ	この接続に使用するプロキシサーバーのタイプ。 次のいずれかのタイプを選択します。 <ul style="list-style-type: none">- SOCKS。SOCKS バージョン 4 または 5 を使用できます。- HTTPS。- Informatica ファイルサーバープロキシ。 使用するプロキシサーバーのタイプをネットワーク管理者に確認してください。
ホスト	ネットワークのプロキシサーバーのホスト名または IP アドレス。
ポート	ネットワークのプロキシサーバーのポート番号。空欄のままにした場合、HTTP のデフォルトポートは 80 であり、SOCKS のデフォルトポートは 1080 です。
ユーザー	プロキシサーバーに接続するときのログインに使用するユーザー名。
パスワード	プロキシサーバーに接続するためのパスワード。HTTP 接続または HTTPS 接続を作成するためのネットワークがプロキシサーバーを使用する場合に必須。

アップロード制限のプロパティ

AS2 ファイルのアップロード時に許可または拒否するファイルのタイプを指定できます。以下の表に、アップロード制限を制御するプロパティを示します。

プロパティ	説明
ファイル拡張子のフィルタタイプ	<p>ファイル拡張子リストの拡張子を承認または拒否するかどうか。</p> <p>以下の値を使用します。</p> <ul style="list-style-type: none"> - フィルタしない。すべてのファイルタイプを承認します。 - 承認。ファイル拡張子プロパティでリストされた拡張子を持つファイルを承認します。 - 拒否。ファイル拡張子プロパティでリストされた拡張子を持つファイルを許可しません。
ファイル拡張子	<p>ファイル拡張子のリスト。ファイル拡張子のフィルタタイプに対応するファイル拡張子を追加します。例えば、ファイル拡張子のフィルタタイププロパティで .csv ファイルおよび .txt ファイルを承認するには、【承認】 を選択してからファイル拡張子のリストに csv および txt を追加します。</p> <p>拡張子をリストに追加するには、テキストボックスに拡張子を入力してから 【追加】 をクリックします。</p> <p>リストから拡張子を削除するには、拡張子を強調表示してから 【削除】 をクリックします。</p>
大文字と小文字が区別されるファイル拡張子	<p>ファイル拡張子リストを使用してフィルタする場合に、大文字と小文字を考慮に入れるかどうか。有効にすると、ファイル拡張子リストで使用される大文字と小文字が一致しない拡張子を使用したファイルはアップロード出来ません。</p> <p>例えば、ファイル拡張子リストに csv があるが CSV はない場合、拡張子 csv を使用したファイルはアップロードできますが、拡張子 CSV を使用したファイルはアップロード出来ません。</p>
拡張子付きのファイルを許可	<p>ファイル拡張子フィルタを有効にするかどうか。有効にすると、このページで設定されたファイル拡張子のプロパティによってアップロードできるファイルのタイプが決まります。</p> <p>デフォルトでは有効になっています。</p>
拡張子なしのファイルを許可	<p>ファイル名に拡張子が含まれていないファイルを許可するかどうか。</p> <p>デフォルトでは有効になっています。</p>
名前なしのファイルを許可	<p>名前のないファイルを許可するかどうか。Secure Agent は、次の形式を使用して名前なしでファイルを保存します: as2data_<datetime></p> <p>datetime は、ミリ秒を含む現在のタイムスタンプです。</p> <p>デフォルトでは有効になっています。</p>
ファイル名サフィックスのタイムスタンプ (オプション)	<p>ファイル名にタイムスタンプを付加するかどうか。有効にすると、ファイル名の末尾にタイムスタンプが付加されます。</p>

プロパティ	説明
最大アップロードサイズ	AS2 サーバーがアップロードできる最大ファイルサイズ（メガバイト単位）。デフォルトは 5 MB です。
ファイルが存在する場合	<p>フォルダ内にすでに存在するファイルを再び受け取ったときに実行するアクションを選択します。</p> <p>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"> - 名前の変更: 新しく受け取ったファイルの名前を変更します。 - 追加: 既存のファイルに変更を追加します。 - 上書き: 新しく受け取ったファイルで既存のファイルを上書きします。 - エラー: ファイルがすでに存在する場合、エラーを表示します。

HTTPS サーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、リモート HTTPS サーバーとファイルを交換するように HTTPS サーバーを設定できます。

[エージェント用のファイルサーバー] ページの **[HTTPS サーバー]** タブで HTTPS サーバーのプロパティを設定します。HTTPS サーバーを介してファイルを交換するには、HTTPS ライセンスが必要です。

以下のタイプのプロパティを設定します。

- 全般
- SSL
- リスナ
- MDN (Message Disposition Notification)
- アップロード制限

全般プロパティ

次の表に、HTTPS サーバーの一般的なプロパティを示します。

プロパティ	説明
HTTPS サーバーの有効化	HTTPS サーバーを有効にするかどうか。 有効にしない場合、HTTPS サーバーはファイルを受信できません。 デフォルトでは無効になっています。
ポート	HTTPS サーバーのポート番号。 デフォルトは 15400 です。
ローカルアドレス	HTTPS サーバーのローカルアドレス。
SSL の有効化	リモート HTTPS サーバーとの通信で SSL 暗号化を使用するかどうか。 デフォルトでは無効になっています。

SSL プロパティ

以下の表に、SSL のプロパティを示します。

プロパティ	説明
SSL プロトコル	HTTPS 接続を保護するために SSL と TLS のどちらのプロトコルを使用するか。 次のいずれかの値を選択します。 <ul style="list-style-type: none">- TLS 送信を保護するために、SSL の新しいバージョンである Transport Layer Security が使用されます。- SSL。送信を保護するために、従来の Secure Socket Layer プロトコルが使用されます。 デフォルトは SSL です。
SSL プロトコル 有効	許容する TLS と SSL のバージョンをカンマで区切って指定します。 サポートされているバージョンは次のとおりです。 <ul style="list-style-type: none">- TLS: TLSv1.1、TLSv1.2、および TLSv1.3- SSL: SSLv2Hello および SSLv3 値が未指定の場合、選択したプロトコルのすべてのバージョンが有効になります。
クライアント認証	クライアントにサーバーとの認証に使用する証明書が必要かどうか。 次のいずれかの値を選択します。 <ul style="list-style-type: none">- なし。SSL 接続が証明書を確認せずに実行され、ユーザーはパスワードを使用して認証されます。送信される情報に証明書が必要な場合、接続は失敗します。- 必須。有効な証明書が使用可能にならないと、SSL 接続ではユーザーを接続または認証しません。- オプション。SSL 接続で有効な証明書を検索しますが、証明書がない場合は引き続きパスワード認証を行います。
キーストアの場所	プライベートキーと関連する証明書を保存するキーストアの場所。クライアントは、キーストアファイルを使用して、ファイル統合サービスとの通信を認証します。 パスとファイル名を指定します。
キーストアのパスワード	キーストアにアクセスするためのパスワード。
キーストアタイプ	プライベートキーストアのタイプ。 以下の値を使用します。 <ul style="list-style-type: none">- JKS- PKCS12
キーエイリアス	MDN の署名に使用するプライベートキーのキーエイリアスまたは証明書。
トラストストアの場所	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
トラストストアのパスワード	トラストストアにアクセスするためのパスワード。
トラストストアのタイプ	トラストストアのタイプ。 以下の値を使用します。 <ul style="list-style-type: none">- JKS- PKCS12

リスナのプロパティ

HTTPS サーバーには複数のサーバーリスナを追加できます。サーバーリスナを使用して、HTTPS サーバーに一意的ポートとローカルアドレスを設定します。サーバーリスナをリストに追加するには、[リスナの追加] をクリックします。

次の表に、リスナを追加する際のプロパティを示します。

プロパティ	説明
名前	サーバーリスナの名前。
ポート	リスナが監視するサーバーのポート番号。
ローカルアドレス	サーバーリスナのローカルアドレス。
SSL の有効化	AS2 リスナと通信するために SSL over HTTPS 接続を有効にするかどうか。 有効にしない場合、HTTPS ではなく HTTP を使用して HTTPS リスナとの接続を確立します。 デフォルトでは無効になっています。
SSL プロトコル	SSL を有効にした場合に適用されます。HTTPS 接続を保護するために SSL と TLS のどちらのプロトコルを使用するか。 次のいずれかの値を選択します。 <ul style="list-style-type: none">- TLS 送信を保護するために、SSL の新しいバージョンである Transport Layer Security が使用されます。- SSL。送信を保護するために、従来の Secure Socket Layer プロトコルが使用されます。
SSL プロトコル 有効	許容する TLS と SSL のバージョンをカンマで区切って指定します。 サポートされているバージョンは次のとおりです。 <ul style="list-style-type: none">- TLS: TLSv1.2 および TLSv1.3- SSL: SSLv2Hello および SSLv3 値を指定しないと、選択したプロトコルのすべてのバージョンが有効になります。
クライアント認証	クライアントにサーバーとの認証に使用する証明書が必要かどうか。 次のいずれかの値を選択します。 <ul style="list-style-type: none">- なし。SSL 接続が証明書を確認せずに実行され、ユーザーはパスワードを使用して認証されます。送信された情報のいずれかで証明書が必要となる場合、接続に失敗します。- 必須。有効な証明書が使用可能にならないと、SSL 接続ではユーザーを接続または認証しません。- オプション。SSL 接続で有効な証明書を検索しますが、証明書がない場合は引き続きパスワード認証を行います。
キーストアの場所	クライアントがファイル統合サービスとの通信の認証に使用するプライベートキーおよび関連する証明書を格納するキーストアの場所。 パスとファイル名を指定します。
キーストアのパスワード	キーストアにアクセスするためのパスワード。

プロパティ	説明
キーストアタイプ	プライベートキーストアのタイプ。 次のいずれかの値を使用します。 - JKS - PKCS12
キーエイリアス	HTTPS コネクタのリスナを設定するための証明書のエイリアス。
トラストストアの場所	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
トラストストアのパスワード	トラストストアにアクセスするためのパスワード。
トラストストアのタイプ	トラストストアのタイプ。 次のいずれかの値を使用します。 - JKS - PKCS12

MDN プロパティ

以下の表に、受信メッセージのプロパティを示します。

プロパティ	説明
プロキシタイプ	この接続に使用するプロキシサーバーのタイプ。 次のいずれかのタイプを選択します。 - SOCKS。SOCKS バージョン 4 または 5 を使用できます。 - HTTPS。 - Informatica ファイルサーバープロキシ。 使用するプロキシサーバーのタイプをネットワーク管理者に確認してください。
ホスト	ネットワークのプロキシサーバーのホスト名または IP アドレス。
ポート	ネットワークのプロキシサーバーのポート番号。空欄のままにした場合、HTTP のデフォルトポートは 80 であり、SOCKS のデフォルトポートは 1080 です。
ユーザー	プロキシサーバーに接続するときのログインに使用するユーザー名。
パスワード	プロキシサーバーに接続するためのパスワード。HTTP 接続または HTTPS 接続を作成するためのネットワークがプロキシサーバーを使用する場合に必須。

アップロード制限のプロパティ

HTTPS ファイルのアップロード時に許可または拒否するファイルのタイプを指定できます。

以下の表に、アップロード制限を制御するプロパティを示します。

プロパティ	説明
ファイル拡張子のフィルタタイプ	ファイル拡張子リストの拡張子を承認または拒否するかどうか。 以下の値を使用します。 <ul style="list-style-type: none">- フィルタしない。すべてのファイルタイプを承認します。- 承認。ファイル拡張子プロパティでリストされた拡張子を持つファイルを承認します。- 拒否。ファイル拡張子プロパティでリストされた拡張子を持つファイルを許可しません。
ファイル拡張子	ファイル拡張子のリスト。ファイル拡張子のフィルタタイプに対応するファイル拡張子を追加します。例えば、ファイル拡張子のフィルタタイププロパティで、CSV ファイルおよび.txt ファイルを承認するには、 【承認】 を選択してからファイル拡張子のリストに CSV および.txt を追加します。 拡張子をリストに追加するには、テキストボックスに拡張子を入力してから 【追加】 をクリックします。 リストから拡張子を削除するには、拡張子を強調表示してから 【削除】 をクリックします。
大文字と小文字が区別されるファイル拡張子	ファイル拡張子リストを使用してフィルタする場合に、大文字と小文字を考慮に入れるかどうか。有効にすると、ファイル拡張子リストで使用される大文字と小文字が一致しない拡張子を使用したファイルはアップロード出来ません。 例えば、ファイル拡張子リストに CSV があるが CSV はない場合、拡張子 CSV を使用したファイルはアップロードできますが、拡張子 CSV を使用したファイルはアップロード出来ません。
拡張子付きのファイルを許可	ファイル拡張子フィルタを有効にするかどうか。有効にすると、このページで設定されたファイル拡張子のプロパティによってアップロードできるファイルのタイプが決まります。 デフォルトでは有効になっています。
拡張子なしのファイルを許可	ファイル名に拡張子が含まれていないファイルを許可するかどうか。 デフォルトでは有効になっています。
名前なしのファイルを許可	名前なしのファイルを許可するかどうか。New: Secure Agent は、次の形式を使用して名前なしのファイルを保存します: as2data_<datetime><datetime>は、ミリ秒まで含んだ現在のタイムスタンプです。 デフォルトでは無効になっています。
最大アップロードサイズ (MB)	HTTPS サーバーアップロードのファイルサイズの制限 (MB)。 デフォルトは 5MB です。

SFTP サーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、SFTP サーバーを設定してファイルを交換できます。

SFTP サーバープロパティを **【エージェント用のファイルサーバー】** ページの **【SFTP サーバー】** タブで設定します。以下のタイプのプロパティを設定します。

- 全般的なプロパティ
- アルゴリズムのプロパティ

- ホストキーのプロパティ
- アップロード制限のプロパティ

全般プロパティ

以下の表に、全般的な SFTP サーバーのプロパティを示します。

プロパティ	説明
有効な SFTP サーバー	SFTP サーバーを有効にするかどうか。 有効にしない場合、SFTP サーバーでファイルを送受信出来ません。 デフォルトでは無効になっています。
ポート	SFTP サーバーのポート番号。 デフォルトは 15002 です。
ローカルアドレス	SFTP サーバーのローカル IP アドレス。
SCP の有効化	session control protocol (セッション管理プロトコル) (SCP) を使用して接続を作成するかどうか。 デフォルトでは無効になっています。
アイドルタイムアウト	接続を閉じるまでの接続がアイドルな秒数。 デフォルトは 300 です。
最大ログイン	サーバーに同時にログインできる最大ユーザー数。 デフォルトは 500 です。
ログイン失敗遅延	失敗したログイン試行の間の遅延秒数。 デフォルトは 0 です。
最大ログイン失敗	1 人のユーザーに許可される失敗したログイン試行回数。 デフォルトは 5 です。
ウェルカムメッセージ	サーバーへの接続の確立時に表示するメッセージ。

アルゴリズムのプロパティ

次のアルゴリズムタイプを **【SFTP サーバー】** タブの **【アルゴリズム】** セクションで有効にします。

- 暗号アルゴリズム
- Message Authentication Code (メッセージ認証コード) (MAC) アルゴリズム
- 圧縮アルゴリズム
- キー交換アルゴリズム

SFTP ファイル交換のためのアルゴリズムの使用を設定するときは、次のルールとガイドラインを考慮します。

- アルゴリズムを **【使用可能】** と **【選択済み】** リストの間で移動できます。ファイル統合サービスは **【選択済み】** リスト内に列挙されたアルゴリズムを適用します。
- アルゴリズムタイプに選択済みアルゴリズムがない場合、ファイル統合サービスは **【使用可能】** リスト内に列挙されたすべてのアルゴリズムを適用します。
- ファイル統合サービスは、リストに列挙された順序で上から下にアルゴリズムを適用します。リスト内のアルゴリズムは、上矢印および下矢印を使用して、順序を変更できます。

ホストキーのプロパティ

以下の表に、ホストキーのプロパティを示します。

プロパティ	説明
RSA キーファイルの場所	RSA ホストキーファイルの場所。
RSA キーパスフレーズ	RSA キーのパスフレーズ。
DSA キーファイルの場所	DSA ホストキーファイルの場所。
DSA キーパスフレーズ	DSA キーのパスフレーズ。

アップロード制限のプロパティ

SFTP ファイルの交換時に許可または拒否するファイルのタイプを指定できます。以下の表に、アップロード制限を制御するプロパティを示します。

プロパティ	説明
ファイル拡張子のフィルタタイプ	ファイル拡張子リストの拡張子を承認または拒否するかどうか。 以下の値を使用します。 <ul style="list-style-type: none">- フィルタしない。すべてのファイルタイプを承認します。- 承認。ファイル拡張子プロパティでリストされた拡張子を持つファイルを承認します。- 拒否。ファイル拡張子プロパティでリストされた拡張子を持つファイルを許可しません。 デフォルトは 【フィルタしない】 です。
ファイル拡張子	ファイル拡張子のリスト。ファイル拡張子のフィルタタイプに対応するファイル拡張子を追加します。例えば、ファイル拡張子のフィルタタイププロパティで <code>csv</code> ファイルおよび <code>txt</code> ファイルを承認するには、 【承認】 を選択してからファイル拡張子のリストに <code>csv</code> および <code>txt</code> を追加します。 拡張子をリストに追加するには、テキストボックスに拡張子を入力してから 【追加】 をクリックします。 リストから拡張子を削除するには、拡張子を強調表示してから 【削除】 をクリックします。
大文字と小文字が区別されるファイル拡張子	ファイル拡張子リストを使用してフィルタする場合に、大文字と小文字を考慮に入れるかどうか。有効にすると、ファイル拡張子リストで使用される大文字と小文字が一致しない拡張子を使用したファイルはアップロード出来ません。 例えば、ファイル拡張子リストに <code>csv</code> があるが <code>CSV</code> はない場合、拡張子 <code>csv</code> を使用したファイルはアップロードできますが、拡張子 <code>CSV</code> を使用したファイルはアップロード出来ません。 デフォルトでは無効になっています。
拡張子なしのファイルを許可	ファイル名に拡張子が含まれていないファイルを許可するかどうか。 デフォルトでは無効になっています。
拡張子付きのファイルを許可	ファイル拡張子フィルタを有効にするかどうか。有効にすると、このページで設定されたファイル拡張子のプロパティによってアップロードできるファイルのタイプが決まります。 デフォルトでは有効になっています。

MLLP サーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、リモート MLLP サーバーとファイルを交換するように MLLP サーバーを設定できます。

Minimal Lower Layer Protocol (MLLP) プロトコルは、HL7 メッセージなどの医療業界のメッセージを転送するために使用されます。HL7 は、医療情報システムのメッセージング仕様です。

【エージェント用のファイルサーバー】 ページの **【MLLP サーバー】** タブで MLLP サーバーのプロパティを設定します。

以下のタイプのプロパティを設定します。

- 全般
- Kafka 接続
- リスナ

全般プロパティ

次の表に、MLLP サーバーの全般プロパティを示します。

プロパティ	説明
MLLP サーバーの有効化	MLLP サーバーを有効にするかどうかを指定します。 無効にすると、MLLP サーバーはファイルを受信できません。

Kafka 接続

次の表に、Kafka 接続プロパティを示します。

プロパティ	説明
接続名	MLLP サーバーに使用する Kafka 接続を指定します。利用可能な Kafka 接続のリストを表示するには、 【選択】 をクリックします。使用する Kafka 接続に対応するオプションを選択し、 【OK】 をクリックします。 リスナのターゲットタイプとして Kafka を選択する場合は必須です。

リスナのプロパティ

MLLP サーバーには複数のサーバーリスナを追加できます。サーバーリスナを使用して、MLLP サーバーに一意のポートとローカルアドレスを設定します。

サーバーリスナをリストに追加するには、**【リスナの追加】** をクリックします。個々のリスナを開始または停止できます。リスナを開始または停止する前に、リスナ設定に対して行った編集内容を保存する必要があります。MLLP サーバーには、少なくとも 1 つのリスナが必要です。

注: また、既存リスナの編集や削除も実行できます。リスナを変更または削除する前に、リスナが実行中でないことを確認してください。

次の表に、新しいリスナを追加する際に設定する必要があるプロパティを示します。

プロパティ	説明
名前	MLLP サーバーリスナの名前。リスナの名前は一意である必要があります。
ポート	リスナが監視するサーバーのポート番号。
ローカルアドレス	ファイルサーバーがリッスンするポートをホストしているサーバーの IP アドレス。 ポートとローカルアドレスの組み合わせは一意である必要があります。
アイドルタイムアウト	接続を閉じるまでの接続がアイドルな秒数。 デフォルトは 300 です。
メッセージの検証	リスナが HL7 バージョン 2.8.1 に従って HL7 メッセージの構造を検証するかどうかを指定します。 次のいずれかの値を選択します。 - はい。リスナは HL7 メッセージを検証します。 - いいえリスナは HL7 メッセージを検証しません。
ターゲットタイプ	次のいずれかのターゲットタイプを選択します。 - Kafka: 指定した Kafka 接続にメッセージを保存します。[Kafka] を選択した場合は、Kafka 接続のトピックを選択します。 - ファイル: 指定したディレクトリにメッセージをファイルとして保存します。[ファイル] を選択した場合は、 【ターゲットの場所】 と 【ファイル名のプレフィックス】 を指定します。
トピック名	メッセージをパブリッシュする Kafka トピック。 接続で利用可能な Kafka トピックのリストを表示するには、 【選択】 をクリックします。 使用する Kafka トピックに対応するラジオボタンを選択し、 【OK】 をクリックします。
ターゲットの場所	メッセージを保存する場所。
ファイル名のプレフィックス	メッセージファイル名に使用するプレフィックス。

プロキシサーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、1 つまたは複数のプロキシサーバーを設定できます。

プロキシサーバープロパティを **【エージェント用のファイルサーバー】** ページの **【プロキシサーバー】** タブで設定します。このタブには、使用可能な最新のファイル統合プロキシバージョンが表示されます。

注: プロキシサーバーを DMZ にもインストールします。詳細については、[「ファイル統合プロキシサーバーのインストール」 \(ページ 26\)](#)を参照してください。

プロキシサーバーを追加するには、**【Add Proxy Configuration (プロキシ設定の追加)】** をクリックし、**【保存】** をクリックします。

以下のタイプのプロパティを設定します。

- 全般的なプロパティ
- 内部ファイルサーバーとプロキシサーバーを関連付けるサービスマッピングプロパティ

全般プロパティ

以下の表に、全般的なプロキシサーバーのプロパティを示します。

プロパティ	説明
有効	プロキシサーバーが有効かどうか。 デフォルトは [はい] です。
コントローラのアドレス	プロキシサーバーが組織のファイルサーバーからの管理接続をリスンする DMZ 内のサーバーの外部 IP アドレス。
コントローラのポート	プロキシサーバーが組織のファイルサーバーからの管理接続をリスンする DMZ 内のサーバーのポート番号。 デフォルトは 9100 です。
スレッドの最小数	プロキシサーバーのインストール場所への接続のために予約されたスレッドの最小数。 デフォルトは 10 です。
スレッドの最大数	プロキシサーバーが処理できる同時要求の最大数。 デフォルトは 2000 です。
スレッドキープアライブ時間	終了までのアイドルスレッド待機秒数。 デフォルトは 60 です。

サービスマッピングプロパティ

プロキシサーバーのサービスマッピングを設定するには、[Proxy Server Configuration (プロキシサーバーの設定)] ページで、[Service Mappings (サービスマッピング)] の隣の [追加] をクリックし、マッピングパラメータを設定し、[OK] をクリックします。必要に応じていくつでもサービスマッピングを追加し、内部ファイルサーバーとプロキシサーバーを関連付けられます。

以下の表に、サービスマッピングプロパティを示します。

プロパティ	説明
ラベル	マッピングのラベル。
送信元アドレス	プロキシサーバーの IP アドレス。
送信元ポート	プロキシサーバーのポート番号。
送信先アドレス	内部ファイルサーバーの IP アドレス。
送信先ポート	内部ファイルサーバーのポート番号。
ロードバランサールール	マッピングと一緒に使用するロード分散ルールの名前。ルールの名前は、プロキシサーバーのインストール内にある proxy.xml ファイルにある名前と同一である必要があります。詳細については、 「ファイル統合プロキシサーバーのインストール」 (ページ 26) を参照してください。

ファイル統合プロキシサーバーのインストール

ファイル統合プロキシサーバーを DMZ にインストールし、サーバーパラメータを設定します。サーバーは Windows オペレーティングシステムと Linux オペレーティングシステムにインストールできます。

注: 管理者の Informatica Intelligent Cloud Services で、プロキシサーバーを有効にし、サーバープロパティを設定します。詳細については、「[プロキシサーバー設定プロパティ](#)」 (ページ 24) を参照してください。

fis-proxy-server_<version>.zip ファイルをインストールするには、次の手順を実行します。

1. fis-proxy-server_<version>.zip ファイルを次の場所からダウンロードし、ファイルを DMZ のサーバーにコピーします。
 - Linux。\$<Secure Agent インストールディレクトリ>/downloads/FileIntegrationService
 - Windows。%<Secure Agent インストールディレクトリ>%\downloads\FileIntegrationService
2. Java 17 (OpenJDK または Oracle) をダウンロードし、DMZ 内のサーバーにインストールします。
3. fis-proxy-server_<version>/bin フォルダから、次のファイルのいずれかを編集します。
 - Windows オペレーティングシステムでは、setenv.bat を編集します。
 - Linux オペレーティングシステムでは、setenv.sh を編集します。
 - a. JAVA_HOME を Java 17 の JDK Home または JRE ホームに設定します。
 - b. fis-proxy-server のフォルダパスを FIS_PROXY_HOME に設定します。
4. fis-proxy-server_<version>/config フォルダから、proxy.xml ファイルを編集し、次の変数の値を設定します。

変数	説明
controllerAddress	プロキシサーバーが組織のファイルサーバーからの管理接続をリスンする DMZ 内のサーバーの外部 IP アドレス。
dataAddress	プロキシサーバーが組織のファイルサーバーからのデータ接続をリスンする DMZ 内のサーバーの内部 IP アドレス。
proxyAddress	プロキシサーバーが受信接続をリスンする DMZ 内のサーバーの IP アドレス。
forwardProxyLocalAddress	プロキシサーバーがリモートサーバーへの送信接続を転送プロキシとして確立する DMZ 内のサーバーの IP アドレス。

必要に応じて、ポート番号を変更します。

5. プロキシサーバーを開始するには、次のコマンドのいずれかを実行します。
 - Windows オペレーティングシステムでは、fis-proxy.bat start を実行します。
 - Linux オペレーティングシステムでは、fis-proxy.sh start を実行します。
 6. プロキシサーバーを停止するには、次のコマンドのいずれかを実行します。
 - Windows オペレーティングシステムでは、fis-proxy.bat stop を実行します。
 - Linux オペレーティングシステムでは、fis-proxy.sh stop を実行します。
- プロキシサーバーはログを fis-proxy-server_<version>/logs フォルダに保存します。

ファイルサーバー

【ファイルサーバー】 ページでファイル統合サービスファイルサーバーを停止または開始する事ができます。設定変更の後、ファイルサーバーを停止および開始します。

HTTPS、AS2、SFTP、および MLLP サーバーの停止と開始

HTTPS、AS2、SFTP、または MLLP サーバーを停止または開始するには、次のアクションを実行します。

1. Administrator で、【ファイルサーバー】 を選択します。
2. 【ファイルサーバー】 タブで、サーバーを実行する Secure Agent の名前の横の矢印をクリックします。
3. 【アクション】 メニューから、サーバーを開始または停止するオプションを選択します。

Informatica Intelligent Cloud Services はアクションを示すエントリを監査ログに追加します。

プロキシサーバーの停止と開始

プロキシサーバーを停止または開始するには、次のアクションを実行します。

1. Administrator で、【ファイルサーバー】 を選択します。
2. 【ファイルサーバー】 タブで、プロキシサーバーを停止または開始するファイル統合サービスを実行する Secure Agent を選択します。
3. 【エージェント用のファイルサーバー】 ページで、【プロキシサーバー】 タブを選択します。
4. 停止または開始するサーバーの 【アクション】 メニューから、【停止】 または 【開始】 を選択します。

Informatica Intelligent Cloud Services はアクションを示すエントリを監査ログに追加します。

第 4 章

ファイルサーバーのユーザー

ファイルを組織と交換する各リモートパートナーに、ユーザーアカウントを作成します。このユーザーアカウントによって、パートナーとお客様のサーバーでファイルを交換できるようになります。

リモートパートナーごとに、以下のタイプのプロパティを設定します。

- ユーザー名、電子メールアドレス、パスワードなどの全般的なプロパティ。
- HTTPS、AS2、および SFTP サーバーのサーバー固有プロパティ。
- フォルダ権限。

注: ファイルサーバーユーザーのアカウントは、Informatica Intelligent Cloud Services のユーザーアカウントとは異なります。ファイルサーバーユーザーのアカウントによって、リモートパートナーユーザーがファイルをお客様の組織のファイルサーバーと交換できるようになります。Informatica Intelligent Cloud Services のユーザーアカウントによって、ユーザーは Informatica Intelligent Cloud Services 組織にアクセスできるようになります。

ファイルサーバーユーザーの設定

パートナーユーザーを設定して、パートナーが組織とファイルを交換できるようにします。

ファイルサーバーユーザーを作成すると、そのユーザーは Informatica Intelligent Cloud Services から電子メールを受信します。ユーザーの設定時にシステムで生成されたパスワードを追加するように選択していた場合は、生成されたパスワードがこの電子メールに記載されています。

1. Administrator で、**[ファイルサーバー]** > **[ファイルサーバーのユーザー]** をクリックします。
2. **[ユーザーの追加]** をクリックします。
3. 次のアクションを実行し、**[保存]** をクリックします。
 - ユーザーの全般情報を入力します。
 - ユーザーがファイルを組織内の AS2 サーバーに送信できるようにするには、AS2 プロトコルを有効にし、AS2 設定を設定します。
 - ユーザーがファイルを組織内の SFTP サーバーと交換できるようにするには、SFTP プロトコルを有効にし、SFTP 設定を設定します。
 - ユーザーがファイルを組織内の HTTPS サーバーと交換できるようにするには、HTTPS プロトコルを有効にし、HTTPS 設定を設定します。
 - そのユーザーにフォルダとファイルの権限を追加します。デフォルトでは、ユーザーはデフォルトのホームディレクトリ上のすべて権限を持っています。

ファイルサーバーユーザーのプロパティ

ファイルサーバーユーザーのプロパティを設定します。

全般プロパティ

以下の表に、ユーザーの全般プロパティを示します。

プロパティ	説明
ユーザー名	ファイルサーバーユーザーのユーザー名。
説明	ユーザーの説明。
会社名	組織とファイルを交換するリモートパートナーのユーザーアカウント名。
電子メール	ユーザーの電子メールアドレス。
パスワードの生成	ユーザーのパスワードを作成するかどうか、またはシステムでシステム生成のパスワードを作成できるようにするか。 パスワードには以下の特性を含める必要があります。 <ul style="list-style-type: none">- 8 文字以上で指定する。- 大文字を 1 文字以上含める。- 数字を 1 つ以上含める。- 次の特殊文字を 1 つ以上含める: @ \$! & * ~ - _

AS2 サーバーのプロパティ

以下の表に、ファイルサーバーユーザーの AS2 サーバーのプロパティを示します。

プロパティ	説明
AS2 プロトコルの有効化	AS2 プロトコルが有効かどうか。 AS2 サーバーでファイルを受信しないようにするには、このオプションを無効にします。 デフォルトでは有効になっています。
認証タイプ	[パスワード] 、 [証明書] 、 [両方] 、または [いずれか] が必要かどうか。 認証に [パスワード] を使用する場合、 [全般] タブで定義したパスワード生成が使用されます。 認証に [証明書] を使用する場合、AS2 サーバーの [クライアント認証] 設定を [オプション] または [必須] に設定する必要があります。
ダイジェストアルゴリズム	認証に [証明書] 、 [両方] 、または [いずれか] を使用する場合、パートナー証明書の SHA フィンガープリントを選択します。 次のいずれかの値を選択します。 <ul style="list-style-type: none">- SHA1- SHA224- SHA256- SHA384- SHA512
証明書のフィンガープリント	選択したダイジェストアルゴリズムに対応する SHA フィンガープリントを入力します。

プロパティ	説明
AS2 ID	パートナーユーザーの AS2 ID。
署名証明書エイリアス	メッセージの署名に使用するプライベートキーエイリアス。プライベートキーは、デフォルトのプライベートキーストアにあります。
デフォルトのアップロードフォルダ	AS2 ファイルが受信時に保存される場所。デフォルトの場所は、ユーザーのデフォルトのホームディレクトリです。 空欄の場合、ファイルはホームディレクトリに保存されます。詳細については、 第 6 章、「グローバル設定」 (ページ 35) を参照してください。

SFTP サーバースプロパティ

以下の表に、ファイルサーバーユーザーの SFTP サーバーのプロパティを示します。

プロパティ	説明
有効な SFTP プロトコル	SFTP プロトコルが有効かどうか。 SFTP サーバーでファイルを送受信しないようにするには、このオプションを無効にします。 デフォルトでは有効になっています。
認証タイプ	[パスワード] 、 [パブリックキー] 、 [両方] 、または [いずれか] が必要かどうか。 パスワードが認証に使用される場合、 [全般] タブで定義したパスワード生成が使用されます。 認証に [パブリックキー] を使用する場合、Secure Agent にキーを配置する必要があります。
パブリックキーの場所	Secure Agent 上のパブリックキーの場所への絶対パス。 認証に [パブリックキー] 、 [両方] 、または [いずれか] を使用する場合に適用されます。

HTTPS サーバースプロパティ

以下の表に、ファイルサーバーユーザーの HTTPS サーバーのプロパティを示します。

プロパティ	説明
HTTPS プロトコルの有効化	HTTPS プロトコルが有効かどうか。 HTTPS サーバーでファイルを受信しないようにするには、このオプションを無効にします。 デフォルトでは有効になっています。
認証タイプ	[パスワード] 、 [証明書] 、または [いずれか] が必要かどうか。 パスワードが認証に使用される場合、 [全般] タブで定義したパスワード生成が使用されます。 認証に [証明書] を使用する場合は、HTTPS サーバーの [クライアント認証] 設定を [オプション] または [必須] に設定する必要があります。

プロパティ	説明
ダイジェストアルゴリズム	<p>認証に 【証明書】、【両方】、または 【いずれか】 を使用する場合、パートナー証明書の SHA フィンガープリントを選択します。</p> <p>次のいずれかの値を選択します。</p> <ul style="list-style-type: none"> - SHA1 - SHA224 - SHA256 - SHA384 - SHA512
証明書のフィンガープリント	選択したダイジェストアルゴリズムに対応する SHA フィンガープリントを入力します。

フォルダ権限プロパティ

デフォルトでは、ユーザーのホームディレクトリおよびユーザー名が、ファイルサーバーの **【グローバル設定】** タブに定義されたデフォルトのホームディレクトリの下に作成され、そのユーザーは自分のホームディレクトリに対するすべての権限を持ちます。ユーザーのホームディレクトリが別の場所になるように編集できます。

別のフォルダおよびファイルへの権限を追加するには、**【追加】** をクリックし、権限を定義します。

以下の表に、ユーザーのフォルダ権限プロパティを示します。

プロパティ	説明
エイリアス	権限を付与するフォルダまたはファイルのエイリアス。エイリアスは 【ファイルサーバーのユーザー】 ページの 【名前】 カラムの下に表示されます。
パス	ユーザー権限を付与するフォルダまたはファイルのパス。
タイプ	権限がフォルダまたはファイルのどちらに対するものであるかを決定します。
フォルダ権限	フォルダに対するユーザーの権限。
ファイル権限	ファイルに対するユーザーの権限。
ディスクスペース制限	<p>ユーザーがフォルダ上で使用できるディスクスペースを制限するかどうかと、制限する場合、許可されるディスク上のスペース。</p> <p>フォルダ権限に適用されます。</p>

IP フィルタのプロパティ

以下の表に、ファイルサーバーユーザーの IP フィルタのプロパティを示します。

プロパティ	説明
IP フィルタを有効にしますか?	ファイルサーバーユーザーに対して IP フィルタを有効にするかどうか。デフォルトでは無効になっています。
フィルタタイプ	フィルタタイプを選択します。次のいずれかのオプションを選択します。 <ul style="list-style-type: none">- ブラックリスト。指定された IP アドレスへのアクセスを拒否し、他のすべての IP アドレスへのアクセスを許可します。- ホワイトリスト。指定されたアドレスへのアクセスを許可し、他のすべての IP アドレスへのアクセスを拒否します。 デフォルトはホワイトリストです。
フィルタエントリ	選択したフィルタタイプに基づいて、アクセスを拒否または許可する IP アドレスのリストを入力します。行を追加するには、 【追加】 をクリックします。IP アドレスは、単一、範囲、またはクラスレスドメイン間ルーティング (CIDR) の表記形式で指定します。範囲または CIDR 表記形式では、ハイフンまたはスラッシュとの間にスペースを挟まないでください。例えば、10.1.4.1/24 または 10.1.4.1-10.1.255.255 と入力します。

ファイルサーバーユーザーの削除

ユーザーが組織で作業をしなくなった場合に、ファイルサーバーユーザーを削除する必要がある場合があります。

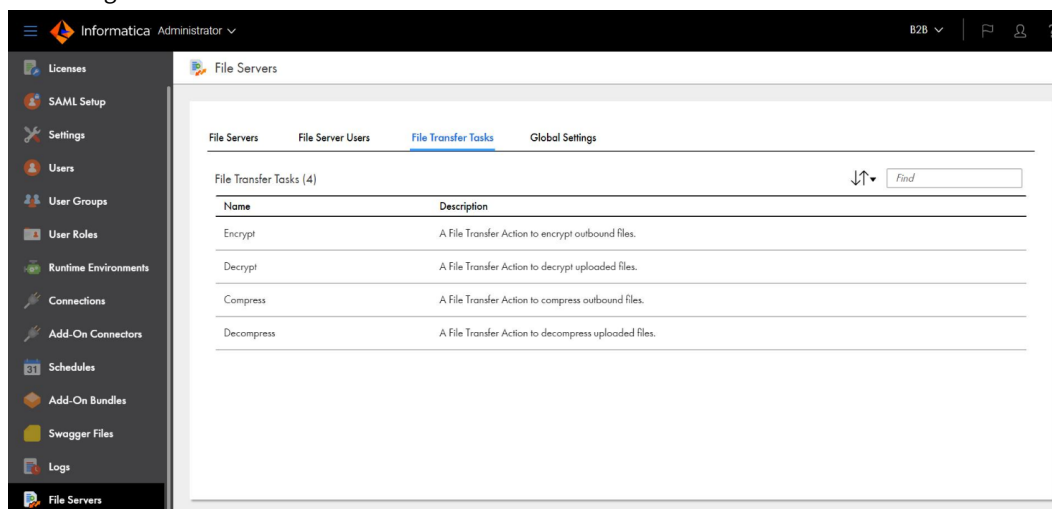
1. Administrator で、**【ファイルサーバー】** > **【ファイルサーバーのユーザー】** を選択します。
2. ユーザー名を含む行で **【アクション】** をクリックし、**【ユーザーの削除】** を選択します。

第 5 章

ファイル転送タスク

ファイル転送タスクは、パートナーのインバウンドおよびアウトバウンドプロセスに関連します。

【ファイルサーバー】 ページには、ファイル統合サービスを使用できる組織内のすべてのランタイム環境と Secure Agent が一覧表示されます。



【ファイル転送タスク】 タブには、定義済みのファイル転送タスクが一覧表示されます。これらのタスクを使用すると、ファイルサーバーからファイルを受信するとき、またはファイルサーバーにファイルを送信ときにアクションを実行できます。このタブには、読み取り専用モードでプロジェクトが一覧表示されます。

【ファイル転送タスク】 タブには、次の定義済みファイル転送タスクが含まれます。

名前	説明
暗号化	アウトバウンドファイルをソースの場所からファイルサーバーユーザーのホームディレクトリに転送するときに、PGP を使用してそれらのファイルを暗号化するファイル転送タスク。
復号化	アップロード済みのファイルをファイルサーバーユーザーのホームディレクトリからターゲットの場所に転送するときに、PGP を使用してそれらのファイルを復号化するファイル転送タスク。
圧縮	アウトバウンドファイルをソースの場所からファイルサーバーユーザーのホームディレクトリに転送するときに、それらのファイルを圧縮するファイル転送タスク。Zip、Tar、Gzip のうちのいずれかの圧縮方式を選択できます。
圧縮解除	アップロード済みのファイルをファイルサーバーユーザーのホームディレクトリからターゲットの場所に転送するときに、それらのファイルを圧縮解除するファイル転送タスク。Unzip、Untar、Gunzip のうちのいずれかの圧縮解除方式を選択できます。

定義済みタスクを実行するために、REST API も使用できます。B2B Gateway を使用してタスクを実行することもできます。

詳細については、*REST API* リファレンスを参照してください。

第 6 章

グローバル設定

ファイル転送用に設定されたすべてのファイルサーバーに適用するプロパティを設定します。

フォルダ設定

【ターゲットの場所】 プロパティを設定して、リモートサーバーから受信したすべてのファイルが保存されるデフォルトのディレクトリを指定します。ユーザー固有のホームディレクトリが、グローバルホームディレクトリの下に作成されます。

注: デフォルトのホームディレクトリの値を変更するときは、常にファイルサーバーを停止してから開始する必要があります。

SMTP サーバーの設定

以下の表に、すべてのリモートファイルサーバーに適用する SMTP サーバーの設定を一覧表示します。

プロパティ	説明
ホスト	電子メールタイプの MDN に使用する SMTP 設定のホスト名。
ポート	SMTP が実行されているポート。
ユーザー名	SMTP サーバーに接続するユーザー名。
パスワード	SMTP ユーザーのパスワード。
接続タイプ	SMTP 接続のタイプ。 次のいずれかの値を選択します。 - ノーマル - implicitSSL - explicitSSL デフォルトは [ノーマル] です。
電子メールから	電子メール MDN の送信元の電子メールアドレス。
名前から	電子メールに表示される名前。

PGP 設定

パブリックキーおよび秘密鍵を保存するディレクトリを指定するために、**【パブリックキーリング】** および **【秘密鍵リング】** を設定します。パスが指定されていない場合、PGP キーリングのデフォルトのパスが使用されます。

注: 複数の Secure Agent がある場合、PGP コマンドラインインタフェース (PGP-CLI) を使用して構成プロパティファイルを編集できます。pgp-configuration.properties ファイルでの PGP 設定の変更を反映するために、

FIS アプリケーションを再起動する必要があります。構成ファイルは、FIS パッケージにバンドルされている PGP クライアントの conf フォルダ内にあります。

暗号化設定

以下の表に、すべてのリモートファイルサーバーに適用される暗号化設定を示します。

プロパティ	説明
キーストアの場所	クライアントがファイル統合サービスとの通信の認証に使用するプライベートキーおよび関連する証明書を格納するキーストアの場所。パスとファイル名が含まれます。
キーストアのパスワード	キーストアにアクセスするためのパスワード。
キーストアタイプ	プライベートキーストアのタイプ。次のいずれかの値を使用します。 <ul style="list-style-type: none">- JKS- PKCS12 デフォルトは JKS です。
キーエイリアス	MDN の署名に使用するプライベートキーのキーエイリアスまたは証明書。
トラストストアの場所	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
トラストストアのパスワード	トラストストアにアクセスするためのパスワード。
トラストストアのタイプ	トラストストアのタイプ。次のいずれかの値を使用します。 <ul style="list-style-type: none">- JKS- PKCS12 デフォルトは JKS です。

索引

A

AS2 サーバーの設定 [8](#)
AS2 ファイルサーバーのプロパティ [10](#)
AS2 ファイルの交換 [8](#)

C

Cloud アプリケーション統合コミュニティ
URL [4](#)
Cloud 開発者コミュニティ
URL [4](#)

I

Informatica Intelligent Cloud Services
Web サイト [4](#)
Informatica グローバルカスタマサポート
連絡先情報 [5](#)

S

SFTP サーバー設定 [8](#)
SFTP ファイルサーバープロパティ [20](#)
SFTP ファイルの交換 [8](#)

W

Web サイト [4](#)

あ

アップグレード通知 [5](#)

し

システムステータス [5](#)

す

ステータス
Informatica Intelligent Cloud Services [5](#)

は

パートナーファイルサーバー [8](#)

ふ

ファイルサーバー
AS2 プロパティ [10](#)
SFTP のプロパティ [20](#)
プロキシのプロパティ [24](#)
設定 [10](#)
停止および開始 [27](#)
ファイルサーバーの設定
グローバル設定 [35](#)
ユーザー [28](#)
ファイル統合サービス
ファイルサーバー [8](#), [10](#)
ファイルサーバーのユーザー [28](#)
ファイルサーバーの停止および開始 [27](#)
プロキシサーバー設定 [8](#)
プロキシファイルサーバープロパティ [24](#)

め

メンテナンスの停止 [5](#)

り

リモートファイルサーバー [8](#)